Report from Dagstuhl Seminar 18152

Blockchains, Smart Contracts and Future Applications

Edited by

Foteini Baldimtsi[1], Stefan Katzenbeisser[2], Volkmar Lotz[3], and Edgar Weippl[4]

1 **George Mason University – Fairfax, US,** foteini@gmu.edu
2 **TU Darmstadt, DE,** skatzenbeisser@acm.org
3 **SAP Labs France – Mougins, FR,** volkmar.lotz@sap.com
4 **Secure Business Austria Research, AT,** eweippl@sba-research.org

Abstract

This report documents the Dagstuhl seminar 18152 "Blockchains, Smart Contracts & Future Applications". While Bitcoin currently works well in practice, there are many open questions regarding the long-term perspective of blockchain technologies, for both public and private/permissioned blockchains. It is yet unclear how processes can be designed to work in predictive ways and how to embed security in the lifecycle of smart contract development and deployment. Furthermore, the distributed nature of the system needs to be considered when thinking about which groups or individuals can influence future developments. Similar to 'real-world' societies, blockchains are based on mutual recognition of conventions. Diverse academic disciplines as well as industry can and need to collaborate to advance research in blockchain and to fully understand how the technology might impact our future lives.

Seminar April 8–13, 2018 – http://www.dagstuhl.de/18152
2012 ACM Subject Classification Theory of computation → Cryptographic protocols,Networks → Peer-to-peer protocols
Keywords and phrases blockchains, consensus algorithms, cryptographic currency, incentive engineering, smart contracts
Digital Object Identifier 10.4230/DagRep.8.4.20
Edited in cooperation with Nicholas Stifter and Philipp Schindler

1 Executive Summary

Edgar Weippl (Secure Business Austria Research, AT)
Foteini Baldimtsi (George Mason University – Fairfax, US)
Stefan Katzenbeisser (TU Darmstadt, DE)
Volkmar Lotz (SAP Labs France – Mougins, FR)

In its beginnings, the technical and socio-economical feasibility of Bitcoin was met with much skepticism; however, this has since changed as both research and practice have outlined the merits of distributed ledger technologies, commonly referred to as "blockchains". Possible applications of blockchains reach from decentralized settlement layers over complex smart contract systems to tailored authenticated data structures that implement systems for identity or supply chain management. Nevertheless, beyond the immediate opportunities and applications lie many open questions regarding the long-term perspective of both permissionless and permissioned blockchain technologies. For example, while scalability and

sustainability are currently topics of active research and development, other aspects such as usability, interoperability and cryptoeconomics have received considerably less attention. In order to anticipate and address future key topics and questions related to blockchain technologies, this seminar strove to provide an interdisciplinary breeding ground.

The participants focused on future applications and developments of this technology and discussed how such complex systems can thrive over a long period of time. Thereby, we started our seminar by outlining and collecting current and potentially future issues from the diverse viewpoints of the participants. These issues include not only current limitations of the underlying technologies, but also problems encountered in real-world applications.

As an example, we considered the various economic, legal and technological uncertainties and problems that have arisen as a consequence of the recent contentious forks in both the Bitcoin (August 2017) and Ethereum (July 2016) networks. While the possibility of such forks was previously well known, it can be argued that provisionary measures and research on effectively dealing with them was immature and could have been addressed much sooner. In any case, the ramifications of these events have and will continue to influence the discussion and development of blockchain technologies.

Beside establishing the relevant issues through numerous talks, subgroups of participants were formed to discuss a specific set of topics. Over the course of the seminar, participants were encouraged to move between groups and provide input to various topics. We hope to have thus enriched the discussion with different viewpoints and to have facilitated a rewarding range of outcomes; at the point of writing, two papers directly resulting from this Dagstuhl seminar are submitted for review. The goal of the seminar was to develop a shared and open agenda that shapes and directs research and development in the area of distributed ledger technologies to face current and future challenges as well as contribute to the positive development of this field.

The talks and working groups of this first Dagstuhl seminar on Blockchains, Smart Contracts and their future applications focused inter alia on the following topics:

- current and future protocols, including alternative consensus protocols
- governance
- interdisciplinary aspects of Blockchain technology (economy, law)
- cross-chain communication
- scalability and costs
- Goldfinger and other attack vectors

2 Table of Contents

3 Overview of Talks

3.1 How to Charge Lightning

Zohar Aviv (Hebrew University – Jerusalem, IL)

On-chain transaction channels represent one of the leading techniques to scale the transaction throughput in cryptocurrencies. However, until now the economic effect of transaction channels on the system has not been widely explored. We studied the economics of Bitcoin transaction channels and presented a framework for an economic analysis of the lightning network and its impact on transaction fees in the blockchain. Our framework allows us to reason about different patterns of demand for transactions and different topologies of the lightning network, and to derive the resulting fees for transacting both on and off the blockchain. Our initial results indicate that while the lightning network does allow for a substantially higher number of transactions to pass through the system, it does not necessarily provide higher fees to miners and, as a result, may in fact lead to lower participation in mining within the system.

3.2 Blockchains are from Mars, TEEs are from Intel. An overview of blockchain and Trusted Execution Environment combination

Ittay Eyal (Technion – Haifa, IL)

In this talk we tried to answer two key questions:

- How can TEEs extend blockchains?
- How can blockchains extend TEE-based distributed algorithms?

Thereby, we explored two particular examples:
TEEs for PoW alternatives:

- Proof of Elapsed Time (PoET): CPU waits an exponentially distributed random time rather than wasting work; however, it wastes cupex (in hardware) instead of software – old HW mines as efficient as new HW.
- Proof of useful Works (Zhang et al. 2017): perform useful work for mining
  - Useful work CPU instructions counted as puzzle solution attempts, enforced by TEE
  - Automatic instrumentation for correct instruction counting and reporting
  - Hierarchical attestation with compliance checker

Efficient and asynchronous Blockchain access payment channels by combining blockchain and TEE powers: TEEchain.

$$TEE_A - \textbf{A-B} - TEE_B \tag{1}$$

Each party's TEE maintains the party's currency, guaranteeing to settle it on the blockchain exactly (at most) once.

The challenges are:

- Form channels between the TEEs
- Enable arbitrary work (if hierarchical attestation)
- TEE crash-fault tolerance
- Multihop payments without synchronous blockchain access

3.3 Perun: virtual payment and state channel networks

Sebastian Faust (TU Darmstadt, DE)

One of the main challenges that hinder further adaption of cryptocurrencies is scalability. Because cryptocurrencies require that all transactions are processed and stored on the blockchain transaction, throughput is inherently limited. An important proposal to significantly improve this are off-chain protocols, where the massive bulk of transactions is executed without requiring the costly interaction with the blockchain. In this talk we introduce Perun – a network of virtual payment and state channels. The main contributions of our work are introducing the concept of virtual channels, and providing the first full specification of arbitrary complex state channel networks. The latter allows users to execute smart contracts in an off-chain way. All our constructions are analysed using the universal composability framework commonly used in cryptography for analysing cryptographic protocols.

3.4 Ouroboros Proof-of-Stake Protocols

Peter Gazi (IOHK – Hong Kong, HK)

Bitcoin and most other existing cryptocurrencies use the so-called Proof-of-Work approach to extend the blockchain: If a party wants to create a new block, they have to solve a computation-intensive puzzle and only once they succeed they are allowed to attach a new block to the chain (containing proof that this considerable amount of work has been invested). This leads to an arms race between miners to invest even more computational power (and, hence, electricity) into solving these puzzles, leading to an already worrying level of energy consumption by Bitcoin. Even worse, this energy requirements scale with the size of the system, so the more mainstream Bitcoin becomes, the more energy will be consumed to maintain its security.

Alternatively, Proof-of-Stake protocols use a different approach to decide about the eligibility of parties to create new blocks. Namely, the probability of each party to "win a lottery" and be allowed to create a new block (in a given time interval) is, by the design of the protocol, proportional to the amount of stake (i.e., coins) owned by that party, as recorded by the ledger itself. Evaluating this lottery can be done very easily and without any extensive computation, thus relieving the system from basing its security on a continuous waste of resources. This seemingly simple idea (which is almost as old as Bitcoin itself), however, turns out to be difficult to implement securely, which is why getting a provably secure Proof-of-Stake protocol is so important and has eluded the community for quite some time.

In this talk, I presented the Ouroboros family of provably secure Proof-of-Stake protocols as well as some exciting ongoing work and open questions in the area.

3.5 Cryptocurrency Analytics – An Agenda for (some more) Interdisciplinary Research

Bernhard Haslhofer (AIT Austrian Institute of Technology – Wien, AT)

From an abstract, birds-eye perspective, cryptocurrencies can be perceived as a network in which different types of actors (e.g., exchanges, darknet marketplaces, payment providers) interact with each other through transaction. The goal of cryptocurrency analytics is to investigate and develop scalable quantitative methods, tools and services that contribute to a better understanding of the structure and dynamics of cryptocurrency ecosystems. One can distinguish between two types of analytics tasks: microscopic analysis focusing on the traceability of transaction chains and macroscopic analysis focusing on the investigation of the entire ecosystem after projecting real-world phenomena, such as ransomware attacks, onto the network.

The goal of this talk was to show how cryptocurrency analytics methods can be used in a number of application scenarios, ranging from science to public authorities to the FinTech sector. As a concrete example, this talk presented the results of a recent macroscopic study that analysed and qualified ransomware payments in the Bitcoin ecosystem. Finally, it outlined open application-oriented research questions, structured by the main technical ingredients that enable cryptocurrency analytics tasks: algorithms and heuristics, attribution data, and computation platforms.

3.6 Goldfinger's Technical Possibilities – Open Questions for Cross-Chain Interlinking

Aljosha Judmayer (SBA Research – Wien, AT)

Goldfinger attacks, initially described by Kroll et al. in 2013, aim to damage the economy of a cryptocurrency such that the attacker achieves utility outside of the very same cryptocurrency. Until lately, this type of attack has not received much research attention, but the fast-growing number of cryptocurrencies has made such kind of scenarios more plausible, as also outlined by Bonneau (2017; 2018).

This talk surveys the literature on Goldfinger attacks and bribing techniques in the area of cryptocurrencies to extent upon existing methods. Thereby, also new directions for attacks are proposed which utilize merged mining as an attack vector. The goal is to show that smart contracts and cross-chain interlinking of different cryptocurrencies are also enabling technologies to perform more attacks than currently envisioned. This leads to the open question if and how the threat model of permissionless cryptocurrencies needs to be adjusted to better account for such kinds of attacks.

3.7 Anonymity in Cryptocurrencies

Sarah Meiklejohn (University College London, GB)

A long line of recent research has demonstrated that existing cryptocurrencies often do not achieve the level of anonymity that users might expect they do, while at the same time another line of research has worked to increase the level of anonymity by adding new features to existing cryptocurrencies or creating entirely new ones. This talk will explore both de-anonymization attacks and techniques for anonymity that achieve provably secure guarantees.

3.8 Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance

Sarah Meiklejohn (University College London, GB)

We initiated a quantitative study of the decentralization of the governance structures of Bitcoin and Ethereum. In particular, we scraped the open-source repositories associated with their respective codebases and improvement proposals to find the number of people contributing to the code itself and to the overall discussion.

We then present different metrics to quantify decentralization, both in each of the cryptocurrencies and, for comparison, in two popular open-source programming languages, Clojure and Rust. We find that for both cryptocurrencies and programming languages, there is usually a handful of people that accounts for most of the discussion. We also look into the effect of forks in Bitcoin and Ethereum, and find that there is little intersection between the communities of the original currencies and those of the forks.

3.9 On the Necessity of a Prescribed Block Validity Consensus: Analyzing the Bitcoin Unlimited Mining Protocol

Bart Preneel (KU Leuven, BE)

Bitcoin has attracted many users, but also has been considered as a technical breakthrough by academia. However, the potential of Bitcoin is largely untapped due to its limited throughput. The Bitcoin community is currently facing its biggest crisis in history, since the community disagrees on how to increase the throughput. Among various protocols, Bitcoin Unlimited recently became the most popular candidate, as it allows miners to collectively decide the block size limit according to the rest network capacity. However, the security of Bitcoin Unlimited is heavily debated and no consensus has been reached as the issue is discussed under different mining incentive models. We systematically tested Bitcoin Unlimited's security using three incentive models; we evaluated the two major arguments of

Bitcoin Unlimited's security: block validity consensus is not necessary for Bitcoin Unlimited's security as such consensus would emerge in Bitcoin Unlimited based on economic incentives. Our results invalidate both arguments and therefore disprove Bitcoin Unlimited's security chains. We also discuss whether a prescribed block validity consensus is a necessary feature of a cryptocurrency.

3.10 Randomness for Blockchains

Philipp Schindler (SBA Research – Wien, AT)

S. Nakamoto proposed the first practical solution for the problem of reaching consensus in a dynamic set of potentially anonymous participants without a prior agreement on this set. Bitcoin achieves this advancement at the cost of high computational requirements for Proof-of-Work, leading to vast amounts of electricity being consumed.

Recently, new protocols – using Proof-of-Stake as a fundamental principle – tried to improve upon Nakamoto's solution. These protocols require a trustworthy source of randomness to maintain desirable security guarantees. However, obtaining trustworthy randomness in a highly decentralized network and under potentially adversarial conditions is by itself a challenging task. Recent academic research as well as projects from the industry try to address this problem by designing random beacon protocols which produce the required random values in regular intervals. We highlight the design challenges of random beacon protocols as well as provide a review and comparison of state-of-the-art protocols.

3.11 Selected Legal Aspects of Blockchain Technology Applications

Sofie Schock (Universität Wien, AT)

From a legal perspective, Distributed Ledger Technologies like the Blockchain technology, raise many fundamental questions. Especially in permissionless Blockchain networks, where no "organiser" exists and where the participants act pseudonymously, existing legal tools reach their limits. It turned out that it is not possible to relate liability in such networks in current legal systems. Although proposals for possible solutions of this problem have been made, it is still a long way to a profound and reasonable legal work up. In this context, it is very important for lawyers to understand the technical principles; therefore, a close collaboration between lawyers and technicians is a desired goal.

3.12 Open Questions in Blockchain Consensus

Nicholas Stifter (TU Wien, AT)

The rise of Bitcoin and its underlying blockchain technology has revitalized the discussion on distributed consensus and connected various scientific disciplines in their quest for reaching a deeper understanding of the characteristics of the Nakamoto consensus. Nevertheless, while research on this topic has led to many valuable insights and advancements in regard to Byzantine consensus protocols, it also raises new fundamental questions:

The sustainability of relying on Proof-of-Work in blockchain consensus is increasingly becoming an issue, while the characteristics and trade-offs of potential alternatives such as Proof-of-Stake or Proof-of-X are still not entirely clear. Apparent miner centralization questions the aspiration of many cryptocurrencies to be decentralized, while incurring scalability difficulties because of this property. Newly proposed consensus protocols for an application in distributed ledgers should strive for simplicity and could benefit from more concise definitions of the requirements and characteristics that they need to satisfy. Introducing game theory to model the behavior of consensus participants, and the formal characteristics and guarantees that can be derived of such assumptions in consensus protocols, is an exciting research direction that has, so far, received relatively little attention. Finally, incentivizing or possibly enforcing consensus participation in decentralized systems, where protocols can be readily modified to create concurrent and competing systems, remains an open question.

3.13 Towards a Generalised Blockchain Fabric

Alexei Zamyatin (Imperial College London, GB)

Since the introduction of Bitcoin in 2008, the field of cryptocurrencies has gained popularity in both academic and private sectors. Today, there exist over 1500 cryptocurrencies and new systems are being launched on a daily basis. However, while most blockchain-based digital currencies are of a decentralized nature, secure asset and information exchange between such systems currently requires a trusted third party, e.g., a centrally banked exchange. Throughout the past years, research into facilitating trustless cross-chain communication has resulted in the proposal of numerous concepts and mechanisms. However, to this date, scientific publications are scarce and only a limited number of introduced concepts has been implemented. In this work, we attempt to provide a taxonomy of relevant properties for cross-chain communication, a categorization of existing protocols, and an overview of current challenges hindering the deployment of such schemes.

4 Working groups

4.1 Futurology

Philipp Schindler (SBA Research – Wien, AT) and Nicholas Stifter (TU Wien, AT)

Predictions about technological advancements and their impact on societies are often largely inaccurate, in particular when made over a larger time span. Nevertheless, anticipating future developments of cryptocurrencies and distributed ledger technologies can help hone in on the core aspects that make up the disruptive potential of these new technologies. The participants of this breakout session engaged in thought experiments on the future impact of blockchain technologies, outlining four different possible scenarios roughly twelve years from now. Hereby, two utopian and two dystopian futures in which the technology prevails or fails respectively, were envisioned. In particular the topic of privacy was a recurring theme, either in the form of an Orwellian nightmare in which total transparency has eroded social cohesion and condensed power among a privileged elite, or in a scenario where the demand and awareness for privacy-enhancing technologies in DLT has led to a broader understanding and ability to effectively and safely use such technologies for the greater good of society. Further, the discussions among participants outlined that the considered utopian and dystopian scenarios lie closely together, whereby the failure of a few key assumptions such as the security of elliptic curve cryptography could quickly turn a positive into a negative outcome.

4.2 DAG

Nicholas Stifter (TU Wien, AT)

This breakout session was focused on the topic of directed acyclic graphs (DAGs) in blockchain protocol designs. Participants were first able to enjoy an introductory course or refresher on the basic concepts and research challenges of DAG-based blockchain designs that was presented by Aviv Zohar. The speaker then further outlined the Spectre and Phantom DAG protocols and gave insights into their development process, as well as the challenges that were faced when ensuring that the designs could provide the desired security, consistency and liveness properties. The group then compared and explored different characteristics of various DAG-based protocols and design proposals such as Spectre, Phantom, Hashgraph, Fruitchains, GHOST, IOTA or Braids in more detail, focusing on the properties and guarantees these protocols can achieve or intend to provide and how they differ from each other. Participants finally engaged in a vivid discussion on security aspects of already deployed DAG protocols and that new projects emerging from the cryptocurrency community often lack rigorous formal analysis and proofs of their underlying concepts.

4.3 Governance

Nicholas Stifter (TU Wien, AT) and Philipp Schindler (SBA Research – Wien, AT)

The goal of this breakout session was to identify and discuss relevant issues and open research questions on the topic of governance for cryptocurrencies and Blockchain/Distributed Ledger Technologies (DLT). As an initial step the question of why governance is needed in the first place was addressed by the participants, assuming that present cryptocurrency and DLT implementations may already violate existing norms and fundamental rights. In this context difficulties arise not only because norms are not clearly defined and are subject to change, rendering them hard to formalize, but also because the underlying technological model of many DLT that facilitates open access with weak identities renders the enforcement of such norms hard or impossible. One informal argument the group gave why governance is needed was: (to) *"modify the system in order to: adjust to unpredicted changes in the environment including norms, specifically about the redistribution of wealth/happiness between the users and people affected by (the existence of) the system."* An important distinction was made between governance questions arising from outside the decentralized system, such as national and international laws and regulations, and governance issues related to the system itself as part of the protocol or operational procedures. Further, different control points and mechanisms for governance were discussed, from which the central observation was made that (software) forks can be employed as an expression of dissent and that the forking mechanism as a governance primitive should receive further study and attention. Finally, the group engaged in the topic of how to effectively approach and study governance questions for DLT and cryptocurrencies. Existing governance models and processes in other open source projects, but also from non-technical systems such as the United Nations or European Union, may provide valuable insights and experience while research on topics such as political communication theories, computational social choice theory or coordination games could help shape a systematic approach.

Participants

- Zohar Aviv
Hebrew University – Jerusalem, IL
- Foteini Baldimtsi
George Mason University – Fairfax, US
- Alex Biryukov
University of Luxembourg, LU
- Rainer Böhme
Universität Innsbruck, AT
- Jan Camenisch
IBM Research-Zurich, CH
- Samuel Christie
North Carolina State University – Raleigh, US
- Ittay Eyal
Technion – Haifa, IL
- Sebastian Faust
TU Darmstadt, DE
- Peter Gazi
IOHK – Hong Kong, HK
- Dieter Gollmann
TU Hamburg, DE
- Raimund Gross
SAP SE – Walldorf, DE
- Bernhard Haslhofer
AIT Austrian Institute of Technology – Wien, AT
- Aljosha Judmayer
SBA Research – Wien, AT
- Stefan Katzenbeisser
TU Darmstadt, DE
- Kwok-Yan Lam
Nanyang TU – Singapore, SG
- Juho Lindman
University of Gothenburg, SE
- Volkmar Lotz
SAP Labs France – Mougins, FR
- Sarah Meiklejohn
University College London, GB
- Bart Preneel
KU Leuven, BE
- Alessandra Scafuro
North Carolina State University – Raleigh, US
- Philipp Schindler
SBA Research – Wien, AT
- Sofie Schock
Universität Wien, AT
- Nicholas Stifter
TU Wien, AT
- Thorsten Strufe
TU Dresden, DE
- Edgar Weippl
Secure Business Austria Research, AT
- Alexei Zamyatin
Imperial College London, GB