On the Security and Scalability of Bitcoin's Blockchain

Ghassan O. Karame
NEC Laboratories Europe
69115 Heidelberg, Germany
ghassan@karame.org

ABSTRACT

The blockchain emerges as an innovative tool which proves to be useful in a number of application scenarios. A number of large industrial players, such as IBM, Microsoft, Intel, and NEC, are currently investing in exploiting the blockchain in order to enrich their portfolio of products. A number of researchers and practitioners speculate that the blockchain technology can change the way we see a number of online applications today. Although it is still early to tell for sure, it is expected that the blockchain will stimulate considerable changes to a large number of products and will positively impact the digital experience of many individuals around the globe.

In this tutorial, we overview, detail, and analyze the security provisions of Bitcoin and its underlying blockchain—effectively capturing recently reported attacks and threats in the system. Our contributions go beyond the mere analysis of reported vulnerabilities of Bitcoin; namely, we describe and evaluate a number of countermeasures to deter threats on the system—some of which have already been incorporated in the system. Recall that Bitcoin has been forked multiple times in order to fine-tune the consensus (i.e., the block generation time and the hash function), and the network parameters (e.g., the size of blocks). As such, the results reported in this tutorial are not only restricted to Bitcoin, but equally apply to a number of "altcoins" which are basically clones/forks of the Bitcoin source code.

Given the increasing number of alternative blockchain proposals, this tutorial extracts the basic security lessons learnt from the Bitcoin system with the aim to foster better designs and analysis of next-generation secure blockchain currencies and technologies.

1. BITCOIN'S BLOCKCHAIN

First introduced in 2008, Bitcoin has witnessed more adoption and attention than any other digital currency to date. Bitcoin is currently integrated across several businesses and has several exchange markets.

Users in Bitcoin execute payments by digitally signing their transactions and are prevented from double-spending their coins (i.e., signing-over the same coin to two different users) through a distributed time-stamping service. This service operates on top of the Bitcoin Peer-to-Peer (P2P) network that ensures that all transactions and their order of execution are available to all Bitcoin users.

To this end, Bitcoin relies on a Proof-of-Work (PoW) scheme that allows users to "mine" for digital coins by performing computations. More specifically, to generate a block, Bitcoin peers must find a nonce value that, when hashed with additional fields (i.e., the Merkle hash of all valid and received transactions, the hash of the previous block, and a timestamp), the result is below a given target value. If such a nonce is found, peers then include it (as well as the additional fields) in a block thus allowing any entity to publicly verify the PoW. Upon successfully generating a block, a peer is typically granted a number of new BTCs. This provides an incentive for peers to continuously support Bitcoin. The resulting block is forwarded to all users in the network, who can then check its correctness by verifying the hash computation. If the block is deemed to be "valid", then the users append it to their previously accepted blocks, thus growing the Bitcoin block chain. Bitcoin relies on this mechanism to resist double-spending attacks; for malicious users to double-spend a BTC without being detected, they would not only have to redo all the work required to compute the block where that BTC was spent, but also they need to recompute all the subsequent blocks in the chain.

Although the literature features a number of blockchain proposals, most existing blockchains leverage (a variant of) Bitcoin's expensive Proof of Work (PoW) consensus mechanism, which currently accounts for more than 90% of the total market capitalization of existing digital currencies.

In the last couple of years, most research was focused on the provisions of Bitcoin as a digital currency. Studies were analyzing the security and privacy of making payments in Bitcoin, the underlying economy of Bitcoin, etc. but completely overlooked a hidden potential within Bitcoin.

Bitcoin is indeed powered by a truly genuine breakthrough, the blockchain. This blockchain is the main engine on which Bitcoin is built, emerges as a novel distributed consensus scheme which allows transactions, and any other data, to be securely stored and verified without any centralized authority. As such, the blockchain fueled innovation, and a number of innovative applications have already been devised by exploiting the secure and distributed provisions of the blockchain.

However, existing experience with Bitcoin's blockchain reveals that there are still many challenges that need to be overcome:

Security Recent studies have shown a number of practical attacks [2–4] on Bitcoin. These attacks leverage weaknesses in the network and consensus layers of Bitcoin's blockchain in order to considerably increase the advantage of an adversary.

Scalability Currently, the Bitcoin blockchain can process a maximum of 7 transactions per second; this number is only ex-

CCS'16 October 24-28, 2016, Vienna, Austria

ACM ISBN 978-1-4503-4139-4/16/10.
DOI: http://dx.doi.org/10.1145/2976749.2976756

pected to increase. If the blockchain were to be used as a decentralized storage medium or were to process the transactional volume of Visa (around 50,000 transactions per second), there are serious concerns about the scalability of the current blockchain design.

Limits of (De-)centralization One of the main attractions of the blockchain lies in its decentralized aspects; the protocol is indeed fully decentralized and each entity in the network "votes" with its computing power. Although the protocol is designed for full de-centralization, a recent study [1] has shown the limits of decentralization in the current deployment blockchain. Currently, only few entities can control the entire process, since participants have considerable incentives to pool their computing power in centralized processes in order to increase their advantage in the network. There are currently several attempts to re-design the proof of work scheme in the blockchain in order to resolve these problems.

2. CONTENTS OF THE TUTORIAL

In this 1.5 hour tutorial, we thoroughly analyze the security provisions of Bitcoin in light of recent published attacks, and we discuss possible countermeasures. For instance, we show that the initial measures adopted in Bitcoin to handle fast payments are not enough to deter double-spending attacks, and discuss a first workable countermeasure against double-spending which is currently integrated in Bitcoin. Fast payments refer to payments where the time between the exchange of currency and goods is short (in the order of a minute). While the Bitcoin PoW-based time-stamping mechanism is essential for the detection of double-spending attacks (i.e, in which an adversary attempts to use some of her coins for two or more payments), it requires tens of minutes to verify a transaction and is therefore inappropriate for fast payments. Clearly, there is only limited value in verifying the payment after the user has obtained the goods (and e.g., left the store) or services (e.g., access to on-line content).

We also show that an adversary can deny the delivery of blocks and transactions to victim Bitcoin nodes for a considerable amount of time. We show that this can be achieved by exploiting Bitcoin bandwidth optimization techniques and the measures that are in place to tolerate network delays and congestion. The minimal requirement for this attack to succeed in practice is simply that the attacker can establish at least one connection to the victim. An even more powerful attack resulting in almost indefinite delays at the victim node only requires that the attacker can fill the victim's remaining open connection slots—without necessarily causing any network partitioning in the Bitcoin network.

These results therefore motivate the need for a careful design of the scalability mechanisms adopted in Bitcoin. While existing mechanisms limit the amount of propagated information in the system to the minimum necessary, we show that these techniques come at odds with security and reduce the ability of the network to e.g., detect double-spending attacks, resolve, or prevent blockchain forks. For instance, these findings suggest that an adversary who commands more than 33% of the computing power in the network can control the fate and security of all Bitcoin transactions. In this respect, we describe a modification of the block request process in Bitcoin to deter this misbehavior. Finally, in this chapter, we discuss the security of online wallets and outline a number of innovative techniques to ensure the protection of private keys against compromise and/or loss.

This tutorial go beyond the mere analysis of reported vulnerabilities of Bitcoin; namely, we describe and evaluate a number of countermeasures to deter threats on the system—some of which have already been incorporated in the system. Recall that Bitcoin has been forked multiple times in order to fine-tune the consensus (i.e., the block generation time and the hash function), and the network parameters (e.g., the size of blocks). For instance, Litecoin and Dogecoin—Bitcoin's most prominent forks—reduce the block generation time from 10 to 2.5 and 1 minute respectively. As such, the results reported in this tutorial are not only restricted to Bitcoin, but equally apply to a number of "altcoins" which are basically clones/forks of the Bitcoin source code.

Finally, we analyze the limits of decentralization in the Bitcoin ecosystem. Namely, based on recent incidents and observations, we show that the vital operations and decisions that Bitcoin is currently undertaking are not decentralized. More specifically, we show that a limited set of entities currently control the services, decision making, mining, and the incident resolution processes in Bitcoin. We also show that third-party entities can unilaterally decide to "devalue" any specific set of Bitcoin addresses pertaining to any entity participating in the system.

3. BIOGRAPHY OF AUTHOR

Ghassan is a Chief Researcher in the Security Group of NEC Research Laboratories in Germany. Until April 2012, he was working as a postdoctoral researcher in the Institute of Information Security of ETH Zurich, Switzerland. He holds a Master of Science degree in Information Networking from Carnegie Mellon University (CMU), and a PhD degree in Computer Science from ETH Zurich.

Ghassan is interested in all aspects of security and privacy with a focus on cloud security, SDN/network security, and Bitcoin/blockchain security. More details about Ghassan can be found at www.ghassankarame.com.

4. REFERENCES

[1] Arthur Gervais, Ghassan Karame, Srdjan Capkun, and Vedran Capkun. Is bitcoin a decentralized currency? In *IEEE Security and Privacy*, 2014.

[2] Arthur Gervais, Hubert Ritzdorf, Ghassan O Karame, and Srdjan Capkun. Tampering with the delivery of blocks and transactions in bitcoin. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 692–705. ACM, 2015.

[3] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg. Eclipse attacks on bitcoin's peer-to-peer network. 2015.

[4] Ghassan O. Karame, Elli Androulaki, and Srdjan Capkun. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS '12, New York, NY, USA, 2012. ACM.