Blockchain-Based Consensus*

Juan A. Garay

Yahoo Labs, Sunnyvale, USA
garay@yahoo-inc.com

Abstract

Distributed consensus (aka *Byzantine agreement* [Pease, Shostak & Lamport, 1980]) is one of the fundamental problems in fault-tolerant distributed computing and cryptographic protocols. It requires correct participants (parties) to reach agreement on initially held values despite the arbitrary behavior of some of them, with the additional requirement (known as *Validity*) that if all the correct participants start off with the same value, then that must be the decision value. The problem has been studied extensively in both the unconditional setting (where no assumptions are made about the computational power of the adversary) and the cryptographic setting, and efficient (i.e., polynomial-time) solutions exist tolerating the optimal number of misbehaving parties and running in the optimal number of rounds, on networks with pairwise authenticated channels.

In many interesting scenarios, however, such as "peer-to-peer" networks, where parties come and go as they please and there are no prior relations among them, such infrastructure (pairwise authenticated channels, public-key infrastructure) is unavailable, thus raising the question whether anything "interesting" can be achieved. In this talk we answer this question in the affirmative, presenting two new probabilistic consensus protocols based on "proofs of work" (POWs, aka "moderately hard functions," "cryptographic puzzles" [Dwork & Naor, 1992]), the technology underlying Bitcoin, the first and most popular decentralized cryptocurrency to date. (In Bitcoin, POWs are implemented using the SHA-256 cryptographic hash function, by finding preimages that produce values in a given smaller domain.)

In more detail, we first extract and analyze the core of the Bitcoin protocol, which we term the Bitcoin *backbone*, and prove two fundamental properties of its "blockchain" approach which we call "common prefix" and "chain quality." The consensus protocols can then be built as applications on top of the backbone protocol, with the Agreement and Validity properties following from common prefix and chain quality, respectively. The first protocol works assuming the adversary's hashing power is bounded by $\frac{1}{3}$ of the network's total hashing power. The second consensus protocol is more elaborate, relies on the notion of robust transaction ledgers, which capture the essence of Bitcoin's operation as a cryptocurrency, and works assuming the adversary's hashing power is strictly less than $\frac{1}{2}$.

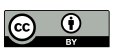
1998 ACM Subject Classification C.2.4 Distributed Systems, D.4.6 Security and Protection

Keywords and phrases Distributed consensus; cryptocurrencies; cryptographic protocols

Digital Object Identifier 10.4230/LIPIcs.OPODIS.2015.5

Category Keynote

* This invited talk is based on "The Bitcoin Backbone Protocol: Analysis and Applications," appearing in *Proc. Eurocrypt 2015*, joint work with Aggelos Kiayias and Nikos Leonardos.



19th International Conference on Principles of Distributed Systems (OPODIS 2015).
Editors: Emmanuelle Anceaume, Christian Cachin, and Maria Potop-Gradinariu; Article No. 5; pp. 5:1–5:1

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