Blockchain – From the Anarchy of Cryptocurrencies to the Enterprise

Christian Cachin

IBM Research, Zürich, Switzerland
cca@zurich.ibm.com

Abstract

A blockchain is a public ledger for recording transactions, maintained by many nodes without central authority through a distributed cryptographic protocol. All nodes validate the information to be appended to the blockchain, and a consensus protocol ensures that the nodes agree on a unique order in which entries are appended. Distributed protocols tolerating faults and adversarial attacks, coupled with cryptographic tools are needed for this. The recent interest in blockchains has revived research on consensus protocols, ranging from the proof-of-work method in Bitcoin's "mining" protocol to classical Byzantine agreement. Going far beyond its use in cryptocurrencies, blockchain is today viewed as a promising technology to simplify trusted exchanges of data and goods among companies. In this context, the Hyperledger Project has been established in early 2016 as an industry-wide collaborative effort to develop an open-source blockchain. This talk will present an overview of blockchain concepts, cryptographic building blocks and consensus mechanisms. It will also introduce Hyperledger Fabric, an implementation of blockchain technology intended for enterprise applications. Being one of the key partners in the Hyperledger Project, IBM is actively involved in the development of this blockchain platform.

1998 ACM Subject Classification C.2.4 Distributed Systems

Keywords and phrases consensus, cryptographic, distributed protocols

Digital Object Identifier 10.4230/LIPIcs.OPODIS.2016.2

Category Keynote

20th International Conference on Principles of Distributed Systems (OPODIS 2016).
Editors: Panagiota Fatourou, Ernesto Jiménez, and Fernando Pedone; Article No. 2; pp. 2:1–2:1

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany