Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 03, March-2021

Electronic Voting System: Blockchain vs Hashgraph

Tasnia Bushra
Department of Computer Science and Engineering
UITS
Dhaka, Bangladesh

***Abstract*— Voting is one of the most important civil right for the people of a democratic country by which the citizens can ensure that the state is being governed lawfully. For centuries, citizens have voted in elections to express their opinions in governance of the country, but the electronic voting system is a relatively new concept. Many countries in the world are currently experimenting with blockchain based voting systems, however, there are significant drawbacks of this method. The hashgraph encryption method is a superior version of the blockchain encryption and eradicates a few of the drawbacks of blockchain. This paper compares the two methods and highlights the advantages of the hashgraph encryption method over the blockchain encryption method.**

Keywords—Voting system, blockchain, hashgraph

I. INTRODUCTION

The three aspects that are needed to need to achieve for an applicable electronic voting system are - Authenticity, Confidentiality, and Integrity. Online voting is still a new technology and its functional implementation still faces substantial obstacles. A few of the common and prominent threats by internet voting system are denial of service, advanced persistent threats, malware, insider attacks, and compromised credentials. Vulnerabilities exposed in electronic systems can compromise democracy and risk the lives of citizens by exposing their identities. Japan, Russia, Sierra Leone, Turkey, and USA are examples of countries which have implemented blockchain based voting system in an experimental environment and found many issues which prevented them from implementing the system in live elections.

II. BACKGROUND INFORMATION

A. Blockchain

The blockchain method is a peer-to-peer technology utilizing encryption and a write-once, append-many electronic ledgers. This encryption method allows private and secure registration information and casted votes to be transmitted over the internet. Public and private tests of blockchain-based mobile voting systems are growing rapidly. However, with an uptick in pilot projects, security experts have warned that blockchain-based mobile voting technology is extremely insecure and has potentially risks to democracy through wholesale fraud or manipulation tactics.

B. Issue Analysis

There are many reasons why blockchain is not beneficial for a voting system. This encryption method assumes that there is no malware in the voter's device. It also assumes that the votes will be permanently public, because if someone can find a way to hack into the blockchain handling the votes, every vote will become public. While blockchain networks may be able to handle small absentee voter populations in test scenarios, the technology could not hand the large amount of information generated by the general voter populace of a voting system in real life. Ballots submitted online can be undetectably edited by a variety of cyberattacks, including malware on a voter's device and server penetration attacks. The latter of which has been demonstrated live and in a test election. Internet voting provides the opportunity for an attacker to engage in harmful disruption and denial-of-service attacks, with the purpose of disabling the system and prohibiting voters from casting ballots which lead to undermining voter trust in the election. Receiving ballots as encrypted attachments can also expose an election system to systemic attacks. Expert attackers can spoof an eligible voter's emails and use fraud ballots to deliver malware that can be used to gain entry into the election system infrastructure. New technologies including blockchain are still unable to resolve the unavoidable security issues fundamental with online voting [1].

One of the biggest challenges to blockchain adoption in current world is scalability. The blockchain network is able to offer a transparent and inflexible record of transactions with decentralized control, but it cannot handle the large volume of transactions that are performed across the world every minute. Blockchain can also be slow in contrast to other legacy transaction processing systems that are able to process tens of thousands of transactions per second. A blockchain network is unable process more than a handful of transactions per second. The Bitcoin blockchain can handle only 3 to 7 transactions per second; while the corresponding figure for Ethereum blockchain can handle 15 transactions per second. Therefore, there is an enormous gap in the scales of operations that can be currently done using blockchain and the existing alternatives to blockchain. Because of its relatively poor performance, many researchers do not consider blockchain technology to be recommendable for large-scale applications.

Another notable disadvantage of the blockchain network is the fact that it relies on intensive computing power which requires a lot of electricity in order to run. Even if we can invent a blockchain technology that can compute the immensely large number of calculations needed for an online voting system, the time and the expense may still be too high a number for it to be implemented in a real-life environment.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 03, March-2021

III. PROPOSED SOLUTION

A. Hashgraph

Hashgraph is a distributed ledger technology developed by Leemon Baird in 2016. Hashgraph is an asynchronous Byzantine Fault Tolerance (aBFT) consensus algorithm that is considered to be capable of securing the platform against attacks [8]. It does not use miners to validate transactions, and uses directed acyclic graphs for time-sequencing transactions without bundling them into blocks [2]. Several experts describe Hashgraph as a continuation of where the idea of blockchain begins while some refer to it as an alternative to blockchain, a technology known as first generation and typified by severe cost, fairness, security, and speed constraints [3]. Some academics think that Hashgraph is less technically constrained than blockchains proper. The Hedera white paper co-authored by Baird describes that at the end of each round, each node calculates the shared state after processing all transactions that were received in that round and the round before that. Then it digitally signs a hash of that shared state, puts the hash in a transaction, and gossips it out to the community of other nodes [4]. The correctness of the entire Hashgraph protocol depends on every participant knowing and agreeing upon the total number of participants in the system, which is difficult to determine correctly in an open distributed system. The advantage of the Hashgraph system is that all the nodes in the system at any given time know how many other nodes there are in that system.

B. Methodology

Hashgraph derives its name from an algorithm which is based on the hashgraph consensus technology that was developed based on the principles of blockchain, the fundamental technology behind cryptocurrency. Blockchain can be fast but unsecure, or it can be secure and slow. Hashgraph was developed with the aim to build a blockchain alternative which would be both fast and secure. Hashgraph can give businesses the benefits that are delivered by blockchain, for example- decentralization, network transparency, and security. The advantage of Hashgraph over blockchain is that it does not have the scalability issue and can potentially process enormous volumes of transactions in seconds. This makes it a better alternative to blockchain for businesses that require encrypted systems. Hashgraph can handle 250,000 transactions per second, which is more than 10 times what blockchain is capable of. Transactions are handled asynchronously, which means that transactions do not have to wait for other transactions before them.

Hashgraph uses a process called a gossip protocol to overcome the bandwidth issue with voting algorithms. As all the nodes are required to communicate with each other, it puts a lot of weight on the bandwidth. The gossip protocol simplifies this process by randomizing it. Each node randomly communicates with another node instead of each node talking to every other node at the same time. This process is called gossip about gossip. Each node shares all the information they have learned with another node, which is similar to sharing other people's gossips. As all information is shared and bandwidth is saved and not overly stressed, eventually, mathematically consensus will be achieved. This protocol is cheaper in Hashgraph because mining is not required. The biggest advantage of Hashgraph is that it is safer than blockchain technology. To successfully attack the system in Hashgraph, a malicious entity will have to attack all nodes in the system at the same time. Such an act is very expensive and would be essentially impossible [5].

Similar to a gossip or rumor being spread, nodes receive messages from other nodes in the Hashgraph network. The nodes then create an event based on the received messages and record the hash of the event. A block in a blockchain has 2 identifiers which are the hash number of the block and the hash number of the previous block. In the Hashgraph nodes, there are 4 identifiers – hash number of the node, hash number of the previous nodes, hash number of the last event the node created, and the hash number of the last event the node received. With these two additional hash numbers, the received messages can be easily spread throughout the network just like gossips. Possessing such characteristics enable Hashgraph to handle 250,000 transactions per seconds. Even the fastest blockchains can perform a maximum of 10,000 transactions per seconds.

The Hashgraph is divided in rounds. One round is created each time one event is able to connect more than 2/3 of the events of the current round by more paths than 2/3 of the node population. Each time a new round is created, the new nodes of the new round will vote to say if they agree upon the data contained in the first row of events of the previous round. To perform this task, they just need to verify that they are connected to these nodes. The last stage is to collect the answers from the 3rd round nodes. The 4th round nodes are required for this task and they need to clearly view the 3rd round nodes. If one of the 4th round nodes succeed to collect a super majority (more than 2/3 of the population) of positive votes upon the data in the 2nd round, then the consensus is found in this data.

C. Advantages

Hashgraph has been designed to provide the benefits of blockchain as a distributed ledger technology without the drawbacks. A distributed / shared ledger is a unison of shared, replicated, and synchronized digital data which are geographically scattered institutions, regions, or countries [6]. Dissimilarly to a distributed database, there is no central administrator [7]. While many ledgers use the gossip protocol, the Hashgraph gossip protocol is combined in the form of "gossip about gossip" with a voting algorithm to reach consensus quickly and securely without proof of work. The gossip protocol shares new information that other nodes are unaware of, and the gossip about gossip includes the origin of the new information. We can have the complete history of who talked to who in the network and the order in which they talked to each other, when the new messages include the hash of the previous messages into one message [3].

The consensus algorithm offers a secure way of handling transactions and ensures that an event is correctly recorded. The order is the most important element in Hashgraph, and the Hashgraph makes sure that no malicious entity can alter the data accuracy or the order in which the events are connected with each other. This way, it protects the network from both double spending problem as well as a 51% attack. It also successfully implements the resistant hash function and digital signatures. Once a transaction is committed, it cannot be

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 03, March-2021

reversed or changed, as this method applies Byzantine fault tolerance.

The fairness concept consists of the idea of being fair to all the nodes in a network. The definition of fairness in this scenario states that an attacker will not be able to learn which two new transactions will make it to the unified order. Fairness works well in Hashgraph if the majority of nodes know about the transaction. This can result in issues if an attacker gets hold of two-third of the participants, because then he can reorder the events without impacting the fairness of the network. There is also no mining requirement of the nodes in Hashgraph.

Gossip methods are considered fairly fast. This is also the case in the Hashgraph's gossip protocol. The events are then spread across the network fast as it is all about gossip-about-gossip. This also means that there is less information required to be propagated over time. The virtual voting utilized in Hashgraph makes it more efficient. But if we take into consideration that each node will require the entirety of the Hashgraph, the size of the inbound will increase over time. For now, we do not know for certain how it can impact the performance of the network. Theoretically, Hashgraph TPS can reach 5,00,000.

D. Disadvantages

There are still several issues with Hashgraph. One of the biggest issue is that this encryption method is a patented technology owned by Swirlds, which could mean that it will simply be a tool for corporations and not for the masses. The method is also not considered decentralized or open-source. A user will need to request an SDK (software development kit) to be able to use the patented algorithm. The algorithm itself is decentralized, but not the company owning the product. Another issue with Hashgraph is that it does not store historical records of all transactions in a process. The records are removed over time. This could be an issue during audits because it would be harder to prove that transactions took place in the past [2].

IV. CONCLUSION

Implementation of a completely secure electronic voting system has many issues that are yet to be solved. Many countries and organizations are working with implementing blockchain based voting systems. The blockchain method has a few issues which prevents us from achieving a completely secure and attack-proof electronic voting system. In this paper, I have focused on the major issues with the blockchain method and proposed a solution which ensures more security and efficiency than the blockchain method. Even though Hashgraph is still a patented technology and not open for the masses, the corporation owning the algorithm has plans to convert the Hashgraph method into a distributed public ledger system which will be accessible to everyone in near future.

ACKNOWLEDGMENT

I thank the authors, professors, and experts mentioned in the References section whose hard work and research helped me in writing this paper.

REFERENCES

[1] S. Greenhalgh, S. Goodman, P. Rosenzweig, and J. Epstein, "Email and Internet Voting: The Overlooked Threat to Election Security", report for U.S Technology Policy Committee and National Election Defence Coalition, 2019.

[2] D. Tapscott and A. Tapscott. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin. 2016, ISBN 9781101980156.

[3] H. Panetto, C. Debruyne, H. Proper, C. Ardagna, D. Roman, R. Meersman. On the Move to Meaningful Internet Systems. OTM 2018 Conferences: Confederated International Conferences: CoopIS, C&TC, and ODBASE 2018, Valletta, Malta, October 22-26, 2018, Proceedings, Part 2. Cham: Springer. p. 281. ISBN 9783030026707.

[4] L. Baird, H. Harmon, and P. Madsen, "Hedera: A Governing Council & Public Hashgraph Network", Hedera, 13 August 2019.

[5] H. Treiblmaier and R. Beck (2018). Business Transformation through Blockchain, Volume 2. Cham: Palgrave Macmillan. p. 98. ISBN 9783319990576.

[6] Distributed Ledger Technology: beyond block chain (PDF) (Report). Government Office for Science (UK). January 2016. Retrieved 29 August 2016.

[7] C. Scardovi (2016). Restructuring and Innovation in Banking. Springer. p. 36. ISBN 978-331940204-8. Retrieved 21 November 2016.

[8] H. Treiblmaier, R. Beck (2018). Business Transformation through Blockchain, Volume 2. Cham: Palgrave Macmillan. p. 98. ISBN 9783319990576.