Blockchain Technologies and Issues

Mohd Yazid Idris [1], Shahrizal Sunar [2], and Azizul Azman [3]

[1,2,3] Media and Game Innovation Center of Excellence (MaGICX),
Institute of Human Centered Engineering (iHumEn), School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia
81310, Skudai, Johor, Malaysia
yazid@utm.my, izohir2@live.utm.my, shahrizal@utm.my, azizulazman@utm.my

Abstract. Blockchain technologies are promising area of research on securing data since last few years. Blockchains are distributed ledgers that removing the need for a centralized authority to host data. In this paper, we review four basic elements in blockchain architecture namely distributed ledger, hashing, consensus algorithm and smart contract. We then highlight the issues in blockchain related to scalability, performance and security. Finally, we discuss several research possibilities drawn from these issues.

Keywords: Blockchain, Smart Contract, Security.

1 Introduction

Blockchain has received considerable attention in almost every field of today's digital world. The very first blockchain was the cryptocurrency called Bitcoin created in 2009 [1]. Since then the new concepts have appeared in blockchain technologies which have led its applicability in almost every sector of today's digital world ranging from finance, medical, gaming, manufacturing, trading, supply chain etc. [2]. The blockchain consisting of several technologies such cryptography, hashing, mathematics, business model, peer to peer communication and distributed database. All these underlying technologies provide an integrated, multifield infrastructure. This paper only focuses on the distributed ledger, hashing, consensus algorithm and smart contract elements of blockchain.

Unlike current existing systems which are based on the concept of centralization, the blockchain relied on the concept of decentralization. The blockchain uses peer to peer network communication and distributed system in a form of blocks which contain ledger to store the transaction information. The blocks are linked to its parent to form a chain. Within this chain each block consists of a block header and block body [3]. The block header contains the blockchain version, hash of previous block, tree root hash and timestamp, whereas the block body contains the detail of transactions. After adding the transaction details, the block is cryptographically locked with the

Proceedings of the International Seminar on Information and Communication Technologies 2019 (ISICT 2019)
2 March 2019, Surabaya, Indonesia.
Institut Teknologi Telkom Surabaya, Indonesia
ISBN: 978-623-94143-0-6

hash of the parent block. Once the block is added to the chain, the block will become immutable. Figure 1 shows the overall framework of the blockchain.

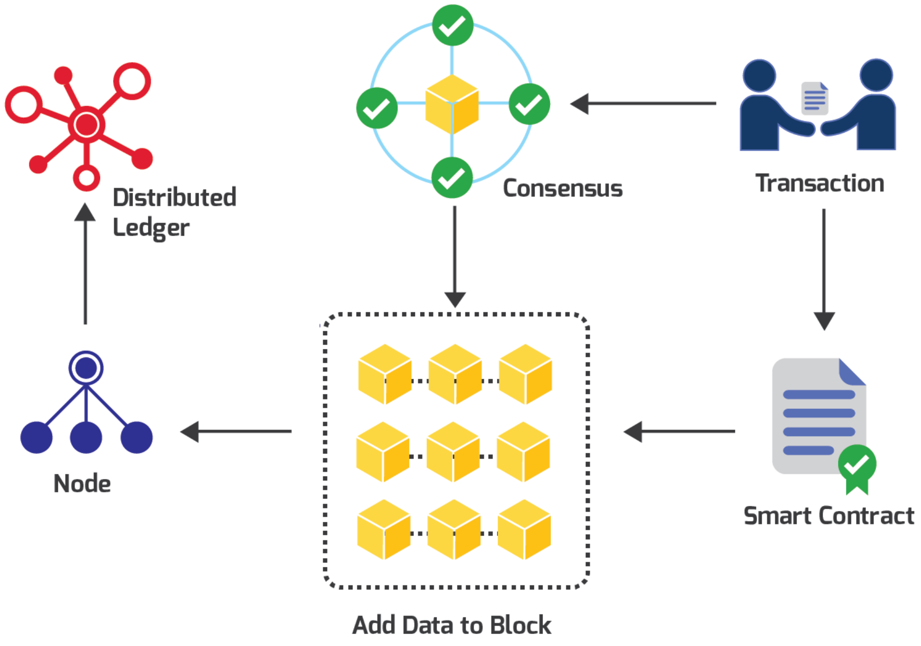

Fig. 1. Overview of the blockchain framework

2 Distributed Ledger

The blockchains are distributed ledger containing all the historical and current transactions organised in a form of blocks. [4]. When a node performed a new transaction, it is verified before adding to a ledger. The ledger is then replicated and synchronized to all the nodes. The distributed ledger provides decentralized access to eliminate the need of a central authority. Furthermore, the data immutability and auditability can be achieved. Firstly, by the means of replication and synchronization of ledger among all the nodes. Secondly, the used of cryptographically signature and timestamp of blocks. In this way any tampering with the transactions or block data can be detected by the nodes.

3 Hashing

Hashing is the fundamental element of the blockchain [5]. Hash function are cryptographic algorithms with variable size input and fix size output. The use of hashing in block chain always result in the same size of hash regardless of the block size. Each block is cryptographically sign with the hash of the previous block, this process of link each block with the previous block creates the chain of traceable blocks. Any modification to a block within this chain will change the hash of that specific block thus breaking the chain with the next block. This provide a safeguard against the tampering of data within the blockchain.

4 Consesus Algorithm

Since blockchain are decentralized systems without the involvement of a third party or trusted authority, there is a need to ensure the consistency of transactions among nodes. Blockchain used the consensus mechanism to achieve this goal. Two major consensus algorithms are Proof of Work (PoW) and Proof of Stake (PoS). Some blockchains use other consensus algorithms such a Practical Byzantine Fault Tolerance (PBFT), Delegated Proof of Stake (DPoS), Proof of Bandwidth (PoB), Proof of Elapsed Time (PoET), Proof of Authority (PoA) [6].

Proof of Work algorithm involves the solving of a mathematical puzzle to establish the credibility of data. The puzzles are designed in such a way that their solution is computationally expensive, but their verification is computationally less expensive. To create a block, a node must solve the PoW puzzle. Once it has solved it, the node will broadcast to other nodes for verification. If there is a consensus among the majority of nodes, the block is added to the chain. Proof of Stake involves the ownership of the token to establish the credibility of data. PoS is less computationally expensive as compared to PoW.Table 1 show some of the popular consensus algorithms.

Table 1. Description some popular consensus algorithms in the blockchain

Consensus Algorithm	Type	Pros	Cons
Proof of Work (PoW)	Decentralized	Ensure that the work has been performed by the node	Computationally expensive
Proof of Stake (PoS)	Decentralized	Attacks more expensive; More decentralized; Energy efficient	Nothing at stake
Delegated Proof of Stake (DPoS)	Partially decentralized	Cheap transactions; scalable; energy efficient	Nothing at stake
Byzantine Fault Tolerance (BFT)	Decentralized	High throughput; low cost; scalable	Semi-trusted

5 Smart Contract

Smart contracts [7] are a piece of code that can be executed by the node automatically to perform a certain task. Because of the smart contracts the blockchainare becoming more applicable in different fields of the digital world. Smart contracts can be written in any programming language. Each smart contract has a unique address which can be used to access the contents of a smart contract. Smart contract as distributed application (dAPPs)provides more autonomy, stability, traceability and security as compared to traditional applications. Fig 2shows the different steps involve in a smart contract.

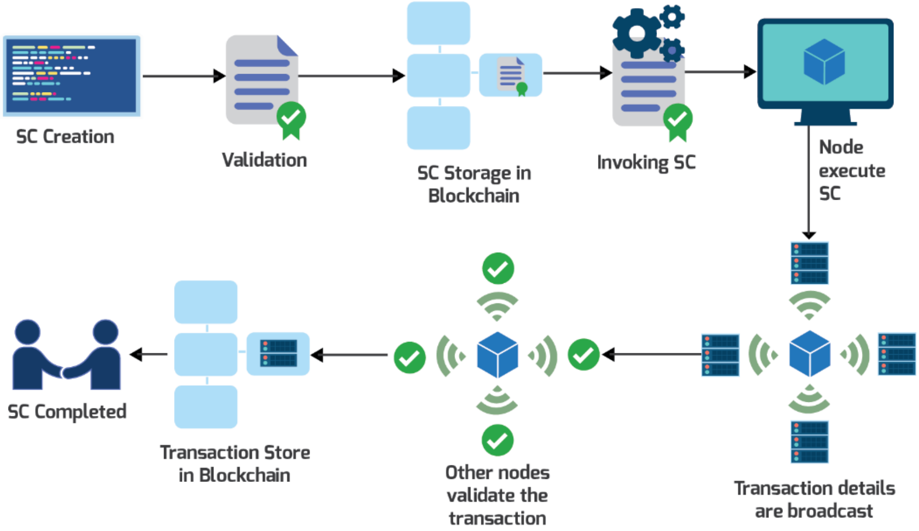
SC Creation
Validation
SC Storage in Blockchain
Invoking SC
Node execute SC
Transaction details are broadcast
Other nodes validate the transaction
Transaction Store in Blockchain
SC Completed

Fig. 2. Steps involved in the smart contract.

6 Scalability Issue

Despite the growth of blockchain technologies and its potential for the various field, there exist some issue that needs to be resolved. Scalability is one of these issues [8]. As the size of the blockchain increase, the scalability becomes a bottleneck. For instance, in Bitcoin,the block size is 1 MB and every block is created after every 10 minutes. Furthermore, the Bitcoin is restricted to 7 transactions per second. These limitations are hurdles in the high-frequency trading business. Increasing the block size, reducing the block generation time and increasing the transaction limit will result in large storage space, high data read/write rate and requires more network bandwidth.

7 Performance Issue

Performance is another issue faced in blockchain [9]. All the blockchain systems that use Proof of Work (PoW) suffers from performance issues. PoW is a computationally extensive task which requires high power machines to perform the consensus algorithm to verify block data. Beside PoW, there are other factors that affect the performance of blockchain such as network size and complexity. When the number of nodes increase in a blockchain, the process of replication and synchronization of ledger in timely frame become critical. Any network problem or delay may result in inconsistent state of blockchain among the nodes.

8 Security Issue

Security of blockchain has become a popular research area particularly the network security of blockchain has received considerable attention among research community. with the popularity of blockchain in various fields and particularly in digital currency, there has been an increase in the cyberattacks against blockchain. In the past years, distributed denial of service (DDoS) attacks which are designed to target centralized systems (client and server) have targeted blockchain. In a decentralized and peer to peer network such as blockchain it is more difficult to launch DDoS attacks. Despite the difficulties of launching DDoS in blockchain, in year 2014 and 2016 there were DDoS attacks against Ethereum and Bitcoin blockchain networks [10]. This shows that even a decentralized system can be subject to DDoS attacks if such attacks are carefully crafted.

There are many security issues discussed in literature [6][11], however in this section we highlight two security issues related to availability and controllability of blockchain. Security issue related to availability includenetwork traceability attacks[12]and eclipse attacks[13]. Network traffic analysis in blockchain peer-to-peer network can reveal IP address, network topology and transmission information. Using this information, network traceability attack can be launched to reveal user identity,transaction details and relationship between various nodes. In blockchain every transaction output is the input to another transaction. By analysis of the distributed ledger of blockchain, an attacker can get the details of generation of a bitcoin, the address of the generating node, timestamp of generation, transactions that are use for spending that bitcoin. Further analysis of these details can also reveal the relationship between different bitcoins and the transactions. An attacker can trace "interested" transactions, the smart contracts used in these "interested" transactions. A further in-depth analysis can lead to the details of smart contract rules.

The analysis of flow of transactions and bitcoins can also be used to reveal the identity of uses. The time of transactions, sender addresses, receiver addresses, smart contract use in transactions can lead to the ownership of multiple addresses own by a same individual. A node in the blockchain network can access the IP addresses and topology details of connected peers. If the attack controls a large number of nodes in blockchain, he can use network analysis tools to get details of other nodes. The collected details can be used to locate the physical geographical location of corresponding node.

Eclipse attacks can be launched by controlling most of the node and distributed architecture. Without the stable nodes in a peer to peer network, the distributed architecture divides tasks among peers using gossip protocols[14]. Eclipse attack exploits this broadcasting of gossip protocolsin a peer-to-peer network to hijack the routing table of certain nodes and send uselessor malicious information. Although, launching an eclipse attack is expensive but once launch the attacker can control the flow of information with in a blockchain network. Eclipse attack can further be used to launch 51% attacks and double spending attacks.

Controllability issues includes blockchain data manipulation by smart contract vulnerabilities [15] such as logic problems, misunderstanding of semantics etc. An attacker can search for such vulnerabilities and exploit the implementation of smart contract. Studies [10][16] have shown various vulnerabilities in the implementation of Ethereum smart contracts. These vulnerabilities exist due to premature reentrance to smart contract, exception disorder, stack overflow, unpredictable state and exposing of smart contract function details.

9 Research Possibilities

Blockchain is an emerging technology with much potential. However, like any other new technology, blockchain is facing many issues and challenges. We have highlighted three issues namely scalability, performance and security. In order to solve these issues, blockchain researchers are introducing blockchain database and distributed file system as complementary solutions to increase scalability in blockchain storage. The improvement in performance of blockchain can be achieved by more frequent implementation of less computational expensive consensus algorithms such as Proof of Stake, Delegated Proof of Stake and Proof of Authority. Furthermore, the recently introduced new version of blockchain architecture Hyperledger [17] to provide high level performance and scalability in modular approach. Meanwhile, for improving smart contracts security many solutions have been proposed by researchers including OYNETE[15], SmartCheck [18] and Gasper [16]. These solutions analyze the smart contract code for the detection of possible vulnerabilities. An automated intelligent solution that not only detect the vulnerabilities but improve the code to eliminate such vulnerabilities is a promising solution.

10 Conclusion

In this paper, we review the basic concept of blockchain namely. distributed ledger, hashing, consensus algorithm and smart contract. Furthermore, we discuss the current issues in blockchain such as scalability, performance and security and outline possible solution to overcome such issues. Apart from these issues, the blockchain technologies have considerable scope when integrated with other technologies such as Internet of Things, Deep Learning and Distributed File Systems. For instance, IoT has many vulnerabilities such as privacy, confidentiality and integrity. Many researchers have proposed solutions to secure the IoT ecosystem. Blockchain by default provides grants authenticity, non-repudiation, and integrity. Integration of IoT and blockchain can be used to develop secure IoT infrastructures. Deep learning and blockchain can be used to develop robust and efficient systems. Deep learning has proven to give promising results when the data is reliable, secure and trusted. Blockchain provides such data. Furthermore, deep learning can be used to make fast and efficient smart contracts. Distributed file systems can also get benefit from blockchain. The ownership of files, authentication of the user in the distributed file system can be managed and store within blockchain.

References

1. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. (2008)
2. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q.: A survey on the security of blockchain systems. Futur. Gener. Comput. Syst. (2017). doi:10.1016/j.future.2017.08.020
3. Antonopoulos, A.: Mastering Bitcoin: unlocking digital cryptocurrencies. (2014)
4. Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K.: Where Is Current Research on Blockchain Technology?—A Systematic Review. PLoS One. 11, e0163477 (2016). doi:10.1371/journal.pone.0163477
5. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: 2017 IEEE International Congress on Big Data (BigData Congress). pp. 557–564. IEEE (2017)
6. Manav Gupta, Perez-Sola, C., Delgado-Segura, S., Navarro-Arribas, G., Herrera-Joancomartí, J., Heilman, E., Kendler, A., Zohar, A., Goldberg, S., Morris, V., Adivi, R., Asara, R., Cousens, M., Gupta, N., Lincoln, N., Mosakowski, B., Sun, H.W., Buchman, E., Solutions, B.B., Singhal, B., Dhameja, G., Panda, P.S., Aggarwal, D., Brennen, G.K., Lee, T., Santha, M., Tomamichel, M., Lin, I.-C., Liao, T.-C., Dhillon David Metcalf Max Hooper, V., Dhillon David Metcalf Orlando, V., Hooper Orlando, M., Metcalf, D., Hooper, M., Laurence, T., Blockchain, M., Prusty, N., Swan, M., Antonopoulos, A.M., Farnham, B., Tokyo, S., Boston, B., Sebastopol, F., Beijing, T., Van Eekelen, M.C.J.D., Doomernik, J.-P., Tuẩn, Đ.M., Karame, G., Androulaki, E.: A Survey of Blockchain Security Issues and Challenges. Int. J. Netw. Secur. 1919, 653–659 (2017). doi:10.6633/IJNS.201709.19(5).01
7. Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., Kishigami, J.: Blockchain contract: Securing a blockchain applied to smart contracts. In: 2016 IEEE International Conference on Consumer Electronics (ICCE). pp. 467–468. IEEE (2016)
8. Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, H.W.: Blockchain Challenges and Opportunities : A Survey Zibin Zheng Shaoan Xie Hong-Ning Dai Xiangping Chen Huaimin Wang. 14, 1–25 (2017). doi:10.1504/IJWGS.2018.095647
9. Bentov, I., Gabizon, A., Mizrahi, A.: Cryptocurrencies Without Proof of Work. Presented at the (2016)

10. Atzei, N., Bartoletti, M., Cimoli, T.: A Survey of Attacks on Ethereum Smart Contracts (SoK). In: Proceedings of the 6th International Conference on Principles of Security and Trust - Volume 10204. pp. 164–186. Springer-Verlag New York, Inc. (2017)
11. Zhu, L., Zheng, B., Shen, M., Gao, F., Li, H.: Research on the Security of Blockchain Data: A Survey.
12. Garay, J., Kiayias, A., Leonardos, N.: The Bitcoin Backbone Protocol with Chains of Variable Difficulty. Presented at the (2017)
13. Vasek, M., Thornton, M., Moore, T.: Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem. Presented at the (2014)
14. Kermarrec, A.-M., van Steen, M.: Gossiping in distributed systems. ACM SIGOPS Oper. Syst. Rev. 41, 2 (2007). doi:10.1145/1317379.1317381
15. Luu, L., Chu, D.-H., Olickel, H., Saxena, P., Hobor, A.: Making Smart Contracts Smarter. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16. pp. 254–269. ACM Press, New York, New York, USA (2016)
16. Chen, T., Li, X., Luo, X., Zhang, X.: Under-optimized smart contracts devour your money. In: 2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER). pp. 442–446. IEEE (2017)
17. Androulaki, E., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Barger, A., Cocco, S.W., Yellick, J., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G.: Hyperledger fabric. In: Proceedings of the Thirteenth EuroSys Conference on - EuroSys '18. pp. 1–15. ACM Press, New York, New York, USA (2018)
18. Tikhomirov, S., Voskresenskaya, E., Ivanitskiy, I., Takhaviev, R., Marchenko, E., Alexandrov, Y.: SmartCheck: Static Analysis of Ethereum Smart Contracts. In: 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB). pp. 9–16 (2018)