DOI: http://dx.doi.org/10.26483/ijarcs.v13i5.6913

Volume 13, No. 5, September-October 2022

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

BLOCKCHAIN IN SECURITY: EVOLUTION, PPLICATIONS AND CHALLENGES

Dr. Maassoumeh (Afsaneh) Javadi
Fairlaigh Dickinson University
School of public and global affairs
Computer Security, United States

Abstract: Currently, blockchain as a core technology of much application has received attention. It is actually a distributed database which maintains a data record list that continuously grows. The secured distributed key behind of blockchain have the potential to address many online transactional applications such as Bitcoin. Due to increasing the usage of blockchain technology, especially in security-based applications, in this paper, we provide an analysis of security issues in the blockchain. Furthermore, we will discuss some use cases as well as challenges in this area.

Keywords: Bitcoin, Blockchain, Encryption, Security,

1. INTRODUCTION

Blockchain is an immutable and decentralized infrastructure ledger which constructed to keep track of all transactions across a peer to peer network [1]. Many believe that blockchain will play an undeniable role in next-generation online trading due to its ability to provide security of the digital transaction. According to a report by the Transparency Market Research, the market worth of global financial blockchain technology is expected to grow to about USD 20 billion by the end of 2024 [2].

Bitcoin [3] is the first cryptocurrency that uses a decentralized registry called distributed ledger technology to implement a trusted payment system in 2008 without third-party authority or central server. All blocks include three main parts: a cryptographic hash of the previous block, transaction data and a timestamp token which protected using PKI digital signature. A decentralized key management system is used in blockchain to provide a secure scheme to solve the double-spending problem [4]. The blocks as a basic component of the blockchain is a continuously growing list of records, which are linked and secured using cryptography.

The separate blocks are identified by a hash value which is generated using a cryptographic hash algorithm (SHA-256) on the header of the block [5]. An individual block has only one parent but can have multiple child each referring to the same parent block while contains same hash in the previous block hash field. All blocks contain a hash of parent block in their own header and the sequence of hashes linking individual block with their parent block creates a big chain pointing to the first block called as genesis block [6].

For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks[1]. The blockchain transaction includes three main steps: create a transaction, verify the transaction and finally enforce transaction to finalize. The blockchain finalizes a transaction through the authentication process work when a person who loans electronic cash forms a block by combining the transactions over the network.

The primary features of blockchain technology include the elimination of intermediaries, ease of use, and simplicity in verification of transactions, improved security, low-cost transparency, decentralization, and immutability. The biggest benefit of it is in its immutability that it is not easy to alter the data, once recorded.

A secured bitcoin protocol has been shown in Fig.1.

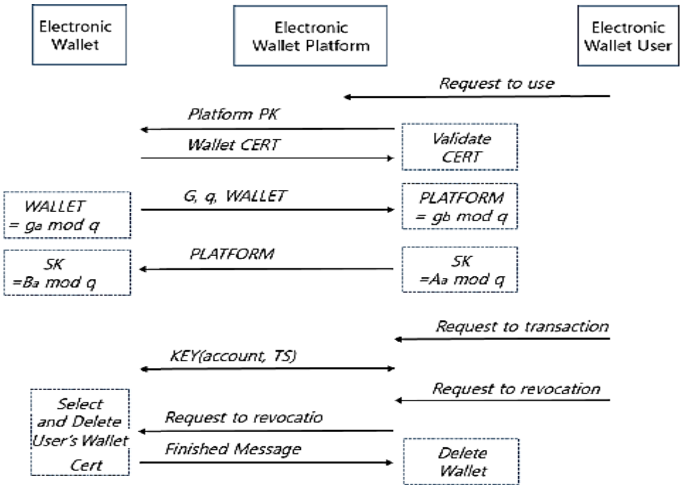

Fig.1. Secure bitcoin protocol [7]

There are three main types of blockchain networks: 1- Public blockchain: which everyone can see all the transactions, expect their transaction to appear on the ledger and everyone can participate to the consensus process, 2- Permissioned (private) blockchain: which usually used inside a company and only specific members are allowed to access it and carry out transactions. 3- Consortium blockchain: which only a limited number of nodes are given the permission to do transaction. The access to the blockchain, however, can be public or restricted to the participants.

This paper explores insight into security in blockchain technology and its evolution and challenges. The paper also classifies the security-based real-word applications of the blockchain. Although many papers have been done to address the subject, most studies do not focus on security- related aspect of blockchain and related evolution.
The rest of the paper is structured as follows. The evolution of blockchain is argued in Section 2. Section
3 discusses some blockchain-based practical systems and applications. Several security issues and discussion are given in Section 4. Finally, concluding remarks are presented in Section 5. BLOCKCHAIN IN

2. BLOCKCHAIN EVOLUTION

In the past, blockchain was known only as a distributed ledger technology for financial transactions. Consequently, it seemed like an enigmatic concept that only technologists could understand it. However, the various advancements in blockchain applications during last years helped more developer and businesses see its potential, especially in cyber-security applications. In this section, we look at the evolution of blockchain technology and its progress [8].

Blockchain Version 1.0: Currency

The implementation of distributed ledger technology led to its first and obvious application: cryptocurrencies. This allows financial transactions based on blockchain technology (for the sake of simplicity often seen as synonyms) to be executed with Bitcoin being the most prominent example in thissegment. It is being used as “cash for the Internet”, a digital payment system and can be seen as the enabler of an Internet of Money [9].

Blockchain Version 2.0: Smart Contracts

The new key concept is smart contracts, small computer programs that live in the blockchain. They are autonomous computer programs that execute automatically and conditions defined beforehand such as the facilitation, verification or enforcement of the performance of a contract. One big advantage this technology offers is the blockchain making it impossible to tamper with or hack smart contracts. So smart contracts reduce the cost of verification, execution, arbitration and fraud prevention and allow transparent contract definition overcoming the moral hazard problem. Most prominent in this field is the Ethereum Blockchain [15] with its aim at allowing the implementation of smart contracts.

Blockchain Version 3.0: Decentralized Applications

Decentralized applications use decentralized storage and communication, so most decentralized applications have their backend code running blockchain on a decentralized peer-to-peer network. In contrast, a traditional application has its backend code running on centralized servers. The decentralized applications can have frontend code and user interfaces written in any language that can make calls to its backend, like traditional applications. But a decentralized application can has its frontend hosted on decentralized storages such as Ethereums swarm [15].

Blockchain Version 4.0: Growth in Applications

With the foundations laid by the previous versions, for use blockchain 4.0 describes solutions and approaches that make blockchain technology usable to business and industry demands. As it discussed in Section 3, the blockchain industry meaning in short terms automation, enterprise resource planning, and integration of different execution systems. However, this industrial revolution demands an increasing degree of trust and privacy protection. When adding blockchain to automated systems one ends up with business integration, allowing cross-system and cross-blockchain business processes, i.e. machines safely and autonomously placing an order for their replacement parts to arrive.

3. THE BLOCKCHAIN-BASED APPLICATIONS

The applications of blockchain are more than just cryptocurrency like bitcoin. Currently, there are high demands for blockchain-based security applications. Decentralized nature of blockchain makes it potentially suitable for the recording of transactions and events. Therefore, as a platform, blockchain’s applications will impact other industry and manufacturing in both financial and non-financial areas [10]. Many companies like Accenture, IBM, and Oracle, among others, have been offering the blockchain as a service for the past couple of years. There are remarkable real-world problems especially in security- related applications that blockchain has the potential to address them. In this paper we focus on only a few important applications of blockchain-based security in real-world as below:

1. Cybersecurity: such as security in peer-to-peer (P2P) networks, web development, and clouds. 2- Financial services [9]: such as payment transactions, security in registration and lending.
2. Governmental Services (GS): GS is another related

concept which is regarding the authority of ownership such as voting, registrations such as passports, driving license and permits.

3. Authentication in trading and business: such as document exchange, insurance, asset exchange, trade agreements.
4. Smart property sector: such as user reputation in real estate, intellectual property, notary, the property ownership tracking.
5. Identification and security: Using in validation the possession of official papers and existing document such as party or device registration, medical records such as Electronic Health Record (EHR) [8] and access control of the legal document.
6. Internet of Things (IoT) as a service to inter-connect between users and objects is used in autonomous devices such as cars, drones, and robots to prevent DDoS attacks [10]. The provision of security based on blockchain technology has attracted the interest of many designers to adapt their platform to achieve this objective.

The above-mentioned applications are just a few examples of areas that can be empowered by blockchain technology. There is also much other application such as supply chain management in large food manufacturing to monitor the product turnover, approval workflows chain and etc. that use the blockchain technology[11].

4. SECURITY CHALLENGES OF BLOCKCHAIN

The blockchain technology has been implemented in cryptocurrency as a safe and decentralized infrastructure ledger. Even the U.S. Defense Advanced Research Projects Agency (DARPA) is considering blockchain technology to create an unhackable messaging system. However, a number of security issues reported in blockchain software, transactions, and wallet [13]. Blockchain-based applications face numerous challenges during their life. In [14], authors perform a survey on the major attacks on the bitcoin system and blockchain-based consensus protocol until 2018. For instance, in 2016, hackers exploited an unforeseen quirk in a smart contract written on Ethereum’s [15] blockchain to steal 3.6 million ether, worth around $80 million at the time, from the Decentralized Autonomous Organization,

(DAO), a new kind of blockchain-based investment fund [16]. Moreover, in [17], the authors reference some risks in different level of danger associated with Bitcoin technology which same can be applied to any blockchain architecture.

Here we discuss major challenges and issues that were greatest concern in literature and real- world blockchain’s applications, especially in the private domain. Covering the potential risks and challenges of the blockchain technology is important to prevent possible side effects that may happen during the implementation.

1- Public and private key security

The main share of blockchain security is associated with the keys used in encryption. Transactions of users fulfilled with the private and public key without identity exposure. However, the study is shown in [18] that key security in blockchain does not guarantee due to privacy leakage. The attacker installs malware and on the devices to leak the user’s personal key and use it to hack the secured transactions. Some researchers have proposed software methods to encounter the problem, while others offer hardware approaches such as a token for the approval of a transaction to protect the personal key. The blockchain, as in the original design, are made to be publicly visible. In the case of cryptocurrency, this is an important feature. However, for governments and corporations, this creates a number of concerns. Governments and corporations have a need to be able to protect and restrict access to their data for a myriad of reasons. However, as discussed in Section 3, the blockchain can be customized to meet the needs and specifications of the applications. A blockchain can be made permissible. This means that people are only able to access parts of the blockchain that are relevant to their tasks. Although creating such blockchains takes a remarkable amount of planning and expertise, it lessens the worry that firms and governments have about the technology, thus making adoption more likely.

2. Administrative Risks

Although the blockchain technology has limitless potential to shake up a variety of industry, it carries its own set of inherent risks. Below, we identified roughly major risks that may arise due to its implementation of the blockchain. One major security flaws occur in the code written for the wallet or code bugs. As evidence, the majority of the attacks that occurred on the bitcoin are due to the code is written for the access and the security of the wallet by the bitcoin exchanges. Third-party software companies usually write this sort of codes for the exchange transactions. Alternatively, technical risks could be rise due to timing and volatility issues in finding and processing of a block. These types of threat might lead to migrate the users towards using other technologies that offer faster services.

Distributed Denial of Service (DDoS) Attack is next risk that frequency happening on the bitcoin exchanges [19]. Although though DDoS attack intrinsically cannot steal the bitcoins from the wallet, it can disrupt the services of the exchange and lower the value of the bitcoin. Some attackers do it before purchasing the bitcoins, while the rest blackmail the owners of the companies to pay a significant amount of money to stop the attack.

3- Lack of regulation and standards

One of the primary blockchain security issues is the lack of regulation and standards [20]. While developers try to benefit the advantages of decentralized blockchain technology as possible, there is no way to learn from the mistakes of previous designers. Further, using a diverse set of rules by different organizations and consortium mean various new security risks for blockchain-based products. Thisunclear outlook leads to frustration of the developers to use this technology in long term. Besides, without clear guidance and a cooperative of community, standardization lead to chaos and reach a consensus.

4- Scalability

With increasing the number of transactions per day, all nodes have to store more and more blocks due to check its validity. One of the security concerns is what happens at full scale? Although DLT architecture is fundamentally scalable, however in bulky scale, after a huge number of changes it will be unspent [21]. Besides, processors throughput are originally restricted in capacity and speed and processing new block requires an interval, fulfill enormous number of transactions would not possible in real-time mode.

5. Untested Code

Nowadays, blockchain is used in many different kinds of cryptocurrencies. Some developers might distortthe result of blockchain performance to attract users due to a vast profit of the business. But in reality, when users want to combine blockchain into their applications, they have to know which blockchain fits their requirements. So blockchain testing mechanism needs to be in place to test different blockchains. Blockchain testing could be separated into two phases [22]: the standardization phase and testing phase. In the standardization phase, all criteria have to be made and agreed. When a blockchain is born, it could be tested with the agreed criteria to valid if the blockchain works fine as developers claim. In the testing phase, blockchain testing needs to be performed with different criteria. For example, a user who is in charge of online retail business cares about the throughput of the blockchain, so the examination needs to test the average time from a user send a transaction to the transaction is packed into the blockchain, capacity for a blockchain block and etc.

6- Processing speed, number of processes per unit of time

As the number of the blocks in blockchain increase, the required resources to fulfill and finalizing the transactions will be rise. In the other words, the trend to use of storage, bandwidth, and compute power required by fully participating nodes in the network will increase. Accordingly, some developer argues that due to low throughput, the blockchain can only process a limited number of transactions. Also, the time required to process a block of transactions is slow. For example, currently, block time process for bitcoin is 10 minutes, while for Ethereum block times are around 14 seconds [15]. These times are even longer during peak moments. Compare that to the nearly instantaneous confirmations we get when using services like Square or Visa.

7-Finalizing of transactions

The unconfirmed transaction has been an enigmatic side of blockchain technology that must pay special attention by designers. The computation time necessary to distribute and finalize a transaction can take several hours inherently. This issue will be prohibitively expensive for little payment in the financial projects. The prof-of-work is a solution to distributed synchronization and the unfinalized issue of choosing which transaction should be involved in the distributed ledger at a time. BLOCKCHAIN IN

8- Coordination with legacy systems

In spite of the general trend to the blockchain-based security, many organizations are hesitant toward a plan to blockchain solutions. It is due to involvement a precise strategy, financial plan and time that would be required in order to achieve successful implementation. In order to adapt to the existing environment with a blockchain-based system, some cases must either completely renovation their system or find an approach to integrate their existing system with the blockchain-enabled solution. However, it may be difficult for blockchain solutions to handle all functions needed by organizations. Consequently, in order to facilitate a smooth transition, considerable changes must be made to the existing systems. This process may take a significant amount of time, funds, and human expertise. In some organization, it may be impossible to adapt two different strategies, and finally, the organizations must decide to replace a new blockchain-friendly system [23].

In addition to above mention challenges, there are also other issues such as selfish mining, 51% attack (also known as a majority attack) and identity that adequately addressed in the literature and have been omitted due to conservation in time and space.

5. CONCLUSIONS

Nowadays, Blockchain becomes more and more popular in academia and industry areas. Anonymity, persistency, decentralization, auditability, and privacy are the major advantages and attraction to use the blockchain technology. But the distributed security scheme of the blockchain could be the main reason for the vast usage of this technology in real-world applications. In this paper, we present a brief introduction to blockchain’s solution and its characteristics and applications. Furthermore, some security challenges and issues which still exist are discussed in section 3 and 4. It seems that blockchain has proven its robustness and security. While we are at almost in the beginning ofthe blockchain technology, it is too early to say that this revolution could fill the gap of security in distributed and network-based applications or not.

REFERENCES

[1] https://blockchain.info

[2] Transparency Market Research, Available online https://www.transparencymarketresearch.com/ blockchain-technology-market.html

[3] https://bitcoin.org/en

[4] A. Antonopoulus, "Mastering Bitcoin: Programming the Open Blockchain", 2nd Edition, O'Reilly Press, 2017.

[5] I. Eyal, A.E. Gencer, E.G. Sirer, and R. Renesse, "Bitcoin-NG: A scalable blockchain protocol", In Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), CA, USA, February 2016.

[6] https://en.wikipedia.org/wiki/Block_chain_(database)

[7] J. Park, and J. Park, "Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions", Symmetry, vol.9, no.8, 2017, 9.164.10.3390/sym9080164.

[8] M. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", IEEE International Congress on Big Data (BigData Congress),USA,2017, DOI: 10.1109/BigDataCongress.2017.85

[9] https://en.wikipedia.org/wiki/Bitcoin_network/

[10] K. Fanning, and D. P. Centers, "Blockchain and its coming impact on financial services", Journal of Corporate Accounting & Finance, vol.27, no.5, p.p.53-57, 2016.

[11] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management", IEEE International Conference on Open and Big Data (OBD), pp.25-30, USA, 2016.

[12] S. Underwood, "Blockchain beyond bitcoin", Communications of the ACM, vol.59, no.11, p.p.15-17, 2016.

[13] P.B. Samuel, "The Primary Challenge to Blockchain Technology", Available online at https:// www.forbes.com, 2017.

[14] M. Kiran, and M. Stannett, "Bitcoin risk analysis" Available: http://www.nemode.ac.uk/wp-content/ uploads/2015/02/2015-Bit-Coin-risk-analysis.pdf , Dec. 2014

[15] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger", Ethereum Project Yellow Paper, vol.151, 2014.

[16] N. Yamada, M. Tsukuda, J. Nemoto, K, Naganuma, N. Nishijima and T. Sato "Work on the Potential and Challenges of Blockchain Technology", Hitachi Review, vol.66, no.1, p.p.31-35, 2017.

[17] A. Lielacher, "Five Challenges Blockchain Technology Must Overcome Before Mainstream Adoption", Bitcoin Magazine, January 2018.

[18] G. Zyskind, and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data", IEEE Security and Privacy Workshops (SPW), pp.180-184, 2015.

[19] M. Pilkington, "Blockchain technology: principles and applications", Research handbook on digital transformations, p.p.225-235, 2016.

[20] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C.P.A. Ogah, and Z. Sun, "Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems", IEEE Internet of Things Journal, vol.4, no.6, pp.1832-1843, 2017.

[21] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security", 2nd International IEEE Conference on Contemporary Computing and Informatics (IC3I), p.p.463-467, India, 2016.

[22] Framework for Blockchain-based business integration, online: https://medium.com/@UnibrightIO/ blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666 , 2017.

[23] M. Conti, S. Kumar, C. Lal and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin", IEEE Communications Surveys & Tutorials, 2018, DOI: 10.1109/COMST.2018.2842460