Blockchain Security Hole: Issues and Solutions

Norul Suhaliana bt Abd Halim[1], Md Arafatur Rahman[1,2(✉)], Saiful Azad[1,2], and Muhammad Nomani Kabir[1]

[1] Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang, 26300 Gambang, Pahang, Malaysia
suliehalim@gmail.com, arafatiium@gmail.com, {saifulazad, nomanikabir}@ump.edu.my
[2] IBM CoE, Universiti Malaysia Pahang, 26300 Gambang, Pahang, Malaysia

Abstract. Blockchain technology is widely known because it is the underlying technology used by the bitcoin. It became more popular because it also can be used as backbone for various applications in finance, media, security and others. One of the main concerns for this technology is how secure the information that the users distributed over the network. This paper studies and highlights the important security issues concerned and discusses the solutions that proposed by the researchers and theoretical solution proposed to address some of the issues. However, this approach needs to be investigated further if it is to be implemented later in the near future. This paper can give direction for future researchers who are interested of this area.

Keywords: Blockchain technology · Security · Public ledger · Cryptocurrencies · PoW · Smart contract · Bitcoin · Decentralized peer-to-peer

1 Introduction

Imagine that one day you, as a user B, really need an amount of money urgently. Borrowing through banks will take some time because of the procedures. Then you find out there is a group of people (network nodes) who voluntarily can give you the money instantly as long as you join their group. The procedure is simple, you just have to announce about your need to all the group members. Then one of them (user B) will keep the details into a limited distributed ledger. He is also called as the "miner". When the ledger is created, the miners will put it through a process. They take the information in the ledger, and apply a puzzle to it, turning it into something else which is a far shorter, seemingly random sequence of letters and numbers known as a hash. It is kept along with the ledger, at the end of the general ledger at that point in time. All of the group members will try to solve the puzzle competitively. After some times, one of them will get the solution for the puzzle. When 51% of the group members verify and approve the solution and the ledger, then the money is yours. That first puzzle solver will be rewarded with certain amount of currency of the group and this process is called 'mining' [1]. After that, the members of the group will proceed with other request to a new ledger and so on. That is the concept of blockchain. It is the solid foundation of the current digital cryptocurrency bitcoin. It can be defined as "a chain of blocks that

F. Saeed et al. (eds.), *Recent Trends in Information and Communication Technology*, Lecture Notes on Data Engineering and Communications Technologies 5, DOI 10.1007/978-3-319-59427-9_76

produce a distributed ledger which contains data of the transaction" [2]. Figure 1 summarizes this process of money transfer.

In 2008, a mystery, unknown author called Satoshi Nakamoto wrote a whitepaper about accomplishing non-reversible and cash-like transactions without using any third party in the middle of it [3]. He stressed more on bitcoin but never mentioned the word 'blockchain'. However, today, blockchain is gaining rapidly popularity than the bitcoin since it was found out that the technology could be used for far more than just for the cryptocurrencies.

Generally, there are three types of blockchain: Public, Private and Hybrid blockchain. Public ledgers are reachable by all users of the Internet. In a private ledger, there is a certain authority that monitors the write-permissions of the blocks added but the Read-permissions are either public or restricted. Between them, there is "partially decentralized" blockchains that form a hybrid between the public and the private blockchains [4].

The puzzle in the earlier story is referring to the term "Proof-Of-Work (PoW)". It can be defined as "a mathematical problem which is difficult to solve but easy to verify the solution [5]". This puzzle is essential to ensure the reliability of the block and is solved competitively by all of the network nodes [6]. Thus, the need for a middle authority of the transaction could be removed [3].

The goal of this work is to summarize the state of the art about major concerned issues in the usage of blockchain: the security issues of the information distributed over the network, and other challenges that the blockchain usage facing. The paper is structured as follows. In Sect. 2 the current applications of blockchain is examined, and continue with Sect. 3, where the security issues and the other challenges are noted down. Next, the proposed solutions of blockchain security are discussed in Sect. 4. Finally, a conclusion is drawn in Sect. 5. Theoretical Research involves qualitative method is used as the methodology of the work.

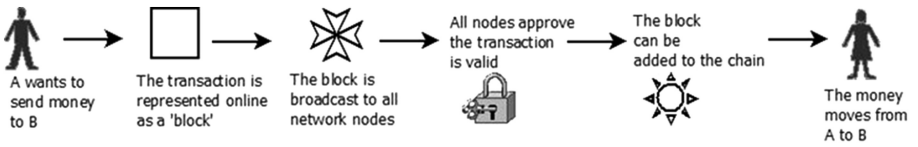

Fig. 1. How a blockchain works.

2 Current Applications

As the underlying support of the bitcoin currency, blockchain technology has intrigues programmers, businesspersons and investors all over the world. The current applications are discussed below.

2.1 Digital Payments (Cryptocurrencies)

Cryptocurrency is a digital token that used as a medium of transactions using encryption to secure the exchange and to control the creation of additional units of the currency. It is

a kind of alternative currencies for paper currencies. Today most of the popular tokens are bitcoin, ethereum and litecoin. In Bitcoin, two unique types of information are distributed: transactions and blocks. Transactions are the natives that allow a value transfer, while blocks are employed to synchronize state across all network nodes [6]. It depends entirely on a network of volunteers to implement a distributed ledger rather than any government agencies. While Bitcoin is an application on a decentralized but mono compute resource, ethereum is a project that performs this framework in a more generalized manner [7]. It is based on Bitcoin protocol and tries to create the generalized technology aiming a trustful object messaging compute framework. It is a blockchain-based programming language that enable code-based contracts and decentralized applications. Lastly, Litecoin uses the same primitive as Bitcoin but it excels than Bitcoin in most ways. Table 1 shows the comparisons among currencies in general [8].

Table 1. Comparison of Bitcoin, Ethereum and Litecoin.

Items	Bitcoin	Litecoin	Ethereum
Coin limit	21 Million	84 Million	infinite
Algorithm	SHA-256	Scrypt	Ethash
Mean block Time	10 min	2.5 min	15 s
Difficulty retarget	2016 block	2016 blocks	1 blocks
Block reward details	Halved every 210,000 blocks	Halved every 840,000 blocks	Halved every 2,895,494 blocks
Initial rewards	50 BTC	50 LTC	5 coins
Current block reward	25 BTC	50 LTC	5 coins
Block explorer	blockchain.info	block-explorer.com	http://etherhub.io

2.2 Smart Contracts

Smart contracts are auto-executing scripts that stored permanently on specific address on the Ethereum blockchain. It permits for the automation of certain processes. It can be defined as "a computerized transaction protocol that executes the terms of a contract" [9]. The aim is to reduce the need for reliable third parties between transacting nodes, and the incidence of harmful or accidental exceptions.

2.3 Database and Record Management

There are many reasons why records management professionals embrace blockchain into their areas. Besides security, flexibility, and cost saving, it is also efficient in many ways. Asset registry is one of the main areas that largely using this technology. Blockhain technology enables the application functionality throughout all businesses fragment in financial, markets and money transactions [10]. The property with blockchain-encoded becomes smart property that is conducted by smart contracts. To

be a smart property, the property could be physical assets like a home or hard-to-value assets like copyrights and stock shares. Any of it can be registered into the blockchain and the person who has the private key could dominate its ownership. The asset's owner can sell the property by transferring the key to another party. Then the asset is called smart property.

2.4 Content Distribution

The technology of blockchain also has revolutionize media industries in order to transform the area to be more secure, fast-access contents and more customer-centric. To date, it is used in the digital content distribution and peer-to-peer broadcast protocol and other services as well.

Digital Content Distribution. A blockchain can be applied to keep a cryptographies hash of digital media file, connecting it with the addresses and identify the creator [11]. Kishigami et al. provides a blockchain-based digital content distribution system and show a prototype of the concept [12]. In the system, the content owner can control everything and the operation should be an easy operation. Figure 2 shows the application of blockchain-based content distribution system in entertainment industries where the author can distribute his content to the network but still have control over it.

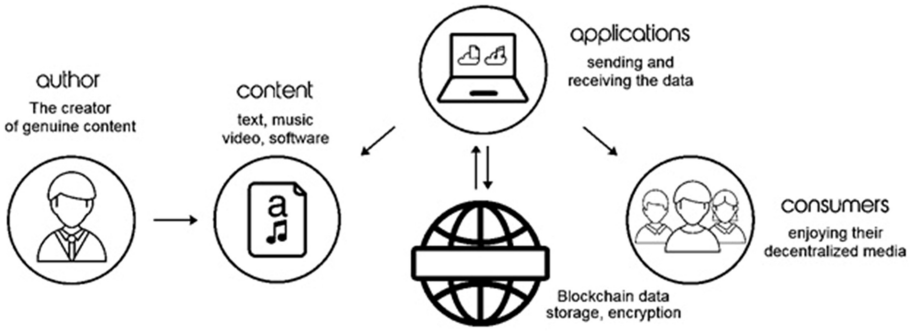

Fig. 2. Blockchain-based content distribution system in entertainment industries.

P2P Broadcast Protocol. Peer-to-peer network are famous for its usage as the multimedia files sharing medium [13]. It contains nodes who behave both as servers and clients and able to request or receive information from other nodes at the same time. Blockchain was a great device for this network since it introduced trustless authentications. This is because the system does not have to concern about external malicious attacks. However, while the blockchain offers a secured and trustless decentralized system, it needs an efficient P2P protocol to calculate the amount of broadcast messages being generated.

3 Security Issues and Challenges

While being used in all areas of applications, there are still security concerns and other challenges that need to be addressed by blockchain community. Below are few of main issues and challenges that have been highlighted by the previous works of the issues researches.

3.1 Security Issues

Transaction Malleability. Transaction malleability is an attack where someone change the unique ID of a transaction before the transaction is confirmed by the network nodes [14]. This open the opportunity for an attacker to interrupts and modify a transaction, causing the transaction legal entity to believe that the original transaction was not confirmed. Since it still having all the valid addresses and public key address, the network will approve it and bitcoins would be transferred to the attacker's account. Then the attacker would complain the issuer that he has not received the supposed bitcoins and hence the company needs to resend the amount of bitcoins [15].

Network Security. Eclipse attacks happen when an opponent controls fragments of the network communication and logically dividing the network, which can increase the synchronization delays. It can be a simple denial of service (DoS) attacks to improved selfish mining and double-spending [16]. In an eclipse attack, the attacker chooses and hides some information from one or more participants, such as delays the delivery of a block to a node.

Double Spending Attack. The double-spending problem is also best referred to the "Two Generals' Problem," [17] where there are two generals whose troops are going to attack a same enemy but situated on different camp bases. The problem is to take both general's agreement on the time of attack, and each of them must know that the other knows they have agreed. This is not easy since acknowledgement of receipt and the message can be lost during the delivery. Thus, a latent infinite chain of messages is needed to reach consensus [18].

Dust Transactions. It is a type of Denial of service (DoS) attacks where very small transactions sending very small amount of bitcoins but taking huge blockchain space [18].

3.2 Other Challenges

Wasted Resources. The mining of blockchain requires severely high computational resources [19]. To chain the blocks, imagine a picket fences builder company. Each worker is paid on a per-picket basis. The only limitation is each worker must design manually the picket from a piece of lumber before placing it in the fence. For those who complete their picket first, it must be approved by the others that the new picket matches the previously created pickets in the fence. If it is a match, the new picket is placed in the fence and chained to the previously pickets. The worker then is paid and all of the other workers must get rid of their unfinished pickets.

Privacy. Transaction In the blockchain, privacy and confidentiality still make up a problem. Each nodes can access other node's data and those who take a look at the blockchain may also see the transactions [20]. There are methods proposed by researches to overcome this issue, but these methods may practical to certain applications only and may not cover all of them.

Redundancy. Having copies of every transaction at every nodes of the network is a very costly redundancy whose only purpose is to remove intermediation. For any financially or legally, it is illogical to have both redundancy and an intermediary simultaneously. For example, a bank will not be too happy either to share all its transactions with all banks or to complete other bank's transactions. It just increases the cost without any imaginable advantage [21].

Regulatory Compliance. Blockchains exist unrelated with the law, as any government authority cannot change their operation. Applying blockchain technology in law or finance areas, with currencies other than Bitcoin will result in regulatory difficulties. Regulations for an infrastructure are very dissimilar from that of blockchain [21].

4 Solutions

This section covers a few proposed solutions from related works of the blockchain security and the comparison of the solutions. Then this paper proposed a solution based on the previous proposed solutions.

4.1 Current Solutions

Pegged Sidechains. This technique uses the two-way peg mechanism where coins are transferred from one blockchain to its sidechain back and forth at a certain exchange rate [22]. Sidechains are another Blockchains that are backed by Bitcoins via Bitcoin Contract, just as ringgit and pounds used to be support by Gold [23]. It approves data from another blockchains. Simplified payment verification (SPV) allows a client to verify that a transaction is included in the Bitcoin blockchain, without have to download whole blockchain. Since not every sidechain can be watched by the parent chain, users import proofs of work from the sidechain into the parent chain in order to prove possession. To use Bitcoin as the parent chain, an addition to the script would be required in order to can identify and approved such SPV proofs.

Collective Signing. Kokoris-Kogias, Eleftherios, et al. in their paper "Enhancing bitcoin security and performance with strong consistency via collective signing" introduces ByzCoin, a protocol that use Byzantine consensus for leveraging scalable collective signing to perpetrate transactions irrevocably within seconds. It adapts Practical Byzantine Fault Tolerance (PBFT) consistency to cryptocurrencies by addressing the issues of open membership, scalability to hundreds of replicas, proof-of-work block conflicts, and the transaction commitment rate. The PBFT provides a strong state machine replication mechanism for providing extremely reliable and constant services.

Two-Factor Authentication. In Bitcoin, the blockchain is known to all users. The transaction sender and receiver address are generated from the public key resulted from the key pairs of both of them. Then the transaction is signed using the Elliptic Curve Digital Signature Algorithm (ECDSA) sender's private key. This algorithm is designed to make certain that only the right owner can spent the bitcoin funds. A user may have many addresses, thus a wallet is used to keep all of these addresses either on the user's device or any online service. This wallet is reachable by the thieves who interested in getting to the bitcoin, so the two-factor authentication for a Bitcoin wallet has been proposed. Using this approach, a device wallet does not keep private keys but just shares of them. The other shares will be kept on another independent device such as the smart phone. Thus, any transaction can only be completed (signed) if both shares of the private key on both devices are accessible [23]. Table 2 shows the comparisons of the proposed techniques.

Table 2. Comparison of proposed techniques.

Items	Pegged sidechains	Collective signing	Two-factor authentication
Mechanism	SPV	PBFT	ECDSA
Objective	Prevent double spending	Addressing openness, scalability, PoW issues	Only right owner can spent the bitcoin
Protocol runtime	-	Less than 1/4 of the system's hash power	3.8 s
Way of work	Verify that a transaction is included in the Bitcoin blockchain	Leveraging scalable collective signing to perpetrate transactions irrevocably in seconds	Generating public keys and transaction is signed using the ECDSA sender's private key

5 Conclusions

Based on the proposed solutions, in theory, another solution can be derived from the combination of the pegged sidechains and the two-factor authentication to address the reversibility and privacy of the blockchain. In this concept, first the Simplified Payment Verification (SPV) will be used to verify that the transaction has been recorded and then the transactions should be signed by the Elliptic Curve Digital Signature Algorithm (ECDSA) sender's private key in order to make sure that only the right owner can spent the fund. Creating a wallet to store the keys is essential but another level of authentication by keeping the shares in different devices would strengthen the security of the transaction. Thus, this idea worth to be explored further in future works of blockchain security with more studies and researches need to be done.

Acknowledgement. This work is partially supported by the RDU grant, (no. RDU160360), funded by University Malaysia Pahang (UMP), Malaysia.

References

1. Dorri, A., Kanhere, S.S., Jurdak, R.: Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187 (2016)
2. Zyskind, G., Nathan, O.: Decentralizing privacy: using blockchain to protect personal data. In: 2015 IEEE Conference on Security and Privacy Workshops (SPW). IEEE (2015)
3. Roth, N.: An architectural assessment of bitcoin: using the systems modeling language. Procedia Comput. Sci. **44**, 527–536 (2015)
4. Pilkington, M.: Blockchain technology: principles and applications. In: Research Handbook on Digital Transformations (2016)
5. Ammous Saifedean, H.: Blockchain Technology: What is it good for? Browser Download This Paper (2016)
6. Decker, C.: On the scalability and security of bitcoin. Ph.D. diss. (2016)
7. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper (2014)
8. Coindesk. http://www.coindesk.com/information/comparing-litecoin-bitcoin/
9. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. IEEE Access **4**, 2292–2303 (2016)
10. Melanie, S.: Blockchain: Blueprint for a New Economy. O'Reilly Media Inc., Sebastopol (2015)
11. Deloitte Global. https://www2.deloitte.com/
12. Kishigami, J., Fujimura, S., Watanabe, H., Nakadaira, A., Akutsu, A.: The blockchain-based digital content distribution system. In: 2015 IEEE Fifth International Conference on Big Data and Cloud Computing, Dalian, pp. 187–190 (2015)
13. Washbourne, L.: A survey of P2P network security. arXiv preprint arXiv:1504.01358 (2015)
14. Christian, D., Wattenhofer, D.: Bitcoin transaction malleability and MtGox. In: European Symposium on Research in Computer Security, pp. 313–326. Springer International Publishing (2014)
15. Rajput, U., Abbas, F., Hussain, R., Eun, H., Oh, H.: A simple yet efficient approach to combat transaction malleability in bitcoin. In: Rhee, K.-H., Yi, J.H. (eds.) 15th International Workshop on Information Security Applications, WISA 2014, Jeju Island, Korea, Revised Selected Papers. Springer International Publishing, Cham (2014)
16. Wust, K.: Security of blockchain technologies. Ph.D. diss. (2016)
17. Bradbury, D.: The problem with Bitcoin. Comput. Fraud Secur. **2013**(11), 5–8 (2015)
18. Kiviat, I.: Beyond bitcoin: issues in regulating blockchain transactions. Duke Law J. **6**, 569 (2015)
19. Chepurnoy, A., Larangeira, M., Ojiganov, A.: A prunable blockchain consensus protocol based on non-interactive proofs of past states retrievability. arXiv preprint arXiv:1603.07926 (2016)
20. Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., Wuille, P.: Enabling blockchain innovations with pegged sidechains (2014)
21. Mann, C., Loebenberger, D.: Two-factor authentication for the bitcoin protocol. In: International Workshop on Security and Trust Management, pp. 155–171. Springer International Publishing (2015)
22. Kokoris-Kogias, E., Jovanovic, P., Gailly, N., Khoffi, I., Gasser, L., Ford, B.: Enhancing bitcoin security and performance with strong consistency via collective signing. arXiv preprint arXiv:1602.06997 (2016)
23. Liang, G., Sommer, B., Vaidya, N.: Experimental performance comparison of Byzantine fault-tolerant protocols for data centers. In: Proceedings of INFOCOM 2012, pp. 1422–1430. IEEE (2012)