Recent Trends in Decentralized Cryptocurrencies (Invited Talk)

Aviv Zohar
The Hebrew University of Jerusalem
Jerusalem, Israel
avivz@cs.huji.ac.il

ABSTRACT

Following Bitcoin's introduction, decentralized cryptocurrencies began to emerge as a new application domain for computer science. Bitcoin's protocol has been researched and improved upon along many fronts: from its underlying incentives, through to its cryptographic primitives and its security. Many research questions and challenges still remain as cryptocurrencies and other financial systems that rely on similar principles gain wider adoption.

CCS CONCEPTS

• **Applied computing** → *Digital cash*;

KEYWORDS

Bitcoin, Cryptocurrencies

ACM Reference format:
Aviv Zohar. 2017. Recent Trends in Decentralized Cryptocurrencies (Invited Talk). In *Proceedings of 49th Annual ACM SIGACT Symposium on the Theory of Computing, Montreal, Canada, June 2017 (STOC'17-KEY),* 1 pages.
DOI: 10.1145/3055399.3079074

1 INTRODUCTION

Bitcoin is an open "permissionless" protocol for a decentralized digital currency that allows anyone to become part of the network and authorize transactions [2]. The currency has been slowly growing in popularity since its launch in January of 2009 by a pseudonymous creator known only as Satoshi Nakamoto. While digital money is not new (credit cards, wire transfers and many other financial transactions have been operating electronically for quite some time), Bitcoin adds an important novel feature: its decentralized nature. Bitcoin has no central entity in charge of the currency or backing it up, and no central issuer. Instead, it is managed by a peer-to-peer network of nodes that process all its transactions securely using the blockchain – the data structure that is used by nodes to record and reach consensus on all transactions that were accepted.

Bitcoin has many fascinating features which make it interesting from both a computational and an economic perspective: Transactions are irreversible (w.h.p.) and public, but users are pseudonymous. Money creation is set according to a predefined schedule. The protocol combines ideas from many areas of computer science. These range from its use of cryptographic primitives to secure transactions, its use of proof-of-work schemes, through its solution to the Byzantine consensus problem, and the robust construction of a P2P network. A growing body of research on the protocol is starting to emerge, tackling questions related to the protocol's scalability, its privacy, the security guarantees it provides, and more. Below I overview some of these topics. An introduction to the protocol and references to related literature can be found in [1, 3].

STOC'17-KEY, Montreal, Canada

DOI: 10.1145/3055399.3079074

2 RESEARCH TOPICS AND CHALLENGES

Scalability: Bitcoin blocks are generated slowly: only once every ten minutes in expectation. As a result, Bitcoin is restricted in its rate of transaction processing. Recent results have shown that as the number of transactions grows, the protocol's security deteriorates, and several modified protocols that improve scalability and transaction processing times have been suggested.
Incentives: The Bitcoin system is more secure against attacks if more computational power is used to generate proof-of-work by honest participants. Nodes are incentivized to join using rewards. Research has thus far identified several problems with the incentive compatibility of the protocol including issues in the propagation of transactions in the network, and in the mining process itself. Risk mitigation in mining pools and related incentives were also studied.
Anonymity: Bitcoin is not fully anonymous. Some information can be extracted about the identities of transacting entities. Improvements to the anonymity of the protocol have been proposed either using mixing, or other advanced techniques such as zero-knowledge proofs (such as in the ZeroCash protocol).
Alternative Currencies and Additional Protocol Layers: The Bitcoin protocol has been the inspiration for several other systems, some unrelated to money (e.g., NameCoin). Additional cryptocurrencies allow for advanced uses such as smart contracts (like the Ethereum system). Other protocol layers such as "the lightning network" allow for fast dedicated transaction channels alongside Bitcoin's blockchain.
Network Security: The connectivity of Bitcoin's P2P network is essential to its security. Attacks on underlying internet protocols and on network formation have also been considered.

REFERENCES

[1] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A Kroll, and Edward W Felten. 2015. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *Security and Privacy (SP), 2015 IEEE Symposium on*. IEEE, 104–121.
[2] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *https://bitcoin.org/bitcoin.pdf* (2008).
[3] Aviv Zohar. 2015. Bitcoin: under the hood. *Commun. ACM* 58, 9 (2015), 104–113.