Basic Properties of the Blockchain

Juan A. Garay
Yahoo Research
garay@yahoo-inc.com

ABSTRACT

As the first decentralized cryptocurrency, Bitcoin [1] has ignited much excitement, not only for its novel realization of a central bank-free financial instrument, but also as an alternative approach to classical distributed computing problems, such as reaching agreement distributedly in the presence of misbehaving parties, as well as to numerous other applications—contracts, reputation systems, name services, etc. The soundness and security of these applications, however, hinges on the thorough understanding of the fundamental properties of its underlying *blockchain* data structure, which parties ("miners") maintain and try to extend by generating "proofs of work" (POW, aka "cryptographic puzzle").

In this talk we follow the approach introduced in [2], formulating such fundamental properties of the blockchain, and then showing how applications such as consensus and a robust public transaction ledger can be built ``on top" of them. The properties are as follows, assuming the adversary's hashing power (our analysis holds against arbitrary attacks) is strictly less than ½ and high network synchrony:

Common prefix: The blockchains maintained by the honest parties possess a large common prefix. More specifically, if two honest parties "prune" (i.e., cut off) k blocks from the end of their local chains, the probability that the resulting pruned chains will not be mutual prefixes of each other drops exponentially in the that parameter.

Chain quality: We show a bound on the ratio of blocks in the chain of any honest party contributed by malicious parties. In particular, as the adversary's hashing power approaches ½, we show that blockchains are only guaranteed to have few, but still some, blocks contributed by honest parties.

Chain growth: We quantify the number of blocks that are added to the blockchain during any given number of rounds during the execution of the protocol. (**N.B.:** This property, which in [2] was proven and used directly in the form of a lemma, was explicitly introduced in [3]. Identifying it as a separate property enables modular proofs of applications' properties.)

The above properties hold assuming that all parties—honest and adversarial—"wake up" and start computing at the same time, or, alternatively, that they compute on a common random string (the "genesis" block) only made available at the exact time when the protocol execution is to begin. In this talk we also consider the question of whether such a trusted setup/behavioral assumption is necessary, answering it in the negative by presenting a Bitcoin-like blockchain protocol that is provably secure without trusted setup, and, further, overcomes such lack in a *scalable* way—i.e., with running time independent of the number of parties [4].

A direct consequence of our construction above is that consensus can be solved directly by a blockchain protocol without trusted setup assuming an honest majority (in terms of computational power).

BCC 2017, April 2, Abu-Dhabi.
ACM ISBN 978-1-4503-4335-0/17/02.
http://dx.doi.org/10.1145/2998181.3020283

CCS Concepts

• Security and privacy~Symmetric cryptography and hash functions • Security and privacy~Pseudonymity, anonymity and untraceability • Theory of computation~Distributed computing models

Author Keywords

Bitcoin; cryptocurrencies; blockchain protocols; consensus problems

BIOGRAPHY

Juan Garay is currently a Sr. Principal Research Scientist at Yahoo Research. Previously, after receiving his PhD in Computer Science from Penn State, he was a postdoc at The Weizmann Institute of Science, and held research positions at IBM T.J. Watson Research Center, Bell Labs and AT&T Labs – Research. His research interests include both foundational and applied aspects of cryptography and information security. Dr. Garay has published extensively in the areas of cryptography, network security, distributed computing, and algorithms; has been involved in the design, analysis and implementation of a variety of secure systems; and is the recipient of over two dozen patents. He has served on the program committees of numerous conferences and international panels—including co-chairing Crypto 2013 and 2014, the discipline's premier conference.

REFERENCES

1. S. Nakamoto. Bitcoin open source implementation of p2p currency. http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source, February 2009.
2. J. Garay, A. Kiayias, and N. Leonardos. The Bitcoin backbone protocol: Analysis and applications. In Advances in Cryptology − EUROCRYPT 2015. LNCS(9057), Springer, April 2015.
3. A. Kiayias and G. Panagiotakos. Speed-security tradeoffs in blockchain protocols. IACR Cryptology ePrint Archive, 2015:1019, 2015.
4. J. Garay, A. Kiayias, N. Leonardos and G. Panagiotakos. Boostrapping the blockchain – directly. IACR Cryptology ePrint Archive 2016: 991 (2016).