DAGSTUHL
REPORTS

Volume 7, Issue 3, March 2017

ISSN 2192-5283

Published online and open access by
Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH, Dagstuhl Publishing, Saarbrücken/Wadern, Germany. Online available at http://www.dagstuhl.de/dagpub/2192-5283

Publication date
December, 2017

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at `http://dnb.d-nb.de`.

Digital Object Identifier: 10.4230/DagRep.7.3.i

Aims and Scope
The periodical *Dagstuhl Reports* documents the program and the results of Dagstuhl Seminars and Dagstuhl Perspectives Workshops.
In principal, for each Dagstuhl Seminar or Dagstuhl Perspectives Workshop a report is published that contains the following:

- an executive summary of the seminar program and the fundamental results,
- an overview of the talks given during the seminar (summarized as talk abstracts), and
- summaries from working groups (if applicable).

This basic framework can be extended by suitable contributions that are related to the program of the seminar, e. g. summaries from panel discussions or open problem sessions.

Contact
Schloss Dagstuhl – Leibniz-Zentrum für Informatik
Dagstuhl Reports, Editorial Office
Oktavie-Allee, 66687 Wadern, Germany
reports@dagstuhl.de
http://www.dagstuhl.de/dagrep

Report from Dagstuhl Seminar 17101

Databases on Future Hardware

Edited by

Gustavo Alonso[1], Michaela Blott[2], and Jens Teubner[3]

1 **ETH Zürich, CH,** `alonso@inf.ethz.ch`
2 **Xilinx – Dublin, IE,** `michaela.blott@xilinx.com`
3 **TU Dortmund, DE,** `jens.teubner@cs.tu-dortmund.de`

Abstract

A number of physical limitations mandate radical changes in the way how we build computing hard- and software, and there is broad consensus that a stronger interaction between hard- and software communities is needed to meet the ever-growing demand for application performance.

Under this motivation, representatives from various hard- and software communities have met at the Dagstuhl seminar "Databases on Future Hardware" to discuss the implications in the context of database systems. The outcome of the seminar was not only a much better understanding of each other's needs, constraints, and ways of thinking. Very importantly, the group identified topic areas that seem key for the ongoing shift, together with suggestions on how the field could move forward. During the seminar, it turned out that the future of databases is not only a question of technology. Rather, economic considerations have to be taken into account when building next-generation database engines.

Seminar March 5–10, 2017 – http://www.dagstuhl.de/17101
1998 ACM Subject Classification C.0 Computer Systems Organization, H.2.4 Database Management Systems
Keywords and phrases computer architecture, hardware support for databases, non-volatile
Digital Object Identifier 10.4230/DagRep.7.3.1

1 Executive Summary

Jens Teubner

Computing hardware is undergoing radical changes. Forced by physical limitations (mainly *heat dissipation* problems), systems trend toward *massively parallel* and *heterogeneous* designs. New technologies, *e.g.*, for *high-speed networking* or *persistent storage* emerge and open up new opportunities for the design of database systems. This push by technology was the main motivation to bring top researchers from different communities – particularly hard- *and* software – together to a Dagstuhl seminar and have them discuss about "Databases on Future Hardware." This report briefly summarizes the discussions that took place during the seminar.

With regards to the mentioned *technology push*, during the seminar *bandwidth*; *memory and storage technologies*; and *accelerators* (or other forms of specialized computing functionality or instruction sets) were considered the most pressing topic areas in database design.

But it turned out that the field is influenced also by a strong push from *economy/market*. New types of *applications* – in particular Machine Learning – as well as the emergence of

Databases on Future Hardware, *Dagstuhl Reports*, Vol. 7, Issue 3, pp. 1–18
Editors: Gustavo Alonso, Michaela Blott, and Jens Teubner

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

"compute" as an independent type of resources – *e.g.*, in the form of *cloud computing* or *appliances* – can have a strong impact on the viability of a given system design.

Bandwidth; Memory and Storage Technologies

During the seminar, probably the most often stated issue in the field was *bandwidth* – at various places in the overall system stack, such as CPU ↔ memory; machine ↔ machine (network); access to secondary storage (*e.g.*, disk, SSD, NVM). But very interestingly, the issue was not only brought up as a key limitation to database performance by the seminar attendees with a software background. Rather, it also became clear that the hardware side, too, is very actively looking at bandwidth. The networking community is working at ways to provide more bandwidth, but also to provide hooks that allow the software side to make better use of the available bandwidth. On the system architecture side, new interface technologies (*e.g.*, NVlink, available in IBM's POWER8) aim to ease the bandwidth bottleneck.

Bandwidth usually is a problem only *between* system components. To illustrate, HMC memories ("hybrid memory cube") provide only 320 GB/s of external bandwidth, but internally run at 512 GB/s per cube ("vault"); in a 16-vault configuration, this corresponds to 8 TB/s of internal bandwidth. This may open up opportunities to build heterogeneous system designs with *near-data processing* capabilities. HMC memory units could, for instance, contain (limited) processing functionality associated with every storage vault. This way, simple tasks, such as data movement, re-organization, or scanning could be off-loaded and performed right where the data resides. Similar concepts have been used, *e.g.*, to filter data in the network, pre-process data near secondary storage, etc.

In breakout sessions during the seminar, attendees discussed the implications that such system designs may have. Most importantly, the designs will require to re-think the existing *(programming) interfaces*. How does the programmer express the off-loaded task? Which types of tasks can be off-loaded? What are the limitations of the near-data processing unit (*e.g.*, which memory areas can it access)? How do host processor and processing unit exchange tasks, data, and results? Clearly, a much closer collaboration will be needed between the hard- and software sides to make this route viable.

But new designs may also shake up the commercial market. The traditional hardware market is strongly separated between the memory and logic worlds, with different manufacturers and processes. Breaking up the separation may be a challenge both from a technological and from a business/market point of view.

The group found only little time during the seminar to discuss another potential game-changer in the memory/storage space. Companies are about to bring their first *non-volatile memory (NVM)* components to the market (and, in fact, Intel released its first round of "3D XPoint" products shortly after the seminar). The availability of cheap, high-capacity, byte-addressable, persistent storage technologies will have profound impact on database software. Discussions during the seminar revolved around the question whether classical persistent (disk-based) mechanisms or in-memory mechanisms are more appropriate to deal with the new technology.

Accelerators

A way of dealing with the technology trend toward heterogeneity is to enrich general-purpose systems with more specialized processing units, *accelerators*. Popular incarnations of this idea are *graphics processors (GPUs)* or *field-programmable gate arrays (FPGAs)*; but there

are also co-processing units for floating-point arithmetics, multimedia processing, or network acceleration.

Accelerators may fit well with what was said above. *E.g.*, they could be used as near-data processing units. But also the challenges mentioned above apply to many accelerator integration strategies. Specifically, the proper *programming interface*, but also the role of an accelerator in the software system stack – *e.g.*, sharing it between processes – seem to be yet-unsolved challenges.

During the seminar, also the role of accelerators specifically for database systems was discussed. It was mentioned, on the one hand, that accelerators should be used to accelerate functionality outside the database's core tasks, because existing hard- and software is actually quite good at handling typical database tasks. On the other hand, attendees reported that many of the non-core-database tasks, Machine Learning in particular, demand a very high flexibility that is very hard to provide with specialized hardware.

New Applications / Machine Learning

Databases are the classical device to deal with high volumes of data. With the success of Machine Learning in many fields of computing, the question arises how databases and Machine Learning applications should relate to one another, and to which extent the database community should embrace ML functionality in their system designs.

Some of the seminar attendees have, in fact, given examples of very impressive and successful systems that apply ideas from database co-processing to Machine Learning scenarios. In a breakout session on the topic, it was concluded that the two worlds should still be treated separately also in the future.

A key challenge around Machine Learning seems to be the very high expectations with regard to the flexibility of the system. ML tasks are often described in high-level languages (such as R or Python) and demand expressiveness that goes far beyond the capabilities of efficient database execution engines. Attempts to extend these engines with tailor-made ML operators were not very well received, because even the new operators were too restrictive for ML users.

Economic/Market Considerations

Somewhat unexpectedly, during the seminar it became clear that the interplay of databases and hardware is not only a question of technology. Rather, examples from the past and present demonstrate that even a technologically superior database solution cannot survive today without a clear business case.

The concept of *cloud computing* plays a particularly important role in these considerations. From a business perspective, compute resources – including database functionality – have become a commodity. Companies move their workloads increasingly toward cloud-based systems, raising the question whether the future of databases is also in the cloud.

A similar line of arguments leads to the concept of *database appliances*. Appliances package database functionality in a closed box, allowing *(a)* to treat the service as a commodity (business aspect) and *(b)* to tailor hard- and software of the appliance specifically to the task at hand, with the promise of maximum performance (technology aspect).

And, in fact, both concepts – cloud computing and appliances – may go well together. Cloud setups enable to control the entire hard- and software stack; large installations may provide the critical mass to include tailor-made (database) functionality also within the cloud.

2 Table of Contents

3 Overview of Talks

3.1 How to integrate FPGAs into data processing systems

Gustavo Alonso (ETH Zürich, CH)

The increasing amount of data and the growing complexity of workloads pose a significant challenge to existing data management systems. Data is growing not only in size but also in variety and heterogeneity. Workloads are more complex not only in regards to performance but also in terms of algorithmic heterogeneity and embedding into interactive systems. Hardware acceleration in general and FPGAs in particular are a credible first step towards addressing many of these challenges and doing so both form the performance perspective but also from an efficiency and functionality standpoint. In this talk I will cover our research journey over the last ten years in pursuit of FPGA based solutions for data processing and data management problems. The talk will follow the evolution of FPGAs as an architectural component in a computer system and illustrate the algorithmic, design, integration, and system issues that need to be solved before FPGAs become mainstream tools. For simplicity, and to keep the discussion focused, I will center the examples around DoppioDB, a relational database engine we have developed over HARP v1 combining a conventional, open source column store engine (MonetDB) with a cache coherent FPGA accelerator.

References

1 Zsolt István, David Sidler, Gustavo Alonso: Runtime Parameterizable Regular Expression Operators for Databases. FCCM 2016: 204–211
2 Kaan Kara, Gustavo Alonso: Fast and robust hashing for database operators. FPL 2016: 1–4
3 Louis Woods, Zsolt István, Gustavo Alonso: Ibex – An Intelligent Storage Engine with Support for Advanced SQL Off-loading. PVLDB 7(11): 963–974 (2014)

3.2 Scaling Neural Networks On Reconfiguable Logic

Michaela Blott (Xilinx – Dublin, IE)

The ongoing research on Neural Networks has started to focus on reducing the computation and storage requirements to make their deployment feasible in energy constraint compute environments. One of the promising opportunities is the reduction of the compute and storage down to a few bit precision whereby these networks achieve close to state of the art accuracy compared to their floating point counterparts. In this talk, we will show an automated framework for implementing these reduced precision (and in the extreme case fully binarized) neural networks on reconfigurable logic that can scale reduced precision neural networks onto an FPGA-based inference accelerator, given a set of fixed design constraints. We show, that the compute performance can scale well beyond typical floating point performance, currently demonstrating 10ks to millions of images per second for inference, 14 TOps compute performance with power consumption < 25W on today's devices. Results on the accuracy, architecture comparison to other approaches and detailed implementation of the latest large networks will also be presented.

3.3 Making the case for a closer DBMS and OS collaboration

Alexander Böhm (SAP SE – Walldorf, DE)

Performance optimization and the creation of highly efficient systems has always been a major focus of the database community. In academia, this is reflected by a vast number of publications that describe sophisticated techniques for all major components and aspects of a DBMS. Recently, the DBMS community broadened its scope towards hardware. This means no longer "just" looking on how to optimize the DBMS itself, but doing hardware/software co-design e.g. by exploiting vector instructions for efficient scans in in-memory databases such as HyPer or SAP HANA.

An important building block however is often ignored / heavily underestimated: The operating system. Modern, enterprise-class in-memory systems spend a lot of time re-implementing OS functionality in userspace, i.e. thread scheduling, memory management, and synchronization primitives, to only name a few.

We as a DBMS community need to pay more attention to the operating system and achieve a better integration instead of replicating and duplicating features and innovations the OS community creates.

3.4 Implications of Secure Computing Platforms for Databases

Ken Eguro (Microsoft Research – Redmond, US)

Main reference A. Arasu, K. Eguro, M. Joglekar, R. Kaushik, D. Kossmann, R. Ramamurthy, "Transaction processing on confidential data using cipherbase", in Proc. of the 31st Int'l Conf. on Data Engineering (ICDE), pp. 435–446, IEEE, 2015.
URL https://doi.org/10.1109/ICDE.2015.7113304
Main reference A. Arasu, S. Blanas, K. Eguro, R. Kaushik, D. Kossmann, R. Ramamurthy, R. Venkatesan, "Orthogonal Security with Cipherbase", in Proc. of the 6th Biennial Conf. on Innovative Data Systems Research (CIDR'13), Microsoft, 2013.
URL https://www.microsoft.com/en-us/research/publication/orthogonal-security-with-cipherbase/

Most DBMS are vulnerable to attack from administrators and hackers. This is because their security is largely limited to on-disk encryption and data is generally held in plaintext when loaded into RAM. While there have been attempts to help address this, by-in-large these solutions have had their own shortcomings. There are a number of up-and-coming secure computing platforms which can unlock new ways to address the security problem. In this talk we cover some of these hardware-based and software-based (but hardware assisted) platforms. We will also discuss the design space in which these platforms can be utilized by DBMS, how the SQL Server Always Encrypted feature will leverage these platforms, and open questions that remain, such as potential security/efficiency tradeoffs

3.5 Databases on Future Hardware

Peter Hofstee (IBM Research Lab. – Austin & TU Delft)

We discussed how scale-out systems are likely to develop in the near future. The most significant changes are likely to come from increases in network and SCM/NVM bandwidth that can rival that of memory in systems with reasonable cost. We discuss how this forces us to rethink the role of main memory and that we need a system concept that allows all components to interact without going through system DRAM. We explain the relatively new coherent attach interfaces on POWER8 and POWER9 and discuss where acceleration can make sense. We give a few database-related examples that can benefit from this new infrastructure: key-value stores, Cassandra, and graph.

3.6 Specialized Hardware for Databases – The Case for Sharing

Zsolt Istvan (ETH Zürich, CH)

In today's computing landscape, with CPU performance stagnating, there is an opportunity in using specialized hardware for accelerating databases and other data processing applications. Specialized hardware, such as FPGAs, enable a more efficient use of silicon, tailored to the problem at hand. Research efforts have already provided several promising operators/operations we could offload, but to be worth the effort hardware needs to support more than one particular operator and cater to a wide range of workloads instead. The question emerges: In the context of databases and data science applications, what is a right way of sharing specialized hardware, such as FPGAs? What if the overhead of sharing is larger than its benefits? Is it possible to retain some level of programmability even if hardware is hidden behind libraries?

While there are already ways to a virtualize the fabric of an FPGA, i.e. offer a slice of the device to each workload or tenant, these are made less attractive by high overheads both in additional circuit size and reprogramming time. Conversely, we could hide FPGAs behind the abstraction of a library that can be called by multiple applications/tenants but this method requires a decision at design time about what operations to hand off to the hardware.

In this talk I sketch the idea of a compromise: On the one hand, FPGAs should be exposed more as libraries or services, rather than bare hardware. This helps with integration and there should be enough similarity between workloads in an appliance, or data processing applications in the cloud, to be able to distill a common "core" functionality a priori. On the other hand, by looking only at the common parts we might miss additional opportunities of acceleration. Plugging custom hardware blocks into the "core" functionality should be still allowed, through use-case-specific interfaces. Since the scope of these custom blocks would be restricted their overhead would be negligible and they could be more realistically generated by high level synthesis tools, even stitched together at runtime from small building blocks (e.g., sub-operators). This, together with sharing, would enable a more flexible use of accelerators.

3.7 Latest trends in Networking

Andrew W. Moore (University of Cambridge, GB)

In this talk, I discuss networking trends at the edge of database environment. Trends in networking go beyond performance improvement – where these are not bound by physical constraints. Datacenter scaling has meant network component costs driven down and led to new configuration (P4) and operation (OpenFlow) languages and revitalisation of formalisms. Such function abstraction of SDN also means the division of work among end-system and network devices is now more flexible; many opportunities throughout.

3.8 Rethinking Memory System Design

Onur Mutlu (Carnegie Mellon University, US)

The memory system is a fundamental performance and energy bottleneck in almost all computing systems. Recent system design, application, and technology trends that require more capacity, bandwidth, efficiency, and predictability out of the memory system make it an even more important system bottleneck. At the same time, DRAM and flash technologies are experiencing difficult technology scaling challenges that make the maintenance and enhancement of their capacity, energy efficiency, and reliability significantly more costly with conventional techniques. In fact, recent reliability issues with DRAM, such as the RowHammer problem, are already threatening system security and predictability.

In this talk, we first discuss major challenges facing modern memory systems in the presence of greatly increasing demand for data and its fast analysis. We then examine some promising research and design directions to overcome these challenges. We discuss three key solution directions: 1) enabling new memory architectures, functions, interfaces, via more memory-centric system design, 2) enabling emerging non-volatile memory (NVM) technologies via hybrid and persistent memory systems, 3) enabling predictable memory systems via QoS-aware memory system design.

3.9 Discussion/Poster Talk: Toward More Automated Specialized Hardware

Pinar Tözün (IBM Almaden Center – San Jose, US)

As the hardware becomes more non-uniform and heterogeneous, it becomes essential for the data management systems to decide on the optimal design options based on the processor types they are running on. If the system is running on hardware that has a combination of different processing units (aggressive, low-power, special purpose, etc.), it should be able to automatically decide on which queries or transactions should run on which types of processors.

If the system is running on a hardware that has support for hardware transactional memory, it should be able to know the types of critical sections that would benefit from switching the synchronization primitive to transactions and the ones that should keep its existing synchronization method. If there are machine learning tasks that would benefit from running on GPUs or could be accelerated via FPGAs, the system should know when to offload these tasks to these units. Nevertheless, this requires a thorough understanding of the specific requirements of a data management system that can exploit the specific features of various hardware types. In addition, it requires interdisciplinary collaborations; especially involving people from data management, computer architecture, and compiler communities. Furthermore, to come up with more economically viable solutions in this area, we need to reach out to cloud providers so that they start building software and hardware infrastructures with heterogeneity in mind.

3.10 Managing Machine Learning on Modern Hardware

Ce Zhang (ETH Zürich, CH)

Main reference H. Zhang, J. Li, K. Kara, D. Alistarh, J. Liu, C. Zhang, "The ZipML Framework for Training Models with End-to-End Low Precision: The Cans, the Cannots, and a Little Bit of Deep Learning", in Proc. of the 34th Int'l Conf. on Machine Learning, Vol. 70, pp. 4035–4043, PMLR, 2016.

URL http://proceedings.mlr.press/v70/zhang17e.html

Recently there has been significant interest in training machine-learning models at low precision: by reducing precision, one can reduce computation and communication by one order of magnitude. We examine training at reduced precision, both from a theoretical and practical perspective, and ask: is it possible to train models at end-to-end low precision with provable guarantees? Can this lead to consistent order-of-magnitude speedups?

We present a framework called ZipML to answer these questions. For linear models, the answer is yes. We develop a simple framework based on one simple but novel strategy called double sampling. Our framework is able to execute training at low precision with no bias, guaranteeing convergence, whereas naive quantization would introduce significant bias. We validate our framework across a range of applications, and show that it enables an FPGA prototype that is up to 6.5x faster than an implementation using full 32-bit precision. We further develop a variance-optimal stochastic quantization strategy and show that it can make a significant difference in a variety of settings. When applied to linear models together with double sampling, we save up to another 1.7x in data movement compared with uniform quantization. When training deep networks with quantized models, we achieve higher accuracy than the state-of-the-art XNOR-Net.

Finally, we extend our framework through approximation to non-linear models, such as SVM. We show that, although using low-precision data induces bias, we can appropriately bound and control the bias. We find in practice 8-bit precision is often sufficient to converge to the correct solution. Interestingly, however, in practice we notice that our framework does not always outperform the naive rounding approach. We discuss this negative result in detail.

3.11 Adaptive FPGA-based Database Accelerators – Achievements, Possibilities, and Challenges

Daniel Ziener (TU Hamburg-Harburg, DE) and Jürgen Teich (Friedrich-Alexander-Universität Erlangen-Nürnberg, DE)

Joint work of Ziener, Daniel; Becher, Andreas; Dennl, Christopher; Teich, Jürgen; Meyer-Wegener, Klaus
Main reference D. Ziener, F. Bauer, A. Becher, C. Dennl, K. Meyer-Wegener, U. Schürfeld, J. Teich, J. S.Vogt, H. Weber, "FPGA-Based Dynamically Reconfigurable SQL Query Processing", ACM Transactions on Reconfigurable Technology and Systems (TRETS), Vol. 9(4), pp. 25:1–25:24, 2016.
URL http://dx.doi.org/10.1145/2845087

In this talk, we show the achievements of our research on adaptive FPGA-based database accelerators as well as possibilities and challenges of such a system. Our approach exploits the capabilities of partial dynamic reconfiguration of FPGAs [1, 2, 3, 4]. After the analysis of an incoming query, a query-specific hardware processing unit is generated on-the-fly and loaded on the FPGA for immediate query execution. With such adaptive accelerator we achieve a 10 times better performance and up to 30 times better energy efficiency compared to software only solution on an x86-based server [5]. The challenges are the needed flexibility as well as the support of many different operations for accelerate real multi-user database scenarios.

References

1 Ziener, D., Bauer, F., Becher, A., Dennl, C., Meyer-Wegener, K., Schuerfeld, U., Teich, J., Vogt, J. S., Weber, H. *FPGA-Based Dynamically Reconfigurable SQL Query Processing*. ACM Transactions on Reconfigurable Technology and Systems (TRETS) 9 (2016) 25:1–25:24

2 Dennl, C., Ziener, D., Teich, J. *On-the-fly Composition of FPGA-Based SQL Query Accelerators Using A Partially Reconfigurable Module Library*. In: Proceedings of the IEEE International Field-Programmable Custom Computing Machines Symposium (FCCM), Toronto, Canada (2012) 45–52

3 Dennl, C., Ziener, D., Teich, J. *Acceleration of SQL Restrictions and Aggregations through FPGA-based Dynamic Partial Reconfiguration*. In: Proceedings of the IEEE International Field-Programmable Custom Computing Machines Symposium (FCCM), Seattle, USA (2013)

4 Becher, A., Bauer, F., Ziener, D., Teich, J. *Energy-Aware SQL Query Acceleration through FPGA-Based Dynamic Partial Reconfiguration*. In: Proceedings of the International Conference on Field Programmable Logic and Applications (FPL). (2014) 662–669

5 Becher, A., Ziener, D., Meyer-Wegener, K., Teich, J. *A Co-Design Approach for Accelerated SQL Query Processing via FPGA-based Data Filtering*. In: Proceedings of 2015 International Conference on Field-Programmable Technology (FPT '15), IEEE (2015)

4 Working groups

4.1 Breakout Session on "Machine Learning and Databases: Options for Integration"

Michaela Blott (Xilinx – Dublin, IE)

Within this breakout session we considered a number of possibilities to integrate machine learning capabilities with databases:

1. The first idea was to offer machine learning algorithms as user defined functions (UDFs).
2. The second suggestion proposed, considered machine learning as part of the extract, transform and load (ETL) functions for data wrangling, cleansing and preparation and as part of the postprocessing. In the latter case, the data as retrieved from the database would simply feed into a ML analysis tool. A given example was HANA feeding into SAS.
3. We briefly discussed self-tuning databases leveraging machine learning algorithms, but considered these as more extravagant.

Numerous reasons for and against integration were pooled together. Pro integration were the following reasons:

1. Machine learning offers new insights and intelligence that can be gained out of existing data.
2. Secondly debugging would be easier.
3. Databses could become more useful.
4. Database community could bring relevant insights to the machine learning community.
5. Databases would provide the means to tracking and version control for machine learning data.
6. This provides an opportunity to add provenance correctly to databases.
7. Integration provides the capability to provide further acceleration.
8. Integration provides the possibility to leverage insights from 50years of database research to new types of problems.
9. There are obvious commonalities, as described in the next paragraph.

On the downsides, the following conclusions were reached:

1. Security concerns were raised.
2. We found concerns around the clash of an open-source software base with customer-owned private code bases.
3. Integration fo software stacks such as python and R might present numerous difficulties, as well as development support, profiling, and version control.
4. Concerns around database administration were raised.
5. Machine learning presents a huge spectrum of algorithms with very different compute and storage requirements.
6. Machine learning algorithms are not mature yet and undergo continuous substantial change.
7. Finally, given the huge compute times of machine learning algorithms that significantly outweighs the transfer time from database to analytics system, the overall benefit of integrating the systems might be negligible.

In summary, the consensus drifted towards keeping machine learning and databases separate. It might be an opportunity for another seminar in a years time or a separate workshop series as well as a more speculative investigation with a closer look at compute, transfer times and specific algorithms. Perhaps a subset of the overall spectrum, such as decision treed and random forests, which are lighter in compute requirements, could provide an ideal opportunity to start with.

4.2 Breakout Session "Accelerators: Where to position them in the stack?"

Zsolt Istvan (ETH Zürich, CH), Markus Dreseler (Hasso-Plattner-Institut – Potsdam, DE), Ken Eguro (Microsoft Research – Redmond, US), Babak Falsafi (EPFL – Lausanne, CH), Henning Funke (TU Dortmund, DE), Peter Hofstee (IBM Research Lab. – Austin & TU Delft), Eliezer Levy (Huawei Tel Aviv Research Center – Hod Hasharon, IL), Gilles Pokam (Intel – Santa Clara, US), Kenneth Ross (Columbia University – New York, US), Margo Seltzer (Harvard University – Cambridge, US), and Pinar Tözün (IBM Almaden Center – San Jose, US)

Accelerators for data processing are emerging and there are multiple possible hardware architectures and interaction models that have been or could be implemented. Our goal was to discuss about where future accelerators should be located in the stack, so that the DB can best take advantage of them. We concluded that accelerators should be part of the platform and managed by the operating system (OS) but expose a programming interface (API) tailored to the application's need, in our case the database engine. This requires some level of co-design between the accelerator and the applications on top.

We defined what we mean by an accelerator for the purposes of this discussion: "A piece of specialized hardware, that is non-critical, but improves efficiency". The consensus in our group was that the accelerator has to be part of the platform and needs to be managed by the operating system. Operating systems already take care of configuring and multiplexing access to different hardware devices that constitute the platform. Any future accelerator should expose to the OS its multiplexing rules, e.g. level of parallelism, whether it is run-to-completion, etc. And in turn the OS should be able to configure the accelerator for context switching, and deploy tasks on it for the applications.

The layers above the platform and OS, however, should be able to provide task descriptors that are specific to their domain (these could be in declarative or imperative form) and specify what data to use for input and where to write outputs. Using co-designed APIs that act as a bridge between accelerator and database ensures that acceleration functions can take advantage of information about workloads etc. readily available in the database. The actual API will be dependent on the implementation of an application/database and such details as the location of the data, whether the accelerator acts synchronously or asynchronously, etc. In some cases it could be beneficial to provide multiple APIs to the same accelerator depending on the level of abstraction the application on top can best utilize.

4.3 Breakout Session "Future Memory/Storage for Databases"

Zsolt Istvan (ETH Zürich, CH), Goetz Graefe (Google – Madison, US), Peter Hofstee (IBM Research Lab. – Austin & TU Delft), Stefan Manegold (CWI – Amsterdam, NL), Ingo Müller (ETH Zürich, CH), Kenneth Ross (Columbia University – New York, US), Kai-Uwe Sattler (TU Ilmenau, DE), Eric Sedlar (Oracle Labs – Redwood Shores, US), Margo Seltzer (Harvard University – Cambridge, US), and Thomas Willhalm (Intel Deutschland GmbH – Feldkirchen, DE)

With future storage and memory solutions becoming increasingly programmable and the line between the two becoming more blurred, the challenge of integrating these with databases for better performance emerges. We are also presented, however, with the opportunity of shaping the functionality of future storage solutions to match the needs of the database. During our discussions we approached the question from both the angle of a computer architect (what features to add or expose) and a database person (how to take advantage of existing/future features). We identified co-design as being necessary and the output of our discussion is a list of meta-data the database can provide to the storage devices (see attachment).

Given that databases have already good understanding about the data they manage, and also about their own internal data structures, they should be able in the future to provide hints about access patterns, etc. to the operating system (OS) to guide the choice of memory/storage device. Furthermore, in case the devices support offloading functionality, this information could be directly shared with the devices. We explored what information about data the DB could push down to the OS and devices (e.g., whether data is persistent or transient, compressible or not, represents pointers or user data, what is the expected read-write ratio, etc.) and ranked these by expected impact. Access pattern information was identified as the most useful that DBs could provide to smarter storage devices of the future. The expectation is that when data is streaming, for instance, bandwidth could be exploited better by the device, and in case it is pointer-driven access, the devices could perform smarter prefetching, or even traverse structures on their own.

From a database perspective we formulated a requirement to guide the design of offloading functionality in storage/memory, namely that stability and predictability is more important than best-case speedup. For instance, a stable 2x improvement will be preferred over a non-guaranteed 5x, because this would make integration with the query planner and cost functions more feasible.

We also concluded that co-design is preferred, because it is important that the DB receives back from the storage status information specific to the meta-data mentioned before. Trying to hide the acceleration features behind opaque layers in the OS will mean missed acceleration opportunities.

4.4 Reproducible Floating-Point Aggregation

Ingo Müller (ETH Zürich, CH), Gustavo Alonso (ETH Zürich, CH), Andrea Arteaga, and Torsten Hoefler

Industry-grade database systems are generally expected to produce the same result for queries run on the same input as software vendors and cloud providers may be liable for non-reproducible behavior of their systems. However, the numerous sources of indeterminism in modern systems make exactly reproducible results difficult to achieve. This is particularly true if floating-point numbers are involved, where the order of the operations affects the final result.

As part of a larger effort to extend database engines with data representations more suitable for machine learning and scientific applications, in this paper we explore the problem of making relational GroupBy over floating-point formats bit-reproducible, i.e., we make any execution of the operator produce the same result up to every single bit. We start from recent algorithms from high-performance computing that make the summation of floating-point numbers into a single sum bit-reproducible. In a SQL query with GroupBy, however, each of the potentially many groups produces a separate sum, so consecutive inputs do not necessarily aggregate to the same sum. As a consequence, a GroupBy operator with a naïvely integrated bit-reproducible summation algorithm incurs a slowdown of factor 4 to 12 compared to the same operator using conventional summation. We thus explore how to modify existing GroupBy algorithms to make them bit-reproducible and efficient. We are able to reduce the slowdown due to reproducibility to a factor between 1.9 to 2.4, thereby providing a solid basis for supporting more complex operations directly in relational engines. We show the trade-offs offered by the different algorithms in extensive experiments and give recommendations on how to use them in practice.

4.5 Breakout Session "Memory and Storage"

Jens Teubner (TU Dortmund, DE), Alexander Böhm (SAP SE – Walldorf, DE), Sebastian Breß (DFKI – Berlin, DE), Markus Dreseler (Hasso-Plattner-Institut – Potsdam, DE), Babak Falsafi (EPFL – Lausanne, CH), Henning Funke (TU Dortmund, DE), Onur Mutlu (Carnegie Mellon University, US), Gilles Pokam (Intel – Santa Clara, US), Jürgen Teich (Friedrich-Alexander-Universität Erlangen-Nürnberg, DE), Pinar Tözün (IBM Almaden Center – San Jose, US), Annett Ungethüm (TU Dresden, DE), and Daniel Ziener (TU Hamburg-Harburg, DE)

A number of exciting new technologies around memory and storage have emerged in the recent years, including Hybrid Memory Cubes (HMC) or various technologies that provided non-volatile memory at near-RAM speeds. In a breakout session, members of the hard- and software communities discussed the opportunities that the new technologies may open up for database acceleration.

The breakout group concluded that the new technologies could indeed help solve the memory bandwidth problems that main-memory database engines have kept struggling with. Most importantly, scatter/gather-type data accesses would excellently fit many database workloads. On commodity hardware, however, such accesses are known to perform poorly. The modern memory technologies have ample bandwidth inside the memory chip, but are limited by the link to the rest of the system. With little add-ons to the memory chips, chips could re-arrange data following a database's needs before shipping data to the CPU. Suitably equipped and configured, a memory chip could, for instance, convert between row- and column-oriented views of a database table on demand. More advanced applications of the concept could even offer "near-memory computing" with feature-rich processing capabilities right inside the memory chips.

The obvious part where non-volatile memories will affect database engines is transaction management. It seems yet unclear, however, how that could look like, since the technology will blur the line between data structures (e.g., database indexes) designed for on-disk or for in-memory.

5 Open problems

5.1 Data management for HPC clusters

Spyros Blanas (Ohio State University – Columbus, US)

Processing petabyte-sized datasets quickly will inevitably require datacenter-scale computers. In such computers, "hot" storage consists of petabytes of DRAM that is fragmented across tens of thousands of nodes. Nodes are interconnected in unique topologies through proprietary networking hardware. The "cold" data access path is a parallel file system (such as Lustre) with many petabytes of network-attached storage.

The optimizations a DBMS currently performs are insufficient when data management becomes a datacenter-scale challenge. We posit that this unique hardware platform is more than a disaggregated collection of compute, memory and storage resources. We instead envision a data processing system that optimizes query processing holistically for the datacenter and carefully orchestrates data processing tasks for better performance.

We identify the following research opportunities: query optimization that predicts and ameliorates detrimental I/O interference; a distributed buffer pool that proactively places data in a multi-tiered but fragmented storage hierarchy; query execution algorithms that directly interface with high-end, low-latency interconnects; holistic I/O optimization for processing massive arrays by automatically collecting semantically richer metadata to guide data placement.

5.2 Tradeoffs in Energy Efficient Data Management

Henning Funke (TU Dortmund, DE), Stefan Noll, and Jens Teubner (TU Dortmund, DE)

Database systems frequently use an over-proportional amount of energy to offer high performance. This has the disadvantage that high energy consumption limits the ability to scale out due to thermal design constraints. One approach to reduce the power intake is to adjust the power states of hardware. This can be done with frequency scaling of CPUs and DRAM and allows finding a better trade off between energy and performance when adapting power states to workload characteristics. However, in many cases users do not want to give up performance. Therefore, we propose to look for other trade offs than performance for energy. One direction, we consider is trading in accuracy for performance.

5.3 Persistent Memory: Opportunities and Challenges

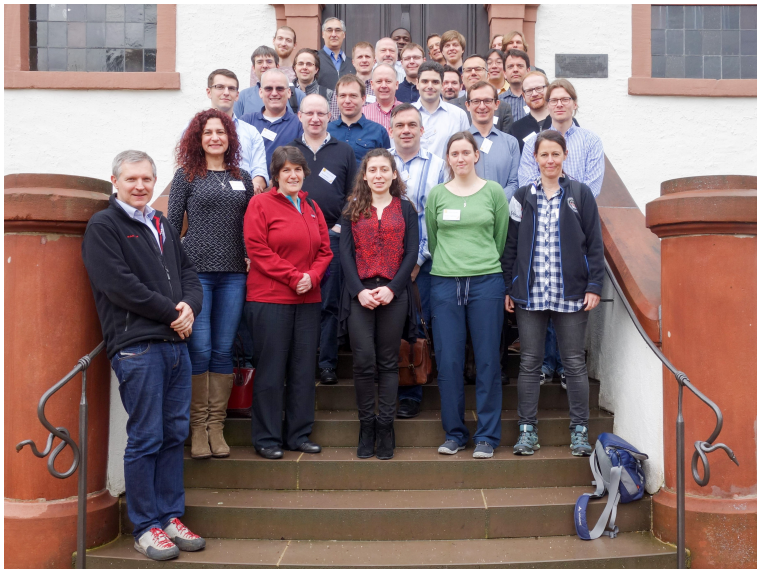
Thomas Willhalm (Intel Deutschland GmbH – Feldkirchen, DE)

Intel and Micron are bringing a new type of non-volatile memory "3D XPoint" to the market. It promises to close the gap between DRAM and flash, in that it will be denser and less expensive than DRAM but faster than flash. This will not only allow to create very fast SSDs but NV-DIMMs based on 3D XPoint. These DIMMs will therefore enable the implementation of persistent memory where durable data can be accessed directly with load/store semantics.

Such a solution will not only leap-frog the performance of storage, but also tear down the barriers of block I/O. On the other hand, it poses new challenges on correctness and a more complex memory hierarchy. Last but not least, the question of data replication over a comparably slow network will become a new challenge.

Participants

- Anastasia Ailamaki
EPFL – Lausanne, CH
- Gustavo Alonso
ETH Zürich, CH
- Carsten Binnig
Brown University – Providence, US
- Spyros Blanas
Ohio State University – Columbus, US
- Michaela Blott
Xilinx – Dublin, IE
- Alexander Böhm
SAP SE – Walldorf, DE
- Peter A. Boncz
CWI – Amsterdam, NL
- Sebastian Breß
DFKI – Berlin, DE
- Markus Dreseler
Hasso-Plattner-Institut – Potsdam, DE
- Ken Eguro
Microsoft Research – Redmond, US
- Babak Falsafi
EPFL – Lausanne, CH
- Henning Funke
TU Dortmund, DE
- Goetz Graefe
Google – Madison, US
- Christoph Hagleitner
IBM Research Zurich, CH
- Peter Hofstee
IBM Research Lab. – Austin, US & TU Delft, NL
- Stratos Idreos
Harvard University – Cambridge, US
- Zsolt Istvan
ETH Zürich, CH
- Viktor Leis
TU München, DE
- Eliezer Levy
Huawei Tel Aviv Research Center – Hod Hasharon, IL
- Stefan Manegold
CWI – Amsterdam, NL
- Andrew W. Moore
University of Cambridge, GB
- Ingo Müller
ETH Zürich, CH
- Onur Mutlu
Carnegie Mellon University, US
- Thomas Neumann
TU München, DE
- Gilles Pokam
Intel – Santa Clara, US
- Kenneth Ross
Columbia University – New York, US
- Kai-Uwe Sattler
TU Ilmenau, DE
- Eric Sedlar
Oracle Labs – Redwood Shores, US
- Margo Seltzer
Harvard University – Cambridge, US
- Jürgen Teich
Friedrich-Alexander-Universität Erlangen-Nürnberg, DE
- Jens Teubner
TU Dortmund, DE
- Pinar Tözün
IBM Almaden Center – San Jose, US
- Annett Ungethüm
TU Dresden, DE
- Stratis D. Viglas
Google – Madison, US
- Thomas Willhalm
Intel Deutschland GmbH – Feldkirchen, DE
- Ce Zhang
ETH Zürich, CH
- Daniel Ziener
TU Hamburg-Harburg, DE



Report from Dagstuhl Seminar 17102

Rethinking Productivity in Software Engineering

Edited by

Thomas Fritz[1], Gloria Mark[2], Gail C. Murphy[3], and Thomas Zimmermann[4]

1 **Universität Zürich, CH,** `fritz@ifi.uzh.ch`
2 **University of California – Irvine, US,** `gmark@uci.edu`
3 **University of British Columbia – Vancouver, CA,** `murphy@cs.ubc.ca`
4 **Microsoft Corporation – Redmond, US,** `tzimmer@microsoft.com`

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 17102 "Rethinking Productivity in Software Engineering". In the following, we briefly summarize the goals and format of the of the seminar, before we provide insights and an outlook, including a few grand challenges, based on the results and statements collected during the seminar.

Seminar March 5–8, 2017 – http://www.dagstuhl.de/17102
1998 ACM Subject Classification D.2.8 Metrics, D2.9 Software Engineering – Management–Productivity, H.5 Information Interfaces and Presentation, H.1.2 User/Machine Systems – Human Factors, H.3.4 Systems and Software – Current Awareness Systems & Performance evaluation (efficiency and effectiveness), H.4.1 Office Automation – Time management & Workflow Management, K.4.3 Organizational Impacts – Employment
Keywords and phrases productivity, software development, human factors, productivity factors, grand challenges
Digital Object Identifier 10.4230/DagRep.7.3.19
Edited in cooperation with André N. Meyer (Universität Zürich)

1 Executive Summary

Thomas Fritz
Gloria Mark
Gail C. Murphy
Thomas Zimmermann

There is an ever-growing demand of software being built and a shortage of software developers to satisfy this demand, despite the immense growth in the number of professional software developers. To address this demand, industry and research are looking into understanding and improving the productivity of individual software developers as well as teams. A substantial amount of research has examined the meaning of software productivity over the past four decades. Much of this research introduces particular definitions of productivity, considers organizational issues associated with productivity, or is focused on specific tools and approaches for improving productivity. In fact, many of the seminal work on software productivity is from the 80s and 90s (Peopleware, Mythical Man-Month, Personal Software Process).

Rethinking Productivity in Software Engineering, *Dagstuhl Reports*, Vol. 7, Issue 3, pp. 19–26
Editors: Thomas Fritz, Gloria Mark, Gail C. Murphy, and Thomas Zimmermann
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

At the same time, software development has changed significantly over the past decades with the rise of agile development, distributed development, more rapid release cycles and the high fragmentation of today's work. Simultaneously the technology available to software engineers has improved with social coding tools like GitHub[1] and StackOverflow[2] and better IDEs. Furthermore, research communities, in particular the HCI and CSCW communities, have made significant advances in supporting knowledge workers to become more productive that one might be able to also transfer to software engineers.

The goal of this seminar was to rethink, discuss, and address open issues of productivity in software development and how to measure and foster productive behavior of software developers. Specifically, we focused on the following questions:

- What does productivity mean for an individual and teams/organizations and how is it measured?
- What are the dimensions and factors of productivity?
- What are the purposes and implications of measuring productivity?
- What are the grand challenges in research on productivity?

[1] http://www.github.com
[2] http://www.stackoverflow.com

2 Table of Contents

3 Introduction

3.1 Seminar Format

In this seminar, we brought together researchers and practitioners with backgrounds in Software Engineering, Human Computer Interaction, and Computer-Supported Collaborative Work who are interested and working on topics related to the productivity of software developers as well as more general knowledge workers. Before the seminar, we conducted a small survey to collect relevant further questions to be addressed in the seminar and the break out groups.

At the seminar, we used a combination of methods to (a) foster vibrant discussions, (b) to address relevant questions on developer productivity as well as to (c) foster interaction and collaborations between attendees. In particular we used a speed dating technique as a way to get to know attendees, short three minute presentations by each attendee to get an overview of everyone's interests and research, fifteen minute talks by a few attendees with various backgrounds to get deeper insights into some of the work in the various areas, and group discussion as well as breakout sessions to enable deeper conversations in smaller groups with the results being reported back to the whole group.

3.2 Productivity – Insights and Outlook

In the following we will present a short summary that we compiled from the discussions, the presentations and the learnings from the attendees. We will thereby focus on the topic of software developer productivity in general, factors of productivity and the grand challenges that lie ahead of us.

Software Developer Productivity

Productivity is a concept that is difficult to define and measure due to its complexity, its multi-facetted nature and the rather broad concept that the term 'productivity' denotes. Depending on the context, other terms such as 'time well spent', 'software quality', 'velocity', or 'satisfaction' might be better suited. Overall it is important to understand and specify the context in which productivity is being measured to determine how to best measure developer productivity. For instance, measuring productivity for the purpose of providing a developer a retrospection of her work and a sense of achievement is very different to measuring productivity for the purpose of evaluating the implementation of a new development process in an organization.

There is a broad range of dimensions that affect the definition and measurement of productivity, such as the specific purpose (e.g. self-assessment, resource allocation, evaluating the success of interventions such as tools and practices, identifying problems, job satisfaction, quality of output), the unit of analysis (e.g. individual, team, organization, inter-organization), the target audience (e.g. personal, manager, customer, shareholder), the time horizon/period (e.g. immediate feedback, ten years later). A more specific definition of the context for measuring productivity will allow you to determine more meaningful measures of productivity.

Another aspect to consider when measuring productivity is the presentation of the measures and the effect of collecting them. Visualizations of productivity measures might be interpreted differently by different people based on background, culture or other reasons and in addition, the sheer collection of certain work related measures might affect the behavior that is being measured or harm the overall outcome (e.g. developers might try to game the system to achieve a better performance rating).

Factors of Productivity

There is a variety of factors of productivity for knowledge workers, such as the skills of the worker, the time of the day, the nature of the task, the attention fatigue, the breaks taken, the work fragmentation, the goals (tangible & intangible), the coordination and deadlines, the team and social factors, or the rewards. Human factors, also known as soft factors, appear to have the biggest effects on overall productivity, yet they are a lot harder to measure. While some of these factors have already been studied in more depth either in the context of general knowledge workers or specifically for software developers, there are still a lot of open challenges and questions.

Open Questions and Grand Challenges

Below is a list of some of the stated open questions and grand challenges by attendees.

- Develop a theoretical framework for productivity.
- Develop an approach that allows to track "everything" at every moment, including detailed data across a company, biometric data from individuals and data on aspects such as satisfaction, mood, fatigue and motivation. Use the data to profile development work and productivity.
- Design and create a company that implements human values and culture of Zappos and compare with other companies to study the effect of these factors on productivity and outcome.
- Examine the difference of software development to all other kinds of knowledge workers and learn what is unique about software development and what is not.
- Define laws or rules of productivity similar to the laws of software evolution, e.g. a happier developer is a more productive developers, a participatory culture in a team is more productive.
- Develop a mapping from questions on productivity to methodology of studying it.
- Conduct a multitude of comparative studies on productivity at different companies or just on different interventions.
- Collect examples of where measuring productivity was done well and had good outcomes, and distill the insights and guidelines from this collection.
- Understand how to support and facilitate productivity?
- Understand how a people's view of productivity affects their productivity and whether changing the motivation from self-improvement to altruism (shifting away from productivity) may increase it (relating productivity to meaning).

3.3 Follow-up Work

Multiple paths forward to continue the work on productivity have been discussed, especially due to the interdisciplinary interest in the topic that can benefit from researchers from various domains, ranging from the organization of another seminar or workshop to the writing of a book and a collaborative grant proposal. At this point in time, we have put together a web site with related work resources and two participants started to organize the co-writing of a book on topics of productivity.

4 Overview of the Main Talks

4.1 Dark side of Global Agile: Challenging Productivity as a Positive

Pernille Bjørn (University of Copenhagen, DK)

URL http://itu.dk/~pbra/pmwiki/pmwiki.php

The talk explore the dark side of global agile – and how introducing agile scrum processes into a global outsourcing setup creates special conditions for software engineering work, which risk taking away empowerment and work/life balance for software engineers in the global south. Being a global software developer working out of the global south is different than working out of the global north. However, such presentation would not be so much about state-of-art and challenges – but rather about posing a question about productivity in software engineering.

4.2 Programming Productivity Primer

Andrew J. Ko (University of Washington – Seattle, US)

URL http://faculty.washington.edu/ajko/

In this talk I present recent evidence about software engineering productivity from multiple levels, including individual, team, organizational, and market perspectives. I discuss important discoveries at each of these levels and pose new questions about the relationships between these levels.

4.3 "Stop trying to do what you're trying to do": Developers' Perceptions of Measuring Productivity

Christoph Treude (University of Adelaide, AU)

URL http://ctreude.ca/

Software developers pursue a wide range of activities as part of their work, and making sense of what they did in a given time frame is far from trivial as evidenced by the large number of awareness and coordination tools that have been developed in recent years. To inform tool design for making sense of the information available about a developer's activity, we conducted a survey with 156 GitHub users to investigate how they would summarize and measure development activity. In addition to proposing several formulas for productivity, participants warned that measuring development activity can be dangerous and that metrics are likely to be gamed. Aspects to consider include the created business value, the quality of work produced, the difficulty of a task, and the context of the work.

4.4 Quantifying mind-wandering in laboratory studies

Marieke van Vugt (University of Groningen, NL)

URL http://www.rug.nl/staff/m.k.van.vugt/

Mind-wandering is a process of task-unrelated thought that could sometimes hinder productivity, but may also be beneficial in other circumstances. We can measure mind-wandering using a triangulation approach, combining first- and third-person measures. Specifically, we give people a boring task and every 30–60 seconds, we ask them whether they were paying attention to the task, or other things. We can then relate objective task performance back to these subjective "thought probes". Studies show that just prior to responding off-task, performance is worse, variability in response time is increased, and event-related potentials have a lower amplitude. It is important to distinguish between mind-wandering that is easy to disengage from, and that is not so disruptive from mind-wandering that is more ruminative in nature and difficult to disengage from. Ruminative mind-wandering can even lower working memory capacity. In short, measures used in the study of mind-wandering may be interesting to include in studies of productivity.

4.5 What is Productivity? Terminology and Influencing Factors

Stefan Wagner (Universität Stuttgart, DE)

URL http://www.iste.uni-stuttgart.de/se/menschen/stefanwagner.html

Increasing productivity is a general goal in software engineering research. Yet, there is a lot of uncertainty about what productivity means in knowledge work and software engineering in particular. I describe a terminology that defines productivity in terms of effectiveness and efficiency which describe the functionality and quality of a software system with respect to its purpose and the effort put into building it. Profitability extends this by including effects of price and cost inflation. Performance furthermore includes marketing or corporate learning.

In Wagner and Ruhe (2008), we collected 51 factors that influence productivity as stated in the literature. There is a huge variety of factors ranging from product and process factors to team and organisational factors. In a recent study (Karimi et al., 2016), we found that also personality (in particular conscientiousness) and programming styles influence productivity in student projects.

Finally, the ProdFLOW approach by Siemens (Ruhe, Wagner, 2008) is an industrial method to first investigate a specific business context by interviews and qualitative analysis to derive the important productivity levers. Only then, we try to measure the improvement of these levers.

Participants

- Christian Bird
Microsoft Corporation – Redmond, US
- Pernille Bjørn
University of Copenhagen, DK
- Marcos Borges
University of Rio de Janeiro, BR
- Duncan Brumby
University College London, GB
- Robert Feldt
Chalmers UT – Göteborg, SE
- Thomas Fritz
Universität Zürich, CH
- James D. Herbsleb
Carnegie Mellon University – Pittsburgh, US
- Christian Janssen
Utrecht University, NL
- Ciera Jaspan
Google Inc. – Mountain View, US
- Katja Kevic
Universität Zürich, CH
- Andrew J. Ko
University of Washington – Seattle, US
- Gloria Mark
University of California – Irvine, US
- André Meyer
Universität Zürich, CH
- Gail C. Murphy
University of British Columbia – Vancouver, CA
- Emerson Murphy-Hill
Google Inc. – Mountain View, US
- Brad A. Myers
Carnegie Mellon University – Pittsburgh, US
- Christopher J. Parnin
North Carolina State University – Raleigh, US
- Martin Robillard
McGill University – Montreal, CA
- Caitlin Sadowski
Google Inc. – Mountain View, US
- Federica Sarro
University College London, GB
- David C. Shepherd
ABB – Raleigh, US
- Janet Siegmund
Universität Passau, DE
- Margaret-Anne Storey
University of Victoria, CA
- Christoph Treude
University of Adelaide, AU
- Marieke van Vugt
University of Groningen, NL
- Stefan Wagner
Universität Stuttgart, DE
- Thomas Zimmermann
Microsoft Corporation – Redmond, US

Report from Dagstuhl Seminar 17111

Game Theory in AI, Logic, and Algorithms

Edited by

Swarat Chaudhuri[1], Sampath Kannan[2], Rupak Majumdar[3], and Michael J. Wooldridge[4]

1 **Rice University – Houston, US,** swarat@rice.edu
2 **University of Pennsylvania – Philadelphia, US,** kannan@cis.upenn.edu
3 **MPI-SWS – Kaiserslautern, DE,** rupak@mpi-sws.org
4 **University of Oxford, GB,** mjw@cs.ox.ac.uk

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 17111 "Game Theory in AI, Logic, and Algorithms".

Seminar March 12–17, 2017 – http://www.dagstuhl.de/17111
1998 ACM Subject Classification I.2.11 [Distributed Artificial Intelligence] Multiagent Systems, F.3.1 Specifying and Verifying and Reasoning about Programs, F.1.1 Models of Computation, F.2 Analysis of Algorithms and Problem Complexity
Keywords and phrases game theory, formal methods, logic, algorithms, equilibria, multiagent systems
Digital Object Identifier 10.4230/DagRep.7.3.27

1 Executive Summary

Swarat Chaudhuri
Sampath Kannan
Rupak Majumdar
Michael J. Wooldridge

The Dagstuhl Seminar *17111: Game Theory in AI, Logic, and Algorithms* was held from March 12–17, 2017. The seminar explored research challenges at the interface of computing and game theory. This area has seen fervent research activity in recent times. Specifically, game theoretic ideas have found currency in three key areas of computer science: in the *algorithms* community, algorithmic game theory is now a well-established sub-field; in *formal methods*, model checking and synthesis problems have been studied using game-theoretic concepts; and in *artificial intelligence*, game theory has come to provide the fundamental conceptual vocabulary for the field of multi-agent systems. Despite this manifest common interest, there is surprisingly little trade between game-theoretic approaches in these different subfields of computer science. Our aim in this seminar was to start to build some bridges between these three areas.

Game Theory in AI, Logic, and Algorithms, *Dagstuhl Reports*, Vol. 7, Issue 3, pp. 27–32
Editors: Swarat Chaudhuri, Sampath Kannan, Rupak Majumdar, and Michael J. Wooldridge

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

2 Table of Contents

3 Program

The seminar's program consisted of an array of talks by speakers from algorithms, formal methods, and artificial intelligence, as well as discussion on how the topics discussed in the various talks connected with each other. Now we summarize this program.

3.1 Monday, March 13

The program for the first day consisted of three tutorials, one from each of the three communities represented at the seminar. The goal of these tutorials was to introduce to the participants the view of game theory from the perspectives of these communities, and to set the stage for subsequent interdisciplinary discussions.

Of the tutorial speakers, Moshe Vardi surveyed the long history of game-theoretic ideas in logic and formal methods, in particular highlighting the deep relationship between game theory and the system synthesis problem. Mihalis Yannakakis surveyed recent developments in algorithmic game theory. Michael Wooldridge spoke about the role of game theory in artificial intelligence, specifically multi-agent systems.

3.2 Tuesday, March 14

The second day started with a session on game-theoretic results of interest in both formal methods and algorithms. In this session, Rasmus Ibsen-Jensen summarized a recent quasi-polynomial algorithm for parity games. After this, Orna Kupferman and Tami Tamir gave a talk on enriching classical definitions of games using techniques from formal methods.

The next session covered games from economics. Evdokia Nikolova spoke of risk-averse selfish routing, while Maria Polukarov discussed trembling hand equilibria of voting games.

The session that followed was on security games. Arunesh Sinha discussed the Stackelberg game approach to safe and secure systems, and Yuan Deng spoke about disarmament games. Antonin Kucera presented a method for efficient strategy synthesis for large and fully connected patrolling graphs.

The next session consisted of two broad talks on privacy. Sampath Kannan gave a broad introduction to algorithmic mechanisms for privacy. Justin Hsu talked about formal methods for privacy.

The day ended with an open problems session. Here, Rayna Dimitrova presented an open problem on robot routing, and Jan Kretinsky presented an open question on winning strategies that are obtained by learning with guarantees. Jean-Francois Raskin spoke about some open questions about how to mix reasoning about certainty and expectation.

3.3 Wednesday, March 15

Wednesday's program was half a day long, given that an excursion was scheduled in the afternoon. The first session of the day focused on the relationship between system synthesis and games. Here, Kim Larsen talked about controller synthesis for cyber-physical systems, and Igor Walukiewicz gave a talk on the challenge of synthesizing distributed systems. Ruediger Ehlers ended the session with a talk on the environment model in synthesis.

In an open problems session that followed, Valentin Goranko presented some challenges in games of pure coordination without communication. Evdokia Nikolova spoke about some open questions about dynamic congestion games in algorithmic game theory, specifically highlighting how models of system dynamics in formal methods may be of interest in algorithms.

3.4 Thursday, March 16

The morning session of this day consisted of two talks on game theory in algorithms. Nicole Immorlica spoke about Yiling Chen gave a talk on informational substitutes and compliments. In addition, Patricia Bouyer talked about average energy games.

In the afternoon, we had a session on learning. Sanjit Seshia gave a talk on modeling human reward functions in autonomous driving, and Eric Balkanski gave a talk on statistical cost sharing, specifically learning fair cost allocations from samples. Thomas Brazdil gave a talk on decision trees.

The final session of the day was on equilibria. Veronique Bruyere talked about subgame perfection, and Kousha Etessami spoke about trembling-hand perfect equilibria, and quasi-perfect equilibria, in n-player extensive form games of perfect recall. The day ended with a talk by Suguman Bansal on computing equilibria in a new class of games called regular repeated games.

3.5 Friday, March 17

The last day of the seminar primarily involved discussions about the role of game theory in the three areas discussed in the seminar.

4 Conclusions

Perhaps the biggest achievement of the seminar was to educate participating resesarchers about the role of game theory in computer science research outside of their immediate subareas. The roles of game theory in the three focus areas of the seminar – algorithms, formal methods, and artificial intelligence – are rather different. Algorithmic game theory tends to focus on algorithmic computation in games (in particular computing solution concepts) and the use of game theoretic techniques in the analysis and construction of distributed computer systems (for example algorithmic mechanism design). In logic and formal methods, games are used in reasoning about branching behaviors of systems and verification of systems containing multiple components, as well as system synthesis. In artificial intelligence, game theoretic concepts are routinely used in the analysis of multi-agent systems. Most researchers working in one of the three areas do not have opportunities to experience the roles of game theory outside of their areas on a day-to-day basis. By offering alternative perspectives on games in computer science, the seminar will possibly influence their future research agendas.

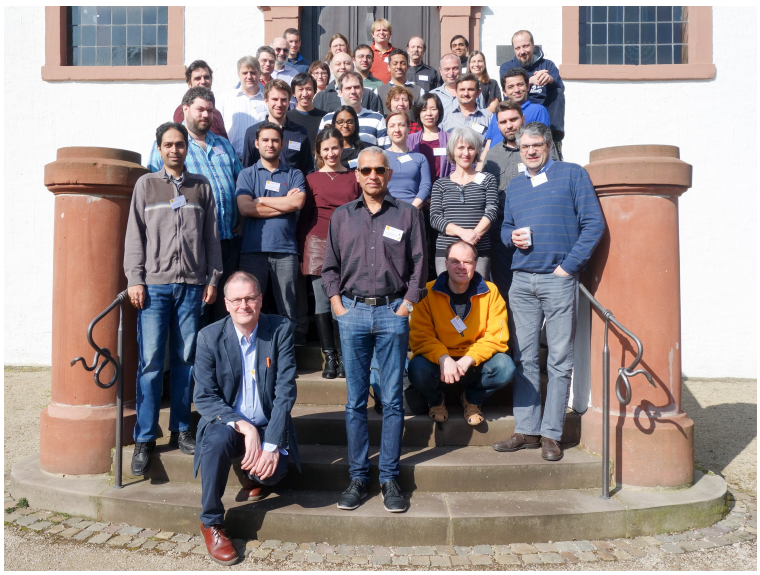
For example, a participant who worked on algorithmic game theory was fascinated by the way formal methods research models dynamics of games, in contrast to much of algorithmic game theory research, which tends to study games that do not evolve over time. There were also discussions on the use of solution concepts such as trembling-hand equilibria, recently

investigated in algorithmic game theory, in formal methods, and the use of techniques from contemporary formal methods in analysis of multiagent systems.

At the same time, the seminar did not lead to a conclusive agenda, with concrete action items, that unifies the three strands of game-theoretic research. This is perhaps not surprising given that the research communities of formal methods, multiagent systems, and algorithms do not have much overlap, and building up any interdisciplinary research agenda takes time. However, we believe that the seminar created some important conversations between game theorists in the three communities that we targeted, and as such, was a moderate success.

Participants

- Natasha Alechina
University of Nottingham, GB
- Eric Balkanski
Harvard University – Cambridge, US
- Suguman Bansal
Rice University – Houston, US
- Patricia Bouyer-Decitre
ENS – Cachan, FR
- Tomás Brázdil
Masaryk University – Brno, CZ
- Véronique Bruyère
University of Mons, BE
- Swarat Chaudhuri
Rice University – Houston, US
- Yiling Chen
Harvard University – Cambridge, US
- Yuan Deng
Duke University – Durham, US
- Rayna Dimitrova
MPI-SWS – Kaiserslautern, DE
- Rüdiger Ehlers
Universität Bremen, DE
- Kousha Etessami
University of Edinburgh, GB
- Bernd Finkbeiner
Universität des Saarlandes, DE
- Valentin Goranko
University of Stockholm, SE
- Julian Gutierrez
University of Oxford, GB
- Paul Harrenstein
University of Oxford, GB
- Hanno Hildmann
Univ. Carlos III – Madrid, ES
- Justin Hsu
University of Pennsylvania – Philadelphia, US
- Rasmus Ibsen-Jensen
IST Austria – Klosterneuburg, AT
- Nicole Immorlica
Microsoft New England R&D Center – Cambridge, US
- Wojtek Jamroga
Polish Academy of Sciences – Warsaw, PL
- Sampath Kannan
University of Pennsylvania – Philadelphia, US
- Jan Kretinsky
TU München, DE
- Antonin Kucera
Masaryk University – Brno, CZ
- Orna Kupferman
Hebrew University – Jerusalem, IL
- Martin Lange
Universität Kassel, DE
- Kim Guldstrand Larsen
Aalborg University, DK
- Rupak Majumdar
MPI-SWS – Kaiserslautern, DE
- Nicolas Markey
IRISA – Rennes, FR
- Daniel Neider
MPI-SWS – Kaiserslautern, DE
- Evdokia Nikolova
University of Texas – Austin, US
- Doron A. Peled
Bar-Ilan University – Ramat Gan, IL
- Sophie Pinchinat
IRISA – Rennes, FR
- Maria Polukarov
University of Southampton, GB
- Jean-Francois Raskin
Free University of Brussels, BE
- Sanjit A. Seshia
University of California – Berkeley, US
- Arunesh Sinha
University of Michigan – Ann Arbor, US
- Tami Tamir
The Interdisciplinary Center – Herzliya, IL
- Moshe Y. Vardi
Rice University – Houston, US
- Igor Walukiewicz
University of Bordeaux, FR
- Michael J. Wooldridge
University of Oxford, GB
- Mihalis Yannakakis
Columbia University – New York, US



Report from Dagstuhl Seminar 17112

Using Networks to Teach About Networks

Edited by

Timur Friedman[1], Aiko Pras[2], and Jürgen Schönwälder[3]

1 **UPMC Sorbonne Université – Paris, FR,** timur.friedman@upmc.fr
2 **University of Twente – Enschede, NL,** a.pras@utwente.nl
3 **Jacobs University Bremen, DE,** j.schoenwaelder@jacobs-university.de

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 17112 "Using Networks to Teach About Networks". The seminar brought together people with mixed backgrounds in order to exchange experiences gained with different approaches to teach computer networking. Despite the obvious question of *what to teach*, special attention was given to the questions of *how to teach* and *which tools and infrastructures can be used effectively* today for teaching purposes.

Seminar March 12–15, 2017 – http://www.dagstuhl.de/17112
1998 ACM Subject Classification K.3.0 General, K.3.1 Computer Uses in Education, K.3.2 Computer and Information Science Education, C.2.0 General, C.2.1 Network Architecture and Design, C.2.2 Network Protocols, C.2.3 Network Operations, C.2.5 Local and Wide-Area Networks, C.2.6 Internetworking
Keywords and phrases computer networks, Internet, education, peer instruction, online learning, educational technologies
Digital Object Identifier 10.4230/DagRep.7.3.33

1 Executive summary

Timur Friedman
Aiko Pras
Jürgen Schönwälder

Computer networks have become a common utility and the Internet provides new opportunities for education. In addition, we see an increasing deviation of the deployed Internet from the basic principles driving the design of computer networks. All this has an impact on how we educate young minds in computer networking and hence it is required to rethink how education in computer networking should be organized, which topics are essential to cover and which ones are merely nice illustrations of core concepts. Furthermore, it seems necessary to think about using the Internet itself more intensively to develop new educational materials. In order to start a discussion of such educational aspects, a Dagstuhl seminar titled Using Networks to Teach About Networks has been organized. Some questions discussed during the seminar were:

- Which topics should be taught in a typical undergraduate course? What are the essential basic principles that need to be understood? Which topics should be covered in a typical graduate course? How to deal with the fact that architectural concepts are often violated in real networks?

- How should topics be taught? How to best use the Internet for teaching how the Internet works? How can we more easily 'mesh' teaching materials? Can we better organize the sharing of video content, assignments, or experimental setups? Do we need an open source platform for teaching materials? What about open source books on computer networks replacing traditional textbooks?
- What is the experience with modern teaching styles, such as pure online courses like MOOCs or flipped classrooms? Which role should project work play? How can novel teaching ideas best be leveraged and integrated into existing educational concepts?

2 Table of Contents

3 Presentations

Several prepared presentations were given during the seminar. The slides of the presentations can be found on the shared documents page of the seminar [4].

3.1 Collaborative teaching and learning (Jordi Domingo-Pascual)

Jordi Domingo-Pascual (UPC) discussed in his presentation which concepts to teach and at which level. He stressed the point that the real Internet can be used for teaching purposes and he further developed the idea of collaborative teaching, i.e., the option to run labs concurrently at multiple institutions and to let students collaborate over the Internet to do experiments with the Internet.

3.2 Anytime and anyplace learning (John Domingue)

John Domingue (OU) stressed the need to support anytime and anyplace learning. He reviewed in his presentation how the EU-funded FORGE project has been providing tools that integrate network experimentation facilities developed by the FIRE project into an online learning system.

3.3 Active learning experience (Gunnar Karlsson)

Gunnar Karlsson (KTH) explained how he has redesigned his introductory computer networking course to move away from teacher centered instruction towards active learning [7]. Active learning has been shown to increase student performance in science, engineering, and mathematics [6]. Gunnar redesigned his course by reducing the scope of what he teaches and leaving data communication as well as network architecture and standardization as self-study for the students. The course now has continuous examination in the form of five mini-exams, three mandatory laboratory sessions, two mandatory individual written reports and four mandatory case studies as group work with reports and presentations in class. Active learning is realized by posing a problem and letting students discuss solutions in smaller groups (2-3 students) before groups report their results and compiling a joint solution at the board.

3.4 Experience with the rake philosophy (Jean-Yves Le Boudec)

Jean-Yves Le Boudec (EPFL) discussed that he sees two different options, namely to either teach all the details of all networking protocols (largely infeasible) or to be focused on the general principles, leaving the mountains of details to further study. Jean-Yves Le Boudec adopted the rake philosophy where he is covering depths by carefully selected labs and breadth by extrapolation based on lectures and labs. During classes, he uses an active learning approach where students are asked in a first step to invent their own solution to a given problem and in a second step the student's solution are compared to existing solutions. The idea is that students only have to learn the difference to their own solution.

3.5 Educating future systems programmers (Lisa Yan)

Lisa Yan (Stanford) reported about their experiences with running an undergraduate networking course that stresses implementation work. The course material is centered on questions such as "How does the Internet work?", "What is the theory behind how the Internet works?", and "Why was the Internet developed this way?". Students spend a large amount of their time on intensive programming tasks in which students basically implement their own IP router from scratch. Tools like Mininet, VirtualBox, Wireshark, and Mahimahi are used within an OpenEDX environment. The instructors use the flipped classroom approach in class meetings.

3.6 Educating future researchers (Lisa Yan)

Lisa Yan (Stanford) reported that their graduate course is largely focused on reproducing research. Students first summarize a research paper and afterwards they try to reproduce the research results. Students are encouraged to interact and collaborate with other researchers, in particular the authors of the original research papers the students are trying to reproduce. Letting graduate students reproduce research has been found beneficial for the students since they have to understand a paper in detail and they build up a personal relationship with the authors. Furthermore, the knowledge that a research results has been reproduced is valuable for the research community as a whole.

3.7 Using learning analytics (Marc-Oliver Pahl)

Marc-Oliver Pahl (TUM) talked about learning analytics, i.e., the measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimizing learning and the environments in which it occurs. Marc-Oliver Pahl is using learning analytics intensively in his courses and labs to continuously improve teaching. Students can always see their results and their relative ranking. He recently started experiments trying to predicting learning outcomes. This, of course, can also be risky as such predictions may change the student's attitude towards a course or lab.

3.8 Recording learning achievements (John Domingue)

John Domingue (OU) discussed the usage of blockchain technology in order to record learning achievements. The basic idea is to move the storage of data about achievements from organizations issuing certificates to a distributed blockchain. The benefit is that data is owned and controlled by students instead of educational institutions while increasing transparency and reducing risks of fraud.

4 Breakout Groups

The seminar participants did split into four smaller groups in order to discuss some topics in more detail. The following sections summarize the results of the breakout group discussions.

4.1 Content of computer networking courses

Most people follow, at least partially, traditional textbooks (e.g., the James Kurose and Keith Ross textbook [8]) or online textbooks such as Olivier Bonaventure's computer networking book [1] or Jean-Yves Le Boudec's tutorial on rate adaptation, congestion control, and fairness [2]. While there is a common core of topics that people seem to cover, there are also many differences due to the different functions courses have in the various curricula or differences in the target audiences. Topics typically covered are Internet architecture, physical layer, link layer, IP layer, intra-domain routing, inter-domain routing, congestion control, application layer protocols, network security, building simple networks, practical assignments (a more detailed discussion can be found on the shared documents page of the seminar [4]). There are, however, often significant differences in the details and in which order and depths topics are covered.

Overall, it seems desirable to move towards a modular framework of composable educational units. Such a framework could facilitate the exchange and evolution of educational material. Educational material in this context covers textual resources (books, book chapters, articles, ...), presentation slides, videos, exercise sheets, programming tasks, lab experiments, quizzes, and exam questions. Furthermore, it is desirable to add metadata to educational material, such as authors, editors, contributors, license conditions (preferably creative commons BY). In addition, it seems to be useful to track where educational materials are used. It was also suggested to discuss course units in the context of competence levels, for example based on the Revised Bloom Taxonomy [11], which distinguishes in the cognitive dimension *remembering*, *understanding*, *applying*, *analyzing*, *evaluating*, and *creating* and in the knowledge dimension *factual knowledge*, *conceptual knowledge*, *procedural knowledge*, and *metacognitive knowledge*.

While there was general agreement that it is desirable to more easily share educational materials, it is less clear how to reward people for sharing material in a form that is easily reusable and which kind of infrastructure is necessary to organize the sharing process.

4.2 Teaching methods

Computer networking courses differ based on the target groups (primarily electrical engineering students versus primarily computer science students) and on the place of the course in the curriculum (typically 2nd or 3rd year). In general, students tend to have problems switching between different views and facets of a concept (e.g., understanding the interplay of different protocol layers) and thinking in terms of an asynchronous distributed system.

A general goal of teaching methods is to encourage students to be active, i.e., to make them ask questions or to let them develop solutions to certain computer networking problems. The following teaching methods were discussed in more detail:

- Flipped classroom: The flipped classroom teaching method assumes that teaching materials are studied by students at home before the class session, while in-class time is devoted to discussions or exercises [3, 5]. A common problem is that students who are not used to flipped classroom style of teaching often come unprepared or they misunderstood the content. This makes discussion in classes sometimes difficult and courses can mutate into "sandwich classrooms", where students first self-study before having a classroom discussion, often followed by another self-study phase.

- Students grading students: Several people reported positive experience with letting students grade results produced by other students or letting students create teaching materials that are reviewed by their peers. Overall, students tend to be fair, they often grade tougher than the regular instructors. Of course, involving students not only in the production of solutions to given problems but also in the assessment of solutions is not a cheap grading tactic; instructors need to carefully monitor the process and they are in charge of grading the student's assessments. Using the students grading students approach requires that clear guidelines are provided, that expectations are clearly communicated, and that sufficient anonymity is provided (double blind), which may require a certain minimum class size. A radical example of this educational approach is École 42 and 42 USA.
- Conference-style seminars: Some attendees reported about their positive experience with letting students write reports about selected topics and to organize a double-blind review process where students have to evaluate reports written by other students. Students are allowed to revise their reports based on the reviews before giving a short presentation about the topic in class. Grading is based on the reviews a student has written and the presentation, but not on the report itself.
- Student competitions: Some attendees reported positive experiences with posting challenges that lead to competitions between student groups. The challenges are well defined tasks that must be solved in a given timeframe. In order to stimulate competition, it is crucial to have a live scoring system providing student teams with direct feedback about their performance relative to others. Grading depends on the achievement of the student teams. It is possible to include a presentation of the winning solution at the end. Student competitions require that a longer timeslot is available, ideally a day or at least half a day, so that students can concentrate on the task given to them.

The sizes of computer networking courses vary significantly between different academic institutions. Scaling courses to large numbers of students requires careful planning, in particular when it comes to lab sessions or programming assignments. It is important to find ways to prevent plagiarism. For program code, structural similarity testing tools like MOSS can be useful. Systems like Turnitin can help detect plagiarism in written reports. It is important that any usage of such tools is announced well ahead of the assignments, ideally at the beginning of a course or lab. For communication outside the classroom, collaborations systems like Piazza have been found useful. Some institutions use fully fledged online learning platforms such as OpenEDX or Moodle.

4.3 Tools and testbeds

In addition to regular command line tools, a number of more specialized tools are already widely used in lab courses and to a lesser extent in classrooms. Wireshark is widely used to dissect packets and to analyze captured packet traces. Wireshark is also good for understanding packet flows or specific protocol interactions. There are also some repositories of open packet traces ([10, 9, 12]) that can be used in student projects. Commonly used flow analysis tools are Bro, Tranalyzer, ntop, or nfdump. A powerful packet generation tool is Scapy.

Network emulation tools seem to be replacing network simulators such as NS3. Emulation tools are able to scale up to the sizes typically needed for undergraduate courses (or labs) and the learning curve is usually lower. Mininet seems to be a popular solution together

with its cousin Mininext, which however does not seem to be actively maintained. There are in addition graphical network emulation tools such as GNS3, which can also emulate command line interfaces of commercial routers.

Different approaches can be used to make experiments on the Internet. The PlanetLab platform can be used to let students gain experience with running software on a live distributed system. However, for simple experiments, it has been found useful to implement a more student friendly interface on the PlanetLab infrastructure that makes it easy to run simple experiments without all the usual PlanetLab account and slice management overhead. This approach has been used in Timur Friedman's network measurement MOOC. The RIPE Atlas measurement infrastructure has been found easy to use for network measurements, in particular due to the availability of easy to use APIs. The same is true for the RIPE Stat service, which makes it easy to retrieve a lot of metadata about the Internet resources, both via a web interface or via an API.

For many labs, it is useful to have access to good visualization tools. It is a benefit if students already know standard tools like gnuplot or statistical analysis tools like R. Some specific visualization tools that have been found useful are BGPlay and TPlay. Visualization tools that have been found missing are tools that can properly visualize network dynamics.

4.4 Educational technology

Educational technology can be used to scale up courses to large numbers of students or to allow students to study at their own pace independent of classroom meetings that are imposing a fixed learning pace on all students. Furthermore, educational technology can deliver detailed insights about how students learn and which topics they find difficult to understand. Typical problems that were experienced while using educational technology are related to cheating, keeping students motivated, and keeping students focused. Technical setup problems still exist although things seem to improve. Problematic are tutoring interactions (many questions pop up during the night before a deadline) and there is generally a lack of useful and actionable feedback.

Cheating problems can be reduced by having a strong authentication system (Coursera for example uses fingerprints and webcam pictures). Hardware authentication devices such as YubiKey may further help in multi-factor authentication systems. Another helpful approach to reduce cheating is randomization or even personalization of tests.

In order to keep students motivated, it is useful to present content in small units and to integrate questions regularly to assess the learning progress. It is also useful to construct breaks by switching learning media frequently, e.g., switching from video content to a quiz, then back to video content followed by a practical experiment and so on. Another motivator can be some form of competitions. It can be useful to think of a course as a computer game with multiple levels that can be reached.

The goal of learning analytics is generally to improve learning materials and keeping in touch with the virtual learner groups of an online course. Online learning systems allow to collect a lot of data but it remains unclear which information should be collected and which information should not be collected. There are certain ethical and legal considerations and of course privacy concerns. For example, should the time spent per learning element be used to customize tests or exams? How comparable are such personalized exams? What about correlation with demographic data? And who (student, tutor, instructor) is allowed to have access to which data (and for which purposes)?

Since the production of online learning material is very time intensive and hence expensive, it is useful to find ways to collaborate and to share learning materials. However, there is also a value of a diversity of teaching approaches. By sharing educational units at a large scale, there is a certain risk that less people will be thinking about how to best explain certain concepts and hence we may loose valuable fresh ideas.

5 Demonstrations

Seminar participants were invited to demonstrate educational approaches or tools that they found useful. The following sections summarize some of the demonstrations.

5.1 Blended learning for teaching networks (Marc-Oliver Pahl)

Marc-Oliver Pahl (TUM) demonstrated iLab, a blended learning hands-on course concept. The didactic concept builds on four phases: (a) lecture (1.5 hours), (b) individual preparation ($\approx$ 6 hours), (c) practical teamwork ($\approx$ 10 hours), and (d) individual oral exams (20 minutes). An eLearning system has been implemented to support these four phases and to collect data for learning analytics. The didactic approach has been used successfully with $\approx$ 2000 Bachelor and Master students so far.

5.2 Internet security MOOC (Aiko Pras and Anna Sperotto)

Aiko Pras (UT) and Anna Sperotto (UT) showed their work on a MOOC on Internet Security, running on the OpenEDX platform. They have created short explanatory videos and student exercises that are often customized for each student. For example, they create different traffic traces for each student, which makes it difficult for students to simply copy a solution created by some other student. The Internet security MOOC is currently running at a small scale for testing purposes. Aiko Pras reported that the availability of the OpenEDX infrastructure at the University of Twente already motivated other colleagues to use the online learning infrastructure for their courses as well. Hence, you will find a collection of additional courses on the platform that were not initially envisaged.

5.3 Student competitions (Pieter-Tjerk de Boer)

Pieter-Tjerk de Boer (UT) is successfully using student competitions for educational purposes and he intends to make them available to other universities. He demonstrated an assignment where students have to design and implement a medium access control protocol to share a time-slotted medium fairly and efficiently among four nodes. The students are provided with a template of a program that decides whether a node uses an announced time-slot or not. The challenge given to the students is to design algorithms that try to avoid collisions and improve the utilization of the channel. Student groups design and implement their own algorithms and run them against a server. The server calculates efficiency and fairness scores that are immediately shown to all participants. This immediate feedback motivates students to engage in a competition between student groups, which generally improves student activity and learning outcomes.

5.4 Measurement data analysis exercise (Fabio Ricciato)

Fabio Ricciato (UL) explained how he is teaching the pitfalls of measurement data analysis. He provides students with datasets together with a short description how the datasets have been produced. The students are given the task to analyze the dataset and answer some (apparently) simple questions. The assignment is inspired by common problems that are typically encountered in real dataset, such as incomplete context information and ambiguous meta-data, and it is designed to expose the risks of a superficial (mis)use of the most basic statistical concepts. Fabio Ricciato did run his toy measurement data analysis exercise as part of the PhD school on traffic monitoring and analysis, which was part of 8th Traffic Monitoring and Analysis workshop (TMA 2016). In general, letting students make mistakes they can learn from seems to be an effective approach. Another useful method is to review mistakes made by others, e.g., by critically discussing with the students the methodological pitfalls encountered in some papers. The key message made by Fabio Ricciato was that inducing the students to discover "how NOT to do things" is not less important than explaining directly how things should be done – a pedagogical attitude that he summarizes as "teaching by negatives".

5.5 Traffic mining and analysis (Stefan Burschka)

Stefan Burschka (RUAG) provided an overview how he is teaching traffic mining and troubleshooting techniques. His approach is to confront students with scenarios where it is necessary to develop creative approaches to solve puzzles given to students. The idea is to motivate students to pay attention to little details while at the same time students should learn that data always exists in a certain context that is very important in order to interpret the data in a correct way. In order to mine large datasets (packet captures larger than 1 TB) effectively, he is developing an extensible tool called Tranalyzer, that can efficiently extract flows without being bound to a very narrow definition of a traffic flow. Stefan Burschka did run his traffic mining exercise as lab sessions of the 10th Autonomous Infrastructure, Management and Security conference (AIMS 2016).

6 Conclusions

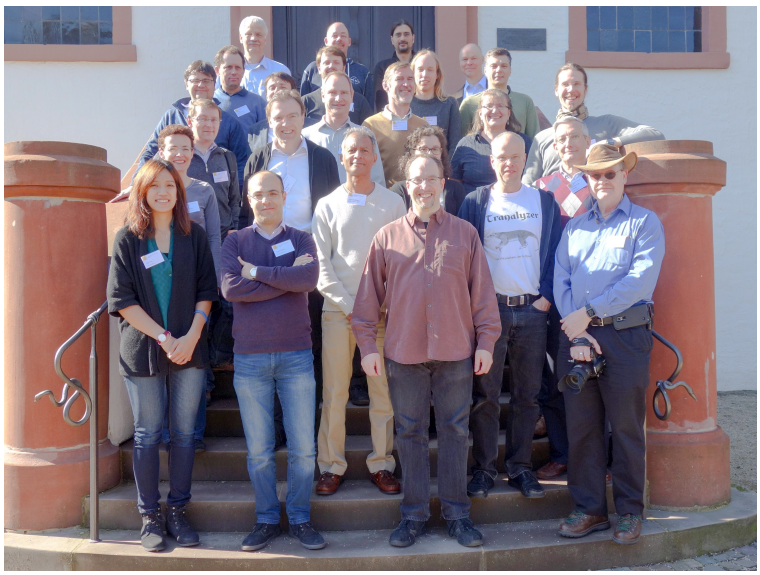
It became clear during the seminar that the way people teach computer networking courses is undergoing changes. During the time available at the seminar, it was possible to establish a common sense about the various ideas tried at different institutions. A reoccurring topic are the high costs for the production and maintenance of educational materials. In particular, the production and maintenance of good laboratory assignments is very time intensive. It would be nice if there were ways to organize more effective collaboration in order to more easily share educational materials and to mesh course and lab components.

References

1. O. Bonaventure. Computer networking: Principles, protocols and practice, 2016. URL: http://cnp3book.info.ucl.ac.be/.
2. J.-Y. Le Boudec. Rate adaptation, congestion control and fairness: A tutorial, 2016. URL: http://ica1www.epfl.ch/PS_files/LEB3132.pdf.
3. Catherine H. Crouch and Eric Mazur. Peer instruction: Ten years of experience and results. *American Journal of Physics*, 69(9):970–977, 2001. doi:10.1119/1.1374249.
4. Dagstuhl Seminar 17112 – Using Networks to Teach About Networks: Materials. URL: http://materials.dagstuhl.de/index.php?semnr=17112.
5. L. Deslauriers, E. Schelew, and C. Wieman. Improved learning in a large-enrollment physics class. *Science*, 332(6031):862–864, 2011.
6. S. Freeman, S. L. Eddy, M. McDonough, M. K. Smith, N. Okoroafor, H. Jordt, and M. P. Wenderoth. Active learning increases student performance in science, engineering, and mathematics. *Proceedings of the National Academy of Sciences of the United States of America (PNAS)*, 111(23):8410–8415, 2014. doi:10.1073/pnas.1319030111.
7. G. Karlsson and S. Janson. The flipped classroom: a model for active student learning. In L. Engwall, E. D. Corte, and U. Teichler, editors, *From books to MOOCs? Emerging models of learning and teaching in higher education*, pages 127–136. Portland Press Limited, 2016.
8. J. F. Kurose and K. W. Ross. *Computer Networking: A Top-Down Approach*. Pearson, 6 edition, 2012.
9. NETRESEC Pcap Files. URL: http://www.netresec.com/?page=PcapFiles.
10. Simple Web Traces. URL: https://traces.simpleweb.org/.
11. Leslie Owen Wilson. Anderson and krathwohl – bloom's taxonomy revised, 2016. URL: http://thesecondprinciple.com/teaching-essentials/beyond-bloom-cognitive-taxonomy-revised/.
12. Wireshark Sample Captures. URL: https://wiki.wireshark.org/SampleCaptures.

Participants

- Olivier Bonaventure
UC Louvain – Louvain-la-Neuve, BE
- Alessio Botta
University of Naples, IT
- Stefan Burschka
RUAG – Bern, CH
- Georg Carle
TU München, DE
- Marinos Charalambides
University College London, GB
- Pieter-Tjerk de Boer
University of Twente – Enschede, NL
- Wouter de Vries
University of Twente – Enschede, NL
- Jordi Domingo-Pascual
UPC – Barcelona, ES
- John Domingue
The Open University – Milton Keynes, GB
- Timur Friedman
UPMC Sorbonne Université – Paris, FR
- Gunnar Karlsson
KTH Royal Institute of Technology – Stockholm, SE
- Jean-Yves Le Boudec
EPFL – Lausanne, CH
- Simone Opel
Berufskolleg der Stadt Bottrop, DE
- Marc-Oliver Pahl
TU München, DE
- Cristel Pelsser
University of Strasbourg, FR
- Aiko Pras
University of Twente – Enschede, NL
- Bruno Quoitin
University of Mons, BE
- Fabio Ricciato
University of Ljubljana, SI
- Jürgen Schönwälder
Jacobs University Bremen, DE
- Anna Sperotto
University of Twente – Enschede, NL
- James P. G. Sterbenz
University of Kansas – Lawrence, US
- Burkhard Stiller
Universität Zürich, CH
- Iyad Tumar
Birzeit University, PS
- Klaus Wehrle
RWTH Aachen University, DE
- Harald Weikert
IsarNet AG -– München, DE
- Lisa Yan
Stanford University, US



Report from Dagstuhl Seminar 17121

Computational Complexity of Discrete Problems

Edited by

Anna Gál[1], Michal Koucký[2], Oded Regev[3], and Till Tantau[4]

1 **University of Texas – Austin, US,** panni@cs.utexas.edu
2 **Charles University – Prague, CZ,** koucky@iuuk.mff.cuni.cz
3 **New York University, US**
4 **Universität zu Lübeck, DE,** tantau@tcs.uni-luebeck.de

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 17121 "Computational Complexity of Discrete Problems". The first section gives an overview of the topics covered and the organization of the meeting. Section 2 lists the talks given in alphabetical order. The last section contains the abstracts of the talks.

Seminar March 19–24, 2017 – http://www.dagstuhl.de/17121
1998 ACM Subject Classification Theory of Computing
Keywords and phrases Computational Complexity
Digital Object Identifier 10.4230/DagRep.7.3.45
Edited in cooperation with Bruno Loff

1 Executive Summary

Anna Gál (University of Texas – Austin, US)
Michal Koucký (Charles University – Prague, CZ)
Oded Regev (Courant Institute – New York, US)
Till Tantau (Universität Lübeck – DE)

Introduction and goals

Computational complexity studies the amount of resources (such as time, space, randomness, or communication) that are necessary to solve computational problems in various models of computation. Finding efficient algorithms for solving computational tasks is crucial for practical applications and becomes even more important with the use of computers becoming part of everyday life. Despite a long line of research, for many problems that arise in practice it is not known if they can be solved efficiently – in particular in polynomial time.

Beside questions about the existence of polynomial time algorithms for problems like Satisfiability or Factoring where the best known algorithms run in exponential time, there is a huge class of practical problems where algorithms with polynomial running time (e.g. cubic or even quadratic time) are known, but it would be important to establish whether these running times are best possible, or to what extent they can be improved.

These fundamental questions motivate developments in various areas from algorithm design to circuit complexity, communication complexity and coding theory. During this Dagstuhl Seminar, we discussed some of the most exciting recent developments in those areas related to computational complexity.

Computational Complexity of Discrete Problems, *Dagstuhl Reports*, Vol. 7, Issue 3, pp. 45–69
Editors: Anna Gál, Michal Koucký, Oded Regev, and Till Tantau

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

The seminar "Computational Complexity of Discrete Problems" has evolved out of the series of seminars entitled "Complexity of Boolean Functions," a topic that has been covered at Dagstuhl on a regular basis since the foundation of this research center. An important feature of the current research in computational complexity is the integration of ideas from different subareas of computational complexity and from other fields in computer science and mathematics. We have aimed to attract researchers from various subareas connected to core questions in boolean function complexity and foster further fruitful interactions.

2 Table of Contents

3 Organization of the seminar

40 researches from around the world participated in the seminar including a substantial number of young researchers. Each day we had two to three *regular* talks in the morning and in the afternoon. In addition to that we dispersed in the schedule a set of short talks that we called *talks to talk about*. The regular talks allowed participants to explain in depth various problems and results. The short talks were meant for posing open problems and for brief announcements. They were usually scheduled before the meal time so that participants could discuss the problems over the meal. This schedule proved quite successful as it allowed for plenty of time for discussions in impromptu groups in the afternoon as well as it gave essentially everyone interested the opportunity to speak.

3.1 Topics covered by the seminar

The talks of the workshop fit into several subareas of computational complexity. We summarize the talks next. Detailed abstracts of the talks can be found at the end of this report.

3.1.1 Circuit complexity

Proving lower bounds on the size of circuits and formulas computing specific functions is one of the main goals of computational complexity. However, proving such lower bounds seems exceedingly hard. Avishay Tal presented a new method of amplifying formula size lower bounds from non-approximability lower bounds. As an application he showed the currently best formula size lower bound.

The difficulties of proving lower bounds can be sometimes formally analyzed. In past several *barriers* for proving strong lower bounds have been identified. The most intriguing one is the Natural Proof framework of Razborov and Rudich for Boolean circuit lower bounds. Ben Lee Volk presented a Natural Proof framework for proving *algebraic* circuit lower bounds. He explained its connection to succinct hitting sets for algebraic circuits.

Many circuit lower bounds we currently have fit into the Natural Proof framework, e.g., lower bounds for $\mathrm{AC}^0[p]$ circuits. In a surprising twist, Valentine Kabanets used Natural Proof Properties from these proofs to construct new learning algorithms for $\mathrm{AC}^0[p]$.

One of the tools to reason about circuits is provided by the logical framework of descriptive complexity. Heribert Vollmer developed a model-theoretic characterization of the counting class $\#\mathrm{AC}^0$ based on counting winning strategies in certain games.

Sasha Golovnev asked about devising new circuit lower bound techniques other than gate-elimination as the gate-elimination technique implies better algorithms for circuit-SAT.

The Minimum Circuit Size Problem is a particular computational problem with inputs being truth-tables of functions and the goal being to determine the size of the smallest circuit computing the function. This problem is not know to be in P nor NP-hard, it is a candidate NP-intermediate problem. Rahul Santhanam discussed the unusual complexity properties of the Minimum Circuit Size Problem and its relevance to circuit lower bounds.

Eric Allender presented further new hardness results for the Kolmogorov-complexity variant of the Minimum Circuit Size Problem and its relationship to the circuit variant.

3.1.2 Proof complexity

Proof complexity aims at separating complexity classes by proving lower bounds on various proof systems. It also helps in understanding the running time of various satisfiability algorithms and heuristics. Meena Mahajan defined a new cutting plane based proof system for refuting Quantified Boolean Formulas (QBF) and exhibited exponential lower bounds for this proof system.

Johan Håstad used new random restrictions for Tseitin contradictions to obtain exponential lower bounds for bounded-depth Frege systems.

Jakob Nordström presented a technique to prove exponential lower bounds for polynomial calculus for the functional pigeonhole principle with consequences for running time of a certain class of SAT-solvers.

Related to the barriers for proving lower bounds one may naturally ask what kind of mathematics is necessary to prove lower bounds or *upper* bounds. Igor Carboni Oliveira exhibited existence of languages in P for which one cannot prove within Cook's theory PV that they have running time $O(n^k)$.

Pavel Hrubeš posed a communication complexity open problem with consequences for cutting plane lower bounds.

3.1.3 Pseudorandomness and derandomization

Pseudorandom generators are useful for replacing truly random strings by pseudorandomly chosen ones in running randomized algorithms. Pseudorandom generators should have small support, be easy to compute and algorithms should behave on them in approximately the same way as on random strings chosen truly at random.

Rohit Gurjar used geometric view to construct pseudorandom generators for weight assignments for graphs and matroids that isolate a perfect matching in bi-partite graphs and a common bases of two matroids. This puts the two problems in uniform quasi-NC.

Dieter van Melkebeek presented a new simple pseudorandom generator with seed length $O(\log^{3/2} n)$ to isolate a shortest path in a directed graph with consequences for non-deterministic and unambiguous log-space.

Randomness extraction is a process of purifying random strings from biased sources of random strings. Gil Cohen surveyed recent developments in multi-source extractors and presented the key ideas for a simplified construction of such extractors.

3.1.4 Codes and communication complexity

Error correcting codes have multitude of applications in computational complexity and beyond. Obtaining good codes of various properties with efficient encoding and decoding is of primal interest for theory and applications. Swastik Kopparty described list-decoding algorithm for lifted Reed-Solomon codes.

Motivated by codes for distributed storage, Shachar Lovett presented results on the Birkhoff polytope graph with applications to the alphabet size of codes for the distributed storage.

A special class of errors for which one can use particular codes are erasures. If the data are not protected by the code but we have several noisy copies of the data we may still attempt to reconstruct the data. Anindya De discussed the number of samples one needs to reconstruct a string x from its noisy version where the noise erases coordinates of x.

A super-efficient decoding algorithm does not need to read the whole encoded string of data to reliably recover a single bit of the original data. This is called local decoding, and related to it is the local correction. It is a major open question to construct good locally-decodable and locally-correctable codes with constant number of queries. Or Meir exhibit

new unexpected constructions of locally-correctable codes in the regime of non-constant number of queries.

In the realm of communication complexity where we want to optimize the number of bits transmitted between parties jointly computing some function, Harry Buhrman presented an intriguing concept of clean communication complexity and posed open problems related to that.

Motivated by proving computational lower bounds, Or Meir presented open questions for direct sum of relationships, and Bruno Loff discussed asymmetric direct-sum theorems.

3.1.5 Fine-grained complexity

Recently a new area emerged in computational complexity so called *fine-grained complexity*. It aims to understand the complexity of various problems at very fine-tuned level with direct consequences for practice. Mohan Paturi presented the Least-Weight Subsequence Problem and its relationship to the fine-grained complexity of various other problems.

Motivated by practical applications, Matthias Krause introduced a new stream cipher with provable time-memory trade-off's and better internal state complexity than known ciphers.

Pavel Dvořák summarized results and open problems on the fixed-parameter tractability of Steiner tree problem.

3.1.6 Other models

Several participants addressed fundamental properties of boolean functions. Shachar Lovett asked questions about sparsity of polynomial representation of boolean functions, and Sourav Chakraborty posed a question regarding lower bounding the Fourier min-entropy of a boolean function in terms of its degree.

Prahladh Harsha presented problems regarding the decay of the value in multi-player parallel repetition games, a direct generalization of the celebrated *Parallel Repetition Theorem*.

Lance Fortnow introduced a new notion of *compression complexity* which addresses a question dual to Kolmogorov complexity namely, how complex has to be a string compression algorithm.

Rüdiger Reischuk disproved a conjecture about a particular learning algorithm for alternating finite automata and presented an alternative algorithm with required properties for the same problem.

Nikhil Bansal presented an elegant algorithm to solve the Subset Sum Problem in polynomial *space*.

Shay Moran talked about the classical problem of 20-questions when we limit the complexity of the allowed questions.

Mike Saks presented open questions regarding the randomized complexity of the on-line labeling problem.

3.2 Conclusion

Understanding the computational complexity of various problems is the primary goal of theory of computing. Over the years we are witnessing a continuous stream of new ideas and techniques in various areas of complexity for example, in communication complexity, arithmetic circuit complexity and derandomization. This seminar gave us the opportunity

to discuss some of these exciting developments and there was a general consensus among the participant that the meeting was helpful in facilitating new ideas and collaborations for further research.

We like to thank the staff at Dagstuhl who – as usual – provided a marvelous surrounding to make this a successful meeting with ample space for undisturbed interactions between the participants.

4 Overview of Talks

4.1 New Insights on the (Non)-Hardness of Circuit Minimization and Related Problems

Eric Allender (Rutgers University, US)

Joint work of Eric Allender, Shuichi Hirahara
Main reference E. Allender, S. Hirahara, "New Insights on the (Non)-Hardness of Circuit Minimization and Related Problems", ECCC Technical Report TR17-073, 2017.
URL https://eccc.weizmann.ac.il/report/2017/073/

The Minimum Circuit Size Problem (MCSP) and a related problem (MKTP) that deals with time-bounded Kolmogorov complexity are prominent candidates for NP-intermediate status. We show that, under very modest cryptographic assumptions (such as the existence of one-way functions), the problem of approximating the minimum circuit size (or time-bounded Kolmogorov complexity) within a factor of $n^{1-o(1)}$ is indeed NP-intermediate. To the best of our knowledge, these problems are the first natural NP-intermediate problems under the existence of an arbitrary one-way function.

We also prove that MKTP is hard for the complexity class DET under non-uniform NC^0 reductions. This is surprising, since prior work on MCSP and MKTP had highlighted weaknesses of "local" reductions (such as NC^0 reductions). We exploit this local reduction to obtain several new consequences:

- MKTP is not in $AC^0[p]$.
- Circuit size lower bounds are equivalent to hardness of a relativized version $MKTP^A$ of MKTP under a class of uniform AC^0 reductions, for a large class of sets A.
- Hardness of $MCSP^A$ implies hardness of $MKTP^A$ for a wide class of sets A. This is the first result directly relating the complexity of $MCSP^A$ and $MKTP^A$, for any A.

4.2 Clean quantum and classical communication protocols

Harry Buhrman (CWI – Amsterdam, NL)

Joint work of Harry Buhrman, Matthias Christandl, Christopher Perry, Jeroen Zuiddam
Main reference H. Buhrman, M. Christandl, C. Perry, J. Zuiddam, "Clean quantum and classical communication protocols", arXiv:1605.07948v3 [quant-ph], 2016.
URL https://arxiv.org/abs/1605.07948

By how much must the communication complexity of a function increase if we demand that the parties not only correctly compute the function but also return all registers (other

than the one containing the answer) to their initial states at the end of the communication protocol? Protocols that achieve this are referred to as *clean* and the associated cost as the *clean communication complexity*. Here we present clean protocols for calculating the Inner Product of two n-bit strings, showing that (in the absence of pre-shared entanglement) at most $n + 3$ qubits or $n + O(\sqrt{n})$ bits of communication are required. The quantum protocol provides inspiration for obtaining the optimal method to implement distributed $CNOT$ gates in parallel whilst minimizing the amount of quantum communication. For more general functions, we show that nearly all Boolean functions require close to $2n$ bits of classical communication to compute and close to n qubits if the parties have access to pre-shared entanglement. Both of these values are maximal for their respective paradigms.

4.3 Unprovability of circuit upper bounds in Cook's theory PV

Igor Carboni Oliveira (Charles University – Prague, CZ)

Joint work of Igor Carboni Oliveira, Jan Krajíček
Main reference J. Krajicek, I. C. Oliveira, "Unprovability of circuit upper bounds in Cook's theory PV", arXiv:1605.00263v3 [math.LO], 2016.
URL https://arxiv.org/abs/1605.00263

We establish unconditionally that for every integer $k > 1$ there is a language L in P such that it is consistent with Cook's theory PV that L is not in SIZE(n^k). Our argument is non-constructive and does not provide an explicit description of this language.

4.4 Towards the FEI conjecture

Sourav Chakraborty (CWI – Amsterdam, NL)

FEI conjecture is a well-known conjecture. The conjecture states that the Fourier entropy is less than a constant multiple of the average sensitivity. A weakening of the conjecture states that the min-entropy is less than approximate degree of the function. A even more weakening is that if g is a 1/3- approximating polynomial of a Boolean function f, then at least on the the coefficients of g has to be bigger than $1/2^d$, where d is the degree of g.

4.5 Recent advances in randomness extractors and their applications

Gil Cohen (Princeton University, US)

A randomness extractor is a function that "extracts" or "purifies" the randomness of a defective source of randomness. Randomness extractors have applications in abundance and unexpected connections to error-correcting codes, expander graphs and pseudorandom generators. In this talk we survey recent developments in randomness extractors theory

and give a simplified, weaker, construction of multi-source extractors so as to present the underlying ideas.

4.6 New results in trace reconstruction

Anindya De (Northwestern University – Evanston, US)

Joint work of Anindya De, Ryan O'Donnell, Rocco Servedio
Main reference A. De, R. O'Donnell, R. Servedio, "Optimal mean-based algorithms for trace reconstruction", arXiv:1612.03148v1 [cs.CC], 2016.
URL https://arxiv.org/abs/1612.03148

There is an unknown n-bit string x. A "trace" is a random substring of x formed by deleting each bit with probability (say) 1/2. Suppose an algorithm has access to independent traces of x. How many does it need to reconstruct x? The previous best method needed about $\exp(n^{1/2})$ traces. We give a simple "mean-based" algorithm that uses about $\exp(n^{1/3})$ traces (and time). We also show that any algorithm working in the restricted "mean-based" framework requires $\exp(n^{1/3})$ traces. The main tool in our work is elementary complex analysis.

4.7 Compression Complexity

Lance Fortnow (Georgia Institute of Technology – Atlanta, US)

Joint work of Lance Fortnow, Stephen Fenner
Main reference A. Fenner, L. Fortnow, "Compression Complexity", arXiv:1702.04779v1 [cs.CC], 2017.
URL https://arxiv.org/abs/1702.04779

The Kolmogorov complexity of x, denoted $C(x)$, is the length of the shortest program that generates x. For such a simple definition, Kolmogorov complexity has a rich and deep theory, as well as applications to a wide variety of topics including learning theory, complexity lower bounds and SAT algorithms.

Kolmogorov complexity typically focuses on decompression, going from the compressed program to the original string. This paper develops a dual notion of compression, the mapping from a string to its compressed version. Typical lossless compression algorithms such as Lempel-Ziv or Huffman Encoding always produce a string that will decompress to the original. We define a general compression concept based on this observation.

For every m, we exhibit a single compression algorithm q of length about m which for n and strings x of length $n \geq m$, the output of q will have length within $n - m + O(1)$ bits of $C(x)$. We also show this bound is tight in a strong way, for every $n \geq m$ there is an x of length n with $C(x)$ about m such that no compression program of size slightly less than m can compress x at all. We also consider a polynomial time-bounded version of compression complexity and show that similar results for this version would rule out cryptographic one-way functions.

4.8 Non-gate-elimination circuit lower bounds

Alexander Golovnev (New York University, US)

Joint work of Alexander Golovnev, Edward A. Hirsch, Alexander Knop, Alexander S. Kulikov
Main reference A. Golovnev, E. A. Hirsch, A. Knop, A. S. Kulikov, "On the Limits of Gate Elimination", in Proc. of the 41st Int'l Symp. on Mathematical Foundations of Computer Science (MFCS 2016), LIPIcs, Vol. 58, pp. 46:1–46:13, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2016.
URL http://dx.doi.org/10.4230/LIPIcs.MFCS.2016.46

We study lower bounds in the following computational model: Boolean circuits where each gate has fan-in two, and there are no restrictions on the fan-out or depth of the circuit. The circuit size of a Boolean function f is defined as the minimal number of internal gates (i.e., non-input gates) in a circuit computing f. It is easy to show by counting that almost all Boolean functions have exponential circuit size, however no functions of high circuit complexity are known to lie in **NP**.

Essentially, the only known method of proving lower bounds in this model is gate elimination. The best known lower bound is slightly greater than $3n$. It is shown that the currently known gate elimination techniques cannot prove a lower bound of cn for a small explicit constant c. (c here depends on the exact definition of gate elimination, and for most applications can be thought of as small as 5 or 10.)

One of the few examples of lower bounds in this model which does not use gate elimination is the work of Chashkin [2]. He proves a lower bound of $2n - o(n)$ on the complexity of the parity-check matrix of Hamming codes. A classical example of a lower bound which does not use gate elimination is a lower bound of Blum and Seysen [1] who show that an optimal circuit computing AND and OR must have two separate trees computing outputs (which also gives a lower bound of $2n - 2$). Melanich [3] proved a similar property and a lower bound of $2n - o(n)$ for a function whose outputs compute products of specific subsets of inputs.

Question Is it possible to extend the ideas used in non-gate-elimination proofs to get stronger lower bounds?

References

1 Norbert Blum and Martin Seysen. Characterization of all optimal networks for a simultaneous computation of AND and NOR. *Acta informatica*, 21(2):171–181, 1984.
2 Aleksandr V. Chashkin. On the complexity of Boolean matrices, graphs and their corresponding Boolean functions. *Diskretnaya matematika*, 6(2):43–73, 1994.
3 Olga Melanich. Personal communication, 2012.

4.9 Derandomizing Isolation Lemma: A geometric approach

Rohit Gurjar (Tel Aviv University, IL)

Joint work of Rohit Gurjar, Stephen Fenner, Thomas Thierauf
Main reference S. Fenner, R. Gurjar, T. Thierauf, "Bipartite perfect matching is in quasi-NC", in Proc. of the 48th Annual ACM SIGACT Symp. on Theory of Computing (STOC 2016), pp. 754–763, ACM, 2016.
URL http://doi.acm.org/10.1145/2897518.2897564

We present a geometric approach towards derandomizing the Isolation lemma for a given family, i.e., deterministically constructing a weight assingnment which ensures a unique

minimum weight set in the family. The idea is to work with a polytope corresponding to the family of sets. In this talk, we present the approach in terms of general polytopes and describe a sufficient condition on the polytope for this approach to work. The approach gives a quasi-polynomially bounded weight assignment. Finally, we show that two specific families – perfect matchings in bipartite graphs and common base sets of two matroids – satisfy the required condition and thus, we get an isolating weight assignment for these cases. This also puts the two problems in quasi-NC.

4.10 Multiplayer parallel repetition for expander games

Prahladh Harsha (TIFR – Mumbai, IN)

Joint work of Irit Dinur, Prahladh Harsha, Rakesh Venkat, Henry Yuen
Main reference I. Dinur, P. Harsha, R. Venkat, H. Yuen, "Multiplayer parallel repetition for expander games", arXiv:1610.08349v2 [cs.CC], 2016.
URL https://arxiv.org/abs/1610.08349

We investigate the value of parallel repetition of one-round games with any number of players $k \geq 2$. It has been an open question whether an analogue of Raz's Parallel Repetition Theorem holds for games with more than two players, i.e., whether the value of the repeated game decays exponentially with the number of repetitions. Verbitsky has shown, via a reduction to the density Hales-Jewett theorem, that the value of the repeated game must approach zero, as the number of repetitions increases. However, the rate of decay obtained in this way is extremely slow, and it is an open question whether the true rate is exponential as is the case for all two-player games.

Exponential decay bounds are known for several special cases of multi-player games, e.g., free games and anchored games. In this work, we identify a certain expansion property of the base game and show all games with this property satisfy an exponential decay parallel repetition bound. Free games and anchored games satisfy this expansion property, and thus our parallel repetition theorem reproduces all earlier exponential-decay bounds for multiplayer games. More generally, our parallel repetition bound applies to all multiplayer games that are connected in a certain sense.

We also describe a very simple game, called the GHZ game, that does not satisfy this connectivity property, and for which we do not know an exponential decay bound. We suspect that progress on bounding the value of this the parallel repetition of the GHZ game will lead to further progress on the general question.

4.11 A Generalized Method for Resolution and Polynomial Calculus Lower Bounds

Jakob Nordström (KTH Royal Institute of Technology – Stockholm, SE)

Joint work of Massimo Lauria, Mladen Miksa and Jakob Nordström

We study the problem of certifying unsatisfiability of formulas in propositional logic. For proof systems such as resolution and polynomial calculus it is known that if the clause-

variable incidence graph of a CNF formula is an expander, then proving that this formula is unsatisfiable is hard. We further develop techniques in [Alekhnovich and Razborov '03] to show that if one can "cluster" clauses and variables in a way that "respects the structure" of the formula in a certain sense, then it is sufficient that the incidence graph of this clustered version is an expander. We also give a unified view of resolution and polynomial calculus lower bounds in terms of a 2-player game played on this graph, where the difference between resolution and polynomial calculus is just in which player has to move first.

As a corollary, we prove that the functional pigeonhole principle (FPHP) formulas are hard for polynomial calculus, answering an open question in [Razborov '02]. This result can in turn be used to construct k-colouring instances where the standard encoding requires linear degree, and hence exponential size, for polynomial calculus. This implies a linear degree lower bound for any algorithms based on Gröbner bases, as well as for the algorithm studied in a sequence of papers [De Loera et al. '08, '09, '11, '15] based on Hilbert's Nullstellensatz proofs for a slightly different encoding, thus resolving an open problem mentioned, e.g., in [De Loera et al. '09] and [Li et al. '16].

4.12 On small-depth Frege proofs for Tseitin for grids

Johan Håstad (KTH Royal Institute of Technology – Stockholm, SE)

We prove that a depth-d Frege refutation of the Tseitin contradiction on the grid requires size $\exp(\Omega(n^{1/60(d+1)}))$. We conclude that polynomial size Frege refutations of the Tseitin contradiction must use formulas of depth $\Omega(\frac{\log n}{\log\log n})$.

4.13 The Uncanny Usefulness of Constructive Proofs of Pseudorandomness

Valentine Kabanets (Simon Fraser University – Burnaby, CA)

Joint work of Marco L. Carmosino, Russell Impagliazzo, Valentine Kabanets, Antonina Kolokolova
Main reference M. L. Carmosino, R. Impagliazzo, V. Kabanets, A. Kolokolova, "Learning Algorithms from Natural Proofs", in Proc. of the 31st Conference on Computational Complexity (CCC 2016), LIPIcs, Vol. 50, pp. 10:1–10:24, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2016.
URL http://dx.doi.org/10.4230/LIPIcs.CCC.2016.10

Explicit constructions of pseudorandom objects (e.g., pseudorandom generators, expander graphs, or boolean functions of large circuit complexity) often come with very constructive proofs of existence. For example,

(1) the Nisan-Wigderson (NW) generator based on an assumed "hard" function f (of large circuit complexity) has the constructive analysis: There is an efficient uniform reduction (with oracle access to f) taking an algorithm "breaking" the generator into a small circuit for f;

(2) the Natural Proofs framework of Razborov and Rudich argues that most circuit lower bound proofs come with an efficiently testable property that distinguishes "easy" functions (with small circuit complexity) from random functions;

I'll talk about some recent applications of such constructive proofs. In particular, I'll show that properties (1) + (2) yield an efficient (agnostic) learning query algorithm for every sufficiently strong circuit class that has a natural proof of circuit lower bounds. As an application, the class $AC^0[p]$, for any prime p, is (agnostically) learnable in quasi-polynomial time. (Previously, only the case of AC^0 was known by the results of Linial, Mansour, and Nisan.) [joint with Carmosino, Impagliazzo, and Kolokolova.]

4.14 List-decoding lifted codes

Swastik Kopparty (Rutgers University – Piscataway, US)

Joint work of Alan Guo and Swastik Kopparty
Main reference A. Guo, S. Kopparty, "List-Decoding Algorithms for Lifted Codes", IEEE Trans. Information Theory 62(5):2719–2725, 2016.
URL http://dx.doi.org/10.1109/TIT.2016.2538766

Lifted Reed-Solomon codes are a natural generalization of multivariate polynomial codes. In this talk, I will describe list-decoding algorithms for these codes. They are based on a technical theorem that says that m-variate functions over F_q which are codewords of the lifted Reed-Solomon code, despite being high-degree as m-variate functions, are low degree when viewed as univariate functions over the big field F_{q^m}

4.15 On Stream Ciphers with provable Beyond-the-Birthday-Bound Resistance against Time-memory-Data Tradeoff Attacks

Matthias Krause (Universität Mannheim, DE)

Joint work of Matthias Hamann, Matthias Krause, Willi Meier
Main reference M. Hamann, M. Krause, W. Meier, "LIZARD – A Lightweight Stream Cipher for Power-constrained Devices", IACR Transactions on Symmetric Cryptology, 2017(1):45–79, 2017.
URL http://dx.doi.org/10.13154/tosc.v2017.i1.45-79

A common way to prove the security of a cryptographic construction is to give a formal security proof in a so-called ideal component model. Here it is supposed that a generic adversary, Eve, has chosen-plaintext access to the construction and black-box access to the components of the construction, which are supposed to be ideal.The security of the construction is measured by the minimal number of component- and construction queries which have to be performed by Eve for distinguishing the construction from a random construction, or for recovering the secret key.

In this talk, we consider an ideal component model for stream ciphers, a well-established kind of lightweight symmetric encryption algorithm which produce pseudorandom bitstreams in dependence of of a secret symmetric session key and so-called (public) initial values, and which are widely used in mobile phones, WLAN etc. for an online encryption of secret messages.

Most stream cipher constructions suffer from a vulnerability against generic Time-Memory-Data Tradeoff attacks, which reduce the effective key length to $n/2$, where n denotes the

inner state length of the cipher. This is the reason why modern stream ciphers like TRIVIUM or GRAIN have a comparatively large inner state length of at least 160.

We introcuce and analyze here a new stream cipher construction, the LIZARD-construction, and give a formal proof that the security of this construction against generic Time-Memory-Data Tradeoff attacks is $(2/3)n$.

Based in this we proposed in (Hamann, Krause and Meier 2017) the ultralightweight stream cipher LIZARD, which has an inner state length of only 121.

4.16 Asymmetric direct-sum theorems

Bruno Loff (Charles University – Prague, CZ)

Joint work of Arkadev Chattopadhyay, Michal Koucký, Sagnik Mukhopadhyay

We mention some results about the following communication problem: Alice is given k instances $x_1, \ldots, x_k$ and Bob is given a single instance y, and Bob must learn the vector $(f(x_1, y), \ldots, f(x_k, y))$. This is a so-called *asymmetric direct-sum problem*, and naturally appears in the setting of data-structure lower-bounds.

We show that if the distributional communication-complexity of f under product distributions is at least C, then any randomized protocol to solve the above problem needs to have Alice send $\tilde{\Omega}(kC)$ bits and Bob send $\tilde{\Omega}(C)$ bits of communication.

We also show that this result is tight when f is disjointness, by exhibiting a protocol for $k = n$ where Alice communicates $n\sqrt{n}$ and Bob communicates $\sqrt{n}$ bits.

4.17 The Birkhoff polytope and coding for distributed storage

Shachar Lovett (University of California – San Diego, US)

Joint work of Daniel Kane, Shachar Lovett, Sankeerth Rao
Main reference D. Kane, S. Lovett, S. Rao, "The independence number of the Birkhoff polytope graph, and applications to maximally recoverable codes", arXiv:1702.05773v2 [math.CO], 2017.
URL https://arxiv.org/abs/1702.05773

I will describe a journey that starts at error correcting codes for distributed storage, and leads to graph labeling, the study of the Birkhoff polytope graph, the representation theory of the symmetric group and a structure-vs-randomness extension to the Hoffman bound.

On the technical side, we prove tight bounds for the chromatic number of the Birkhoff polytope graph, and use it to characterize the alphabet size needed for maximally recoverable codes in grid topologies.

4.18 Learning Residual Alternating Automata

Rüdiger Reischuk (Universität zu Lübeck, DE)

Joint work of Maciej Liśkiewicz, Matthias Lutter, Sebastian Berndt

Residuality plays an essential role for learning finite automata. While residual deterministic and nondeterministic automata have been understood quite well, fundamental questions concerning alternating automata (AFA) remain open.

Recently, Angluin, Eisenstat, and Fisman have initiated a systematic study of residual AFAs and proposed an algorithm called AL* an extension of the popular L* algorithm to learn AFAs. Based on computer experiments they conjectured that AL* produces residual AFAs, but have not been able to give a proof.

We disprove this conjecture by constructing a counterexample. As our main positive result we design an efficient learning algorithm, named AL**, and give a proof that it outputs residual AFAs only. In addition, we investigate the succinctness of these different FA types in more detail.

4.19 Understanding Cutting Planes for QBFs

Meena Mahajan (Institute of Mathematical Sciences – Chennai, IN)

Joint work of Olaf Beyersdorff, Leroy Chew, Meena Mahajan, Anil Shukla
Main reference O. Beyersdorff, L. Chew, M. Mahajan, A. Shukla, "Understanding Cutting Planes for QBFs", in Proc. of the 36th IARCS Ann. Conf. on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2016), LIPIcs, Vol. 65, pp. 40:1–40:15, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2017.
URL http://dx.doi.org/10.4230/LIPIcs.FSTTCS.2016.40

We define a new system for refuting false QBFs, by augmenting the propositional cutting planes system with a universal variable reduction rule. We show that lower bounds for the new system can be obtained via two independent techniques. One is the feasible interpolation method, extended to handle the reduction rule. Along with the known lower bounds for real monotone circuits for the Clique function, it yields an exponential lower bound for very simple false QBFs based on Clique. The other is the strategy extraction method: from a cutting planes proof of size s, we extract a decision list of threshold functions, of length s, computing a winning strategy for the universal player. Along with known lower bounds for such decision lists, it yields an exponential lower bound for a very simple false QBF based on the Inner product mod 2 function. These lower bounds also hold for the semantic cutting planes based system.

4.20 Recent developments in high-rate locally-testable and locally-correctable codes

Or Meir (University of Haifa, IL)

Joint work of Swastik Kopparty, Or Meir, Noga Ron-Zewi, Shubhangi Saraf
Main reference S. Kopparty, O. Meir, N. Ron-Zewi, S. Saraf, "High-rate locally-correctable and locally-testable codes with sub-polynomial query complexity", in Proc. of the 48th Annual ACM Symposium on Theory of Computing (STOC 2016), pp. 202–215, ACM, 2016.
URL http://doi.acm.org/10.1145/2897518.2897523

Locally-testable codes (LTCs) and locally-correctable codes (LCCs) are error-correcting codes for which there are extremely efficient algorithms. Specifically, there are algorithms for verifying and decoding that only need to read very few bits of the corrupted codeword. The number of bits that are read is called the "query complexity".

Historically, most work on LTCs and LCCs focused on the parameter regime of constant query complexity. In the recent years, however, a few works considered the parameter regime in which the query complexity is much larger, but still sublinear. It turns out that in such a regime, it is possible to obtain very interesting and unexpected constructions.

In this talk, I will present this new line of research, and focus on a recent paper that obtained the state-of-the-art results.

4.21 Twenty (simple) questions

Shay Moran (University of California – San Diego, US)

Joint work of Yuval Dagan, Yuval Filmus, Ariel Gabizon, Shay Moran
Main reference Y. Dagan, Y. Filmus, A. Gabizon, S. Moran, "Twenty (simple) questions", in Proc. of the 49th Ann. ACM SIGACT Symp. on Theory of Computing (STOC 2017), pp. 9–21, ACM, 2017.
URL http://doi.acm.org/10.1145/3055399.3055422

A basic combinatorial interpretation of Shannon's entropy function is via the "20 questions" game. This cooperative game is played by two players, Alice and Bob: Alice picks a distribution π over the numbers $\{1, \ldots, n\}$, and announces it to Bob. She then chooses a number x according to π, and Bob attempts to identify x using as few Yes/No queries as possible, on average.

An optimal strategy for the "20 questions" game is given by a Huffman code for π: Bob's questions reveal the codeword for x bit by bit. This strategy finds x using fewer than $H(\pi)+1$ questions on average. However, the questions asked by Bob could be arbitrary. In this paper, we investigate the following question: *Are there restricted sets of questions that match the performance of Huffman codes, either exactly or approximately?*

Our first main result shows that for every distribution π, Bob has a strategy that uses only questions of the form "$x < c$?" and "$x = c$?", and uncovers x using at most $H(\pi) + 1$ questions on average, matching the performance of Huffman codes in this sense. We also give a natural set of $O(rn^{1/r})$ questions that achieve a performance of at most $H(\pi) + r$, and show that $\Omega(rn^{1/r})$ questions are required to achieve such a guarantee.

Our second main result gives a set $\mathcal{Q}$ of $1.25^{n+o(n)}$ questions such that for every distribution π, Bob can implement an *optimal* strategy for π using only questions from $\mathcal{Q}$. We also show

that $1.25^{n-o(n)}$ questions are needed, for infinitely many n. If we allow a small slack of r over the optimal strategy, then roughly $(rn)^{\Theta(1/r)}$ questions are necessary and sufficient.

4.22 Fast Space-efficient subset sum

Nikhil Bansal (TU Eindhoven, NL)

Joint work of Nikhil Bansal, Shashwat Garg, Jesper Nederlof, Nikhil Vyas
Main reference N. Bansal, S. Garg, J. Nederlof, N, Vyas, "Faster Space-Efficient Algorithms for Subset Sum and k-Sum", in Proc. of the 49th Ann. ACM SIGACT Symp. on Theory of Computing (STOC 2017), pp. 198–209, ACM, 2017.
URL http://doi.acm.org/10.1145/3055399.3055467

I will describe a randomized algorithm for the subset sum problem that runs in $2^{0.86n}$ time and uses polynomial space, provided the algorithm has read only random access to exponentially many random bits. Previously, all algorithms with running time less than 2^n used exponential space, and obtaining such a guarantee was open. Our algorithm is based on two main ingredients. First, Floyd's space efficient technique for cycle finding, which is also referred to as the Pollard Rho method, and second some additive combinatorics of subset sums. Time permitting, I will also talk about extensions to problems such as k-sum, knapsack, binary integer linear programming.

4.23 Random formulas in Cutting Planes

Pavel Hrubeš (The Czech Academy of Sciences – Prague, CZ)

Joint work of Pavel Pudlák, Pavel Hrubeš
Main reference P. Hrubeš, P. Pudlák, "Random formulas, monotone circuits, and interpolation", ECCC, 2017.
URL https://eccc.weizmann.ac.il/report/2017/042/download/

I discuss results and open problems related to random CNFs in the Cutting Planes proof system.

4.24 On the Fine-grained Complexity of One-Dimensional Dynamic Programming

Ramamohan Paturi (University of California – San Diego, US)

Joint work of Marvin Künnemann, Ramamohan Paturi, Stefan Schneider
Main reference M. Kunnemann, R. Paturi, S. Schneider, "On the Fine-grained Complexity of One-Dimensional Dynamic Programming", in Proc. of the 44th Int'l Colloquium on Automata, Languages, and Programming (ICALP 2017), LIPIcs, Vol. 80, pp. 21:1–21:15, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2017.
URL http://dx.doi.org/10.4230/LIPIcs.ICALP.2017.21

In this paper, we investigate the complexity of one-dimensional dynamic programming, or more specifically, of the Least-Weight Subsequence (LWS) problem: Given a sequence of

n data items together with weights for every pair of the items, the task is to determine a subsequence S minimizing the total weight of the pairs adjacent in S. A large number of natural problems can be formulated as LWS problems, yielding obvious $O(n^2)$-time solutions.

In many interesting instances, the $O(n^2)$-many weights can be succinctly represented. Yet except for near-linear time algorithms for some specific special cases, little is known about when an LWS instantiation admits a subquadratic-time algorithm and when it does not. In particular, no lower bounds for LWS instantiations have been known before. In an attempt to remedy this situation, we provide a general approach to study the fine-grained complexity of succinct instantiations of the LWS problem. In particular, given an LWS instantiation we identify a highly parallel core problem that is subquadratically equivalent. This provides either an explanation for the apparent hardness of the problem or an avenue to find improved algorithms as the case may be.

More specifically, we prove subquadratic equivalences between the following pairs (an LWS instantiation and the corresponding core problem) of problems: a low-rank version of LWS and minimum inner product, finding the longest chain of nested boxes and vector domination, and a coin change problem which is closely related to the knapsack problem and (min,+)-convolution. Using these equivalences and known SETH-hardness results for some of the core problems, we deduce tight conditional lower bounds for the corresponding LWS instantiations. We also establish the (min,+)-convolution-hardness of the knapsack problem. Furthermore, we revisit some of the LWS instantiations which are known to be solvable in near-linear time

4.25 The Minimum Circuit Size Problem and its Complexities

Rahul Santhanam (University of Oxford, GB)

Joint work of Shuichi Hirahara, Igor Carboni Oliveira, Rahul Santhanam

Recent work in complexity theory has emphasized the links between complexity lower bounds and algorithmic problems such as circuit satisfiability, derandomization and learning. An important computational problem in this connection is the Minimum Circuit Size Problem (MCSP), where the input is the truth table of a Boolean function and the question is whether the function has small circuits.

MCSP belongs to NP, but it and its variants have several unusual and interesting features, which distinguish it from other natural problems in NP. I will discuss these features, survey previous work on the problem, and explain the relevance of MCSP to circuit lower bounds, learning and natural proofs.

This talk is partly based on 2 recent works of the speaker, one with Igor Carboni Oliveira on "Conspiracies between Circuit Lower Bounds, Learning Algorithms and Pseudorandomness" and the other with Shuichi Hirahara "On the Average-Case Complexity of MCSP and its Variants".

4.26 Computing Requires Larger Formulas than Approximating

Avishay Tal (Institute for Advanced Study – Princeton, US)

Main reference A. Tal, "Computing Requires Larger Formulas than Approximating", ECCC, 2016.
URL https://eccc.weizmann.ac.il/report/2016/179/

A de Morgan formula over Boolean variables $x_1, \ldots, x_n$ is a binary tree whose internal nodes are marked with AND or OR gates and whose leaves are marked with variables or their negation. We define the size of the formula as the number of leaves in it. Proving that some explicit function (in P or NP) requires large formula is a central open question in computational complexity.

In this work, we introduce a size-amplification hardness reduction for de-Morgan formulas. We show that average-case hardness implies worst-case hardness for a larger size. More precisely, if a function f cannot be computed correctly on more than $1/2 + 2^{-k}$ of the inputs by any formula of size s, then computing f correctly on all inputs requires size ks. The tradeoff is essentially tight. Quite surprisingly, the proof relies on a result from quantum query complexity by Reichardt.

As an application, we improve the best known formula size lower bounds for explicit functions by logarithmic factors to $n^3/\log(n)$. In addition, we propose candidates for explicit functions that we believe have formula size n^4, and prove non-trivial super-quadratic formula size lower bounds for them using our reduction.

4.27 Derandomizing Isolation in Space-Bounded Settings

Dieter van Melkebeek (University of Wisconsin – Madison, US)

Joint work of Dieter van Melkebeek, Gautam Prakriya
Main reference D. van Melkebeek, G. Prakriya, "Derandomizing Isolation in Space-Bounded Settings", in Proc. of the 32nd Computational Complexity Conf. (CCC 2017), LIPIcs, Vol. 79, pp. 5:1–5:32, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2017.
URL http://dx.doi.org//10.4230/LIPIcs.CCC.2017.5

Isolation is the process of singling out a solution to a problem that may have many solutions. It plays an important role in the design of efficient parallel algorithms as it ensures that the various parallel processes all work towards a single global solution rather than towards individual solutions that may not be compatible with one another. For example, the best parallel algorithms for finding perfect matchings in graphs hinge on isolation for this reason. Isolation is also an ingredient in some efficient sequential algorithms. For example, the best running times for certain NP-hard problems like finding hamiltonian paths in graphs are achieved via isolation.

All of these algorithms are randomized, and the only reason is the use of the Isolation Lemma – that for any set system over a finite universe, a random assignment of small integer weights to the elements of the universe has a high probability of yielding a unique set of minimum weight in the system. For each of the underlying problems it is open whether deterministic algorithms of similar efficiency exist.

I will talk about the possibility of deterministic isolation in the space-bounded setting. The question is: Can one always make the accepting computation paths of nondeterministic space-bounded machines unique without changing the underlying language and without

blowing up the space by more than a constant factor? Or equivalently, does there exist a deterministic logarithmic space mapping reduction from directed st-connectivity to itself that transforms positive instances into ones where there is a unique path from s to t?

I will present some recent results towards a resolution of this question, obtained jointly with Gautam Prakriya. Our approach towards a positive resolution can be viewed as derandomizing the Isolation Lemma in the context of space-bounded computation.

4.28 Succinct Hitting Sets and Barriers to Proving Algebraic Circuits Lower Bounds

Ben Lee Volk (Tel Aviv University, IL)

Joint work of Micahel Forbes, Amir Shpilka, Ben Lee Volk
Main reference M. A. Forbes, A. Shpilka, B. L. Volk, "Succinct Hitting Sets and Barriers to Proving Algebraic Circuits Lower Bounds", in Proc. of the 49th Ann. ACM SIGACT Symp. on Theory of Computing (STOC 2017), pp. 653–664, ACM, 2017.
URL http://doi.acm.org/10.1145/3055399.3055496

This talk presents a framework of "algebraically natural lower bounds" for algebraic circuits, which is similar to the natural proofs notion of Razborov and Rudich for boolean circuit lower bounds, and captures nearly all lower bound techniques known. However, unlike the boolean setting, there has been little concrete evidence demonstrating that this is a barrier to obtaining super-polynomial lower bounds for general algebraic circuits.

We show that the existence of an algebraic natural proofs barrier is equivalent to the existence of succinct derandomization of the polynomial identity testing problem. That is, whether the coefficient vectors of polylog(N)-degree polylog(N)-size circuits is a hitting set for the class of poly(N)-degree poly(N)-size circuits. Further, we give an explicit universal construction showing that if such a succinct hitting set exists, then our universal construction suffices.

We assess the existing literature constructing hitting sets for restricted classes of algebraic circuits and modify some of these constructions to obtain succinct hitting sets, thus suggesting evidence supporting the existence of an algebraic natural proofs barrier.

Our framework is similar to the Geometric Complexity Theory (GCT) program of Mulmuley and Sohoni, except that here we emphasize constructiveness of the proofs while the GCT program emphasizes symmetry. Nevertheless, our succinct hitting sets have relevance to the GCT program as they imply lower bounds for the complexity of the defining equations of polynomials computed by small circuits.

4.29 Descriptive Complexity of Arithmetic Complexity Classes

Heribert Vollmer (Leibniz Universität Hannover, DE)

Joint work of Juha Kontinen, Anselm Haak, Juha Kontinen, Heribert Vollmer
Main reference A. Durand, A. Haak, J. Kontinen, H. Vollmer, "Descriptive Complexity of #AC0 Functions, in Proc. of the 25th EACSL Annual Conference on Computer Science Logic (CSL 2016), LIPIcs,

Vol. 62, pp. 20:1-20:16, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2017.
URL http://dx.doi.org/10.4230/LIPIcs.CSL.2016.20

We study the class $\#AC^0$ of functions computed by constant-depth polynomial-size arithmetic circuits of unbounded fan-in addition and multiplication gates. Inspired by Immerman's characterization of the Boolean class AC^0, we develop a model-theoretic characterization of $\#AC^0$, which can be interpreted as follows: Functions in $\#AC^0$ are exactly those functions counting winning strategies in first-order model checking games.

Extending this, we introduce a new framework for a descriptive complexity approach to arithmetic computations. We define a hierarchy of classes based on the idea of counting assignments to free function variables in first-order formulas. We completely determine the inclusion structure and show that #P and $\#AC^0$ appear as classes of this hierarchy. In this way, we unconditionally place #AC0 properly in a strict hierarchy of arithmetic classes within #P.

5 Open problems

5.1 The direct sum of the fork relation

Or Meir (University of Haifa, IL)

An old open problem in complexity theory is proving a direct-sum theorem for deterministic communication complexity. While partial results are known for total Boolean functions [1], nothing is known for relations. As a first step toward attacking this problem, I suggest proving a direct-sum theorem for the fork relation of Grigni and Sipser [MS].

References

1 Tomás Feder, Eyal Kushilevitz, Moni Naor and Noam Nisan. *Amortized Communication Complexity*. SIAM Journal of Computing 28(4), pages 736–750, 1995.
2 Michelangelo Grigni and Michael Sipser. *Monotone Separation of Logarithmic Space from Logarithmic Depth*. J. Comput. Syst. Sci. 50(3), pages 433–437, 1995.

5.2 Parameterized approximation scheme for Steiner tree

Pavel Dvořák (Charles University – Prague, CZ)

Joint work of Pavel Dvořák, Andreas Feldmann, Dušan Knop, Tomáš Masařík, Tomáš Toufar, Pavel Veselý

We study the Steiner tree problem. In this problem a graph $G = (V, E)$ is given where the set of vertices is split into two disjoint sets of terminals and Steiner vertices. The task is to find a minimum connected subgraph of G which contains all terminals. We consider a parameter p, which is the number of Steiner vertices in the optimal solution. This problem is W[2]-hard and APX-hard. Thus, we try to find an algorithm for the problem which runs in time $f(p, e)$ poly(n), where n is the size of G and f is some computable function, and returns e-approximation of the solution. We succeeded in directed and undirected cases. And we

know that there is no such algorithm for the weighted directed case (with some standard complexity assumptions). We still try to solve the case when the input graph G is weighted and undirected.

5.3 The randomized complexity of online labeling

Michael E. Saks (Rutgers University – Piscataway, US)

Joint work of Jan Bulánek, Michal Koucký

In the online labeling problem with parameters n and m we are presented with a sequence of n *items* from a totally ordered universe U and must assign each arriving item a label from the label set $\{1, 2, \ldots, m\}$ so that the order of labels (strictly) respects the ordering on U. As new items arrive it may be necessary to change the labels of some items; such changes may be done at any time at unit cost for each change. The goal is to minimize the total cost. An alternative formulation of this problem is the *file maintenance problem*, in which the items, instead of being labeled, are maintained in sorted order in an array of length m, and we pay unit cost for moving an item.

The parameter m, the size of the *label space* must be at least the number of items n for a labeling to be possible. There are two natural ranges of parameters which have received the most attention. In the case of *linearly many labels* we have $m = cn$ for some $c > 1$, and in the case of *polynomially many labels* we have $m = \theta(n^C)$ for some constant $C > 1$. The size r of the universe U is also a parameter which is not discussed explicitly in most of the literature on the problem. If $r \leq m$, the problem can be solved with cost n, since then we can simply fix an order preserving bijection from U to $\{1, \ldots, m\}$ in advance. In this paper we assume $U = \{1, \ldots, 2^n\}$.

The problem was introduced by Itai, Konheim and Rodeh [6] who also gave an algorithm for the case of linearly many labels having worst case total cost $O(n \log(n)^2)$. In the special case that $m = n$, algorithms with cost $O(\log(n)^3)$ per item are known [7, 2]. It is also well known that the algorithm of Itai et al. can be adapted to give total cost $O(n \log(n))$ in the case of polynomially many labels. All of these algorithms are deterministic.

Tight lower bounds are known for most ranges of m. In the case that $m = n^{O(1)}$, Dietz, Seiferas and Zhang [5] proved an $\Omega(n \log(n))$ lower bound. Bulánek, Koucký and Saks proved [4], proved an $\Omega(n \log(n)^2)$ lower bound in the case of linearly many labels, and $\Omega(n \log(n)^3)$ lower bound for the case $m = n$. The same authors with Babka and Čunát [1] proved a $\Omega(n \log(n)/(\log\log(m) - \log\log(n)))$ lower bound, that holds for all $n \leq m \leq 2^n$. When $m = O(1)$ this matches the above-mentioned bound proved by [5].

All of these lower bounds apply only to *deterministic* algorithms, leaving open the possibility of better randomized algorithms. As usual we measure the cost of a randomized algorithm as the worst case over all input sequences of a given length n of the expected number of moves made by the algorithm. This corresponds to running the algorithm against an *oblivious adversary* who selects the input sequence having full knowledge of the algorithm, but not of the random bits flipped in the execution of the algorithm.

Bulánek, Koucký and Saks[3] showed that the $\Omega(n \log n)$ bound (proved in [5]) for deterministic algorithms in the case of polynomially many labels $m = n^{O(1)}$, extends to randomized algorithms.

The randomized complexity in the case of a linear number of labels, $m = O(n)$ remains open.

References

1 Babka, M., Bulánek, J., Čunát, V., Koucký, M., Saks, M.: On Online Labeling with Polynomially Many Labels. In *ESA*, 121–132 (2012)

2 Bird, R., Sadnicki, S.: Minimal on-line labelling. *Inf. Process. Lett.*, 101(1), 41–45 (2007)

3 Bulánek, J., Koucký, M., Saks, M., On Randomized Online Labeling with Polynomially Many Labels. ICALP (1) 2013:291–302

4 Bulánek, J., Koucký, M., Saks, M., Tight lower bounds for online labeling problem, *SIAM J. Computing* 44(6), 1765–1797 (2015)

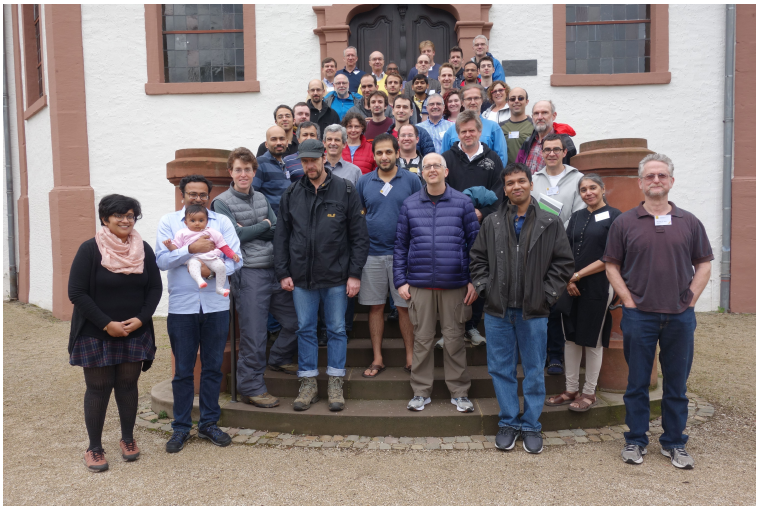
5 Dietz, P., Seiferas, J., Zhang, J.: A tight lower bound for online monotonic list labeling. *SIAM J. Discrete Math.*, 18(3), 626–637 (2004)

6 Itai, A., Konheim, A., Rodeh, M.: A sparse table implementation of priority queues. In *ICALP*, 417–431 (1981)

7 Zhang, J.: Density Control and On-Line Labeling Problems. *PhD thesis*, University of Rochester (1993).

Participants

- Eric Allender
Rutgers University, US
- Nikhil Bansal
TU Eindhoven, NL
- Harry Buhrman
CWI – Amsterdam, NL
- Igor Carboni Oliveira
Charles University – Prague, CZ
- Sourav Chakraborty
CWI – Amsterdam, NL
- Gil Cohen
Princeton University, US
- Anindya De
Northwestern University – Evanston, US
- Pavel Dvorak
Charles University – Prague, CZ
- Lance Fortnow
Georgia Institute of Technology – Atlanta, US
- Anna Gál
University of Texas – Austin, US
- Alexander Golovnev
New York University, US
- Rohit Gurjar
Tel Aviv University, IL
- Kristoffer Arnsfelt Hansen
Aarhus University, DK
- Prahladh Harsha
TIFR – Mumbai, IN
- Johan Hastad
KTH Royal Institute of Technology – Stockholm, SE
- Pavel Hrubes
The Czech Academy of Sciences – Prague, CZ
- Valentine Kabanets
Simon Fraser University – Burnaby, CA
- Swastik Kopparty
Rutgers University – Piscataway, US
- Michal Koucký
Charles University – Prague, CZ
- Matthias Krause
Universität Mannheim, DE
- Bruno Loff
Charles University – Prague, CZ
- Shachar Lovett
University of California – San Diego, US
- Meena Mahajan
Institute of Mathematical Sciences – Chennai, IN
- Or Meir
University of Haifa, IL
- Shay Moran
University of California – San Diego, US
- Jakob Nordström
KTH Royal Institute of Technology – Stockholm, SE
- Ramamohan Paturi
University of California – San Diego, US
- Pavel Pudlák
The Czech Academy of Sciences – Prague, CZ
- Oded Regev
New York University, US
- Rüdiger Reischuk
Universität zu Lübeck, DE
- Michael E. Saks
Rutgers University – Piscataway, US
- Rahul Santhanam
University of Oxford, GB
- Ronen Shaltiel
University of Haifa, IL
- Avishay Tal
Institute for Advanced Study – Princeton, US
- Till Tantau
Universität zu Lübeck, DE
- Thomas Thierauf
Hochschule Aalen, DE
- Jacobo Torán
Universität Ulm, DE
- Dieter van Melkebeek
University of Wisconsin – Madison, US
- Ben Lee Volk
Tel Aviv University, IL
- Heribert Vollmer
Leibniz Universität Hannover, DE



Report from Dagstuhl Seminar 17131

Mixed Criticality on Multicore / Manycore Platforms

Edited by

Liliana Cucu-Grosjean[1], Robert Davis[2], Sanjoy K. Baruah[3], and Zoë Stephenson[4]

1 **INRIA – Paris, FR,** liliana.cucu@inria.fr
2 **University of York, GB,** rob.davis@york.ac.uk
3 **University of North Carolina at Chapel Hill, US,** baruah@cs.unc.edu
4 **Rapita Systems Ltd. – York, GB,** zstephenson@rapitasystems.com

Abstract

This report provides an overview of the discussions, the program and the outcomes of the second Dagstuhl Seminar on Mixed Criticality on Multicore/Manycore Platforms. The seminar brought together researchers working on mixed criticality real-time applications, industrialists from the aerospace, railway, and automotive industries, and experts in certification.

Seminar March 26–31, 2017 – http://www.dagstuhl.de/17131
Keywords and phrases mixed-criticality multicore manycore real-time-systems
Digital Object Identifier 10.4230/DagRep.7.3.70
Edited in cooperation with Adriana Gogonel

1 Executive Summary

Liliana Cucu-Grosjean
Robert I. Davis
Sanjoy K. Baruah
Zoë Stephenson

Real-time applications are characterized by the need for both functional correctness and temporal correctness (appropriate timing behaviour). Real-time systems are present in many diverse areas such as avionics, automotive, space, robotics, and medical applications to cite only a few. Mixed Criticality Systems (MCS) have become an important topic for the real-time systems community. The first cluster of the European collaborative projects on MCS has been completed in September 2016, indicating a maturing of the related concepts within both industry and academia. Nevertheless many of the challenges brought about by the integration of mixed criticality applications onto multicore and manycore architectures remain to be solved. In reality mixed criticality problems have inherited the difficulty of real-time systems: being at the frontier of several domains including real-time scheduling, real-time operating systems / runtime environments, and timing analysis, as well as hardware architectures. This seminar promoted lively interaction, cross fertilization of ideas, synergies, and closer collaboration across different sub-communities of academics and industrialists from aerospace, automotive, and railway industries with specific interests in MCS, as well as with experts in certification.

Mixed Criticality on Multicore / Manycore Platforms, *Dagstuhl Reports*, Vol. 7, Issue 3, pp. 70–98
Editors: Liliana Cucu-Grosjean, Robert Davis, Sanjoy K. Baruah and Zoë Stephenson

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

In common with the first Dagstuhl Seminar on Mixed Criticality Systems, this seminar also focused on the two key conflicting requirements of MCS: separation between criticality levels for assurance and sharing for resource efficiency, along with the related requirement of time composability. An important aspect of this seminar was the presentation of different industry perspectives on the key problems. These perspectives formed the starting point of our seminar, with the first day mainly dedicated to industry statements on current practice and their perception of current work on MCS. The academic participants benefited from substantial and detailed arguments from the industry speakers. There were lively interactive discussions during the talks which led to much improved understanding of current industry practice, as well as helping to build a common vocabulary between academic and industry participants. The first day concluded with presentations by academic speakers presenting their thoughts on more practical mixed criticality models.

The next three days each included sessions devoted to an invited tutorial from a academic speaker. These covered the one-out-of-m multicore problem, Networks-on-Chip and mixed criticality, resource management, and statistical approaches to worst-case execution time estimation. The remaining sessions covered a range of fascinating open problems. In addition, a number of ad-hoc small working groups formed to collaborate on specific topics. We are pleased to report that a significant number of these initial collaborations have gained traction resulting in further work after the seminar, and in some cases the development and submission of papers.

Organization of the seminar report. Section 3 is an overview of the industry talks and Section 4 provides an overview of the academic talks. Section 5 presents working group discussions. Section 6 summarizes open problems discussed during the seminar. Finally outcomes from the seminar are listed in Section 7.

As organizers, we would like to thank Prof. Reinhard Wilhelm for joining us, Dagstuhl's Scientific Directorate for allowing us to run a second seminar on mixed criticality systems, and to the staff at Schloss Dagstuhl for their superb support during the seminar itself.

Finally, we would like to thank all of the participants for the very lively and open discussions. As organizers, we appreciated the feedback and enthusiasm which made running the seminar a great pleasure.

2 Table of Contents

3 Overview of industrial talks

3.1 Mixed Criticality Systems – view from the industry side

Cristian Maxim (Airbus S.A.S. – Toulouse, FR)

In avionics industry criticality is a designation of the level of assurance against failure needed for a system component and the notion of mixed-criticality is treated differently than in research domain. In my presentation I spotted the differences between the Vestal model and the approach in industry, explaining notions like safety integrity level and design assurance level (DAL). In industry the DAL is determined from the safety assessment process and hazard analysis and each software is included in one of the five distinct levels. The presentation focused on the way these levels are obtained and gave examples of softwares and the corresponding DALs. The main discrepancies between the levels of criticality in avionics and Vestal's model are:

1. In industry the criticality is given to a function while in research the criticality applies to a task.
2. For certification, the airplane manufacturers are supposed to give one WCET value while in research the concept of multiple WCET values for higher criticality tasks is observed.
3. The difficulty of implementation of Vestal's model makes it hard to benefit from the better CPU usage given by the existence of WCET for low criticality of certain tasks.
4. Task dropping is not conceivable in industry and the spatial isolation doesn't allow failure in a function to affect other functions.
5. The mode change in case of time violations would imply a new certification procedure and that is to costly to be practical. In the second part of the presentation, the IMA (integrated modular avionics) concept was presented as a midway between research and industry, focusing on the isolation procedures.

3.2 Real-Time Systems in Railway

Stefan Resch (Thales – Wien, AT)

In the railway domain systems with various timing requirements are to be found. By nature these systems are distributed over long distances. There are elements on track side such as axel counters, point control and signals, as well as interlocking systems in data centers and operation management centers controlling large parts of a country's railway network. On the trains there are on-board systems supervising and assisting the driver and communicating with the interlocking systems and operation control through balises (electronic beacons) or via GSM-R and radio block centers. The timing requirements of all these systems are highly dependent on their provided functions.

To avoid re-developing services for fault-tolerance, communication, real-time, etc., Thales provides a generic platform for its safety-critical railway applications – the TAS Control Platform[1]. It provides hardware boards, software runtimes, development tools and a system safety case according to CENELEC EN 50129. TAS Control Platform is certified to the highest safety integrity level SIL4 as generic safety product. This is achieved by implementing a safety middleware on top of a COTS operating system and hardware. This layer provides replication and supervises all capabilities that are used by the safety-critical applications and provided by the underlying COTS layer, also with respect to the real-time. With a stable API to the applications hardware obsolescence is mitigated in the middleware and the COTS OS.

In the railway domain high integrity is required for safety, but availability is not a direct safety property since railway systems are fail-safe. This can be illustrated with the example of setting a route for a train in a railway network. First all elements of the route, such as points, tracks and signals are reserved. Then all points are commanded to be set into the correct position for the route. The points then report their updated positions. As soon as all elements of the route are in a correct state, the entry signal is set to permissive. In case one of these steps cannot be completed, the setting of the route is aborted. This example illustrates that rather than relying on a concrete action to be completed within a certain amount of time the railway approach is to wait until the system has reached the correct state. An example with tighter timing requirements is that of sending an emergency stop signal via the radio block center to a train. Here, as well as in the previous example, the overall reaction time must be guaranteed by all involved systems.

As in other safety-critical domains, in railway the criticality of a function is derived from the potential damage and likelihood of it being faulty. The application designer then has to ensure that the system design satisfies the according requirements. With respect to scheduling this means that the tasks of the application will have sufficient resources on the computing platform available. In case of mixed criticality, where several applications are integrated on top of the same hardware platform, the required resources must be guaranteed for all the integrated applications. In exceptional overload situation the platform might provide only limited resources to tasks that are marked by the application designer as low priority, independent of their application's level of criticality. This allows graceful degradation of the system, but is a result of the application design and has no direct relation to the criticality level of an application.

Applications on top of TAS Control Platform are supervised through timeouts and the periodic synchronization between different computing boards in redundant architectures. Based on their communication and computation demand and the TAS Control Platform synchronization granularity they can define and supervise whether their reaction time meets the requirements. The actual reaction time is then determined through measurements and verified during the system integration tests.

In the future TAS Control Platform wants to provide the applications the possibility to execute a generic integration test with respect to application requirements and then be deployed in different environments.

[1] This project has received funding from the ECSEL Joint Undertaking under grant agreement No 692455. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation program and Austria, Denmark, Germany, Finland, Czech Republic, Italy, Spain, Portugal, Poland, Ireland, Belgium, France, Netherlands, United Kingdom, Slovakia, Norway.

3.3 An independent assessors perspective

Philippa Ryan (Adelard – London, GB)

Independent audits and assessments provide essential unbiased review of computer systems. In domains such as nuclear, defence, avionics and railway they are required by regulators. Few standards offer up to date guidance to deal with the complexity of mixed criticality and multi-core. Current focus is on safety, but security informed safety is increasingly important. With a limited amount of time and budget to perform an audit, how can the assessor be persuaded the system is acceptably safe and secure?

3.4 Mixed Criticalities in Avionic Systems

Sascha Uhrig (Airbus – München, DE)

Mixed criticality systems on multicores will become very important in the avionic domain in the future. This is because more and more functionality needs to be integrated on light-weight computers demanding for less space and energy. In addition to that the new functionalities need to be even more reliable and available than current high criticality systems, for example because of the demand on autonomous flying vehicles. Current approaches exploiting high multicore performance by switching between two modes according to the actual execution state, i.e. execution times, are good starting points. Nevertheless, these approaches can be difficult to implement (and certify) in avionic systems because of their nature to change the timing (schedule) and consequently the behaviour of the complete system dynamically. Such mode switches will most probably not occur in standard situations tested on ground but in unforeseen situations in which a different behaviour can have unpredictable results. Accordingly, such systems must be designed even more careful than current highly critical systems and future mixed criticality systems are still challenging.

3.5 Mixed Criticality and Real-Time in Automotive

Dirk Ziegenbein (Robert Bosch GmbH – Stuttgart, DE)

The talk gives a short overview of safety criticality, current approaches to real-time assurance as well as future challenges. In automotive systems, the criticality is given as ASIL (Automotive Safety Integrity Level) of a certain function. Since typically several SW and HW units work together to implement the function as well as to fulfil ASIL requirements, the paradigm to drop lower criticality tasks is not applicable in general. This is explained using an example. Timing assurance today is typically based on measured execution times and scheduling analysis or simulation. With the advent of multi-cores this well-known WCET abstraction does no longer hold due to cross-core influences. The trend towards large-scale software integration on heterogeneous HW platforms increases the need to find a new way to characterize the sequential SW units for system-level performance analysis.

4 Overview of academic talks

4.1 Deriving precise execution-time distributions of tasks

Sebastian Altmeyer (University of Amsterdam, NL)

Research on the timing behaviour of embedded real-time systems has been primarily focused on determining the worst-case execution time (WCET). This focus is clearly motivated by the need for timing verification, i.e, the need to guarantee at design time that all deadlines will be met. While a WCET estimate can be used to verify that a system is able to meet deadlines, it does not contain any further information about how the system behaves most of the time. An execution time distribution does contain this information and can provide useful insights regarding the timing behaviour of a system. Furthermore, a correct execution time distribution can be used to evaluate the precision and correctness of (worst-case) execution time analyses. We have recently developed a measurement-based framework that derives execution time distributions by exhaustive evaluation of program inputs. We overcome the scalability and state-space explosion problem by i) using static analysis to reduce the input space and ii) using an anytime algorithm which allows deriving a precise approximation on the execution time distribution. We would like to extend this research to overcome some restrictions on the hardware and execution environment. But foremost, we would like to use the framework to evaluate the precision of recently developed timing analysis approaches.

4.2 Realistic task model for multicore processors

Sebastian Altmeyer (University of Amsterdam, NL)

While processor architectures have changed fundamentally within the last decades, the task model that we still use today remained remarkably simple. Besides periods and deadlines, we mostly argue about execution time bounds. Each variation of this task model creates a plethora of new research questions, be it by defining different execution time bounds per criticality level, or per processor type. What rarely changes, however, is the assumption that the execution time bounds are complete and safe and encompass the entire processor system, irrespective of any interference on shared resources. Such a coarse abstraction mismatches the complexity of modern processors, especially for multi-core architectures with complex bus architectures and memory hierarchies: The processor itself is often not the only scarce resource anymore that needs to be scheduled. Arguing about the computation time is not very useful, when instead the memory bandwidth is the performance bottleneck.

The research problem that I would like to work on within this context are, amongst others:

- How realistic is the current assumption of a single execution time bound, valid for all scenarios, and how much performance do we lose?
- How can we define a more realistic task model that accurately represents not only the computation time, but also other shared resources?

4.3 Towards a (more) realistic task model for multicore processors

Sebastian Altmeyer (University of Amsterdam, NL)

While processor architectures have changed fundamentally within the last decades, the task model that we still use today remained remarkably simple. Besides periods and deadlines, we mostly argue about execution time bounds. Each variation of this task model creates a plethora of new research questions, be it by defining different execution time bounds per criticality level, or per processor type. What rarely changes, however, is the assumption that the execution time bounds are complete and safe and encompass the entire processor system, irrespective of any interference on shared resources. Such a coarse abstraction mismatches the complexity of modern processors, especially for multi-core architectures with complex bus architectures and memory hierarchies: The processor itself is often not the only scarce resource anymore that needs to be scheduled. Arguing about the computation time is not very useful, when instead the memory bandwidth is the performance bottleneck.

The research problems that I would like to work on within this context are, among-st others:

- How realistic is the current assumption of a single execution time bound, valid for all scenarios, and how much performance do we lose?
- How can we define a more realistic task model that accurately represents not only the computation time, but also other shared resources?

4.4 The One-Out-of-m Multicore Problem

James H. Anderson (University of North Carolina at Chapel Hill, US)

The multicore revolution is having limited impact in safety-critical application domains. A key reason is the "one-out-of-m" problem: when validating real-time constraints on an m-core platform, excessive analysis pessimism can effectively negate the processing capacity of the additional $m - 1$ cores so that only "one core's worth" of capacity is utilized even though m cores are available. Two approaches have been investigated previously to address this problem: mixed-criticality allocation techniques, which provision less-critical software components less pessimistically, and hardware-management techniques, which make the underlying platform itself more predictable. A better way forward may be to combine both approaches, but to show this, fundamentally new criticality-cognizant hardware-management trade offs must be investigated. To enable such an investigation, my research group has developed a mixed-criticality scheduling framework called MC^2 that supports configurable criticality-based hardware management. This framework allows specific DRAM memory banks and areas of the last-level cache (LLC) to be allocated to certain groups of tasks. A linear-programming-based optimization framework is available for sizing such LLC areas. In this talk, I will discuss the design of MC^2 and the analysis that underlies it and present the results of an experimental study conducted to evaluate its efficacy. This study shows that mixed-criticality allocation and hardware-management techniques can be much more effective when applied together instead of alone.

4.5 Schedulability Analysis as Evidence?

Björn B. Brandenburg (MPI-SWS – Kaiserslautern, DE)

As part of the certification of safety-critical systems, it is required to make a *safety case*. Such a safety case rests on a series of *arguments* that establish that all unacceptable risks are being mitigated. These arguments in turn must be supported by *evidence* that has been produced using an effective, and widely accepted, *methodology*.

In the context of real-time systems – and in particular in the context of mixed-criticality real-time systems, which distinguish themselves by consisting of complex mixes of workloads with diverse timing requirements and non-obvious correctness criteria, which makes their analysis exceedingly difficult – the generally accepted methodology of ruling out the risk of timing errors is *schedulability analysis*, i.e., static analysis that determines whether all timing constraints will be met at runtime in all possible execution scenarios.

The general consensus of real-time researchers is that schedulability analysis should be employed as part of safety certification of critical real-time systems (e.g., as found in avionics or the automotive industry), as the alternative – purely testing-based methods – cannot yield strong guarantees, and thus inherently constitute a considerable source of uncertainty (or residual risk). In contrast, published and peer-reviewed schedulability analyses are considered to yield *sound* results that leave no room for doubts.

Unfortunately, this trust in published and peer-reviewed schedulability analyses is, historically speaking, not justified: over the years, significant flaws and gaps in proofs have been found in a surprisingly large number of well-known results, including in the foundational Liu & Layland analysis of rate-monotonic scheduling, in the response-time analysis of tasks with arbitrary deadlines, in the response-time analysis of non-preemptive tasks (or network messages as in CAN), in the literature on self-suspensions, in the analysis of multiprocessor real-time scheduling with affinity constraints, and in the worst-case blocking analysis of several classic multiprocessor real-time locking protocols (to name just a few examples; there exist many more).

For the design and certification of mixed-criticality systems, which by definition include critical components, this represents a major open problem: *how can we make complex schedulability analysis truly trustworthy?*

Given the community's collective past record, just following the same procedure as before – primarily, manual "pen and paper" proofs and vetting to a varying degree of rigor by peer-reviewers – is arguably not going to work. Rather, a fundamentally more rigorous approach is needed.

Motivated by these observations, I argue that *schedulability analyses intended for use in safety-critical systems* should be *formally proven* with the help of a proof assistant such that all proofs are *machine-checked* to rule out human error. Following such an approach, the trust relies solely in the specification, and no longer in the much longer and much more intricate proofs (which no longer have to be trusted to be correct, as they can be automatically verified at the push of a button).

Given both that, historically, specification errors are much rarer than flaws in proofs, and that it is much easier to manually check a specification than it is to follow a proof in full detail, the adoption of machine-check-able proofs would represent a major advancement in the analysis and certification of real-time systems, and would enable unprecedented assurance in the temporal correctness of critical systems.

Towards this goal, I highlight one particular project – *PROSA*, a framework based on the Coq proof assistant – that is spearheading the drive towards a comprehensive foundation for formally verified schedulability analysis, and discuss and explain its major advantages as well as the remaining risks (such as specifications with contradicting hypotheses), and what is being done to mitigate them.

4.6 How to Gracefully Degrade

Alan Burns (University of York, GB)

Many approaches have been proposed for managing criticality-induced mode changes. A quick review is given, issues of integration are addressed as is the role that HI-crit tasks should take when there is a system overrun.

4.7 Resilient Mixed-Criticality Systems

Alan Burns (University of York, GB)

Certification authorities require correctness and resilience. In the temporal domain this requires a convincing argument that all deadlines will be met under error free conditions, and that when certain defined errors occur the behaviour of the system is still predictable and safe. This means that occasional execution-time overruns should be tolerated and where more severe errors occur levels of graceful degradation should be supported. With mixed-criticality systems, fault tolerance must be criticality aware, i.e. some tasks should degrade less than others. In this talk resilience is defined, and ways in which all levels of criticality can contribute to resilience are outlined. Discussions following this talk lead to a paper being produced that was offered for publication to the 2017 IEEE Real-Time Systems Symposium.

4.8 Reliability Optimization in MC2 Systems

Thidapat Chantem (Virginia Polytechnic Institute – Arlington, US)

Reliability is an important consideration for many safety- and mission-critical systems. Broadly, reliability is influenced in part by soft (transient) errors and in part by permanent device or component failures. In addition, system reliability cannot typically be improved by independently minimizing the occurrence of soft and hard errors. This is because preventing the occurrence of a soft error by increasing the voltage, for instance, may inadvertently reduces component lifetimes due to the potentially high temperature. Either a soft or

hard error could cause deadline misses, or worse. With the increasing prevalence in mixed-criticality systems due to the size, weight, and power constraints, providing predictable and reliable performance in hard real-time systems becomes more important than ever. Since task assignment and scheduling is the main influencer of voltage and frequency assignment, a system-level, reliability-aware task assignment and scheduling framework is needed. I am interested in designing an adaptive fault tolerance framework that is able to (probabilistically) guarantee the schedulability of high-criticality tasks in face of soft errors and component failures.

4.9 Worst Case Execution Time measurement-based approach

Liliana Cucu-Grosjean (INRIA – Paris, FR), Adriana Gogonel (INRIA – Paris, FR), and Cristian Maxim (Airbus S.A.S. – Toulouse, FR)

The time behaviour of Cyber-Physical Systems relies on the execution time of programs representing the cyber parts of such systems. Our time estimation method is based on a measurement-based one providing results in absence of sufficiently large intervals of simulation while using the Extreme Value Theory (EVT). According to EVT if the maximum of execution times of a program converges, then this maximum of the execution times $C_i, \forall i \geq$ will converge to one of the three possible curves Frechet, Weibull, and Gumbel corresponding to a shape parameter $\xi < 0, \xi > 0$ and $\xi = 0$, respectively.

- Block size estimation. We compare all GEV curves obtained by varying the block size from 4 to $\frac{n}{4}$ where n is the cardinal of the set of execution times. We keep the block size corresponding to the shape parameter closest to 0, which corresponds to a Gumbel. We calculate the generalized EV curve corresponding to this parameter.
- Threshold level estimation. We compare all GPD curves obtained by varying the threshold levels u from 0% to 100%. We keep the threshold level u_0 such that the curve defined by $E(X - u_0) \approx u - u_0$ experiences linearity. The linearity of E indicates that the GPD curve goes close to a Gumbel. We calculate the generalized EV curve corresponding to u_0.
- Comparing GEV and GPD pWCET estimates. The comparison of the GEV and GPD curves is done using the distance between the two distributions defined as $CRPS(GEV, GPD) = \sum_{z=x_{min}}^{z=x_{max}} [f_{GEV}(z) - f_{GPD}(z)]^2$. We consider in our experiments GEV and GPD as sufficiently close when $CRPS(GEV, GPD) \leq e$ with $e \approx 10^{-12}$. Other possible values of e, based for instance on the criticality level the pWCET estimation, may be decided. In order to decrease the error introduced by such estimation, we recommend calculating the pWCET estimate as a combination of GEV and GPD results. A joint pWCET estimate is obtained by choosing for each probability the largest value between GEV and GPD.

4.10 Practical Mixed-Criticality Model: Challenges

Arvind Easwaran (Nanyang TU – Singapore, SG)

Joint work of Arvind Easwaran, Vijayakumar Sundar, Bibin Nair
Main reference A. Easwaran, V. Sundar, B. Nair, "Mixed Criticality Scheduling Research in Automotive: Making Research More Practical", Workshop on Collaboration of Academia and Industry for Real World Embedded Systems (CAIRES) 2016.
URL https://caires2016.inria.fr/

The current trend in the automotive industry is focused towards Electronic Control Unit (ECU) consolidation. Increasing the number of ECUs to satisfy increased demand in the safety and comfort features of the vehicle is not a sustainable solution. Mixed criticality scheduling can be one of the key factors to drive ECU consolidation. Academic research has been focusing on different scheduling techniques and mode change protocols for mixed criticality systems. The research is further motivated with the introduction of ISO26262 which is a functional safety standard for safety critical applications in automotive. Functional safety of the automotive applications is represented in terms of Automotive Safety Integrity Levels (ASIL). Although the terms 'ASIL' of ISO26262 and 'criticality' of the existing research work looks similar, there is no clarity in the exact relationship between them. This can be attributed to the factors involved in determining the ASILs. There is also a need to validate the assumptions made in the existing research work with the safety critical behaviour of the applications. Certain assumptions may not even reflect the actual behaviour of automotive applications. This talk focuses on such issues for building mixed criticality systems. Solutions can be arrived at by considering various factors that might be missing in the current mixed criticality models considered by the research community.

4.11 Runtime Verification, Runtime Enforcement, and Mixed Criticality System Design

Sébastien Faucou (University of Nantes, FR)

Mixed criticality is a way to think about uncertainty of parameters during the design of a critical system. A mixed criticality system must be capable of graceful degradation in order to preserve its critical functions when something goes wrong, i.e. when a design assumption is violated at runtime. To do so, it must (i) detect the violation; and (ii) react to this violation to ensure the preservation of its critical activities.

Similar problems have been studied in the formal methods community. Problem (i) is akin to runtime verification. Problem (ii) is akin to runtime enforcement. The objective of the talk is to establish a parallel between these problems and mixed criticality system design, and draw attentions to some works developed in the formal method community that could provide rigorous techniques to build proved components for mixed criticality systems.

Runtime verification has already been used in the context of mixed criticality system design, with promising results. Still, further investigations are required to identify its benefits and limits. For runtime enforcement, it is still not clear if it is powerful and/or scalable enough to provide satisfying answer to our problem.

4.12 Energy efficiency in factories: Benefit of renewable energy, IoT and Automatic Demand Response

Laurent George (ESIEE – Champs sur Marne, FR)

Demand Response is a new approach to smooth pics of energy consumption at the scale of a country. Demand response can be used by a legacy energy provider to prevent from buying energy at the highest price on spot markets. When receiving a demand response request, a factory is requested to decide whether it could stop (or reduce) its energy consumption and for how long. Re-scheduling the activity of equipments in a production line by using standby or shutdown modes can help reducing energy consumption in factories. This requires taking scheduling decisions concerning the production line on relatively short reaction times (few minutes) upon demand response request. The benefit of Demand Response for a factory is that it gets paid for not consuming by legacy energy provider.

4.13 Real-Time Mixed-Criticality Wormhole Networks

Leandro Soares Indrusiak (University of York, GB)

Joint work of Leandro Soares Indrusiak, Alan Burns, James Harbin
Main reference L. S. Indrusiak, J. Harbin, A. Burns, "Average and Worst-Case Latency Improvements in Mixed-Criticality Wormhole Networks-on-Chip", in Proc. of the 27th Euromicro Conference on Real-Time Systems (ECRTS 2015), pp. 47–56, IEEE, 2015.
URL https://doi.org/10.1109/ECRTS.2015.12
Main reference A. Burns, J. Harbin, L. S. Indrusiak, "A Wormhole NoC Protocol for Mixed Criticality Systems", IEEE Real-Time Systems Symposium (RTSS 2014), pp. 184–195, IEEE, 2014.
URL https://doi.org/10.1109/RTSS.2014.13

Wormhole switching is a widely used network protocol due to small buffering requirements on each network router, which in turn results in low area and energy overheads. This is of key importance in multi-core and many-core processors based on Networks-on-Chip, as the area and energy share of the on-chip interconnect itself can reach up to 30% of the area and energy used by the whole processor. However, the nature of wormhole switching allows a single packet to simultaneously acquire multiple links as it traverses the network, which can make worst-case packet latencies hard to predict. This becomes particularly severe in large and highly congested networks, where complex interference patterns become the norm.

This talk focuses on the use of priority-preemptive wormhole networks, and the latest research on analytical methods aimed at predicting worst-case packet latency over such networks. Then, I'll show how to extend the network and the respective analysis to provide different levels of guarantees to network packets of different criticality sharing the same network. By doing that, highly-critical packets will always be given sufficient service, even in situations of overload or degraded network capacity.

4.14 Fixed-Priority Scheduling without Any Adaptation in Mixed-Criticality Systems

Jian-Jia Chen

Main reference G. von der Bruggen, K.-H. Chen, W.-H. Huang, J.-J. Chen, "Systems with Dynamic Real-Time Guarantees in Uncertain and Faulty Execution Environments", IEEE Real-Time Systems Symposium (RTSS 2016), pp. 303–314, IEEE, 2016.
URL http://dx.doi.org/10.1109/RTSS.2016.037

In many practical real-time systems, the physical environment and the system platform can impose uncertain execution behaviour to the system. For example, if transient faults are detected, the execution time of a task instance can be increased due to recovery operations. Such fault recovery routines make the system very vulnerable with respect to meeting hard real-time deadlines. In theory and in practical systems, this problem is often handled by aborting not so important tasks to guarantee the response time of the more important tasks. However, for most systems such faults occur rarely and the results of not so important tasks might still be useful, even if they are a bit late. This implicates to not abort these not so important tasks but keep them running even if faults occur, provided that the more important tasks still meet their hard real time properties. In this paper, we present Systems with Dynamic Real-Time Guarantees to model this behaviour and determine in [1] if the system can provide full timing guarantees or limited timing guarantees without any online adaptation after a fault occurred. We present a schedulability test, provide an algorithm for optimal priority assignment, determine the maximum interval length until the system will again provide full timing guarantees and explain how we can monitor the system state online. The approaches presented in [1] can be applied to mixed criticality systems with dual criticality levels.

References

1 Georg von der Bruggen, Kuan-Hsun Chen, Wen-Hung Huang, Jian-Jia Chen: Systems with Dynamic Real-Time Guarantees in Uncertain and Faulty Execution Environments. RTSS 2016: 303-314

4.15 Improve the scalability of mixed-criticality parallel real-time systems

Jing Li (Washington University – St. Louis, US)

Recent years have witnessed the convergence of two important trends in real-time systems: growing computational demand of applications and the adoption of processors with more cores. As real-time applications now need to exploit internal parallelism to meet their real-time requirements, they face a new challenge of scaling up computations on a large number of cores.

Randomized work stealing has been adopted as a highly scalable scheduling approach for general-purpose computing for parallel programs. In randomized work stealing, each core steals work from a randomly chosen core in a randomized and decentralized manner. Randomized work stealing has been proved to have a high-probability bound on the execution

time of a parallel job on multiple cores. In other words, it can complete the execution of a parallel job by the job's deadline with a high probability, when given sufficient number of cores. However, in the worst case (with very low probability), it could still run a parallel job sequentially. Therefore, if a parallel task is executed by randomized work stealing, the variation in the parallel execution times of the task depends not only upon the fluctuation in its computational demand, but also upon the randomness of its internal scheduling by work stealing.

The mixed-criticality real-time model typically captures the uncertainty of task executions to improve the average resource efficiency while providing hard guarantees in the worst case. Therefore, to improve the scalability of parallel real-time tasks, we could consider exploiting the work stealing strategy and model its variation in task execution times under the mixed-criticality framework. To do so, we need to consider the following problems.

- First, consider the simple scenario where a parallel task always releases jobs with the same parallel structure and computation. How can we modify the work stealing strategy to provide different (parallel) execution time estimates, so that it fits the Vestal model for mixed-criticality systems? In particular, the modified work stealing strategy must provide a worst-case progress guarantee that is better than executing a parallel task sequentially.
- Based on the modified work stealing strategy, can we design a mixed-criticality scheduling algorithm for parallel tasks executed by work stealing? Can we design a global mixed-criticality scheduling algorithm, so that low-criticality tasks can use the under-utilized cores by the high-criticality tasks while providing progress guarantee to high-criticality tasks?
- Finally, we need to consider the more general case where a parallel task releases jobs with different parallel structures and different computational demands and these parallel jobs are executed by work stealing. How can we simultaneously model the fluctuation in task's computational demand and the randomness of its internal scheduling by work stealing to improve the resource efficiency of the system?

4.16 Resource management in DREAMS

Claire Pagetti (ONERA – Toulouse, FR)

Joint work of Guy Durrieu, Gerhard Fohler, Gautam Gala, Sylvain Girbal, Daniel Gracia Pérez, Eric Noulard, Claire Pagetti
Main reference G. Durrieu, G. Fohler, G. Gala, S. Girbal, D. Gracia Pérez, E. Noulard, C. Pagetti, S. Pérez, , "DREAMS about reconfiguration and adaptation in avionics", in Proc. of the 8th Conf. on Embedded Real Time Software and Systems (ERTS'16).
URL https://hal.archives-ouvertes.fr/hal-01258701
URL https://www.youtube.com/watch?v=Wr6gxlS8c0w&feature=youtu.be

The DREAMS (Distributed REal-Time Architecture for Mixed Criticality Systems) FP7 project addresses the design of a cross-domain architecture for executing applications of different criticality levels in networked multi-core embedded systems. A DREAMS architecture is composed of several multi-code chips (such as the ST Micro Spidergon NOC or the Freescale T4240) connected through a TTEthernet network.

This presentation focuses on the adaptation strategies and their implementation in the avionic demonstrator. Adaptations only take place upon failures on a core, with the purpose to bring the system back to a functioning state. We consider two types of failures:

1. A permanent core failure. Intensive integration of small devices on chip increases the permanent failures occurrence due to various phenomena such as aging, wear-out or infant mortality.
2. A temporal overload situation, resulting in deadline miss without corrective action.

We will describe the resource management proposed in the DREAMS middle-ware. We will then detail the adaptation strategies defined for mitigating the above-defined failures. Finally we will give the main ideas of the implementation for the avionic demonstrator.

4.17 Probabilistic Analysis for Mixed Criticality Scheduling with SMC and AMC

Dorin Maxim (LORIA & INRIA – Nancy, FR), Liliana Cucu-Grosjean (INRIA – Paris, FR), Robert Davis (University of York, GB), and Arvind Easwaran (Nanyang TU – Singapore, SG)

Main reference D. Maxim, R. Davis, L. Cucu-Grosjean, A. Easwaran, "Probabilistic Analysis for Mixed Criticality Scheduling with SMC and AMC", in Proc. of the Workshop on Mixed Criticality Systems (WMC 2016), collocated with RTSS 2016.
URL https://www-users.cs.york.ac.uk/ robdavis/papers/WMC2016pAMC.pdf

This work introduces probabilistic analysis for fixed priority preemptive scheduling of mixed criticality systems on a uniprocessor using the Adaptive Mixed Criticality (AMC) and Static Mixed Criticality (SMC) schemes. We compare this analysis to the equivalent deterministic methods, highlighting the performance gains that can be obtained by utilising more detailed information about worst-case execution time estimates described in terms of probability distributions.

4.18 Timing Compositionality – Challenges and Opportunities

Jan Reineke (Universität des Saarlandes, DE)

Joint work of Sebastian Hahn and Michael Jacobs
Main reference S. Hahn, M. Jacobs, J. Reineke, "Enabling Compositionality for Multicore Timing Analysis", in Proc. of the 24th Int'l Conf. on Real-Time Networks and Systems (RTNS'16), pp. 299–308, ACM, 2016.
URL http://doi.acm.org/10.1145/2997465.2997471

How does the execution time of a task respond to interference on shared resources like processor cores, caches, or buses? A common assumption is that a task's response time increases by the amount of interference it experiences. We call this the "compositionality assumption". It underlies most of the approaches to response-time analysis for multi-cores systems known today.

In recent work, we have shown that this assumption is both unsound and imprecise even for simple microarchitectures. I would like to discuss, how to overcome this problem to enable sound and more precise multi-core timing analysis.

5 Working Group Discussions

5.1 The Meaning and Use of probabilistic Worst-Case Execution Time (pWCET) Distributions

Robert I. Davis and Alan Burns

Research into probabilistic Worst-Case Execution Time (pWCET) analysis can be classified into two main categories:

- *Analytical methods*: referred to as *Static Probabilistic Timing Analysis (SPTA)* [4, 7, 2, 1, 12]. SPTA is applicable when some part of the system or its environment contributes random or probabilistic timing behaviour. SPTA methods analyse the software and use a model of the hardware behaviour to derive an estimate of worst-case timing behaviour represented by a pWCET distribution, that is valid for any possible inputs and paths through the code. SPTA does not execute the code on the actual hardware.
- *Statistical methods*: referred to as *Measurement-Based Probabilistic Timing Analysis (MBPTA)* [3, 10, 11, 6, 15, 13]. MBPTA makes use of measurements (*observations*) of the overall execution time of a software component, obtained by running it on the actual hardware, using test vectors i.e. inputs that exercise a relevant subset of the possible paths through the code. These methods use a statistical analysis of the observations based on *Extreme Value Theory* (EVT) to estimate the pWCET distribution.

It is important to understand the precise meaning of a pWCET distribution since this impacts how such information can be used. In fact there are two subtly different meanings originating from SPTA and MBPTA.

The timing behaviour of a system may be characterised as deterministic or it may depend on some element that can be characterised by a random variable, for example a random replacement cache. In general, uncertainty about the timing behaviour of a system can be classified into two categories:

- *Aleatoric variability* depends on chance or random behaviour within the system itself or its environment.
- *Epistemic uncertainty* is due to things that could in principle be known about the system or its environment, but in practice are not, because the information is hidden or cannot be measured or modelled.

While complex software running on advanced time-predictable hardware may in theory exhibit deterministic timing behaviour and therefore have a single absolute WCET, in practice this actual WCET often cannot be determined and must therefore be estimated. Such an estimate is subject to epistemic uncertainty. In contrast, software running on simple time-randomised hardware exhibits aleatoric variability in its execution time. SPTA can be used to model aleatoric variability, but must deal with any epistemic uncertainty by upper bounding its effects in the model used. MBPTA can be used with systems that are characterised by either or both aleatoric variability and epistemic uncertainty.

As an example, it is instructive to consider a thought experiment involving two hypothetical systems. Both systems have 10 inputs which can take values in the range 1-6.

- **System A**: has two paths through the code. The first path is taken if the sum of the input values is odd, and takes 40 cycles to execute. The second path is taken if the sum of the input values is even, it has 10 instructions, each of which takes a random amount

of time from 1-6 cycles to execute (independent of any other instruction or input value). Thus the overall execution time of this path resembles the total from rolling 10 fair dice.

- **System B**: has a single path, it uses a huge internal 10-dimensional array (with 6^{10} entries) that maps from the values of the 10 inputs to a delay. The values for the delays are the totals for each possible permutation of 10 dice rolls; however, they are randomly arranged in the array, and we do not necessarily know what that arrangement is. Further, half of the values have been set to 40 cycles; again, we do not necessarily know which ones. This system looks up its execution time from the table, using the input values, and executes in total for that amount of time.

Intrinsically, System A has only aleatoric uncertainty, while System B has only epistemic uncertainty.

Consider applying SPTA to System A. With an accurate model of the instruction timing behaviour, SPTA could be used to compute a pWCET distribution that upper bounds the timing behaviour of this system *irrespective* of its inputs.

In the context of SPTA, the meaning of a pWCET distribution can be defined as follows, building on the definition in [7]:

▶ **Definition 1.** The pWCET distribution from SPTA is a tight upper bound[2] on all of the probabilistic execution time (pET) distributions that could be obtained for each individual combination of inputs, software states, and hardware states, excluding the random variables which give rise to variation in the timing behaviour. (Note, each individual pET distribution depends on the random variables, but not on the inputs or states, which are fixed in a particular combination).

In the absence of any random variables contributing to probabilistic timing behaviour, then the above definition of a pWCET distribution reduces to the familiar one for a single valued WCET obtained via conventional static WCET analysis. It is a tight upper bound on all the execution times that may be obtained for different combinations of inputs, software states, and hardware states.

If the random variables contributing to a probabilistic execution time behaviour are independent, then it follows that the pWCET distribution obtained by SPTA is independent with respect to any particular execution of that component. (This is the case, since the pWCET distribution from SPTA upper bounds every possible pET distribution). This has implications for the use of pWCET distributions, since they are independent they may be composed using basic convolution to derive probabilistic Worst-Case Response Time (pWCRT) distributions [8, 14], which can then be compared to the appropriate deadline to determine the probability of a deadline miss.

Next, consider System B. Applying SPTA using a precise model of the software and hardware would result in a single WCET, since there are no random variables involved, and we assume no information about the frequency of any combination of input values. By contrast, if we apply MBPTA, then we can estimate the WCET; however, this estimate has *epistemic* uncertainty. There are things we do not know about the system when we consider it as a "black box", and we have only taken a sample of execution time observations, hence we cannot be 100% confident that our estimate is correct.

In the context of MBPTA, the meaning of a pWCET distribution can be defined as follows:

[2] In the sense of the greater than or equal to operator defined on the 1 - CDF of the distributions [9].

▶ **Definition 2.** The pWCET distribution from MBPTA is a statistical estimate giving an upper bound p on the probability that the execution time of a component will be greater than some arbitrary value x, valid for any possible distribution of input values that could occur during deployment.

Thus the pWCET distribution characterises the probability $(1 - p)$ that the WCET of a component will be no greater than some arbitrary value x [5], or as noted by Edgar and Burns [10] the pWCET distribution reflects the *confidence* we have that the statement, *"the WCET does not exceed x for some threshold x"* is true.

We note that the definitions of a pWCET distribution originating from MBPTA and by SPTA are different. The definition from SPTA reflects aleatoric variability, while that from MBPTA reflects epistemic uncertainty.

Since the pWCET definition from MBPTA reflects epistemic uncertainty, i.e. what isn't known about the system, then if it turns out that a WCET estimate x is exceeded, it is possible that it could be exceeded for *every* one of a number of runs of the component in a sequence, depending on the input values used. This is the case since the pWCET distribution effectively gives the probability that *at least one* run of the component has an execution time which exceeds x, but given that event, it provides no additional information about the execution times of individual runs.

For example, for System B, let us assume that MPBTA [6] estimates that there is a probability of 10^{-y} that the WCET exceeds x. However, if that WCET estimate is exceeded, then it could be that it is exceeded *every* time the component runs, depending on the particular input values used. This has implications for how the pWCET distribution may be used in probabilistic schedulability analysis. Assuming a pWCET distribution derived via MBPTA where a WCET of x has an exceedance probability of 10^{-y}. We may only infer that N runs of the component have a probability of no more than 10^{-y} of exceeding a total execution time of Nx. Contrast this with a similar pWCET distribution derived via SPTA. In this case, assuming the aleatoric variability was due to independent random variables, then it would be valid to apply basic convolution to upper bound the overall execution time of N runs. This conclusion would not in general be sound with a pWCET distribution derived via MBPTA, due to its different meaning.

In the case of System A, the pWCET distribution from SPTA tells us that the probability that the execution time on any single run will exceed x is 10^{-y}. If we observe a value larger than x at some point in a large number of runs, then that is not in itself incompatible with the information that we have, which characterises aleatoric variability. By contrast, in the case of system B, the pWCET distribution from MBPTA gives us a *measure of confidence* that the WCET is no more than x. If we observe a value larger than x then that confidence falls to zero.

Acknowledgments. The ideas in this short paper were presented and discussed in an ad-hoc working group comprising Liliana Cucu-Grosjean, Adriana Gogonel, Cristian Maxim, Iain Bate, Philipa Conway, Zoe Stephenson, Alan Burns and Robert Davis.

References

1 S. Altmeyer, L. Cucu-Grosjean, and R. I. Davis. Static probabilistic timing analysis for real-time systems using random replacement caches. *Springer Real-Time Systems*, 51(1):77–123, 2015.

2 S. Altmeyer and R. I. Davis. On the correctness, optimality and precision of static probabilistic timing analysis. In *Proceedings of the Conference on Design, Automation and Test in Europe (DATE)*, pages 26:1–26:6, 2014.

3 A. Burns and S. Edgar. Predicting computation time for advanced processor architectures. In *Proceedings of the Euromicro Conference on Real-Time Systems (ECRTS)*, pages 89–96, 2000.

4 F. J. Cazorla, E. Quiñones, T. Vardanega, L. Cucu, B. Triquet, G. Bernat, E. Berger, J. Abella, F. Wartel, M. Houston, L. Santinelli, L. Kosmidis, C. Lo, and D. Maxim. Proartis: Probabilistically analyzable real-time systems. *ACM Transactions on Embedded Computing Systems*, 12(2s):94:1–94:26, May 2013.

5 L. Cucu-Grosjean. Independence a misunderstood property of and for probabilistic real-time systems. *In Real-Time Systems: the past, the present and the future*, pages 29–37, 2013.

6 L. Cucu-Grosjean, L. Santinelli, M. Houston, C. Lo, T. Vardanega, L. Kosmidis, J. Abella, E. Mezzetti, E. Quiñones, and F. J. Cazorla. Measurement-based probabilistic timing analysis for multi-path programs. In *Proceedings of the Euromicro Conference on Real-Time Systems (ECRTS)*, pages 91–101, July 2012.

7 R. I. Davis, L. Santinelli, S. Altmeyer, C. Maiza, and L. Cucu-Grosjean. Analysis of probabilistic cache related pre-emption delays. In *Proceedings of the Euromicro Conference on Real-Time Systems (ECRTS)*, pages 168–179, July 2013.

8 J. L. Diaz, D. F. Garcia, K. Kim, C-G. Lee, L. Lo Bello, J. M. Lopez, S. L. Min, and O. Mirabella. Stochastic analysis of periodic real-time systems. In *Proceedings of the IEEE Real-Time Systems Symposium (RTSS)*, pages 289–300, 2002.

9 J. L. Diaz, J. M. Lopez, M. Garcia, A. M. Campos, Kanghee Kim, and L. L. Bello. Pessimism in the stochastic analysis of real-time systems: concept and applications. In *Proceedings of the IEEE Real-Time Systems Symposium (RTSS)*, pages 197–207, Dec 2004.

10 S. Edgar and A. Burns. Statistical analysis of wcet for scheduling. In *Proceedings of the IEEE Real-Time Systems Symposium (RTSS)*, pages 215–224, Dec 2001.

11 J. Hansen, S. A. Hissam, and G. A. Moreno. Statistical-based WCET estimation and validation . In *Proceedings of the Workshop on Worst-Case Execution Time Analysis (WCET)*, volume 252, 2009.

12 B. Lesage, D. Griffin, S. Altmeyer, and R. I. Davis. Static probabilistic timing analysis for multi-path programs. In *Proceedings of the IEEE Real-Time Systems Symposium (RTSS)*, pages 361–372, Dec 2015.

13 G. Lima, D. Dias, and E. Barros. Extreme value theory for estimating task execution time bounds: A careful look. In *Proceedings of the Euromicro Conference on Real-Time Systems (ECRTS)*, July 2016.

14 D. Maxim and L. Cucu-Grosjean. Response time analysis for fixed-priority tasks with multiple probabilistic parameters. In *Proceedings of the IEEE Real-Time Systems Symposium (RTSS)*, pages 224–235, Dec 2013.

15 L. Santinelli, J. Morio, G. Dufour, and D. Jacquemart. On the Sustainability of the Extreme Value Theory for WCET Estimation. In *Proceedings of the Workshop on Worst-Case Execution Time Analysis (WCET)*, pages 21–30, 2014.

6 Open problems

6.1 Mixed criticality scheduling under resource uncertainty

Kunal Agrawal (Washington University - St. Louis, US)

Most real time scheduling theory for mixed criticality systems deals with uncertainty about task parameters and assumes that resources remain the same as the system executes. For cloud and shared environments, however, one can imagine that resource availability changes as the system executes. I would like to explore if we can use the ideas developed in mixed criticality scheduling to provide tiered guarantees of the following form: If "adequate" resources are available, the scheduler must schedule all tasks. If fewer resources are available, the scheduler is allowed to drop "low-criticality" tasks, but must still schedule the important tasks.

6.2 Deriving Optimal Scheduling Policies for MC Task Systems

Sathish Gopalakrishnan (University of British Columbia - Vancouver, CA)

Assuming execution time distributions are available for tasks in a mixed-criticality setting, how do we use this distributional information to schedule tasks? One approach, where tasks – depending on their criticality levels – have an acceptable failure rate is to model the entire task system using chance-constrained Markov decision processes. This model can then be used to derive a feasible scheduling policy (when one exists). I will briefly describe some progress made and challenges that remain.

6.3 Guaranteeing some service upon mode switch in mixed-criticality systems

Zhishan Guo (University of Missouri - Rolla, US)

6.3.1 Introduction

Epistemic uncertainty widely exists in real-time systems that the precise nature of the external environment, as well as the run-time behavior of the implemented platform, cannot be predicted with complete certainty prior to deployment. However, systems nevertheless must be designed and analyzed prior to deployment in the presence such uncertainty – the widely-studied [3] Vestal model [12] for mixed-criticality workloads addresses uncertainties in estimating the worst-case execution time (WCET) of real-time code. Different estimations, at different levels of assurance, are made about these WCET values; it is required that all functionalities execute correctly if the less conservative assumptions hold, while only the more critical functionalities are required to execute correctly in the (presumably less likely) event that the less conservative assumptions fail to hold but the more conservative assumptions do.

Here we briefly introduce some generalizations of the Vestal model, where degraded (but non-zero) level of services can be guaranteed for the less critical functionalities even in the event of only the more conservative assumptions holding. If such service degradation is represented by a shorter allowed execution for each job, or a longer period, recent work has suggested some MC scheduling algorithms; while for other degradation definition, we seek for further discussions perhaps with the industry.

6.3.2 Low Critical ≠ Non Critical

The original Vestal model was very successful in dealing with the resource inefficiency with the verification of mixed-criticality systems. However, this model has met with some criticism from systems engineers; e.g., in the event of some (Hi criticality) jobs executing beyond their less pessimistic WCET estimates, LO-criticality jobs are treated same as non-critical jobs that no guarantees can be made to their service.

This desideratum was addressed in [1] by introducing an additional less pessimistic WCET parameter for LO-criticality jobs – a guaranteed service level regardless of the behaviors/executions of HI-criticality jobs. Following the MC-Fluid framework [10] that was shown to have the best possible speedup factor (4/3) [5] versus clairvoyant optimal scheduler, we have identified in [4] a nice scheduler that handles such LO-criticality service separately. MC-Fluid framework assumes fluid scheduling which may involve too many preemptions.

The authors in [10] have suggested to follow the DP-Fair framework [6], while we believe the number of preemptions can be hugely reduced if we follow Boundary Fair [13] with well defined per-mode boundary setting at task release – see our recent submission [7] for more details. EDF based methods maybe another option – some recent work has studied the uniprocessor scheduling case [11].

The aforementioned schedulers may deal with a degraded utilization requirement for LO-criticality tasks upon a mode switch. However, a shorter execution or a longer period may not be enough (or proper) to guarantee certain level of service – a piece of code may need the original estimated execution length to finish any single execution, while the timeliness remains the same (i.e., the result is useful only when a job is finished within the same deadline conditions). A degraded service may be defined as the allowance of certain portion of jobs to be dropped, while others remain the same execution time and deadline. This leads to the (m,k)-firm deadline scheduling problem, on which there is no existing solution for mixed-criticality system schedulability analysis, and may worth investigating – see our recent submission [8] for more details.

References

1 A. Burns and S. Baruah. Towards a more practical model for mixed criticality systems. In WMC2014.

2 S. Baruah, V. Bonifaci, G. D'Angelo, H. Li, A. Marchetti-Spaccamela, S. Van Der Ster, and L. Stougie. The preemptive uniprocessor scheduling of MC implicit-deadline sporadic task systems. ECRTS 2012.

3 A. Burns and R. Davis. Mixed-criticality systems: A review. http://www-users.cs.york.ac.uk/burns/review.pdf.

4 S. Baruah, A. Burns, and Z. Guo. Scheduling mixed-criticality systems to guarantee some service under all non-erroneous behaviors. ECRTS 2016.

5 S. Baruah, A. Easwaran, and Z. Guo. MC-Fluid: simplified and optimally quantified. RTSS 2015.

6 S. Funk, G. Levin, C. Sadowski, I. Pye, and S. Brandt. DP-Fair: a unifying theory for optimal hard real-time multiprocessor scheduling. Real-Time Systems, 2011.

7 Z. Guo, S. Sruti, and N. Guan. From fluid into non-fluid: multi-processor mixed-criticality scheduling with limited preemption. In submission.

8 Z. Guo, K. Yang, S. Arefin, S. Vaidhun, and H. Xiong. Uniprocessor Mixed-Criticality Scheduling with Graceful Degradation. In submission.

9 M. Hamdaoui and P. Ramanathan. A service policy for real-time customers with (m,k) firm deadlines. FTCS 1994.

10 J. Lee, K.-M. Phan, X. Gu, J. Lee, A. Easwaran, I. Shin, and I. Lee. MC-Fluid: Fluid model-based mixed-criticality scheduling on multiprocessors.RTSS 2014.

11 D. Liu, J. Spasic, N. Guan, G. Chen, S. Liu, T. Stefanov, and W. Yi. EDF-VD Scheduling of Mixed-Criticality Systems with Degraded Quality Guarantees. RTSS 2016.

12 S. Vestal. Preemptive scheduling of multi-criticality systems with varying degrees of execution time assurance. IEEE RTSS 2007.

13 D. Zhu, X. Qia, D. Mossél, and R. Melhem. An optimal boundary fair scheduling algorithm for multiprocessor real-time systems. Journal of Parallel and Distributed Computing, vol. 71, no. 10, pp. 1411–1425, 2011.

6.4 Regarding the Optimality of Speedup Bounds of Mixed-Criticality Schedulability Tests

Zhishan Guo (University of Missouri - Rolla, US)

Much existing research on Mixed-Criticality (MC) scheduling (see [3] for a review) has focused on dealing with the Vestal model [12], where different WCET estimations of a single piece of code are provided. This is typically a consequence of different tools for determining worst-case execution time (WCET) bounds being more or less conservative than each other. It is known [1] that mixed criticality (MC) scheduling under such model is highly intractable, such that polynomial-time optimal solution is impossible unless $P = NP$. As a result, *speedup bound* is widely used in MC scheduling for measuring how close to optimal is a given schedulability analysis.

- A schedulability test $\mathcal{A}$ has *speedup factor* of $s (s \geq 1)$, if any task set that is schedulable by any algorithm on a given platform with processing speed of 1, it will be deemed schedulable by Test $\mathcal{A}$ upon a platform that is s times as fast.

Of course, when deriving MC schedulers and associated schedulability tests, one of the goals is to identify/prove a relative small speedup bound (that is closer to 1). A minimum possible speedup is often presented as the "*optimal* speedup bound" of a given MC scheduling problem. However, we would like to point out that:

- Optimality of scheduler should not be derived against optimal speedup bounds.

6.4.1 Non-Optimal Schedulers with Optimal Speedup Bounds

For scheduling (dual-criticality) Vestal job set on a uniprocessor platform, it has been shown [2] that OCBP algorithm (following the idea of Audsley's priority assignment mechanism) has an optimal speedup bound of $(\sqrt{5} - 1)/2$. However, several algorithms has been identified to *strictly dominate* OCBP; e.g., Lazy Priority Adjustment [8], LE-EDF [10] [9] – with the same speedup bound and at *all* time, better schedulability.

Similar results can be observed when we consider the scheduling of Vestal task set as well. It has been shown that 4/3 is the best speedup that any non-clairvoyant scheduler can achieve. Upon proposing a speedup-optimal uniprocessor scheduler named EDF-VD [2], improvements on the schedulability can still be made, e.g., [7] [6]. As for the multiprocessor case, it is proved [3] that both MC-Fluid [10] and MCF [3] achieve the optimal speedup of 4/3. However, MCF is a simplified version of (and is dominated by) MC-Fluid. Moreover, improvements on schedulability can be further made to MC-Fluid [11].

6.4.2 Speedup over Non-Clairvoyance?

When deriving speedup bounds, in most of the existing works of the community, the proposed algorithm is compared with a *clairvoyant optimal scheduler*, and adapts the necessary conditions for MC schedulability. This may not be a very fair way of comparison since the penalty for unawareness

of the future is applied into the speedup bounds. Following the varying-speed MC model [5] [4], we have identified an on-line optimal[3] scheduler in [9] that has a speedup factor significantly greater than 1 when comparing to an optimal clairvoyant algorithm. However, such a speedup factor only reflects the price one must pay for not knowing the future (or the difficulty of the scheduling problem itself) – it has nothing to do with the MC scheduler design anymore. In other words, most existing speedup bounds may only be capturing the gap between clairvoyance and non-clairvoyance.

Since MC schedulability analysis is for off-line verification of correctness of real-time systems, all possible scenarios should be taken into consideration (which is non-clairvoyance). We believe speedup results comparing to optimal non-clairvoyance schedule may be worth investigating for MC systems.

References

1 S. Baruah. Mixed criticality scheduling is highly intractable. http://www.cs.unc.edu/b̃aruah/Submitted/02cxty.pdf.

2 S. Baruah, H. Li, and L. Stougie. Towards the design of certifiable MC systems. IEEE RTAS 2010.

3 S. Baruah, A. Easwaran, and Z. Guo. MC-Fluid: simplified and optimally quantified. RTSS 2015.

4 S. Baruah and Z. Guo. Scheduling mixed-criticality implicit-deadline sporadic task systems upon a varying-speed processor. RTSS 2014. IEEE Computer Society Press.

5 S. Baruah and Z. Guo. Mixed-criticality scheduling upon varying-speed processors. IEEE RTSS 2013.

6 A. Easwaran. Demand-based MC scheduling of sporadic tasks on one processor. IEEE RTSS 2013.

7 P. Ekberg, W. Yi. Bounding and shaping the demand of generalized mixed-criticality sporadic task systems. Real-Time Systems, 50(1): 48-86, 2014.

8 C. Gu, N. Guan, Q. Deng, and W. Yi. Improving OCBP-based scheduling for MC sporadic task systems. RTCSA 2013.

9 Z. Guo and S. Baruah. The concurrent consideration of uncertainty in WCETs and processor speeds in mixed criticality systems. IEEE RTNS 2015.

10 S. Baruah and Z. Guo. Mixed-criticality scheduling upon varying-speed multiprocessors. Leibniz Transactions on Embedded Systems, 1(2): 3:1–3:19, 2014.

11 S. Ramanathan and A. Easwaran. MC-fluid: rate assignment strategies. WMC 2015.

6.5 MC-ADAPT: Adaptive Mixed Criticality Scheduling through Selective Task Dropping

Jaewoo Lee (University of Pennsylvania - Philadelphia, US)

Mixed-criticality real-time scheduling aims to ensure deadline satisfaction of higher-criticality tasks, while achieving efficient resource utilization. To this end, many approaches have been proposed to execute more lower-criticality tasks without affecting the timeliness of higher-criticality tasks. Those previous approaches however have at least one of the two limitations; i) they penalize all

[3] If an *on-line optimal* scheduling strategy fails to maintain correctness for a given MC instance I, no non-clairvoyant algorithm can ensure correctness for I (without making lucky guesses to the future).

lower-criticality tasks at once upon a certain situation, or ii) they make decision how to penalize lower-criticality tasks at design time. As a consequence, they under-utilize resources by imposing an excessive penalty on low-criticality tasks.

Unlike those existing studies, our approach aims to minimally penalize lower-criticality tasks by fully reflecting the dynamically changing system behavior into adaptive decision making. We propose a new scheduling algorithm which supports selective task dropping and develop its runtime schedulability analysis capturing the dynamic system state. Our proposed algorithm adaptively decides task dropping based on the runtime analysis.

To determine the quality of task dropping, we propose the speedup factor for task dropping. While the conventional speedup factor for the MC scheduling problem only evaluates MC scheduling algorithms in terms of the worst-case schedulability, we apply the speedup factor for the task dropping problem, which is an extended version of the MC scheduling problem. The task dropping problem is an optimization problem for task dropping under different MC scheduling scenarios.

6.6 Schedulability, Probabilities and Formal Methods

Luca Santinelli

The abstract is about developing probabilistic schedulability analysis with formal methods, in particular the Continuous Time Markov Chain models for jobs and tasks with continuous input distribution as probabilistic Worst-Case Execution Time (pWCET).

The open problem presented composes of building jobs and tasks CTMC models which are able to capture every [probabilistic] execution behavior; the models composed constitutes the real-time system with its jobs/tasks ordering. Then, such models can be formally verified with properties like deadline miss ration and systems schedulability. With the model proposed, alternative properties for already existing scheduling algorithms of newly proposed probabilistic schedulability algorithms would be verified.

6.7 Safety Calling

Zoë Stephenson (Rapita Systems Ltd. - York, GB)

There is a need for vocabulary and models to support discussion between researchers in the domain of mixed-criticality scheduling and experts in the field of safety analysis. In this abstract, I explain why this is important and what form this could take.

In a traditional scheduling regime such as a preemptive, fixed-priority scheduler, we present an argument showing that the system is schedulable with respect to some assumptions. Those assumptions relate to jitter, timing anomalies (particularly regarding the cache), task switch latency and the validity of WCET figures. The scheduler typically provides overrun monitoring, and the system design would typically also include a watchdog, to detect cases where the schedulability prediction is incorrect. The safety engineer then designs responses to the detection of this condition – for example, rebooting a partition, switching to a diverse implementation with fewer features, switching to a reversionary schedule, or resetting the entire controller.

When we move to mixed-criticality scheduling, we get the following features:

- Scheduling algorithms that aim to provide better overall utilisation of resources, particularly multicore resources

- Flexibility in the predictions made at design time so that the system designer can bias confidence in execution time bounds towards higher-criticality functionality and take advantage of this biased confidence in the schedulability analysis
- Flexibility in the behaviour of the scheduler in responding to violations of these execution-time bounds

With this flexibility, there are new considerations in the system design and safety analysis, and clear communication will make it easy to work with these considerations. The aim is to help the safety engineer to devise appropriate mitigation strategies for overruns, dividing the work up between system requirements and scheduler requirements within a process such as the following:

1. System design identifies functions allocated to software. Each has an associated assurance level representing the severity of the consequence of a failure to provide the function.
2. Software design identifies components to implement functions; components also have assurance levels.
3. Software design creates a schedule for the components, and presents this to the safety analysis in the form of response time bounds, relative confidence (compared to the project's traditional approach) and possible responses for exceeding those time bounds. The aim is to describe the capabilities of the scheduler and show how confidence and responses can match up with the components' assurance levels.
4. Safety analysis feed the scheduler behaviour, as well as other functional and non-functional behaviours, into system safety assessment and determine whether additional measures are needed for assuring adequate provision of system functions. These become derived requirements that call for design changes such as resets, reversionary task-sets or watchdogs, and additional analyses.
5. Software design, system design and safety analysis iterate until appropriate assurance is reached.
6. Safety analysis completes the assurance argument that mitigation strategies for the software components are appropriate for the criticality levels of the functions they provide.

From these steps a picture emerges of a scheduler response model, structured as:

- Function and Component
  - WCRT
  - WCRT confidence
  - Overrun response
    - Call an exception handler
    - Cancel (this task / some other tasks)
    - Reduce releases (this task / some other tasks)
    - Increase clock frequency
    - Reduce algorithm detail
    - Switch schedule
    - ...

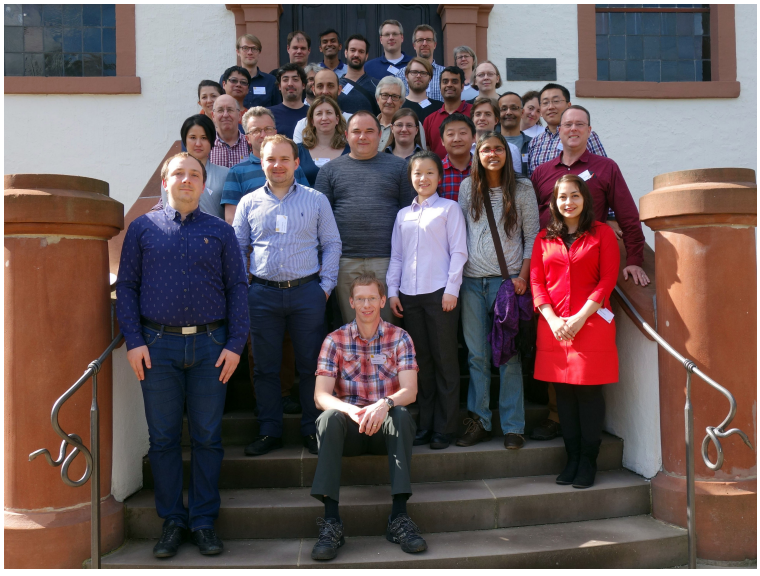
The range of WCRT confidence descriptions and possible responses will depend on the exact mixed-criticality scheduler in use. By presenting the scheduling approach in terms of confidence and overrun responses, the model provides useful detail for the safety analyst and improves the ability of the system to take full advantage of the facilities provided by advanced scheduling algorithms.

7 Outcomes of the seminar

- *On the Meaning of probabilistic Worst-Case Execution Time (pWCET) Distributions and their use in Schedulability Analysis* by Robert I. Davis, Alan Burns, David Griffin. Under submission.
- *Resilient Mixed-Criticality Systems* by A. Burns, R.I. Davis, S. Baruah, I. Bate. Under submission.
- *On the Existence of a Cyclic Schedule for Non-Preemptive Periodic Tasks with Release Offset* by Mitra Nasri and Emmanuel Grolleau. Under submission.
- *Uniprocessor Mixed-Criticality Scheduling with Graceful Degradation* by Zhishan Guo, Kecheng Yang, Samsil Arefin, Sudharsan Vaidhun, and Haoyi Xiong. Under submission.
- *Sustainability in Mixed-Criticality Scheduling* by Zhishan Guo, Sai Sruti, Bryan Ward, and Sanjoy Baruah. Under submission.
- *Sustainability in Mixed-Criticality Scheduling* by Ying Zhang, Zhishan Guo, Lingxiang Wang, Haoyi Xiong, and Zhenkai Zhang. Under submission.

Participants

- Kunal Agrawal
Washington University – St. Louis, US
- Sebastian Altmeyer
University of Amsterdam, NL
- James H. Anderson
University of North Carolina at Chapel Hill, US
- Sanjoy K. Baruah
University of North Carolina at Chapel Hill, US
- Iain Bate
University of York, GB
- Enrico Bini
University of Turin, IT
- Björn B. Brandenburg
MPI-SWS – Kaiserslautern, DE
- Alan Burns
University of York, GB
- Thidapat Chantem
Virginia Polytechnic Institute – Arlington, US
- Jian-Jia Chen
TU Dortmund, DE
- Liliana Cucu-Grosjean
INRIA – Paris, FR
- Robert Davis
University of York, GB
- Arvind Easwaran
Nanyang TU – Singapore, SG
- Pontus Ekberg
Uppsala University, SE
- Sébastien Faucou
University of Nantes, FR
- Madeleine Faugère
Thales Research and Technology – Palaiseau, FR
- Christian Ferdinand
AbsInt – Saarbrücken, DE
- Laurent George
ESIEE – Champs sur Marne, FR
- Adriana Gogonel
INRIA – Paris, FR
- Sathish Gopalakrishnan
University of British Columbia – Vancouver, CA
- Emmanuel Grolleau
ENSMA – Chasseneuil, FR
- Zhishan Guo
University of Missouri – Rolla, US
- Leandro Soares Indrusiak
University of York, GB
- Jaewoo Lee
University of Pennsylvania – Philadelphia, US
- Jing Li
Washington University – St. Louis, US
- Martina Maggio
Lund University, SE
- Alberto Marchetti-Spaccamela
Sapienza University of Rome, IT
- Cristian Maxim
Airbus S.A.S. – Toulouse, FR
- Dorin Maxim
LORIA & INRIA – Nancy, FR
- Mitra Nasri
MPI-SWS – Kaiserslautern, DE
- Claire Pagetti
ONERA – Toulouse, FR
- Kirk Pruhs
University of Pittsburgh, US
- Gurulingesh Raravi
ISEP Porto, PT
- Jan Reineke
Universität des Saarlandes, DE
- Stefan Resch
Thales – Wien, AT
- Philippa Ryan
Adelard – London, GB
- Luca Santinelli
ONERA – Toulouse, FR
- Zoë Stephenson
Rapita Systems Ltd. – York, GB
- Sascha Uhrig
Airbus – München, DE
- Wang Yi
Uppsala University, SE
- Dirk Ziegenbein
Robert Bosch GmbH – Stuttgart, DE



Report from Dagstuhl Seminar 17132

Opportunities and Risks of Blockchain Technologies

Edited by

Roman Beck[1], Christian Becker[2], Juho Lindman[3], and Matti Rossi[4]

1 **IT University of Copenhagen, DK,** beck@itu.dk
2 **Universität Mannheim, DE,** christian.becker@uni-mannheim.de
3 **University of Gothenburg and Chalmers UT, SE,** juho.lindman@ait.gu.se
4 **Aalto University, FI,** matti.rossi@aalto.fi

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 17132 "Opportunities and Risks of Blockchain Technologies". Blockchain-based applications such as Bitcoin or Ethereum are emerging technologies, but a dramatic increase in industrial and academic interest in the technology is evident. Start-ups and large financial players are working intensely on blockchain-based applications, making this one of the most promising drivers of financial innovation. However, the design and implementation of blockchain-based systems requires deep technical know-how in various areas, as well as consideration of economic and societal issues. These opportunities and challenges provided the starting point for the Dagstuhl Seminar where we analyzed and synthesized the current body of knowledge on the emerging landscape of blockchain technologies. We linked cryptographic economic systems to already established research streams around trust-related issues in payment systems and digital currencies, and digital asset management.

Seminar March 26–29, 2017 – http://www.dagstuhl.de/17132
1998 ACM Subject Classification D.2.0 Software Engineering, K.6.5 Security and Protection
Keywords and phrases bitcoin, blockchain, cryptocurrencies, trust networks, trust platforms
Digital Object Identifier 10.4230/DagRep.7.3.99

1 Executive Summary

Juho Lindman
Roman Beck
Christian Becker
Matti Rossi

Introduction

The Dagstuhl seminar "Opportunities and Risks of Blockchain Technologies" had 21 participants from universities, public institutions, and enterprises. Blockchain is both an information technology as well as an economic innovation. As a technical innovation it is a new version of a distributed transactional database technology, especially suited for decentralized environments of limited or imperfect trust. As an economic innovation it offers novel tools to any problem domain where there exists a need for a reliable record of transactions in a decentralized environment where not all parties, whether humans or machines, can be fully trusted.

Opportunities and Risks of Blockchain Technologies, *Dagstuhl Reports*, Vol. 7, Issue 3, pp. 99–142
Editors: Roman Beck, Christian Becker, Juho Lindman, and Matti Rossi
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Computer scientists have researched key issues of blockchain technologies such as technical availability, tools, standards, and applications that enable these networks. Our seminar aimed to bridge the gap between this research stream and research perspectives from Service Science, Wirtschaftsinformatik, and Information Systems. We brought together a multi-disciplinary group of academic and industry researchers; specifically those working in fields such as open platforms, open source, distributed trust platforms, cryptocurrency tools, as well as the related social and legal challenges.

We set to analyze and synthesize the current body of knowledge on the emerging landscape of blockchain technologies. We linked the emerging phenomenon of cryptographic economic systems to already established research streams around trust-related issues in payment systems, online currencies, and supply chain management through group work and keynotes. We worked on four theme groups:

1. Research centers
2. Blockchain and Fintech
3. Essence and future of blockchain technologies
4. Impact/changing institutions

In the following we look at each of these shortly. The full report contains a number of position papers that explore these issues in further detail.

Research centers

The research center work group sought ways of strengthening the European and global research on blockchain. A starting point was a proposal to form a network of similar minded Blockchain experts and research groups across Europe. Several groups from countries such as in Denmark, Ireland, UK, and Switzerland could start as a loosely coupled interest group to work on potential research agendas and teaching curricula. The Blockchain seminar at Dagstuhl can be regarded as the starting point for the formation of the research network. Based on this network, the next step would be to convince funding agencies and industry to write research proposals for the DRAO (Distributed Research Autonomous Organization). The idea of DRAO is that the Blockchain research center should not be just another research center, doing research on Blockchain, but actually should be based on Blockchain, as a distributed autonomous research organization.

Furthermore, the group discussed a proposal for Blockchain teaching and education. This would result in a suite of courses on various areas, possibly as follows:

Computer Science Foundations

- Cryptography, authentication and signature methods.
- Distributed computing, distributed algorithms, understanding of the tradeoffs, consensus protocols
- Distributed systems
- Domain specific languages for contracts and for protocols.
- Large scale software engineering for distributed ledger development, software engineering
- Program analysis and software quality, objective way of verifying properties

Information Systems Economics

- Economic theories on incentive models, auctions and mechanism design (basically game theory insights)
- Inter-organizational, distributed governance and management theories

- Collective economies, reputation and trust management
- Digital Mindset and management of digital personas
- Ethics and critical reflections of Blockchain and societal implications

Information Systems Management and Organization

- Innovation Design: from Blockchain idea to prototype
- Digital Entrepreneurship: from Blockchain prototypes to markets
- Taxation, auditing and integration of Blockchain in organizations

IT Law

- Legal implications of Blockchain, property rights, ownership, responsibilities

Blockchain and Fintech

Our second worgroup dealt with the relationship between Blockchain and the Fintech industry. The group produced a matrix of different financial and legal functions, tools required to handle those and the potential of Blockchain to replace solutions to these functions.

Essence and Future of Blockchain Technologies

The workgroup on the essence of blockchain technologies set out to understand what forms the core of the technology. Its preliminary definition is that a blockchain implementation should contain First, the data storage that implements a distributed ledger system (DLS), the actual Blockchain, which is the data structure used in DLS is a hash-linked chain of blocks. A block is a collection of transactions that form the ledger. Furthermore, a Consensus Mechanism allowing for (de-)Centralization of power to decide which transactions are valid in the network. The innovative combination of the above mentioned three components give DLS interesting characteristics that we describe in the next section.

Impacts/changing institutions

This workgroup set out to understand the relationship between technical change and social change. It tried chart the relationship of blockchain and institutions. The discussion centered around the resilience of institutions and the need for stop gap measures, which are often provided by quite traditional public infrastructures and legal frameworks. In some cases, institutions will have to put conditions in place to allow blockchain to work (in particular to avoid harm). The idea of Blockchain being able to replace or eliminate trust was a central topic and it was noted that this can be an issue in cases of fraud (e.g. Ethereum fork as an example). The group also discussed who provides stable identifiers and who decides what can be stored in a given ledger. Similarly, the assignment of value and ownership and their control remain important issues that are now seen as tertiary to the technology. Key questions arising from this were:

- How will blockchain solutions that work well in theory or as prototypes function when used as large-scale solutions?
- Are certain groups or communities better suited to adopt blockchain?

Final comments

We believe that despite some hiccups (e.g., DAO fork) blockchain will emerge as an important technological and economical phenomenon. Its key properties and impacts should be studied intensively to allow for new innovations in the financial sector and other areas, where the technology's affordances promise to create value. The work continues through a manifesto in Business & Information Systems Engineering, a viewpoint in Communications of the ACM, and a special issue in the Journal of the Association for Information Systems.

2 Table of Contents

3 Overview of Talks

3.1 Smart Money: Blockchain-Based Customizable Payments System

Michel Avital (Copenhagen Business School, DK)

Joint work of Jonas Hedman; Lars Albinsson

Abstract. Legal tender in the form of coins and banknotes is expected to be replaced at one point in the future by digital legal tender. This transformation is an opportunity for central banks to rethink the idea of money and overhaul the prevailing payment systems. Digital legal tender is expected to reduce transaction costs by providing seamless real-time payments. In addition, digital legal tender that is based on blockchain technology can provide a foundation for customizable "smart money" which can be used to manage the appropriation of money and its use. In essence, the smart money is a customizable value exchange instrument that relies on computer protocols to facilitate, verify, and enforce certain conditions for its appropriation as payment, e.g. who may use the money, where, and for what. If we believe that digital legal tender will become ubiquitous, then the emergence and diffusion of smart money is inevitable and deserves further investigation.

Keywords: money, legal tender, digital money, customizable money, payment system, blockchain, distributed ledger technology.

The infrastructure of payment transactions is interrelated to the nature of money. Not long ago, ships were used to carry coffers of gold and silver coins which had intrinsic value. The growth and dynamics of worldwide commercial markets set the stage for the development of government-issued fiat money in the form of compact paper notes. The digitalization of bank accounts and the establishment of global communication networks, such as SWIFT, was instrumental in the development of today's electronic fund transfer (EFT) system and the virtualization of money. On the horizon, legal tender in the form of coins and banknotes is expected to vanish and be replaced by a digital legal tender that will be exchanged on distributed ledger technology (DTL) based platforms (Avital et al., 2016). Subsequently, the ubiquity of DLT platforms is expected to speed up money transactions as well as to provide the foundation for customizable "smart money" that can be used to manage the appropriation of money and its use as a medium of exchange.

In the last decade, we witness fundamental changes in the inter-bank exchange and payment infrastructure that are designed to tighten control and transparency. Many of these changes are fueled by regulatory pressure to mitigate particular security and compliance issues, such as money laundering, terrorism, corruption, and increase competition. For instance, the European Union (EU) are in the process of creating a single payment market in through the enforcement of the Single Euro Payments Area (SEPA) and the Payment Service Directive 2 (PSD2). The PSD2 forces banks and financial institutions to open up their payment infrastructure to provide third party payment providers with access to bank accounts and initiate payments [4].

Besides the regulatory changes, members in the banking sector experience increasing competition from non-bank players that offer similar and substitute services. Internet giants, such as Facebook, Alibaba, and Google, as well as device manufacturers, such as Apple and Samsung, have entered the financial market, together with at least 12000 Fintech startups [6]. These firms are dependent on the innovative utilization of existing and emerging technologies to challenge the incumbents of the financial sector [2, 7].

The regulatory changes, the technology development, and the competitive challenges are the new normal for any player in the financial sector. Therefore, it is not surprising that legacy organizations and especially banks make massive investments in the current payment infrastructure in an attempt to defend and bolster their respective market position [5]. The new emerging payment infrastructure is designed not only to address the regulatory and competitive issues; it also provides an opportunity to further develop money as a multifaceted medium of exchange that portrays more than merely monetary value. Subsequently, global transaction banking in the future would need to treat payment as a rich construct that goes beyond amount and effective transaction date.

Today, money is a general-purpose medium of exchange with unrestricted usage, i.e. money can be used by anyone to pay for virtually any product or service anywhere. In contrast, besides seamless real-time payments, the future DLT-based infrastructure offers opportunities to customize payments with sophisticated money that portrays a set of customizable conditions in addition to monetary value– i.e. smart money. In essence, the smart money is value exchange instrument that is based on computer protocols which facilitate, verify, or enforce preset conditions for its appropriation as payment, e.g. who may use the money, what products and services can be bought, and where.

Smart money can be used by society, organizations or individuals to manage the appropriation of money and its use as a customizable medium of exchange. Consider the following example:

Gill and Mark, two loving vegetarian parents, have decided to restrict Peter's (their 15-year-old son) use of his weekly allowance. Peter often used his lunch money to buy hamburgers and sodas, so his parents decided to control his use of his lunch money. The transfer of the weekly lunch allowance goes from Gill and Mark's bank account to Peter's mobile wallet, which also entails his identification cards and debit card. On the balance page, he can see how much money he has on his mobile wallet and his bank accounts. The amount of virtual cash is displayed in a pie chart diagram (green, red, and blue) with the amount on. The green pie is money to be used for school lunch. Red money is for clothes. The blue money is to be used for any purpose. The green and red money are the designed money from his parents to buy lunch at school and new pair of jeans and cannot be used for anything else. So, now Peter cannot buy hamburgers for lunch. Instead, he has to buy the regular vegetarian school lunch. Peter is, of course, outrageous and thinks that his freedom and privacy is hampered, but his parents who pay for the lunch are happy campers.

The idea of restricted-use money is not new – it is quite common as a proprietary currency. For instance, governments issue "food stamps" that can be used for food purchase only in designated locations, casinos issue proprietary "chips" that can be used for gambling, and airlines issue "frequent flyer miles" that can be used for flying tickets [3]. In contrast to such proprietary currency, the smart money is a customizable general purpose legal tender that can be restricted or conditioned as desired. Instead of functioning as a designated proprietary fixed-purpose token, smart money (just like a smart contract) affords a customizable multi-purpose digital medium of value exchange in everyday use by anyone.

The transition into smart money-based monetary system requires intermediary platforms that help financial institutors and users alike to experience the new technology and develop it further without abandoning the familiar and trustworthy legacy system. A transition period is necessary not only to allow banks and governments to experiment with different flavors and configurations as well as to develop a support infrastructure but also to allow developing public confidence in the new monetary system. While smart money can provide ample economic incentives to both governments and banks, it is not clear if smart money will

appeal to business organizations let alone the general public. Clearly, one way to develop public interest in adopting smart money would be to develop it as complementary currency [8] that is aligned with the worldview and value systems of intended users. For example, green money that supports or prefers environmentally friendly products and services, healthy money that supports health-oriented products and services, local money that supports local business, and so on.

We envision a multitude of cases where smart money can be of interest. In addition to numerous business opportunities, it will, of course, create a public debate concerning technical and organizational issues as well as social and ethical issues. Different stakeholders, such as banks, merchants, consumer agencies, politicians, health organizations, human rights and refugee organizations among others will take different positions from their respective perspectives. If we believe that digital tender will become ubiquitous in global transactions banking, then the emergence and diffusion of DLT-based smart money is inevitable and deserves further investigation.

References

1 Avital, M., Beck, R., King, J.L., Rossi, M. and Teigland, R. (2016). "Jumping on the blockchain bandwagon: Lessons of the past and outlook to the future." Proceedings of the 37th International Conference on Information Systems, Dublin, Ireland

2 Chae, J, and Hedman J. (2015). "Business models for NFC-based mobile payments." Journal of Business Models, 3(1), 29-48.

3 Chan, M., Kemp, S., and Finsterwalder, J. (2016). "The concept of near money in loyalty programmes." Journal of Retailing and Consumer Services, 31, 246-255.

4 Cortet, M., Rijks, T., and Nijland, S. (2016). "PSD2: The digital transformation accelerator for banks." Journal of Payments Strategy and Systems, 10(1), 13-27.

5 Hedman, J., and Henningsson, S. (2015). "The new normal: Market cooperation in the mobile payments ecosystem." Electronic Commerce Research and Applications, 14(5), 305-318.

6 McKinsey. (2014). Global Payments 2014: A Return to Sustainable Growth Brings New Challenges.

7 Scott, A., and Bolotin, L. (2016). Introducing the Open Banking Standard: Helping customers, banks and regulators take banking into a truly 21st-cnetury, connected digital economy (ODI-WP-2016-001).

8 Seyfang, G., and Longhurst, N. (2013). "Desperately seeking niches: Grassroots innovations and niche development in the community currency field." Global Environmental Change, 23(5), 881-891.

3.2 On Hostile Blockchain Takeovers

Joseph Bonneau (Stanford University, US)

Abstract. Most research modelling Bitcoin-style distributed consensus protocols (sometimes called "Nakamoto consensus") has focused on attempts to prove incentive compatibility. That is, models attempt to prove that under certain assumptions about attacker motivation a protocol will exhibit desired stability properties such as an exponentially low probability of long chain forks or a distribution of mining rewards that is close the amount of work contributed (called fairness or chain quality). Typically, models assume that the utility

function for all participants in the system is the amount of monetary rewards acquired within the protocol (e.g. for Bitcoin, the amount of mining rewards earned denominated in BTC). This leads to the most tractable models.

It is often acknowledged that a more realistic utility function is monetary rewards denominated in an external currency (such as US dollars). For this reason, some mining strategies which deviate from the standard protocol and lead to increased in-system rewards may yield less utility if they affect the exchange rate and therefore provide fewer ex-system rewards. However, modeling the impact of miner behavior on exchange rates is difficult, so this analysis is usually qualitative.

Rarely considered is a miner whose goal is not simply to acquire monetary rewards, but to destabilize a blockchain (even at a financial loss). Such a miner, who can fairly be called an attacker to the system, was called a Goldfinger attacker by Kroll and Felten (KF 2013). They can also be conceptualized as a hostile takeover, a term that is more appropriate for proof-of-stake systems.

I argue that revisiting the dynamics of a Goldfinger-style attack may yield new insights into the stability of blockchain protocols. In particular, it provides an interesting comparison between ASIC-dominated blockchains (such as Bitcoin), commodity hardware-dominated blockchains (such as Ethereum), and proof-of-stake systems.

Methods of obtaining mining capacity. For an attacker aiming to subvert a proof-of-work blockchain, they must obtain control of a large amount of mining capacity. We can consider whether the attacker is obtaining mining capacity permanently or temporarily, and whether they are introducing new capacity into the system or capturing existing mining capacity. This yields four basic attack strategies:

Temporary control. Obtain new capacity: **Rent.** Obtain existing capacity: **Bribe.**
Permanent control. Obtain new capacity: **Build.** Obtain existing capacity: **Buy out.**

Note that an immediately that a difference emerges between three types of systems:

- For ASIC-dominated blockchains, such as Bitcoin, the rent strategy is not possible because there is a negligible amount of Bitcoin mining hardware that is not already dedicated to Bitcoin mining.
- For pure proof-of-stake blockchains, neither rent nor build are possible, as the "capacity" in the system is fixed.

We can make some initial observations about each approach.

Rental attacks (on Ethereum). Rental is only possible for commodity-hardware mined blockchains. Ethereum fits this description today as mining is dominated by graphics cards (GPUs). An attack would consist of renting a large amount of capacity from a system such as Amazon's Elastic Compute Cloud (EC2). Currently, EC2 rents NVIDIA K80 GPUs for about USD0.20 per hour at spot prices (bulk discounts are available), which can perform about 24 MH/s, a little more than 1 millionth of the Ethereum network hash rate. So, as a very rough estimate for about USD400,000/hr an attacker could rent enough hardware to perform a 51 percent attack on Ethereum. Presumably only a few hours of such an attack would be sufficient to cause a major loss in value to the system, which has a market cap of over USD2.5 billion. Thus, it appears that Ethereum is relatively vulnerable to Goldfinger attacks.

It is worth noting that GPU rental is relatively inefficient. Currently Ethereum miners earn roughly USD40,000/hr in block rewards, whereas renting this capacity on EC2 would cost 10x those rewards. This premium means, however, that the attack has no long-term risk for the attacker.

Building attacks. Consider the cost of building enough new mining capacity to subvert Bitcoin. We can take as a representative example the AntMiner S7, a recent ASIC miner. It retails for about US$500 and can perform nearly 5 TH/s. Conveniently, this is about one millionth of the network hash rate-implying an upfront capital cost of about $500 million to obtain enough hash power to perform a 51 percent attack on Bitcoin. Of course, this figure is very approximate and it would be far cheaper to buy this hardware in bulk. Still, it appears to be roughly 3 orders of magnitude more expensive to perform such an attack on Bitcoin than to perform the rental attack described above on Ethereum. Bitcoin's market cap is a little less than an order of magnitude higher, but this still implies a capacity-building attack is 2 orders of magnitude more expensive (not to mention considerably slower and more complex logistically) to execute. This is an argument in favor of ASIC-friendly mining puzzles.

As for building attacks on Ethereum, the most efficient GPU hardware available currently costs about USD10/MH/s, suggesting a cost of about USD200 million to build towards 51 percent capacity. Note that this is several times more expensive (relative to the market cap) than for Bitcoin. Perhaps more capacity has been built for Ethereum as it is recyclable.

Bribery attacks. Mechanisms for bribery attacks were considered by Bonneau (Bonneau 2016). There are several approaches, including direct bribery, running a mining pool that pays excess rewards, smart contracts which deliver payment, or leaving bribes available on an attacker's fork. It is difficult to estimate the premium an attacker would need to pay to break miner loyalty and convince them to work on a fork that would be highly detrimental to the system. With negligible premiums, bribery is very cheap, requiring only half of the rate of network rewards (about USD40,000/hr for Ethereum or USD100,000/hr for Bitcoin). Presumably, similar economics apply to proof-of-stake systems.

Buy-out attacks. Buy-out attacks would involve either purchasing mining capacity from current owners or purchasing currency (in a proof-of-stake system). The cost of such an attack appears straightforward. For proof-of-work systems, it should cost about half of the net present value of all future mining rewards (with a steepened discount rate due to reflect likely future growth in network capacity). For proof-of-stake systems, half of the value of the system must be bought up.

It appears that proof-of-stake systems are much more secure here, as the attacker must buy half of all value of the system, whereas with proof-of-work the attacker must only buy half of the future mining rewards (which must be strictly less valuable than the entire market cap). In this case the term "hostile takeover" seems appropriate.

In either case, there is an interesting possibility of a race to the door among current capacity owners. Imagine that an attacker credibly announces they will buy out half of all capacity and then use it to destroy the system. Current capacity owners will have a strong incentive to sell to avoid being left in the 49% which does not sell and hence loses everything. As they being to sell and the attack appears more likely to succeed (which is easy for the attacker to signal as the amount of capacity grows) this could lead to a death spiral of lowered prices and increased confidence the attack will succeed.

Commodity proof-of-work systems appear less likely to suffer from a race-to-the-door, since capacity owners who do not sell to the attacker can still sell their hardware even if the attack succeeds.

Countermeasures. For all of the attack models, there is the possibility of countermeasures by current capacity owners. Current owners can respond in kind to building, renting, or bribing. With buy-outs, they can attempt to set a market floor by offering to buy more capacity themselves. This may be a profitable strategy-if a race-to-the-door is in progress

which has lowered the value of capacity, it may be profitable to buy if the attack fails and prices rebound.

Note that an attacker may respond to a buy-out attack by building (or renting) new hardware. This may be a wise strategy for a coalition of miners who would otherwise be stuck with a worthless 49 percent mining share after a successful attack. This countermeasure is not possible for proof-of-stake systems, in which a successful buy-out attack will be permanent.

Comparison. At first glance, proof-of-stake systems appear less vulnerable to Goldfinger attacks. They are not vulnerable to rental or building attacks. Bribery attacks appear similar, while buy-out attacks appear strictly more difficult. However, proof-of-stake is more fragile in that building new capacity is not available as a countermeasure.

Commodity proof-of-work systems appear more resilient to buy-out attacks as a race to the door is less likely to develop. However, ASIC proof-of-work systems are not vulnerable to rental attacks.

Open questions.

- Is the cost of Goldfinger attacks a useful lower bound on the security of a given system?
- Is there a strict ordering between the three main types of system considered here in terms of resilience to Goldfinger attacks? Or are they incomparable?
- Which attack strategy is the most plausible in practice?
- Is there a minimum amount of reward miners should receive (relative to the market cap of the coin) for security purposes, to ensure the disincentive to sell is high? Or will this simply cause more capacity to be built?

3.3 Can Blockchain Be Used to Secure and Enhance Groupware Communication in a Distributed Messaging Environment?

Peter Eklund (IT University of Copenhagen, DK)

Abstract. For many years I worked with security and law enforcement agencies with fundamental requirements for secure communications. While there are few guarantees that communications will never be intercepted and decrypted, secure communication is largely ameliorated by RSA encryption (to various strengths), legislative policy and, in the modern era, by the shear volume of communications occurring. Researchers even now talk about pre- and postquantum secure encryption, so even super-computational adversaries are envisaged in the defense of encrypted systems.

Spoofing attacks on the other hand, where one or more parties in the communication masquerades as a trusted information source, can never be entirely eliminated with encryption alone. Spoofing has increasingly become a tool for criminals and oppositional (supra-)national cyber-agencies. Spoofing attacks have even been used militarily, to stealth field resources, and to feint the existence of field resources where they do not exist.

There are two main types of spoofing, IP spoofing [5], where the TCP/IP packets are intercepted and the 'man in the middle' replaces the IP address of the legitimate message with his own. Usually, IP spoofing occurs at the DNS level, so the DNS resolves an otherwise legitimate URL to a fake one1. IP spoofing is also the basis for denial of service attacks [1], where a host site is overwhelmed with pings from IP address which appear legitimate,

but are not. Interestingly, one way to overcome this is to use a massively distributed PP distributed network – like a P-to-P Napster topology – to fragment the message content and make direct interception only viable so far as intercepting a small fragment of an encrypted message.

Address Resolution spoofing is another form of spoofing [5]. The ARP (Address Resolution Protocol) is used in resolving spoofed IP addresses with Media Access Control or MAC addresses for data transmission. ARP spoofing occurs when the attacker transmits spoofed ARP communications across a local area network in an effort to link the interceptors MAC address to the IP address of a legitimate network user. Any information intended for that user's IP address will, when the technique is used successfully, be transmitted to the attacker, instead of legitimate intended recipient [5]. ARP spoofing is usually employed to steal data, modify it in transit, or for otherwise scrambling communications traffic on a LAN. The technique also enables denial-of-service and man-in-the-middle attacks as well as session hijacking. My research question is therefore, **"can blockchain be used to eliminate or minimize the risk of spoofing attacks in a communication network, and if they can be used what is the performance hit from using it?"**.

Together with a student of mine at the IT University of Copenhagen – the student has himself, as part of a startup activity, developed a groupware communication tool (http://dallr.com) – we are looking to compare the performance hit on the users in the communication environment by comparing three different implementations of the tool. The first is the existing tool wrapped in a VPN, the second is a version that uses proof-of-stake [4] and Tendermint (https://tendermint.com) as the blockchain middleware, and the final variant is a version of the tool running on the Ethereum blockchain (https://www.ethereum.org), using proof-of-work as the consensus mechanism.

The objective of our work is **'to show, by way of engineering a proofof-concept and software simulation, how performant the blockchain varients are with the VPN version. Namely, by introducing irrefutability and decentralisation from a proof-of-stake blockchain, we can achieve non-assailable spoofing security, but can we can do so in a away acceptable to the systems users'**. In this case, acceptable to the system users means that the performance overhead introduced by the blockchain middle-ware results in latencies of less than 200ms for a system of 1000 users [6]. The key empirical work here is to achieve 200ms latencies but to measure, at what actual cost? How many database servers, content servers and web-services infrastructure is required to make this work to latency goal, and what are their specifications (cost) of the architecture needed to achieve this timing?

Importantly also, if proof-of-stake is the consensus mechanism, there is necessarily some trade-off against the distributivity of the consensus provers across the blockchain, and likely therefore a more centralized control authority results. A secondary research question is therefore under the proof-ofstake a trade-off, does the system still exhibit the characteristics of true distributed consensus protocol, or is it it is more closely identified as a centralized authority?

References

1 Denial-of-service attack-detection techniques. IEEE Internet Computing, 10(1):82–89, 2006.
2 Daniel J. Bernstein. Introduction to post-quantum cryptography, pages 1–14. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.
3 Rita Boland. Military website spoofing is no laughing matter. SIGNAL Magazine, 2011.

4 Aggelos Kiayias, Ioannis Konstantinou, Alexander Russell, Bernardo Machado David, and Roman Oliynykov. A provably secure proof-of-stake blockchain protocol. IACR Cryptology ePrint Archive, 2016:889, 2016.
5 Andrew Lockhart. Network Security Hacks. O'Reilly and Associates, Inc., Sebastopol, CA, USA, 2004.
6 Fiona Fui-Hoon Nah. A study on tolerable waiting time: How long are web users willing to wait? In AMCIS, page 285. Association for Information Systems, 2003.
7 F. Valeur, G. Vigna, C. Kruegel, and R. A. Kemmerer. Comprehensive approach to intrusion detection alert correlation. IEEE Transactions on Dependable and Secure Computing, 1(3):146–169, July 2004.

3.4 Evolving the Social in the Socio-Technical System of Blockchain

John Leslie King (University of Michigan - Ann Arbor, US)

Abstract. Blockchain technology seems promising in its own right, and might be "disruptive." We have a poor track record predicting what new technologies mean over the long run, and an even poorer record knowing in advance what is truly disruptive. However, there is considerable experience with social evolution. Blockchain is already is a socio-technical system. Even if Blockchain technology enables changes in the social, prediction of technology is flawed. The evolution of some aspects of the socio-technical system is easier to predict. Often the social is more important than the technology in the evolution of the socio-technical system.

Blockchain technology has already had *some* important effects, as seen with the cybercurrendy Bitcoin. This illustrates that many social dimensions are unresolved. Central banks have deliberated on whether to permit use of the cybercurrency, with some prohibiting and some permitting. This paper covers four issues regarding the social evolution of the Socio-Technical System of Blockchain.

The Social Importance of Financial Systems. Financial systems – Blockchain's first large application area – has high social importance. Maintaining the stability of such systems is as important as the state's maintaining a monopoly on the use of force. Financial systems are vital to social welfare. Few national or regional banking authorities permit financial services without adherence to strict regulatory structures. An example is counterfeit, outlawed since ancient times and subject to harsh penalties. Suppression of counterfeit became more important by the advent of fiat money that has no intrinsic value (e.g., precious metal content). Laws prohibit fraud, manipulation, insider trading, and other behaviors considered damaging to financial systems. Financial authorities maintain "full faith and credit" as essential to a stable economy and society. Authorities and those they represent take this seriously. The legal framework for financial systems evolved with new technologies, usually with delay. The bigger the potential social change brought by technology, the longer the delay.

Understanding Trust. New technologies often bring new ways of looking at basic social issues such as trust. Trust is an ancient issue, recognized as important for millennia, but not well understood. Trust is tied to identity and verification, but we do not really understand how. We will learn more as Blockchain grows. There is an historical analog. Human capacity for natural language was deepened by efforts at natural language processing (NLP) by

computers. “Machine translation” (MT), or translating one natural language faithfully into another using computers, was in the early days of computers thought to be “just around the corner.” In the 1950s there was optimism that MT would be accomplished in one or two decades. Yet more than 60 years has passed and MT still has not delivered. MT is better than it once was, but it is not faithful. Human capability in natural language was shown by NLP to be far more sophisticated than the NLP experts imagined. Technology and techniques were no match for reality. MT might one day achieve its potential, but the ease with which humans do “natural” things masks how amazing those things are. We often do not realize this until we start trying to demonstrate that technology and technique can do such things. Technology and technique thereby become part of research efforts to understand these deeply “human” skills. Replacing them with automated aids might remain as an endeavor, but learning shifts to research.

The Socio-Technical Imperative. Technologies that affect human welfare through systemic effects reach far beyond “the technology.” A well-established example is combustion of fossil fuels in Carnot engines that exploit the heat gradient. Carnot engines enabled a significant part of the industrial revolution, primarily through external combustion, especially steam engines or transport as in ships and trains as well as manufacturing. Later there were internal combustion engines (e.g., gasoline and diesel engines and turbines) used in transport and to produce electricity. Much of the 19th and 20th centuries were devoted to finding sources of fossil fuels and operating the social systems to supply them and to defend those supply lines. Modern organization was constructed to provide the products and services made possible by Carnot engines. In the 21st Century much concern shifted to managing the by-products of combustion, especially as carbon has moved from the lithosphere to the atmosphere and made the “greenhouse” effect important in climate change. Similarly, long-term health and environmental effects have emerged around materials used in modern systems (e.g. chlorinated hydrocarbons, asbestos, dioxins, heavy metals like mercury and lead, and radioactive isotopes of elements such as strontium and plutonium). Technology became increasingly important to social welfare, and socio-technical systems evolved to provide subsidy (e.g. limits on possible liabilities from nuclear power generation mishaps), regulation (e.g., restriction of atmospheric and water pollution) and control (mandatory safety and risk mitigation actions). Many technologies now evolve socio-technical systems before they appear in the marketplace.

Management of Risk. Risk has become a determining factor, and effective risk management is required of any technical innovation. However, the context of risk has not remained fixed over time. At one time concern was limited largely to the capital at risk. Investors wanted to know what would happen under different possibilities: project failure, capital loss, inadequate investment return. Capital risk remains, but liabilities now include benefits and liabilities from the consequences of the original action that might materialize later, (e.g. intellectual property rights, health problems in offspring of those originally exposed to particular materials). Systemic future effects are taken into account to understand and manage the implications of new technology. Debates occur between those who want to buffer the downside on every foreseeable risk vs. those who wish to desire uninhibited innovation and argue that problems can be remedied after they occur. In the most extreme and cartoon-like of these debates, the former are characterized as Luddites who stand in the way of progress, while the latter are characterized as ignorant of problems that have arisen from new technologies that that created effects that could not be remedied (e.g., premature death) or that cost a great deal to remedy later.

Taken together these four issues will shape the evolution of Blockchain from a technological innovation into socio-technical systems. It is too late to keep Blockchain technology out of the socio-technical systems realm because the first major application of the technology has been to financial systems, Such systems are inevitably socio-technical. Financial authorities are vigilant, ready to take action on anything new, in part because the realm of finance has certainly inherently conservative aspects that deflect or slow down innovation, and in part because history shows instances in which the unscrupulous have exploited new technologies to take money from others by fraud. Blockchain will *never* escape the gravity well of socio-technical systems because it was first applied in an area that is inherently part of socio-technical systems. It's path has become set.

The evolution of the Blockchain socio-technical system will revolve at least in part around trust. Many – perhaps most or all – potential applications of Blockchain technology are to arenas where trust is important. Applications in finance entail the concept of "full faith and credit" and are inherently an institutional and social. Applications in health records, trade documentation, and so on are also institutional. Blockchain technologies cannot do away with trust issues because trust is embedded in social life and has been for a very long time. It might be part of what makes humans human (e.g., part of the genetic code), even if often manifested in social structures. However, Blockchain technology could, at least in principle, shift trust from institutional authorities to technology around scarcity, security and contracting. Blockchain uses blocks that are scarce (usually computationally so) and can therefore carry economic value. If the blocks and the links that connect them in a chain can be made secure, the system can be relied on. Blockchain retains a transparent and reliable record of transactions enabling binding contracts. This, in principle, enables distributed trust, but this trust is in the system rather than in the technology, per se. The scarcity issue might be covered adequately, but security (and therefore contracting) are less certain. The Bitcoin world has been "hacked" more than once, and people are confronted daily with evidence of unauthorized access to "cyber" systems, making Cybercurrency (or anything else cyber) suspect. As long as there is public uncertainty about security, most people will trust Blockchain only if a trusted institution serves as "residual claimant" on trouble. This extends beyond security to any threat to the technology, including limitations on scale, scope, or speed of operation. Some of these threats to Blockchain technology will materialize with use, and not before. We will not know they are issues until we encounter them.

The socio-technical imperative is reinforced by incumbents. Incumbents support continuity in existing systems, and will not embrace disruptions that will diminish their influence. The proponents of Blockchain are not incumbents with power, but are seen as "fringe" players. If Blockchain gains influence this will change over time. But it is not easy to change existing systems due to legal and regulatory apparatus that cannot be changed without time-consuming processes (e.g., allowing for public comment). Incumbents can also find ways to appropriate aspects of important new technologies, ensuring that they remain powerful in any new socio-technical regime. The popular discourse is replete with stories of how disruptive technologies have empowered the new and decimated the old, but a careful look at socio-technical system evolution suggests that incumbents are not easily replaced, while the new are easily recruited to become incumbents. That is, the "upstarts" become "incumbents" pretty quickly. Meet the new boss; same as the old boss.

Finally, risks seldom fall and remain disproportionately on those who cannot bear them. The larger institutional order that manages risk at the societal level will most likely manage risk in Blockchain applications. This is because social institutions protect other social institutions to permit risk to remain managed as in the past. For example, when the U.S.

insurance industry refused to insure nuclear power plants against all possible liabilities in the case of mishaps, the U.S. Congress stepped in with legislation that capped liability for nuclear power plant mishaps at levels far below what most experts recognized as potential liabilities. Thus, commercial insurance companies insured nuclear power plants. It is questionable whether online purchasing would have taken off as it has were credit card companies (and by extension, payment systems like PayPal built on the credit card system) bore the risks of fraudulent use of consumer accounts. Most consumers could use payment systems based on credit cards with essentially no risk. (This benefit has been generally extended to consumers for all such uses of these payment systems.) The risks inherent in Blockchain – and all important technologies carry risks – will be borne by institutions (e.g., the U.S. Federal Deposit Insurance Corporation in finance), or by new institutional agencies that cannot "walk away" from responsibility.

3.5 Open Source Software Research and Blockchain

Juho Lindman (University of Gothenburg / Chalmers UT, SE)

Abstract. This short paper investigates ways in which earlier open source software (OSS) research can help us explain blockchain-related phenomena. We review OSS literature and identify three such areas: 1) blockchain and OSS 2.0, 2) community development, and 3) forks.

Introduction. Earlier work on cryptocurrencies has used the openness of the software source code to decrease the risks of a system being perceived as a security black box and thus increase development trust. Both early examples of blockchain technology – Bitcoin and Ethereum – were open source projects. However, it should be noted that OSS is also contested in this context: There is an ongoing discussion regarding the importance of the source code openness and the underlying technological infrastructure. In this paper, we do not try to solve this issue but instead provide some insights OSS research may offer as blockchain moves forward.

Blockchain and OSS 2.0. We investigate Bitcoin and Ethereum as examples of blockchain technology. Bitcoin (protocol and crypto-currency) was introduced in 2008 and implemented as an open source project [6]. Later, the Bitcoin Foundation was founded to support development efforts [10] that rely on the global OSS developer community. Ethereum was introduced in 2013. The main driver was the disagreements concerning what kinds of scripting to include in Bitcoin to enable smart contracts. Ethereum quickly attracted a large following.

Discussion regarding open and openness gained a boost in 1999 when a group of OSS proponents, including Eric Raymond (1999) and Bruce Perens (1999), decided to increase OSS credibility. Their literature led to a fertile but contested research terrain tightly coupled with the increased industrial engagement of OSS by commercial companies [15]. The result was a steady increases in the industrial use of OSS [3] and OSS-like practices for software production (Linden et al., 2009). Over time, the tools and practices related to OSS changed (for example, from Sourceforge to GitHub(s) and intranet-based implementations of OSS). Ultimately, even the most critical voices found themselves engaged with OSS (for example, Microsoft joined the Linux Foundation on Nov 16, 2016).

Thus, OSS 2.0 relies on commercial involvement [3], but enthusiasm around Bitcoin / Ethereum from companies, entrepreneurs, and industries grew quickly compared to similar earlier developments in other OSS projects. One of the reasons is quite obvious: Blockchain proponents understood early that the developer community would need help from the cryptocurrency users, vendors, and intermediaries or the network to grow and to realize benefits.

Another interesting similarity between OSS and Blockchain is the strong political polarization of these innovations, not unlike what happened with the first free software vs. commercial software and then free software vs. OSS in the 90s [15]. Many early enthusiasts for OSS and Blockchain were motivated by the "bazaar-style" radical decentralization of the technology (often motivated by liberal political philosophy). In OSS, the divergent interest of incumbent companies and volunteer communities was identified – and at least partly solved – using different kinds of OSS 2.0 approaches.

Community-driven development. Research in open platforms [11, 4] and in "openness" [1] provide useful starting points to discuss Blockchain. Openplatforms literature discusses third party participation in design, and the key elements to this are boundary resources.

Open source research has discussed OSS governance of the development communities, meaning OSS project direction, control, and coordination [8]. The governance consists of three literature streams: 1) different incentives for independent developers to participate in open efforts (for example, [5], 2) efforts to provide support for the coordination activities (for example, [2]), and 3) encourage building a welcoming culture [8].

Forks. Forks have been a topic of research for some time in OSS [7]. There is variation in how the term is used, but usually fork means a situation where the developer community disagrees on the development roadmap (or a different focal issue), and this results in a situation where several different competing and backward-incompatible versions of the code base are in use.

In most open source projects, forks are both a safeguard of openness and detrimental to the development efforts because they dilute contributions and developers during the different versions (Fogel 2006: 88, Moody 2009). Viseur (2012) found the majority of forks studied were motivated by a need for technical specialization, and forks rarely were followed by the extinction of the original. Robles and González-Barahona (2012) claimed, based on an in-depth analysis of 220 forks, that they take place in all software domains, can be friendly or competitive, and have become more frequent in recent years. For example, Ethereum has undergone already four so-called hard forks (backwardincompatible), so this research is becoming pivotal again.

Summary. OSS research offers several insights that may be usable in Blockchain context regarding how to solve different kinds of tension between voluntary communities and commercial companies. The artefact's openness is obviously an interesting point of departure, but more critical questions may be related to guaranteeing the incentives of the different actors and matching divergent interests. The re-emergence of forks also raises questions where OSS may provide some analytical tools for discussion.

References

1 Aksulu, A. and M. Wade (2010). "A comprehensive review and synthesis of open source research." Journal of the Association for Information Systems 11(11): 576.

2 Crowston, K., et al. (2005). "Coordination of free/libre and open source software development."
3 Fitzgerald, B. (2006). The Transformation of Open Source Software. MIS Quarterly, 30, 3, 587-598.
4 Ghazawneh, A. and O. Henfridsson (2013). "Balancing platform control and external contribution in third-party development: the boundary resources model." Information Systems Journal 23(2): 173-192.
5 Lerner, J. and Tirole, J. (2002). Some Simple Economics of Open Source. Journal of Industrial Economics, 50, 2, 197-234, June.
6 Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
7 Nyman, L. (2015). Understanding Code Forking in Open Source Software: An examination of code forking, its effect on open source software, and how it is viewed and practiced by developers. Helsinki, Finland, Hanken School of Economics.
8 Markus, M. L. (2007). "The governance of free/open source software projects: monolithic, multidimensional, or configurational?" Journal of Management and Governance 11(2): 151-163.
9 erens, B. (1999). The Open Source Definition. In: Dibona, C. and Ockman, S. (eds.). Open Sources: Voices from the Open Source Revolution. O'Reilly Media, Sebastopol, CA.
10 Teigland, R., et al. (2013). "Breaking out of the bank in Europe-exploring collective emergent institutional entrepreneurship through bitcoin."
11 Tiwana, A., et al. (2010). "Research commentary-Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics." Information systems research 21(4): 675-687.
12 aymond, E. (1999). The Cathedral and The Bazaar – Musings On Linux And Open Source By An Accidental Revolutionary. O'Reilly Associates, Sebastopol, CA.
13 obles, G. and González-Barahona, J. (2012) A Comprehensive Study of Software Forks: Dates, Reasons, and Outcomes. Proceedings of the 8th IFIP WG 2.13 International Conference, OSS 2012, Hammamet, Tunisia.
14 Viseur, R. (2012) Forks impacts and motivations in free and open source projects. International Journal of Advanced Computer Science and Applications, Vol. 3, No. 2.
15 Weber, S. (2004). The Success of Open Source. Harvard University Press, Harvard, MA.

3.6 Blockchain-Enhanced Trust in International Trade

Gerhard Schwabe (Universität Zürich, CH)

Abstract. Many industries struggle to improve the processes, which involve large volumes of exchanged documents between different untrusted organizations. While transporting goods, monetary payments are needed. To enable these payments and ensure that the goods are transported, financial institutions play an intermediary role in relationships between buyers and sellers. Managing payment processes for trade includes the process of document exchange (e.g. invoices, insurance certificates, shipment documentation, etc.) between different organizations, while sold goods are on their way from the seller to the buyer. These processes become more cumbersome and their complexity increases if transactions cross national borders. International trade for goods and services accounted for more than USD24 trillion USD in 2014 (World Trade Organization 2015). By its very nature, trade can feature several interactions between previously unknown, untrusted third parties. In addition to the

potential trust issue between buyer and seller, several intermediate entities might be involved in the process. Every additional intermediary increases the risk of process delays or fraud, and also causes higher processing costs for collection, verification and coordination of the required documentation. Fraud risks are exasperated by lacking coherent overarching legal rules and law enforcement mechanisms.

Introduction. Many industries struggle to improve the processes, which involve large volumes of exchanged documents between different untrusted organizations. While transporting goods, monetary payments are needed. To enable these payments and ensure that the goods are transported, financial institutions play an intermediary role in relationships between buyers and sellers. Managing payment processes for trade includes the process of document exchange (e.g. invoices, insurance certificates, shipment documentation, etc.) between different organizations, while sold goods are on their way from the seller to the buyer. These processes become more cumbersome and their complexity increases if transactions cross national borders. International trade for goods and services accounted for more than 24 trillion USD in 2014 (World Trade Organization 2015). By its very nature, trade can feature several interactions between previously unknown, untrusted third parties. In addition to the potential trust issue between buyer and seller, several intermediate entities might be involved in the process. Every additional intermediary increases the risk of process delays or fraud, and also causes higher processing costs for collection, verification and coordination of the required documentation. Fraud risks are exasperated by lacking coherent overarching legal rules and law enforcement mechanisms. As a best practice today, payment transactions between untrusted sellers and buyers are often facilitated through a letter of credit (LoC). A LoC is "an agreement that the bank of the buyer, called the issuing bank, will arrange a credit to guarantee payment as soon as the supplier can prove that the goods have been shipped" (Hulstijn and van der Torre 2005). Such inefficiencies as delays, paper-heaviness, lack of trust between the intermediary organizations, as well as risks of fraud hamper the overall process of trade. In order to let organizations, which are exposed to lack of trust, work together effectively, interorganizational trust has to be established. However, the more stakeholders are involved into the process, the less inter-organizational trust exists: they have not enough knowledge to trust each other, they are based in different countries with different legal systems, the working partners change often, etc.

The process is very costly, bears the risk delaying the shipment, and relies on trust established by a third party, such as banks. Blockchain technology is often seen as a disruptive way to transform processes that rely on a trusted third party into a much leaner, decentralized and automated form. In our research, we follow the goal to explore the potential of blockchain technology and smart contracts for international trade at the example of a LoC. Thus, we look how blockchain technology can be used to enhance trust in international trade.

We follow a Design Science Research (DSR) methodology (Hevner et al. 2004; Gregor and Hevner 2013; Nunamaker et al. 2015). Our key contribution is an explanatory design theory (Baskerville and Pries-Heje 2010) for enhancing trust in international trade at the example of a Letter of Credit. We built a prototype for a blockchain based LoC (called BLOC) and validated it in several rounds in dialogue with representatives from a leading logistics company and four Swiss banks. By doing so, we contribute to scientific discourse on blockchain technology and its applications and explore how a blockchain-based system may replace the trust in the monetary processes in the domain of trade finance. Furthermore, we bring value and useful knowledge to practitioners who face the problem of working with large numbers of documents, which should be created, accessed or amended by different parties, and also be tamperproof.

Related work. International trade has been always considered as an important driver of global prosperity. Since in international trade, business partners often lack reciprocal trust, currently an effort must be made to establish the exact financial terms between an importer and an exporter (Antras and Foley 2011). This relationship between importers and exporters can be handled without any mediation (Antras and Foley 2011). However, if the stakes are high, the process is often intermediated by banks on both sides, and the process can also involve more actors (e.g., an insurance, a carrier), which influence the whole process of contract execution. If there was trust between all involved stakeholders, such transaction costs could be avoided, since they would render these activities unnecessary. Trust is a crucial component for successful transactions regardless of whether they are executed in a physical or virtual space (e.g., online marketplaces) (Son et al. 2006).

Due to the nature of international trade, we regard the lack of inter-organizational trust to be unavoidable. However, we argue that to a large extent, inter-organizational trust could be replaced with mutual trust in an IT artefact. While there may be genuine trust in the blockchain technology itself, on an application level, trust in IT artefacts rarely appears in isolation. It rather must be viewed in conjunction with the trustworthiness of other actors in a 'trust network', most importantly the provider of the technology (Söllner et al. 2016). There can be a trust transfer in both directions: the application of a trustworthy artefact may enhance the trustworthiness of the provider and vice versa.

In our study, we propose a design solution, which is based on the blockchain technology and in particular the concept of smart contracts. By the year 2016, the blockchain technology has received significant attention both by researchers and practitioners, and is often considered to bear the potential for a technological revolution not only in the field of FinTech, but in any other domain that might benefit from a secure and trustworthy history of events or data records. From a technical perspective, the technology of blockchain represents a distributed ledger, which allows the users of the network to agree following the concept of consensus and, therefore, build trustless agreement which exclude possible intermediaries from the process. Due to these properties, the Ethereum blockchain appears to be a promising technological basis for creating an IT artefact in which multiple stakeholders can trust as a substitute for lacking inter-organizational trust.

Exploring the proposed solution. In our work, we developed a system that replaces inter-organizational trust by trust in a blockchainbased IT artefact, and thus facilitates trade administration between parties that otherwise have no means to trust each other. To solve this, our architecture and BLOC incorporate multiple features that support the establishment of trust in IT according to prior work (Söllner et al. 2012). In fact, the blockchain technology itself delivers multiple such characteristics off the shelf. One of those properties is transparency, since all data on the blockchain are public by default, which makes it possible for anyone to read all data stored on the blockchain. In addition, it can be argued that public blockchain implementations have a benevolent operator, since they are run entirely decentralized, i.e. due to the absence of a controlling operator, there is no possibility of a non-benevolent operator. Even though the prototypical solution was kept very simple by design, and did not map the business logic that exhibits anything remotely close to the complexity of real-world processes in the investigated domain, the experts confirmed that all business requirements for solving the investigated problem were met. They were also confident that a solution such as the one proposed could be developed or integrated into a more generic, scalable business process support platform, which could be used even in a real-world context.

First, from the technological point of view the blockchain technology itself shows potential for several use cases in the domain of international trade, as it can eliminate fraud issues, and overcome issues the result from a lack of trust when dealing with unknown counterparties.

Moreover, the nature of smart contacts, as self-executable programs, could bring value to the business and significantly automate the overall process and, therefore, reduce transaction and administrative costs. Two interview partners even admitted for LoC to be a relatively unattractive product for their respective banks, which they might readily stop to offer if they could safely do so without losing customers for more profitable areas of business. Bearing this in mind, their openness towards automation of the LoC process with a blockchain-enabled solution is not surprising.

Second, the immutability of the information saved in the blockchain is beneficial in a way that the origin of the documents, and any amendments in the document flow could be tracked. This increases the transparency of the process, and thus creates trust in the information system. Therefore, blockchain can be used to compensate for the missing trust in the inter-organizational relationship. However, the blockchain technology is relatively new, and development of applications on its basis still have experimental character, therefore, it is not sufficiently clear where its boundaries are and in which use cases blockchain can unfold its full potential. Critics might point out that transaction costs and throughput with blockchain might not yet be ready for enterprise-grade applications. Other researchers have gathered first evidence regarding the transaction costs and throughput on the Ethereum blockchain, discussing the trade-offs regarding costs, trustworthiness and latency of the public Ethereum blockchain as compared to private instances (Weber et al. 2016). We are therefore confident that the current performance limitations of blockchain will be solved in the future. Our work seeks to solve the problems inherent to storing and exchanging documents required for complex processes across multiple organizational boundaries, and often spanning multiple languages and legal frameworks. In addition to offering a solution to the practical problem, this research also illustrates a use case for distributed ledger technologies outside the realm of financial transactions (as seen in the Bitcoin blockchain), particularly with Ethereum's blockchain implementation and its smart contract feature.

In environments where stakeholders have no means to trust each other, as regularly encountered in the domain of international trade, designing IT artefacts that replace inter-organizational trust with trust in the IT artefact itself, is crucial for the involved parties to benefit from the same transaction cost reduction.

We argue that the blockchain technology includes features necessary for creating trust in an information system and, therefore, addresses and has potential to resolve at least several of above discussed challenges, namely many unknown stakeholders, fraud and a missing common framework, lack of transparency, and different IT capabilities. Considering the relatively young, and not entirely uncontroversial history of Ethereum and blockchain, it can be argued whether or not the technology itself is trustworthy for a specific purpose. Therefore, it is essential to consider carefully, in which cases the use of blockchain makes sense, and where another technology with different properties might be advantageous.

We conclude that the LoC process still faces important challenges, which we set out to solve using a DSR approach. In particular, current LoC processes still display inefficiencies like being paper-heavy processes, including manual processing of transactions, and risks which hamper the trade finance sector. We propose a blockchain-based design theory to eliminate the problems related to the lack of trust in inter-organizational processes in the domain of international trade. Moreover, we conclude that such an architecture would be beneficial for any domain that involves a large number of the documents in a supply chain or workflow, with many stakeholders that are geographically distributed, and particularly when fraud is a potential issue.

Limitations and future work. We did not make observations of how the process is going on in detail from perspectives of different parties (banks, carriers, insurance companies, etc.). This task does not seem trivial because of the nature of the process, as it refers to cross-border shipments and relationships between organizations which are located in different countries.

We believe that the insights from this study can bring a valuable contribution as it highlights the problems in the trade finance industry which are similar to processes from other areas (for example, in logistics, energy sector, medical sector, etc.). In doing so, we bring a better understanding of the issues in inter-organizational relationships, and discuss opportunities and challenges for the application of the blockchain technology in this scenario. We see a high potential in developing studies also in other domains and testing whether the formulated design theory holds up there, too.

Furthermore, the external validity of the study should be improved, this should be addressed in the future research activities. Therefore, we would also like to inspire the researchers to make their impact into the research on blockchain considering a large variety of aspects, from underlying cryptology and its limitations to ecosystems.

References

1 Antras P, Foley CF (2011) Poultry in motion: a study of international trade finance practices. National Bureau of Economic Research
2 Baskerville R, Pries-Heje J (2010) Explanatory design theory. Business and Information Systems Engineering 2:271–282.
3 Gregor S, Hevner AR (2013) Positioning and Presenting Design Science Research for Maximum Impact. MIS Quarterly 37:337–355. doi: 10.2753/MIS0742-1222240302
4 Hevner AR, March ST, Park J, Ram S (2004) Design Science in Information Systems Research. MIS Quarterly 28:75–105. doi: 10.2307/25148625
5 Hulstijn J, van der Torre L (2005) Analyzing Control Trust in Normative Multiagent Systems. BLED 2005 Proceedings 6.
6 Nunamaker JF, Briggs RO, Derrick DC, Schwabe G (2015) The Last Research Mile: Achieving Both Rigor and Relevance in Information Systems Research. Journal of Management Information Systems 32:10–47. doi: 10.1080/07421222.2015.1094961
7 Söllner M, Hoffmann A, Hoffmann H, Wacker A, Leimeister JM (2012) Understanding the formation of trust in IT artifacts. Association for Information Systems,
8 Söllner M, Hoffmann A, Leimeister JM (2016) Why different trust relationships matter for information systems users. European Journal of Information Systems 25:274–287.
9 Son J-Y, Tu L, Benbasat I (2006) A descriptive content analysis of trust-building measures in B2B electronic marketplaces. Communications of the Association for Information Systems 18:6.
10 Weber I, Xu X, Riveret R, Governatori G, Ponomarev A, Mendling J (2016) Untrusted business process monitoring and execution using blockchain. In: International Conference on Business Process Management. Springer, pp 329–347
11 World Trade Organization (2015) International Trade Statistics 2015.

3.7 Autonomous pension funds on the blockchain

Peter Sestoft (IT University of Copenhagen, DK)

Abstract. We propose that life-based pension funds, such as those that pay a whole life annuity, can be fully autonomous and operate without a central trusted pension fund. In particular, payments and benefits, asset management, and estimation of liabilities (reserves, discounted future cash flows) can in principle be implemented using self-executing contracts, for instance on a blockchain infrastructure such as Ethereum.

Core activities of a pension fund. We consider life-based insurance-style pension funds, such as those that pay a whole life insurance: a guaranteed income stream to the insured person from retirement age until his or her death.

A pension fund comprises the following activities: (a) Enter contracts with pension customers; (b) receive a stream of payments from active, eg. working, pension customers; (c) pay a stream of benefits to retired and disabled pension customers; (d) regularly send forecasts to pension customers of their expected future benefits based on the contracts and the payments made; (e) invest and manage the assets that result from payments minus benefits; (f) regularly report to regulators to demonstrate that assets are suf- ficient to cover liabilities, namely, the obligations to pension customers; (g) pay taxes on the payments and benefits streams; (h) in general, react to life events, notably disability, retirement and death, of the pension customers.

Autonomous pension funds. We propose that all of these activities may be implemented using selfexecuting contracts on a distributed ledger such as Ethereum, and discuss some of the concerns raised by and requirements for implementing this idea. We might call an organization, or distributed algorithm, along these lines an autonomous pension fund (APF). We argue that it is technically feasible to create such an entity as an autonomous organization:

- Activities (b), (c) and (g) are mainly processing of contract-regulated payments and seem clearly implementable using self-executing contracts and a cryptocurrency.
- Activities (d) and (f) can be based on the highly developed actuarial mathematics in the Scandinavian/German tradition, typically formalized with stochastic state models and Thiele's differential equations. This approach can be implemented and operationalized in software in a very general form, as evidenced by eg. Edlund's Actulus Portfolio Calculator.
- Activity (e) could be run in the manner of TheDAO on Ethereum (though preferably without the mistakes and vulnerabilities). How to invest the assets can be decided by voting, with automatically imposed limits on composition (expected return, risk, maturity, . . .) of the investments, to match them to the liabilities as forecast using actuarial mathematics.
- Activity (h) depends on insurance-related life status and events being reportable in a trustworthy and automated way, so that self-executing contracts can act on them. This is very nearly the case in much of northern Europe. Life status includes gender, age, marital status, citizenship and tax status; and life events include retirement, becoming unemployed, becoming disabled, retiring, recovering from these events, and death.
- The life-based pension contracts mentioned in (a) can be formalized in a domain-specific language, that is then used in (b), (c), (d), (f), (g) and (h), and in constraining the investment decisions in (e) so that the asset composition matches the expected obligations. Namely, given such formal pension contracts, one can compute expected future cashflows,

discounted expected obligations (reserve) and risk of default (as per EU Solvency 2 requirements); and one can generate pension forecasts, distribute monthly payments (into the fund) on pension products, compute monthly benefits, and more. A prototype of such a domain-specific language has developed, though not for blockchain use, in a collaboration between the company Edlund A/S, Copenhagen University, and the IT University of Copenhagen.

- Life-based insurance and pension operate on more "objective" states (active, disabled, retired, dead) of the insured than most property insurance, where more human work is needed to assess the degree of damage, counter insurance fraud, and so on. Hence life-based insurance and pension are amenable to a larger degree of automation than is property insurance.

Challenges and advantages. Some crucial questions and concerns about the practical feasibility of an autonomous pension fund include:

- Pension promises are extremely long-term obligations. A 25-year old woman entering the labor market in 2017 may retire in 2062 and may expect to rely on her pension income until 2087 or even longer. What reasons does she have to trust that the autonomous pension fund keeps it promises, or even exists, over such a long time span? Clearly, regulation plays a role here, but so does trust in the technology
- Pension funds are heavily regulated, nationally (in highly countryspecific ways) and internationally (eg. EU Solvency 2). This is both to reassure pension customers the pension funds are able to fulfil their promises, and to ensure that the pension products they sell agree with tax regulation.
- What pension products are preferred by customers is considerably in- fluenced by what tax deductions they offer, and by what pension products are mandated eg. in general labor market agreements ("overenskomster"). Thus products offered by the autonomous pension should be certified by tax authorities to allow for expected deductions and to satisfy the general requirements.
- An autonomous pension fund would avoid many of the costs of commercial pension funds, such as those owned by banks whose shareholders expect a return on their investments. Even the many Danish pension funds that are customer-owned (such as most labor market funds, PFA, ...) and in general very efficient, have non-negligible costs. Danish pension funds manage approximately 500 billion Euro, corresponding to 1.6 times annual GDP, and with such large amounts of money under management, even small inefficiencies translate into large absolute costs.

References

1 The DAO of accrue. A new, automated investment fund has attracted stacks of digital money. The Economist. May 21st 2016.
2 Christiansen, Grue, Niss, Sestoft, Sigtryggsson: An Actuarial Programming Language for Life Insurance and Pensions. International Congress for Actuaries 2014, Washington DC.
3 Edlund Actulus Portfolio Calculator, https://edlund.dk/loesninger/actulus
4 DIRECTIVE 2009/138/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).
5 Emin Gun Sirer: Thoughts on The DAO Hack, blog post 17 June 2016, http://hackingdistributed.com/2016/06/17/thoughts-on-the-dao-hack/

3.8 De-hyping DLT and Pragmatic Use of DLT in Banking

Udo Milkau

Abstract. Some authors of well selling books such as Don and Alex Tapscott assign tremendous potentials to blockchain, the technology underlying Bitcoin. Blockchain - or technically: Decentralized Ledger Technology (DLT) - is recognised as a "truly open", distributed and "democratic", and "immutable" platform that fundamentally changes what we can do online, how we do it, and who can participate. According to their views, the new technology facilitates peer-to-peer transactions without any intermediary such as bank or governing body. Accordingly they titled their latest book (2016) "Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World". However, a practitioner in a bank has to ask three questions:

1. What problem is the technology solving and what is the economic benefit?
2. What changes in business models can be catalysed and/or triggered by DLT?
3. And the third question is what social benefit can be provided by DLT?

This Provocation Paper will briefly discuss those three questions and try to "de-hype" the technology behind blockchain from the point of view of tangible real-world implementations.

Evolution and Taxonomy of Blockchain and Distributed Ledger Technology. The original idea of Satoshi Nakamoto's concept paper (pseudonym, 2008) was to develop Bitcoin as "A Peer-to-Peer Electronic Cash System" with the blockchain as the combination of existing technologies as underlying platform to solve this one and only problem. This issue is related to two well-known problems in distributed computing:

- The Byzantine Generals Problem, describing issues in establishing a secure synchronisation of participants, who exchange messages e.g. payment transactions, in a distributed network of unknown nodes, which cannot be trusted ex-ante.
- The Double Spending Problem, meaning the possibility to spend electronic cash (as a sequence of zero's and one's) twice by broadcasting multiple malicious transactions into a distributed network without any central entity that keeps track of the state of the network by providing a central "clock" to validate the correct sequence of transactions (original vs. copy).

A list of examples for the re-used technological building blocks is given in Table 1. Nevertheless, a key for the solution for "Electronic Cash" was the change of paradigm as Bitcoin applies a game theoretical approach with the selection of one neutral referee to achieve distributed consensus. This "blockchain" – in the original design for Bitcoin – comes with a number of assumptions and limitations: It is a closed-loop, repeated game played by peers without any hierarchy, but also without any generic link to the physical world (such as e.g. represented by central bank money).

It is a probabilistic system with only eventual consistency (see e.g. Decker und Wattenhofer, 2013). In principle, eventual consistency is not new to banking and accounting (!), but has to be understood. It is based on a number of technological parameters, which - by design - make the Bitcoin blockchain inefficient and very costly, slow and with limited capacity, and fully readable or transparent (as contradiction to "anonymous" physical cash).

The original design of the Bitcoin blockchain is an alternative model for payments, which has to be compared and to compete with (i) traditional payment transactions between interoperable banks based on fiat / central bank money and (ii) centralised platforms such

as e.g. PayPal, American Express or Western Union, which perform and book payments internally, and have interfaces to the outside world and the two sides of the market (typically merchants and consumers).

The development of the original Bitcoin blockchain is shown in Figure 1. Without going into the details, the actual Bitcoin ecosystem departed significantly from design and assumptions. Today, the Bitcoin "processing" is centralised in four - and interconnected - "mining pools" representing 80 percent of the hashing power as a proxy for the contribution to the system; and the formal and/or informal governance is concentrated at a handful of "core developers". Additionally, Bitcoin users do not want to run a payment system at all – they want to pay and – for certain reasons – use a means of payments comparable to PayPal, AliPay, VISA, MasterCard, iDEAL, paydirekt et cetera. Last but not least, attempts to give Bitcoins some "official" painting were unsuccessful1 due to insufficient asset protection.

It can be discussed, whether Bitcoin is in a dead-end road. Nevertheless, a number of derivatives of the original blockchain approach have been developed. Figure 1 is an attempt to compile the taxonomy of the current development, but has to be limited on major trends of the development. First, one finds a rather nice oxymoron with the proposals for "central bank digital currencies" based on blockchain. However without a link to settle transaction in central bank money - e.g. securities transactions or trade finance businesses – a blockchain would be limited to closed-loop systems. Second, a number of developments have been proposed to improve some of the deficits of Bitcoins. One example is the implementation of "off-chain channels" for transactions (such as duplex micropayment channels), and the other one is additional anonymity by "zero knowledge" (which in turn has assumptions and limitations by itself).

Third, extensions have been made to include "smart contracts", i.e. tuning complete scripts to represent a state machine, to the blockchain. In an open "public" blockchain approach, the replication of the distributed database including those "stored procedures" results in a global state machine running on all nodes with all readable scripts and all transactions in parallel. Although many enthusiast seem to be fascinated by such public programmable blockchains like Ethereum (and many others), Ethereum is an example for more forks of the development with (i) an announced change from "proof-of-work" to a new consensus model called "Casper" and (ii) the foundation of a "private" Ethereum Enterprise Alliance end of Feb. 2017.

Fourth, a number of commercial initiatives focussed on permissioned consensus protocols (without distributed ledgers), e.g. Ripple with the "Interledger Protocoll" or the R3 consortium with Corda™, which is "inspired by the blockchain".

Fifth, SWIFT as traditional payment network between interoperable banks is testing DLT based on the open source "Hyperledger" in the framework of its Global Payment Initiative (GPI). As all those trends (and many more) are derivatives of the original set of building blocks of the blockchain, the practical question for use of DLT in banking will be:

How can some building blocks (technology and game theory; as e.g. illustrated in Table 1) be combined to solve actual business problems and do those solutions provide advantages compared with more "traditional" elements by an economic evaluation of costs, quality-of-service, speed, or security and cyber resilience?

From "Code is Technology" to "Code is Law – Layers of Business Processes. The original concept of Bitcoin blockchain can be described as a distributed "golden record" for the rights to transfer a token (representing "electronic cash" in a closed-loop peer-to-peer system). Concerning the extension of "smart contracts", one can e.g. find the following definition on the webside of www.ethereum.org:

"Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference. These apps run on a custom built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property. This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middle man or counterparty risk." (accessed: 11.3.2017)

Applying a reality check on this statement, one can find some critical constrains:

- applications Yes, i.e. computer code, scripts, stored procedures et cetera!
- run exactly as programmed4 But who will corrects code errors in the future during the life cycle of a "smart contract"?
- without any possibility [=] third party interference But with possible interference of "peers" as demonstrated during the so called "The DAO" hack!
- represent the ownership of property [and] move funds But any ownership (and legal transfer) depends on the applicable legal framework such as e.g. securities law legislation and the access to funds as legal tender!
- without counterparty risk No, as any contract with a promise of repayment in the future (loan, mortgage, bond, promissory note et cetera) will have a counterparty risk in general (and "escrow" would be a contradictio in adiecto to any credit arrangement)!

That constrains reveal that technology is only one layer in a contractual relationship (although the terminology "smart contracts" entails a misunderstanding about the capabilities of a piece of computer code). Figure 2 provides a schematically structure of the different layers from "technology" to "law"5 and "risk". In between "governance" and "standards" are needed to handle to dynamic aspect of any non-trivial computer code (with errors to be corrected and changes to be made during the life cycle of the code) and to provide lingua franca for all participants in a network industry.

With the right understanding about possibilities and constrains of a new computer technology, DLT can be the trigger or catalyst for industry-wide or even cross-industry discussions and development of "distributed" business processes and "networked" business models. One historical example for an innovation, which triggered the development of law over centuries in different countries, is securities law legislation. Starting with the "technology" of tradable shares as "securities" based on paper documents, new legal concepts of the representation of ownership ("shareholding") developed. This process is still ongoing, as the European harmonisation of the Securities Law Legislation is one of the Giovannini barriers to be worked on.

The "inspiration by blockchain" and discussion about business models in the 21st century may be the largest efficiency gain, the blockchain will bring to financial services in the future.

The Blockchain as a Sociology Experiment. The question "Cui bono" from the discussion about DLT, could be answered very lightly: For the time being writers, consultants, and careerists in financial services have a measurable benefit. Nevertheless, DLT concerns some basic questions of the "digital" society in the 21st century. Maybe, it is merely a temporal correlation by chance, but the concept paper by the pseudonym "Satoshi Nakamoto" was written in 2008 at the peak of the global financial crisis (triggered by the preceding sub-prime mortgage crisis). The idea of (electronic) cash without any intermediaries including banks and central banks is far from being new. Friedrich August von Hayek demanded in his book "Denationalisation of Money" (1976) an end to the monopoly of governments on (central

bank) money and proposed a competition, as entrepreneurs should be permitted to innovate in the monetary sector, such as by creating "neutral" currencies or minting commodity money?

The second question is related to the first one, a competition of currencies could once more lead to monopolies – especially if we remember the development of the Bitcoin systems from a peer-to-peer network to an onion-like hierarchy. Joi Ito pointed out: "[T]here is currently centralisation in the form of mining pools and core development, [but] the protocol is fundamentally designed to need decentralisation to function at all." (Ito, 2015) Therefore, research is needed to understand the dynamic development of networks in competition, and especially of social networks. The third issue is the question of the "costs of trust". Niklas Luhmann wrote his seminal book "Vertrauen: ein Mechanismus der Reduktion sozialer Komplexität" in 1968. Regarding "trust is a mechanism to reduce social complexity", trust provides a reduction in transaction costs and has an economic benefit. The substitution of trust of "permissionless" blockchains like Bitcoin comes with associated costs leading to the question of a desirable social optimum in a balance between trust and technology.

A last questions concerns the motivation of those promoters of "smart contracts" claiming that "Code is Law" would be an improvement to the current contract law (in the different versions of diverse legal legacies). From the author's point of view, this "mechanistic conception" of the world is an expression of the wish to avoid the uncertainty and complexity of the 21st century and to turn back the wheel to a reductionist concept as e.g. expressed by Frederick Winslow Taylor in his book "Priciples of Scientific Management" of 1911 based on his experiences of the business practices of the 19th century. All the more, it is very strange that a keynote speaker at a payment conference explained – obviously without any sarcasm – [quote David G.W. Birch, 9.3.2017)

"The blockchain is the solution to our problems [in financial industry]" "In fact, it's the solution to most industries' problems" "The blockchain is a religion"

Conclusion. For a rational discussion about measurable benefits, it seems to be necessary to "de-hype" DLT. The technology itself can provide advantages – such as e.g. demonstrated in a transatlantic payment transaction in eight seconds between ATB Financial, Calgary and ReiseBank, Frankfurt in 2016. However, DLT has to be compared with other existing technologies in cost-benefit analysis.

Beyond technology, the discussion about DLT can be a catalyst for new business processes, business models, or even further development of legislation. Bringing partners from different industries and government together to develop more efficient and holistic cross-industry solutions would be highly appreciated – even though the final technology would be merely "inspired by blockchain".

Finally, DLT is linked to a number of issues, which are important for social benefit in the 21st century.

Further research about the motivation behind "blockchain" could a helpful to analyze expectations, wishes, and fears about the "digital society" of the future.

References

1 Tapscott D., and Tapscott A. (2016) "Blockchain Revolution: how the technology behind bitcoin is changing money, business, and the world", Penguin, 2016.
2 "Satoshi Nakamoto" (pseudonym, 2008) "Bitcoin: A Peer-to-Peer Electronic Cash System", available at: http://bitcoin.org/bitcoin.pdf
3 Akkoyunlu, E.A., Ekanadham, K. and Huber, R.V. (1975) "Some Constraints and Trade-offs in the Design of Network Communications", SOSP '75 Proceedings of the fifth ACM

symposium on Operating systems principles, Austin, Texas, Nov. 19-21, ACM New York, NY, pp 67-74.

4 Lamport, L., Shostak, R. and Pease, M. (1982) 'The Byzantine Generals Problem', ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, pp. 382–401.

5 Fischer, M. J., Lynch, N. A. and Paterson, M. S. (1985) 'Impossibility of Distributed Consensus with One Faulty Process', Journal of the Association for Computing Machinery, Vol. 32, No. 2, pp. 374–382.

6 Blum, M. Feldman, P., and Micali, S. (1988). 'Non-Interactive Zero-Knowledge and Its Applications', Proceedings of the twentieth annual ACM symposium on Theory of computing (STOC 1988), pp. 103–112

7 Haber, S. and Stornetta, W.S. (1991) "How to time-stamp a digital document", Journal of Cryptology, Vol. 3/2, pp 99–111.

8 Dwork, D. und Naor, M. (1992) "Pricing via Processing or Combatting Junk Mail" in: Ernest F. Brickell "Advances in Cryptology – CRYPTO' 92", Lecture Notes in Computer Science, Vol. 740, 1993

9 Parnas, D.L. (1994) "Software aging", ICSE '94 Proceedings of the 16th international conference on Software engineering, Sorrento, Italy, May 16-21, 1994, IEEE Computer Society Press Los Alamitos, CA, pp 279-287.

10 Brewer, E., 2000, "Towards robust distributed systems," 19th annual ACM Symposium, Principles of Distributed Computing (PODC 00), ACM, pp 7-10.

11 National Institute of Standards and Technology (2001) "Secure Hash Algorithm 2"

12 Osipkov, I., E. Y. Vasserman, N. Hopper, and Y. Kim, 2007, "Combating double-spending using cooperative P2P systems," paper presented at ICDCS, 2007, 27th International Conference on Distributed Computing Systems (ICDCS '07), pp 41.

13 Hoepmann, J. H., 2008, "Distributed double spending prevention," 15th International Work-shop on Security Protocols, Lecture Notes in Computer Science 5964, pp 2010.

14 Bott, J. and Milkau, U. (2017), 'Central bank money on blockchain – A payments perspective', Journal of Payments Strategy and Systems Volume 11, Spring 2017.

15 Milkau, U., Neumann, F. and Bott, J. (2016) "Development of distributed ledger technology and a first operational risk assessment", Capco Journal of Financial Transformation, Vol. 44., pp 20- 30.

16 Decker, Ch. und Wattenhofer, R. (2013) "Information Propagation in the Bitcoin Network", 13th IEEE Int. Conference on P2P-Computing, September 2013.

17 Lessig, L. (2000) "Code Is Law", Harvard Magazine, 1.1.2000; http://harvardmagazine.com/2000/01/code-is-law-html; accessed 11.3.2017

18 Ito, J. "Why Bitcoin Is and Isn't Like the Internet", 23.1.2015; joi.ito.com/weblog/2015/01/23/whybitcoin-is-.html (accessed: 11.3.2017)

19 Luhmann, N. (1968) "Vertrauen: ein Mechanismus der Reduktion sozialer Komplexität".

20 Birch, D.G.W. (2017) "Blockchain and Reality or what's in the blocks?", Keynote, European Payment Summit 2017, Den Hague, 8.3.2017

3.9 Bitcoin – a social movement maintained currency under attack

Marella Venkata (Aalto University, FI), Juho Lindman (University of Gothenburg/Chalmers UT, SE), Matti Rossi (Aalto University, FI), and Virpi Tuunainen (Aalto University, FI)

Abstract. Bitcoin is an open source cryptocurrency system used for the money transfers and payments without involving a financial institution. Bitcoin revolutionized the financial industry and the fiat currencies. However, bitcoin was never studied from a social movement perceptive in the literature. Typically, social movements occur when people are dissatisfied with the existing system and are looking for a change that would solve their problems. The first version of Bitcoin was released after the collapse of the Lehman Brothers, people lost their trust in the financial institutions due to the lack of transparency in their operations. A system with higher transparency was seen as a superior solution for currency and payment related questions. Bitcoin turned out to be such a system. There is no centralized authority that governs the bitcoin. All the stakeholders involved with the bitcoin are pseudonymous. Security and trust comes from the underlying technology called blockchain.

Blockchain is a decentralized and distributed database where all the transactions are recorded in a ledger. Blockchain stores the information across a network of personal computers usually called as nodes. When a transaction occurs, all the nodes in the system are notified and process it. Every node in the network can access the information and process the transactions. No single node in the system can manipulate the data because all the other nodes have access to correct information. Hence, blockchain is extremely secure.

Bitcoin is considered as a cryptocurrency because everyone accepted it as a currency. But, in reality, bitcoin is just a ledger of all the transactions that are stored across several nodes. Bitcoins are traded with the fiat currencies at bitcoin exchanges. A bitcoin exchange is a place where you can buy or sell your bitcoins using fiat currencies. Since the inception of the bitcoin, these bitcoin exchanges have become targets for the hackers. Many of these exchanges lost millions of dollars of bitcoins. They are few exchanges that declared bankruptcy after these cyber-attacks. If the bitcoins are stolen from any bitcoin exchange, the whole bitcoin economy loses the money and the value of the bitcoin diminishes. Hence, the value of bitcoin is a very volatile.

Bitcoin as a Social Movement. From a framing theory perspective of social movement, collective action frames are classified as diagnostic framing, prognostic framing, and motivational framing. Diagnostic Framing is related to problem framing and identification. Prognostic Framing involves clearly stating the solution to the described problem or a clear plan or a strategy on how to execute the plan. Motivational Framing calls for action to make things better by using vocabulary to motivate people. Bitcoin can be projected as a motivational framing as it provides a solution to the existing problem by improving the transparency and eliminating the third parties. (Robert D. Benford, 2000).

Data collection. Data is collected from several news articles and blog postings. It includes blogs such as bitcointalk, reddit, coindesk, the register etc. All the important postings are collected from the blogs for analysis and patterns are recognized from them. From these patterns, we identified the various kinds of the cyber-attacks and classified them into four groups. We further investigated the data and observed the responses that exchanges have taken to solve the problem.

Classification of Cyber-Attacks. Basing on the nature of the attack, we classified these attacks into four different categories as Code Bugs, User Errors, DDoS Attack and 51 per cent Hash Rate Attack. We also studied the responses of the exchanges for these attacks. These responses include Code Revision, implementing computer security measures, temporary suspension and complete shutdown of the exchanges.

Security Flaws in the code written for the wallet. (Code Bugs): The majority of the attacks that occurred on the bitcoin are due to the code written for the access and the security of the wallet by the bitcoin exchanges. Third-party software companies usually write this code for the exchanges. Examples of these companies are BitGo, Slock.it, Linode, Flexcoin, and Instawallet. For instance, Bitfinex teamed up with BitGo and created a multi-signature wallet whose keys are divided among a number of owners to mitigate the risk of giving them to one user. But, BitGo server was hacked and the exchange lost USD 66 million. Flexicon programmers were unable to implement the concurrency property on the distributed system. Bitcoinica alleged a hack at the web hosting provider Lionde.

User's Mistakes (User Errors): The second major cause for the attacks on the Bitcoin is due to the user's mistakes to implement the security measure on the wallet computer. Most of the users failed to follow the basic safety guidelines on the computers containing wallet. Bitfloor lost a quarter million dollars when the attacker accessed the unencrypted wallet backup key. Inputs.io email account got compromised, due to which the hosting account got compromised. Unauthorized Users who had accessed the computer with wallets. Allinvain's computer was attacked by some virus like Trojan horse, which could assess the encrypted wallet file.

Distributed Denial of Service Attacks . (DDoS Attack): DDoS Attack is happening very frequency on the bitcoin exchanges. Though DDoS Attack cannot steal the bitcoins from the wallet, it can disrupt the services of the exchange and lower the value of the bitcoin. Some attackers do it before purchasing the bitcoins, while the rest blackmail the owners of the companies to pay a significant amount of money to stop the attack.

51 percent Hash Rate Attack: 51 percent hash rate is an issue with the blockchain. If any mining pool can acquire 51 percent of hash rate, they get control on all the transactions of the blockchain and start double spending the transactions. Ghash mining pool came close to 50 percent hash rate in two instances. There is no mechanism on Bitcoin blockchain that can prevent this from happening at this point.

Classification of Responses for the Cyber-Attacks.

Shutdown: When exchanges lose a significant number of bitcoins during the attacks, they shut down their operations completely. Usually, the flaws in the code (or) failure to implement the computer security measure are the key reasons for the shutdown of the exchanges. Some exchanges try to repay their customers after the shutdown.

Temporary Suspension: In order to control the loss from the attacks, exchanges temporarily suspend their services and resume once the problem is solved. Temporary suspension of services will reduce the impact of the cyber-attacks. DDoS attacks disrupt the normal operations of the exchange and force them to suspend their services.

Code Revision: If the cyber-attack occurs due to the flaws in the newly added code, the exchanges will revert/revise the existing code to a safe state. Exchanges may lose the new features added by the code, but, will be able to contain the cyber-attack.

Computer Security Measure: When the cyber-attack happens due to any security flaws on the wallet machine, the users (or the exchanges) counter them by implementing computer security measures. Few of these security measures include encrypting the wallet keys, installing the antivirus and preventing the unauthorized access to the computer.

Classification of Stakeholders. Bitcoin is an open source project. Unlike, most open source projects where developers are the only key stakeholders, Bitcoin project involves multiple key stakeholders. We divided the people interacting with the Bitcoin into nine different types of stakeholders as Developers, Hackers, Investors, Exchanges, Vendors, Users, Supporters, Enthusiasts and Legal entities. Depending on the way each stakeholder interacts with the bitcoin, we categorized these nine different stakeholders into three categories as Functional, Economic and External groups. Developers and hackers are categorized as a functional group, while Investors, Users, Exchanges and Vendors come under Economic group. Supporters, Enthusiasts and Legal entities are considered as an external group. Bitcoin is an open source P2P transfer protocol, where developers have access to the source code. All the developers share their ideas and code enhancements through an online forum named "Bitcointalk.org". Investors are those people, who put their money in the bitcoin and wait for a while excepting the value of the bitcoin to raise. These people treat bitcoin like stocks. Users view bitcoin as frictionless currency transfer system from one person to another person. They use bitcoin primarily for money transfer purposes and commercial purposes. Enthusiasts are ones who are interested in the bitcoin, who follow the news and keep track of how things are emerging on the bitcoin platform. Researchers are part of this group. Supporters like the idea of eliminating the centralized authority. They are interested in the concept that a system can work without the inference of third parties. Libertarians are an example for this category. Hackers try to steal the bitcoins from the economy. Their main objective is to make money for themselves and diminish the reliability of the bitcoin. Exchanges are places where people can buy and sell the bitcoins. Vendors are the stores or outlets that accept bitcoins for micropayments. Bitcoin is a contentious issue for legal regulators, tax authorities, and legal agencies due to the anonymous nature of the system and lack of centralized control over the system. The legality of trading bitcoins depends on the geographic location.

Impact of Cyber Attacks on Stakeholders: Whenever a cyber-attack happens, the economic layer of the bitcoin stakeholders loses the money. Among these four stakeholders, exchanges are always the primary targets of the hackers because of the high amount of stakes involved with them. Investors are the secondary targets as they buy a lot of bitcoins and wait until the value raises. Users and vendors loss is insignificant as they have relatively low investment on bitcoin. Hence, we will examine the exchanges and investors reaction to cyber-attacks.

Over the past few years, the hackers targeted several bitcoin exchanges. The biggest attack among them was the Mt.Gox attack, where the exchange lost about 350 million dollars. Mt. Gox was the largest bitcoin exchange, roughly handling 70 percent of the bitcoin transactions. The company just posted a note on their website to the clients saying, "decision was taken to close all transactions for the time being" (Hajdarbegovic, 2014). When the losses are huge, the exchanges don't provide any information to the clients and shuts down their services. The second major attack on the bitcoin exchange was the bitfinex after which, the value of the bitcoin plummeted by 20 percent. Bitfinex remains offline, with its message announcing the hack still visible to users. Unlike Mt.Gox, Bitfinex acted responsibly. They answered the questions to customers through the social media. Yet, some of the investors lost trust in the bitcoin exchange (Higgins, August).

Biomat is the third biggest bitcoin exchange located in Poland. They lost 17000 bitcoins when their wallet, which was saved on Amazon Web Services (AWS) was erased due to a change in settings. It is one of the rarest case where the exchange openly acknowledged that they have implemented a wrong technical solution by using the Amazon Web Services. BitQuick server was compromised for a short duration. The exchange immediately issued a statement saying that they temporarily shut down the server and are investigating the cyber-attack. Similarly, Bitcash, a Czech Republic exchange openly acknowledged that their server has been hacked, compromised 4000 wallets of its clients. But, the company also used strong words to describe the situation by saying, "Unfortunately, the nightmare became a reality." (Bradbury, 2013). It would incur loss of trust and confidence among the investors when the exchange uses such strong negative statements. BIPS, a Danish Bitcoin Exchange lost 1295 bitcoins from the wallets for their clients, which worth USD1 Million. The founder of the BIPS made an announcement saying, "Web Wallets are like a regular wallet that you carry cash in and not meant to keep large amounts in". But, this statement was criticized by the clients saying, "our data is secure at BIPS". So yeah, I felt pretty goddamn secure leaving my BTC balance there." (Khandelwal, 2013). Another website named Inputs.io was hacked, the owner, who goes by a pseudo name 'Tradefortess' reported the issue two weeks after the attack. He made an apology to the clients saying, "I know this doesn't mean much, but I'm sorry, and saying that I'm very sad that this happened is an understatement." (Boase, 2013) Investors trust towards the bitcoin depends on two key factors. Firstly, the investor's personality traits like his attitude, interests, beliefs and experiences with bitcoin. Motivational framing projects bitcoin as a transparent system without a centralized authority. Investors, who are motivated with this concept, would still put their money despite the cyber-attacks. Secondly, it depends on his hugely financial situation of the investor. For instance, investors in the good financial situation and with interest in concept and the idea of the bitcoin might continue to invest in the bitcoin despite losing the money due to the cyber-attacks.

Conclusion. When the cyber-attacks incur huge losses, exchanges do tend to make a very vague statement, hiding the details of the attack. In some cases, they make very discouraging statements to their clients. By using such sort of a rhetoric, exchanges lose their reputation and trust among their clients. Rather, the exchanges should disclose complete details of the cyber-attacks and inform the response that they implemented to recovery from the attack. Exchanges should ensure the clients that such kind of attacks would not reoccur. Cyber-attacks cannot only incurs financial losses but also can create trust deficit among the investors about bitcoin. The intangible loss that occurs due to the trust deficits is of greater magnitude than that of the actual financial loss. Exchanges need to realize that investors can motivated to invest on bitcoin despite the cyber-attack and ensure them that required steps would be taken to prevent similar cyber-attacks in the future.

References

1 Boase, R. (2013, November 7). coindesk. Retrieved from coindesk: http://www.coindesk.com/hackerssteal-bitcoins-inputs-io-wallet-service/

2 Bradbury, D. (2013 , November 12). coindesk. Retrieved from coindesk: http://www.coindesk.com/czech-bitcoin-exchange-bitcash-cz-hacked-4000-user-walletsemptied/

3 Hajdarbegovic, N. (2014, February 25). coindesk. Retrieved from coindesk: http://www.coindesk.com/mt-gox-statement-claims-made-conscious-decision-halttransactions/

4 Higgins, S. (August, 2016 3). coindesk. Retrieved from coindesk: http://www.coindesk.com/bitfinexbitcoin-hack-know-dont-know/
5 Khandelwal, S. (2013, November 25). thehackernews. Retrieved from thehackernews.
6 Robert D. Benford, D. A. (2000). Framing Processes and Social Movements: An Overview and Assessment. Annual Review of Sociology, 611-639.

3.10 Scalable Funding of Blockchain Micropayment Channel Networks

Roger Wattenhofer (ETH Zürich, CH), Christian Decker, and Conrad Burchert

Abstract. The Bitcoin network has scalability problems. To increase its transaction rate and speed, micropayment channel networks have been proposed, however these require to lock funds into specific channels. Moreover, the available space in the blockchain does not allow scaling to a world wide payment system. We propose a new layer that sits in between the blockchain and the payment channels. The new layer addresses the scalability problem by enabling trust-less off-blockchain channel funding. It consists of shared accounts of groups of nodes, which flexibly create one-to-one channels for the payment network. The new system allows rapid changes of the allocation of funds to channels and reduces the cost of opening new channels. Instead of one blockchain transaction per channel, each user only needs one transaction to enter a group of nodes, in which he can create arbitrary many channels. For a group of 20 users with 100 channels between them, the cost of the blockchain transactions is reduced by 90 percent compared to 100 regular micropayment channels opened on the blockchain. This can be increased further to 96 percent if Bitcoin introduces Schnorr signatures with signature aggregation.

Introduction. Bitcoin and other blockchain based payment systems are increasingly popular. This increased popularity introduces new challenges, in particular regarding scalability and transaction speed. During peaks of incoming transactions, the blockchain cannot process them fast enough and a backlog is created. We can witness these problems right now, as transactions take longer to get confirmed by the Bitcoin network, and transaction fees are rising rapidly.

We believe that these challenges need to be addressed before Bitcoin or alternative blockchain based currencies can become mainstream. The fundamental problem of any blockchain is that all transactions must be seen by everybody. Adapting the parameters (maximum size of a block, and time between two blocks) may accommodate more transactions, however only at the cost of increased propagation time and thus higher chances of blockchain forks. More forks introduce more insecurity about double spending and ultimately may prevent the network from converging to a globally consistent state. Allowing a higher transaction rate with different parameters would furthermore increase the requirements to run a full node in the network, leading to less participants and thus less decentralization.

Previous analyses have shown, that Bitcoin cannot support more than 100 transactions per second, e.g., [2, 5]. In comparison, credit card companies easily support tens of thousands of transactions per second, e.g., Visa published to support 56,000 tx/s.

In order to become a real-world payment alternative, blockchain based cryptocurrencies must support at least the transaction volume of credit cards. However, the future may be all about micropayments, transactions involving tiny amounts of money in exchange for, e.g.,

reading a single newspaper article, or driving a short distance with a self-driving vehicle. In a world with micropayments, one may imagine that millions of transactions per second must be supported to really claim scalability.

A second major problem is transaction speed, the time from initiating a transaction until one can assume that the transaction has concluded, and is thus irreversible. With inter block times typically in the range of minutes and multiple blocks needed to reasonably prevent double spending, transactions take minutes to hours until the payment is confirmed. This may be acceptable for longterm Bitcoin investors, but not for everyday shopping or interacting with a vending machine [1].

While it is conceivable to achieve a higher transaction throughput with protocol improvements, blockchain transactions still suffer from the complexity problem of a broadcast based system. New users entering will create more transactions and thus more work for each node. A long term solution needs to overcome the broadcasting principle, and transactions need to be completed with the inclusion of just a few parties.

Micropayment Channel Networks. To solve both, scalability and speed, micropayment channel networks have been proposed. A micropayment channel provides a way to trustlessly track money transfers between two entities off-blockchain with smart contracts. Trustless means that one party can show arbitrary behaviour and it is guaranteed, that each party still eventually receives its last agreed on balance. If both parties are honest they can commit the total balance of many transfers in a single transaction to the blockchain and ignore the smart contracts. If a node crashes or stops cooperating otherwise, the smart contracts can be included in the blockchain and enforce the last agreed on state.

Micropayment channel networks were proposed simultaneously by Poon and Dryja as the Lightning Network [6] and by Decker et al. as Duplex Micropayment Channels [3]. Both approaches lock funds into a shared ownership, a channel, between two participants. To spend from this shared account, both parties need to agree.

Two participants with a joint channel can transfer money directly, which allows for quick transactions. If the parties do not have a channel, a network of multiple micropayment channels can be used together with a routing algorithm to send funds between any two parties in the network. Hashed Timelocked Contracts (HTLCs) provide a scheme to allow atomic transfer over a chain of multiple channels [3, 6, 7]. Intermediate nodes can be paid for their forwarding service by decreasing the amount of sent funds with each hop.

Since micropayment channel networks will keep most transactions off the blockchain, blockchain based currencies may scale to magnitudes larger user and transaction volumes. Also, micropayment networks allow for fast transactions, as a transaction happens as soon as a smart contract is signed – the blockchain latency does not matter.

Problems. Micropayment channel networks create new problems, which have not been solved in the original papers [3, 6]. We identify two main challenges:

- Blockchain capacity. In order to have a dense network, we need a big number of channels. The problem is that each of these channels must be rooted in the blockchain.
- Locked-in funds. Funds are locked in each and every channel. Choosing a partner to collaborate with in a channel is a commitment to that party. Closing the channel and moving the funds into a new channel with a different partner needs expensive blockchain transactions, thus there is a risk involved and partners must be chosen with consideration.

It is desirable to have a dense network to ensure short paths and failure resilience. Assuming a channel lifetime of one year and one blockchain transaction per channel, the current blockchain capacity of 7 transactions per second would allow for about 200 million

channels. For redundancy a user requires more than one channel, therefore this is not sufficient as a world wide payment system.

This estimate is of course a ballpark guess, as multiple blockchain transactions per channel are needed, and the involved Bitcoin scripts result in bigger than average blockchain transactions. On the other hand new technology might facilitate more than 7 transactions per second. A more elaborate analysis was done by Dryja, who estimated the capacity in a similar range [4]. A large scale adoption of micropayment channel networks, where, e.g., Internet Of Things devices have their own Bitcoin wallet, brings the blockchain to its limit.

The locked-in funds should be sufficient to provide enough capacity for peaks of transactions. There is a conflict of the two aims to have a low amount of funds locked up in a channel, while at the same time being flexible for these peaks. This problem becomes more difficult when the lifetimes of channels increase, as one has to predict the dynamics of currency movements in the future.

We will present a solution, which solves both problems. Payment channels will not appear in the blockchain, except in the case of disputes. Users will be able to enter the system with one blockchain transaction and then open many channels without further blockchain contact. Funds are committed to a group of other users instead of a single partner and can be moved between channels with just a few messages inside the collaborating group, which reduces the risk, as an unprofitable connection can be quickly dissolved to form a better one somewhere else. By hiding the channels from the blockchain a reduction in blockchain space usage and thus the cost of channels is achieved. For a group of 20 nodes with 100 channels in between them, this can save up to 96 percent of the blockchain space.

Channel factories. As our main contribution, we introduce a new layer between the blockchain and the payment network, giving a three layered system. In the first layer, the blockchain, funds are locked into a shared ownership between a group of nodes. The new second layer consists of multi-party micropayment channels we call channel factories, which can quickly fund regular two party channels. The resulting network provides the third layer, where regular transfers of currency are executed.

Similar to regular micropayment channels, multi-party channels can be implemented with either timelocks or punishments for dishonest parties. Our implementation with timelocks performs much better, hence we will focus on it. The regular micropayment channels of the third layer can be punishment based or timelock based independent from the implementation of the multi-party channels of the second layer

Full Version. To continue reading, we refer to the full version of this work. It gives a detailed description of the construction of channel factories and different improvements to tolerate crashes of nodes. The improvement in blockchain space usage is evaluated and found to be about 90 percent. With the introduction of signature aggregation, it can be further increased to about 96 percent.

References

1 Bamert, T., Decker, C., Elsen, L., Wattenhofer, R., and Welten, S., Have a snack, pay with bitcoins. In 13th IEEE International Conference on Peer-to-Peer Computing (2013).

2 Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., and Gun ,E., On scaling decentralized blockchains. In 3rd Workshop on Bitcoin Research (2016). http://www.tik.ee.ethz.ch/file/74bc987e6ab4a8478c04950616612f69/main.pdf.

3 Decker, C., and Wattenhofer, R., A fast and scalable payment network with bitcoin duplex micropayment channels. In Symposium on Stabiliza-

tion, Safety, and Security of Distributed Systems (2016). http://www.tik.ee.ethz.ch/file/716b955c130e6c703fac336ea17b1670/duplex-micropayment-channels.pdf.
4 Dryja, T., Scalability of lightning with different bips and some back-of-the-envelope calculations. http://diyhpl.us/wiki/transcripts/scalingbitcoin/hong-kong/overview-of-bips-necessary-for-lightning/.
5 Gervais, A., Karame, G. O., Wust , K., Glykantzis, V.,Ritzdorf, H., and Capkun, S., On the security and performance of proof of work blockchains. In 23rd ACM Conference on Computer and Communications Security (2016). http://dl.acm.org/citation.cfm?doid=2976749.2978341.
6 Poon, J., and Dryja, T., The bitcoin lightning network: Scalable off-chain instant payments, 2016. https://lightning. network/lightning-network-paper.pdf.
7 Russell, R., Lightning networks part ii: Hashed timelock contracts (htlcs), 2015. https://rusty.ozlabs.org/?p=462.

3.11 Intermodal Transportation with Blockchain

Jesse Yli-Huumo (Aalto University, FI)

Abstract. Blockchain technology has been discussed to be the next generation technology in various industry sectors. Blockchain, originally used as the backbone for various cryptocurrencies, provides more decentralized, transparent, secure and trustworthy way to complete transactions between participants in a blockchain environment. Cryptocurrencies can be seen as the first step of blockchain. However, so called blockchain 2.0 and smart contracts have been coined to revolutionize many industries after cryptocurrencies. Whereas blockchain provides trustworthy ledger, smart contracts provide trustworthy calculations to complete contracts and transactions. One of the industries where Blockchain technology could be applied is intermodal transportation, which can be seen currently as a complex and fragmented industry. Blockchain could possibly be the solution to improve complex transportations that consists various actors and means. This proposition paper discusses the possibilities of blockchain technology in intermodal transportation.

Introduction. Blockchain is a distributed database solution that maintains a continuously growing list of data records that are confirmed by the nodes (e.g. companies) who are participated in it [1]. In blockchain, the data is recorded in to a public ledger that contains every transaction ever completed [2]. Blockchain as a solution provides various interesting perspectives on transaction as a process. Since blockchain is a decentralized solution, it does not require any third-party organization in the middle. The public ledger in blockchain is shared to all available nodes that have participated, which makes it more transparent compared to current centralized transactions (e.g. banks). The participants in blockchain are pseudo anonymous, which makes it more secure for nodes to confirm transactions.

At the moment blockchain is often known as the backbone for several cryptocurrencies. Bitcoin is the most famous example of a cryptocurrency. At the moment, there is around 250 000 transactions in a day done with Bitcoin [3]. Bitcoin uses blockchain to record all the currency transactions ever made. Bitcoin does not require any third-party organization in the middle to manage all the transactions [1]. In Bitcoin, the public ledger cannot be modified or deleted after a transaction is approved by all participants (nodes) [2]. Therefore,

Bitcoin can be seen as a good example of utilization of blockchain that provides good data integrity and security characteristics [1].

Data integrity and transparency are important characteristics of blockchain and the reason why its use could be extended also to other industries, services and applications [1]. Whereas cryptocurrencies can be seen as Blockchain 1.0, smart contracts can be seen as Blockchain 2.0 [1]. A smart contract is a contract between two or more parties that is stored to blockchain [4]. Smart contract works as a computerized transaction protocol that executes the terms of a contract [5]. A blockchain-based smart contracts would visible to all users of blockchain. Companies could write smart contracts between each other and they would be stored in blockchain. Blockchain 2.0 and smart contracts have been coined to be the next step for blockchain technology and where it could be applied. There are currently various discussions, ideas and suggestions on what industries blockchain technology could improve by adding more transparency and data integrity to provide trustworthy cooperation between companies who have participated to blockchain. One of these industries could be intermodal transportation.

Intermodal transportation and its current challenges. Intermodal transportation means transportation by more than one form of carrier during a single journey. Especially in very long distance transportation (for example country to country), it will be likely that freights are transported with various transportation methods. A single transportation can include trains, road vehicles, ships and airplanes, which are organized by different transportation companies, couriers, freight forwards and multi-model transport operators.

With various companies, transportation means, information technology systems and tracking systems included to deliver a freight from country A to B, will include challenges especially in data exchange, data integrity and transparency. It is common for logistics industry that even though there are already some standardization in data exchange between transportations, the companies own systems are often closed and industry-specific. This means that in logistics and transportation industry, the information systems are fragmented. There exists a lack of a high-level information system architecture in intermodal transportation and the information about transportations in scattered around companies own information systems. Fragmentation and lack of interoperability in information technology systems could even slow down freight transportation, which can be seen as a challenge that needs to be solved.

In intermodal transportation, the progress towards interoperable information systems has been slow, which is interesting, considering for example current airline-operations and their interoperability (e.g. Amadeus) [6]. The reason might be because intermodal transportation have to handle a variety of transportation operations basically everywhere in the world [6]. The intermodal industry is also by nature fragmented, complex and highly competitive. There exist various stakeholders, working in different modes, cultures, regions, and countries. Everyone in this industry has their own business philosophy to conduct business. There are various relationships between different stakeholders that can easily [6, 7]. Therefore, it can be seen that intermodal transportation has a need for trust between companies.

Can we solve challenges in intermodal transportation with blockchain? Blockchain has been coined by many to be the technical solution to provide a decentralized technology with more transparency, data integrity and security to complete trustworthy transactions between companies. Blockchain has already somewhat proved itself to work with cryptocurrencies and now it is the time to test it also in other industry sectors. The key detail in blockchain is that there is not any role for third-party or middle-man to manage blockchain. In freight

forwarding sector, the key role and responsibilities of a "middle-man" has been traditionally various transportation-related arrangements tasks. It is the responsibility of these arbitrators to arrange that freight transportation goes smoothly and according to agreements and contracts from place A to B. However, the challenge, like in any other industries, is the role of a middle-man and the general trust between companies. How can companies trust that the information and data integrity is trustable during the transportation? How do they know what has happened to their goods during transportation?

Especially, if the transportation has been a failure. Blockchain could possibly solve this issue. In intermodal transportation, blockchain could keep some type of "decentralized situation picture" of all the freights that are part of blockchain infrastructure. It could also give information about their route history, current status information and overall documentation. With blockchain, operators in logistics could always construct a comprehensive and up-todate status of freights that are being transported in the infrastructure. This could be used for example to extract some interesting data about freight forwarding sector, e.g. companies utilization and total transportations (both successful and unsuccessful). Companies that are part of blockchain infrastructure could write smart contracts between each other, which are then confirmed in blockchain by the nodes. The public ledger of all transportations ever made, would increase transparency in intermodal transportation sector.

However, there are various questions and challenges that needs to be solved. It is also important to discuss what are the limitations of blockchain that could affect its applicability in intermodal transportation. In general, it can be seen as a major obstacle to get companies open up their data from their own information systems. This means that there must be some incentive for companies to do this. In addition, this type of blockchain would require extensive work to fetch data constantly from each company's own ERP system, which would require some standarzation between blockchain and ERPs. It would also require some type of hardware solution integration to follow freights in real-time.

Also, for blockchain and participating companies, record liability about each transportation can be seen as one major challenge [8]. Success of blockchain probably correlates to a level of security. Therefore, it is a necessity that blockchain would be secure that companies can have a trust to the system and other companies that information and data is not false. However, blockchain could be one of the most prominent ideas on how to improve transparency, data integrity and security in intermodal transportation.

Questions that need more discussion.

1. What challenges would blockchain solve in intermodal transportation?
2. What are the challenges of blockchain to manage and "oversee" intermodal transportation?
3. What type of blockchain is required for intermodal transportation? Public, private? How can companies join to blockchain?
4. What actors are there in intermodal transportation and what their roles would be in blockchain?
5. How to integrate transportation companies' different information technology systems (ERP) to work in blockchain?
6. What kind of technology is needed to track and monitor freights that the information is up-to-date in blockchain?
7. How to implement so-called mining and proof-of-concept used in Bitcoin to intermodal transportation environment? How are the completed transportations confirmed?
8. What type of smart contracts are needed in intermodal transportation?
9. What legal aspects are required in intermodal transportation for blockchain and smart contracts?

10. How are smart contracts confirmed? If there are e.g. 6 companies included to a single transportation, how is smart contract written, and then also confirmed?
11. How does pseudonymity work in intermodal transportation blockchain? What is the anonymity level of companies participating? If private blockchain, is it even needed?
12. What are the real benefits for companies that would decide to join this type of blockchain?
13. What resources does it require from companies to join blockchain?
14. What are the security issues that needs to be taken in consideration?

References

1 M. Swan, Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., 2015.
2 S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
3 "Bitcoin Block Explorer - Blockchain." [Online]. Available: https://blockchain.info/. [Accessed: 12-Mar-2017].
4 "Making Sense of Blockchain Smart Contracts," CoinDesk, 04-Jun-2016. [Online]. Available: http://www.coindesk.com/making-sense-smart-contracts/. [Accessed: 12-Mar-2017].
5 R. Sharma, "Why Smart Contracts Are the Future of Everything," Investopedia, 25-Jul-2016. [Online]. Available: http://www.investopedia.com/news/understanding-smart-contracts/. [Accessed: 12-Mar-2017].
6 A. Bask, J. Juga, and J. Laine, "PROBLEMS AND PROSPECTS FOR INTERMODAL TRANSPORT: THEORETICAL TOOLS FOR PRACTICAL BREAKTHROUGHS?"
7 C. L. Erickson et al., Challenges and opportunities for an ITS/intermodal freight program: final report. U.S. Dept. of Transportation, Federal Highway Administration, 1999.
8 V. L. Lemieux, "Trusting records: is Blockchain technology the answer?," Records Management Journal, vol. 26, no. 2, pp. 110–139, Jul. 2016.

3.12 Digital Institutions and the Blockchain

Pär Ågerfalk (Uppsala University, SE) and Owen Eriksson

Abstract. Blockchain technology has been suggested as a key technology to ensure trusted transactions in the digital society. There is a great promise but also known technical limitations; transaction speed and ecological footprint are two of the more prominent. However, we would argue that there are even more pressing institutional issues that need to be dealt with for blockchain technology to deliver on its promise. Addressing blockchain technology from an institutional perspective gives rise to some questions, such as:

- What are blocks referring to and how are these referred "things" identified?
- Which are the transactions (the transaction ledger) that are secured using blockchain technology?
- To what things do these transactions refer?
- Who has the authority to declare such "things" as valid institutional objects?
- What are the underlying institutional structures that give a particular blockchain its meaning?
- How do we deal with institutional identity?
- How to ensure the pragmatic validity of transactions?
- Who has the authority to initiate the first transaction secured by a new blockchain?
- How do we deal with accountability?

In this short position paper, we maintain that it is important to conceptually distinguish between the blockchain technology and the transactions (transaction ledger) that are secured using blockchain technology. Essentially, the combination of transaction ledgers and blockchain technology creates new forms of distributed digital institutional systems. Institutions are systems of rules. Such rules, which make the transactions meaningful, govern the transaction ledger, and the blockchain technology is only useful within that institutional context. In the following, we briefly problematise these issues and outline a research project that aims to engage theoretically and empirically with digital institutionalisation in the age of distributed ledgers and the blockchain.

Background. The ongoing digitalisation of society is fundamentally changing the institutions upon which society rests. Digitalisation is also creating new processes of institutionalisation and thus fundamentally changing how society is constructed and construed. For instance, the impact on the logics of the financial sector has been fundamental as digital currencies and cashless transactions have made it to the top in many countries (Worldatlas, 2016). Money is no longer a representation of a gold standard but a digital commodity (Aakhus et al., 2014). In the wake of this development, there are predictions of global banks operated by major IT companies, such as Google, Amazon and Facebook (Hussey, 2016). Also government agencies that want to renew their offerings and ways of working drive digitalisation.

Lantmäteriverket (2016), the Swedish National Land Survey, predicts that the transition from a paper-based to a digital, blockchain based process for property purchases may shorten the lead time from when a sales contract is signed until the ownership of the property is registered in the property register, from 4 months to 2 days. The transition to a digital process promises efficiency, but an equally important aspect is the promise of trust. Traditionally, a key part of building trust is a written signature on a paper document. Contracts, sales agreements and mortgages are stored on paper to build confidence and maintain legitimacy. However, the paper handling is also error prone. A problem with hardcopy mortgage documents is that they may disappear or be destroyed (Lantmäteriverket, 2015).

Blockchain technology enables the development of new types of digital institutions, including ensuring the authenticity of digital files and transactions. The development is enabled through a combination of openness, collective authentication, encryption algorithms and requirements to supply processing power. This technology enables governments and companies to manage documents or information from registers outside the organisation's firewall, without compromising security and confidence. Openness and transparency of government actions and decisions create confidence in companies and government agencies. Clearly, this openness and transparency is in line with the principle of public access. What is new with the digital public sphere and the way it works, is that not only documents but also to the institutional process can be made more open and transparent. Confidence in the institutional processes increases when these processes are openly accessible and evidently difficult to manipulate. This can be implemented, among other things, by making use of blockchain technology, which has even come to be known as the "trust machine".

Digital Institutions. Knowledge of blockchain technology is necessary when it comes to analysing contemporary digital institutionalisation. Such analysis, however, requires also an understanding of the concept of the institution. The social world is a result of institutionalisation that occurs through social interaction and consensus about how to perform activities. This creates trust since an institutionalised behaviour creates a social order based on rules, agreements and standards (Berger and Luckmann, 1966). From an ontological perspective, institutions can be seen as systems of established rules that structure social

interactions (Hodgson, 2006). Studies of institutions have largely been oriented toward the pillars that underlie institutional structures, that is rules, norms and cultural-cognitive aspects (Scott, 2003). What has been overlooked is the digital mediation of institutions and institutionalisation processes (Couldry and Hepp, 2016). Institutionalisation is about how the institutional system is created, reproduced and discontinued. These are processes that occur over time and space and across cultural and organisational boundaries. One way to understand institutionalisation is to turn to Searle (1995, 2005, 2006). Searle explains how institutional facts, such as contracts, money and deeds can be created in and through the execution of communication actions. These communication actions are deontic by virtue of them being used to creating rights, responsibilities and privileges. They must, therefore, be based on public acceptance.

The "Digital Institutionalisation" project. Understanding digital institutionalisation is about understanding and examining the relationship between institutional language, rules, processes, information, actors, actor relationships and the development of digital infrastructures. The aim of the research project 'Digital Institutionalisation' is to, in a profound way, describe how the blockchain affects and is affected by institutionalisation. Issues that may prevent such a development are rules and laws that have not kept up with the development (European Council, 2016; The Telegraph, 2017). Also, outdated IT systems, the so-called 'installed base' can be an obstacle (Tieto, 2014). An important question is also to study who has the power to design and develop a digital institutional system. The development of digital infrastructures is about power structures created or maintained (Eriksson and Goldkuhl, 2013). There are, for instance, a strong belief that technologies such as Blockchain, which enables new means of payment (such as Bitcoin), will change the balance of power in the banking sector. Power is not just about who has the knowledge of the technology. It is about who has power over the development and change of the institutional language, rules, processes, transactions, and institutional facts created.

Given the relatively sparse number of studies on digital institutionalisation in society (Mignerat and Rivard, 2009; DeVaujany et al., 2014), the results of our inquiry mainly provide a deep understanding of how digital institutionalisation occurs over time and space. Such deep understanding has both practical and theoretical implications. Our goal is to describe and to create new concepts, models and theories for how this occurs. We want to describe how an institutional design interweaves rules, languages, institutional processes, and institutional facts, and how blockchain technology could enhance such a design.

References

1 Worldatlas (2016) Top Countries Using Digital Money For Cashless Transactions, http://www.worldatlas.com/articles/which-are-the-world-s-most-cashless-countries.html (last accessed 12 March 2017).
2 Aakhus, M., Ågerfalk, P. J., Lyytinen, K, Te'eni, D. (2014) Symbolic action research in Information Systems: Introduction to the Special Issue, MIS Quarterly, 38(4), 1187–1200.
3 Berger, P. L., Luckmann, T (1966) The Social Construction of Reality: A Treatise in the Sociology of Knowledge, Garden City NY: Anchor Books, ISBN 0-385-05898-5.
4 Couldry, N., Hepp, A. (2016) The mediated construction of reality. John Wiley and Sons.
5 DeVaujany, F. X., Carton, S., Mitev, N., and Romeyer, C. (2014). Applying and theorizing institutional frameworks in IS research: A systematic analysis from 1999 to 2009. Information technology and people, 27(3), 280-317.
6 Eriksson, O., and Goldkuhl, G. (2013). Preconditions for public sector e-infrastructure development, Information and organization, 23(3), 149-176.
7 European Council (2016) Digital single market for Europe.

8 Hodgson, G. (2006). What Are Institutions? Journal of Economic Issues, XI (1).

9 Husssey M. (2016) The banks of Google, Facebook and Amazon, https://thenextweb.com/facebook/2016/05/05/banks-google-facebook-amazon/ (last accessed 27 January 2017)

10 Lantmäteriverket (2015) Säkrare och enklare panträtt i fast egendom, Utredningsrapport, Dnr 501-2015/2584 (In Swedish)

11 Lantmäteriverket (2016) Framtidens husköp i blockkedjan. Ett utvecklingsprojekt med Lantmäteriet, Telia Company, Chromaway och Kairos Future. (In Swedish)

12 Mignerat, M., Rivard, S. (2009), Positioning the institutional perspective in information systems research, Journal of Information Technology, 24 (4), 369–391.

13 Scott, W. R. (2003) Institutional carriers: reviewing modes of transporting ideas over time and space and considering their consequences, Industrial and corporate change, 12(4), 879–894.

14 Searle, J. (1995). The Construction of Social Reality. Free Press.

15 Searle, J. (2005). What is an institution. Journal of Institutional Economics, 1(1), 1–22.

16 Searle, J.R. (2006). Social ontology: Some basic principles. Anthropological Theory, 6 (12).

17 The Telegraph (2017) How to set up a new bank: It'll take you longer than you think and cost more than you think.

18 Tieto (2014) Uppstickare utmanade storbankerna på Bankdagen.

Participants

- Pär Ågerfalk
Uppsala University, SE
- Michel Avital
Copenhagen Business School, DK
- Roman Beck
IT University of Copenhagen, DK
- Christian Becker
Universität Mannheim, DE
- Joseph Bonneau
Stanford University, US
- Marcus Dapp
fortiss GmbH – München, DE
- Peter Eklund
IT University of Copenhagen, DK
- Fritz Henglein
University of Copenhagen, DK
- John Leslie King
University of Michigan – Ann Arbor, US
- Christoph Kreiterling
BaFin, DE
- Juho Lindman
University of Gothenburg | Chalmers UT, SE
- Alberto Montresor
University of Trento, IT
- Christoph Müller-Bloch
IT University of Copenhagen, DK
- Matti Rossi
Aalto University, FI
- Joachim Schrey
Noerr LLP – Frankfurt, DE
- Gerhard Schwabe
Universität Zürich, CH
- Peter Sestoft
IT University of Copenhagen, DK
- Virpi Tuunainen
Aalto University, FI
- Marella Venkata
Aalto University, FI
- Roger Wattenhofer
ETH Zürich, CH
- Jesse Yli-Huumo
Aalto University, FI