Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

A survey on the security of blockchain systems

Xiaoqi Li [a], Peng Jiang [a], Ting Chen [b], Xiapu Luo [a,*], Qiaoyan Wen [c]

[a] *Department of Computing, The Hong Kong Polytechnic University, Hong Kong*
[b] *Center for Cybersecurity, University of Electronic Science and Technology of China, China*
[c] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, China*

HIGHLIGHTS

- We conduct the first systematic examination on security risks to popular blockchain systems.
- We survey the real attacks on blockchain systems and analyze related vulnerabilities exploited.
- We summarize practical academic achievements for enhancing the security of blockchain.
- We suggest a few future directions in the area of blockchain security.

ARTICLE INFO

Article history:
Received 21 January 2017
Received in revised form 11 July 2017
Accepted 14 August 2017
Available online xxxx

Keywords:
Blockchain
Security
Cryptocurrency
Smart contract

ABSTRACT

Since its inception, the blockchain technology has shown promising application prospects. From the initial cryptocurrency to the current smart contract, blockchain has been applied to many fields. Although there are some studies on the security and privacy issues of blockchain, there lacks a systematic examination on the security of blockchain systems. In this paper, we conduct a systematic study on the security threats to blockchain and survey the corresponding real attacks by examining popular blockchain systems. We also review the security enhancement solutions for blockchain, which could be used in the development of various blockchain systems, and suggest some future directions to stir research efforts into this area.

1. Introduction

Since the debut of Bitcoin in 2009, its underlying technique, blockchain, has shown promising application prospects and attracted lots of attentions from academia and industry. Being the first cryptocurrency, Bitcoin was rated as the top performing currency in 2015 [1] and the best performing commodity in 2016 [2], and has more than 300K confirmed transactions [3] daily in May, 2017. At the same time, the blockchain technique has been applied to many fields, including medicine [4–6], economics [7–9], Internet of things [10–12], software engineering [13–15] and so on. The introduction of Turing-complete programming languages to enable users to develop smart contracts running on the blockchain marks the start of blockchain 2.0 era. With the decentralized consensus mechanism of blockchain, smart contracts allow mutually distrusted users to complete data exchange or transaction without the need of any third-party trusted authority. Ethereum is now (May of 2017) the most widely used blockchain supporting smart contracts, where there are already 317,506 smart contracts and more than 75,000 transactions happened daily [16].

Since blockchain is one of the core technology in FinTech (Financial Technology) industry, users are very concerned about its security. Some security vulnerabilities and attacks have been recently reported. Loi et al. discover that 8,833 out of 19,366 existing Ethereum contracts are vulnerable [17]. Note that smart contracts with security vulnerabilities may lead to financial losses. For instance, in June 2016, the criminals attacked the smart contract `DAO` [18] by exploiting a recursive calling vulnerability, and stole around 60 million dollars. As another example, in March 2014, the criminals exploited transaction mutability in Bitcoin to attack `MtGox`, the largest Bitcoin trading platform. It caused the collapse of `MtGox`, with a value of 450 million dollars Bitcoin stolen [19].

Although there are some recent studies on the security of blockchain, none of them performs a systematic examination on the risks to blockchain systems, the corresponding real attacks, and the security enhancements. The closest research work to ours is [20] that only focuses on Ethereum smart contracts, rather than popular blockchain systems. From security programming perspective, their work analyzes the security vulnerabilities of Ethereum smart contracts, and provides a taxonomy of common programming pitfalls that may lead to vulnerabilities [20]. Although a series

[*] Corresponding author.
E-mail addresses: csxqli@comp.polyu.edu.hk (X. Li), cspjiang@comp.polyu.edu.hk (P. Jiang), brokendragon@uestc.edu.cn (T. Chen), csxluo@comp.polyu.edu.hk (X. Luo), wqy@bupt.edu.cn (Q. Wen).

http://dx.doi.org/10.1016/j.future.2017.08.020
0167-739X/© 2017 Elsevier B.V. All rights reserved.

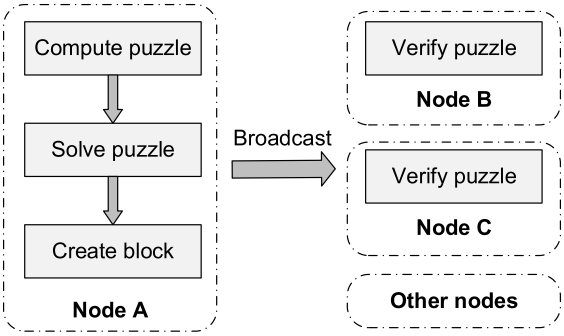

Fig. 1. PoW consensus mechanism.

of related attacks on smart contracts are listed in [20], there lacks a discussion on security enhancement. This paper focuses on the security of blockchain from more comprehensive perspectives. The main contributions of this paper are as follows:

(1) To the best of our knowledge, we conduct the *first* systematic examination on security risks to popular blockchain systems.

(2) We survey the real attacks on popular blockchain systems from 2009 to the present (May of 2017) and analyze the vulnerabilities exploited in these cases.

(3) We summarize practical academic achievements for enhancing the security of blockchain, and suggest a few future directions in this area.

The remainder of this paper is organized as follows. Section 2 introduces the main technologies used in blockchain systems. Section 3 systematically examines the security risks to blockchain, and Section 4 surveys real attacks on blockchain systems. After summarizing the security enhancements to blockchain in Section 5, we suggest a few future directions in Section 6. Finally, Section 7 concludes the paper.

2. Overview of blockchain technologies

This section introduces the main technologies employed in blockchain. We first present the fundamental trust mechanism (i.e., the consensus mechanism) used in blockchain, and then explain the synchronization process between nodes. After that, we introduce the two development stages of blockchain.

2.1. Consensus mechanism

Being a decentralized system, blockchain systems do not need a third-party trusted authority. Instead, to guarantee the reliability and consistency of the data and transactions, blockchain adopts the decentralized consensus mechanism. In the existing blockchain systems, there are four major consensus mechanisms [21]: PoW (Proof of Work), PoS (Proof of Stake), PBFT (Practical Byzantine Fault Tolerance), and DPoS (Delegated Proof of Stake). Other consensus mechanisms, such as PoB (Proof of Bandwidth) [22], PoET (Proof of Elapsed Time) [23], PoA(Proof of Authority) [24] and so on, are also used in some blockchain systems. The two most popular blockchain systems (i.e., Bitcoin and Ethereum) use the PoW mechanism. Ethereum also incorporates the PoA mechanism (i.e., Kovan public test chain [25]), and some other cryptocurrencies also use the PoS mechanism, such as PeerCoin, ShadowCash and so on.

PoW mechanism uses the solution of puzzles to prove the credibility of the data. The puzzle is usually a computationally hard but easily verifiable problem. When a node creates a block, it must resolve a PoW puzzle. After the PoW puzzle is resolved, it will be broadcasted to other nodes, so as to achieve the purpose of consensus, as shown in Fig. 1.

In different blockchain systems, the block structure may vary in detail. Typically in Bitcoin, each block contains `PrevHash`, `nonce`, and `Tx` [26]. In particular, `PrevHash` indicates the hash value of the last generated block, and `Txs` denote the transactions included in this block. The value of `nonce` is obtained by solving the PoW puzzle. A correct `nonce` should satisfy that the hash value shown in Eq. (1) is less than a target value, which could be adjusted to tune the difficulty of PoW puzzle.

$$SHA256(PrevHash \,||\, Tx1 \,||\, Tx2 \,||\, \dots \,||\, nonce) < Target \qquad (1)$$

PoS mechanism uses the proof of ownership of cryptocurrency to prove the credibility of the data. In PoS-based blockchain, during the process of creating block or transaction, users are required to pay a certain amount of cryptocurrency. If the block or transaction created can eventually be validated, the cryptocurrency will be returned to the original node as a bonus. Otherwise, it will be fined. In the PoW mechanism, it needs a lot of calculation, resulting in a waste of computing power. On the contrary, PoS mechanism can greatly reduce the amount of computation, thereby increasing the throughput of the entire blockchain system.

2.2. Block propagation and synchronization

In the blockchain, each full node stores the information of all blocks. Being the foundation to building consensus and trust for blockchain, the block propagation mechanisms can be divided into the following categories [27–29]:

(1) Advertisement-based propagation. This propagation mechanism is originated from Bitcoin. When node `A` receives the information of a block, `A` will send an `inv` message (a message type in Bitcoin) to its connected peers. When node `B` receives the `inv` message from `A`, it will do as follows. If node `B` already has the information of this block, it will do nothing. If node `B` does not have the information, it will reply to node `A`. When node `A` receives the reply message from node `B`, node `A` will send the complete information of this block to node `B`.

(2) Sendheaders propagation. This propagation mechanism is an improvement to the advertisement-based propagation mechanism. In the sendheaders propagation mechanism, node `B` will send a `sendheaders` message (a message type in Bitcoin) to node `A`. When node `A` receives the information of a block, it will send the block header information directly to node `B`. Compared with the advertisement-based propagation mechanism, node `A` does not need to send `inv` messages, and hence it speeds up the block propagation.

(3) Unsolicited push propagation. In the unsolicited push mechanism, after one block is mined, the miner will directly broadcast the block to other nodes. In this propagation mechanism, there is no `inv` message and `sendheaders` message. Compared with the previous two propagation mechanisms, unsolicited push mechanism can further improve the speed of block propagation.

(4) Relay network propagation. This propagation mechanism is an improvement to the unsolicited push mechanism. In this mechanism, all the miners share a transaction pool. Each transaction is replaced by a global ID, which will greatly reduce the broadcasted block size, thereby further reducing the network load and improving the propagation speed.

(5) Push/Advertisement hybrid propagation. This hybrid propagation mechanism is used in Ethereum. We assume that node `A` has n connected peers. In this mechanism, node `A` will push the block to $\sqrt{n}$ peers directly. For the other $n - \sqrt{n}$ connected peers, node `A` will advertise the block hash to them.

Please cite this article in press as: X. Li, et al., A survey on the security of blockchain systems, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.08.020.