Design And Implementation Of Msha256 On Blockchain Using Content Addressable Storage Patterns

Maria Rona L. Perez, John Benedict C. Legaspi, Kirk Alvin S. Awat, Ace C. Lagman, Roman M. De Angel, Rossana T. Adao

Abstract: The blockchain phenomena is no longer about Bitcoin or cryptocurrency, it is beyond a common protocol to make it nearly impossible to create fraudulent transaction. Blockchain based architecture overall performance is subjected to storage expenses with high computational cost. This paper designed a new consensus protocol for Blockchain using Content Addressable Pattern with the adaptation of modified SHA256 algorithm. Although government, business and other entities interest of adapting blockchain to their processes, the complexity issues and operational cost is still a challenge to date. With the newly design consensus protocol the process of validating the transaction that involves tedious mining or solving cryptographic puzzles has been eliminated and move towards using signature to authenticate the transaction. Concatenation of all these elements is a generated hash value using modified SHA256. Since the hash is secured, the transaction is secured. Thus, the implementation of off-chain chanel instead of global consensus addresses the complexity and high computational cost of blockchain technology.

Index Terms: blockchain, MSHA256, content-addressable patterns, consensus protocol, complexity, smart contract.

1 INTRODUCTION

In the past, entities such as government, banks or financial institution policy, and corporations made and filled the role of the trusted parties. They operated a set of protocols that provided a layer of trust, on which all commerce could operate [1]. While these parties worked to increase trust and reliability to reach their maximum capabilities, yesterday's breaking adversity inoculated uncertainty and wariness into the system. The new network of blockchain can form a peer-to-peer platform for these trusted parties. The blockchain has been define by many as disruptive technology but the there are two key aspects of blockchain, its peer-to-peer network and its immutable ledger of transactions. Blockchain is a set of digital ledgers, called block, recorded with transactions or facts and published for the community to view. Those blocks are chained chronologically with digital signatures, hence the name "blockchain"[2]. The blockchain phenomenon does not revolve with cryptocurrency; it is about maximizing its full potential of securing any digitized assets while making it available for everyone's access. In the emergence of Bitcoin by the year 2009, companies started investing for their peer-to-peer network of data storage. Hundreds of millions of dollars were out to keep this decentralized network running. Bitcoin has become the mainstream in blockchain network and continually, still is. As for the smart contract, since its first release and used by Ethereum in 2015, blockchain-based architecture has consequently flowed its path to improve platforms with smart contract based application [3]. Blockchain is evolving really fast, so the question is – what's next? Blockchain technology has cemented itself in every sector of our growing society [4]. From healthcare, education, finance, to even governance, the rise of blockchain doesn't seem to stop.

• *Authors are affiliated with FEU Institute of Technology, P. Paredes St., Sampaloc, Manila, Philippines 1015.*

With the aid of blockchain, this paper designs a consensus protocol to increase user's suitability to initiate the use of blockchain on their processes.

2 BACKGROUND OF THE STUDY

Digitization has truly transformed the industry for enterprises, both large and small. Companies are constantly searching for more efficient techniques to expand their resources and provide the best online user experience. Concerning legal documents and records, one of the best practices is the use of a Document Management System offered by different advanced data solutions. Conversely, today the streamline is to adopt blockchain technology to store digital assets. The adaptation of blockchain technology would enable companies to secure their valuable documents since blockchain provides immutable, fixed and shared data storage. This allows generating transactions without manipulating the existing ones, whilst mitigating modification of previously stored values on blockchain. The mechanism of blockchain is to reach agreement on shared log of data in a decentralize form through a pool of network of unidentified participants and relying only on computations. However, using this type of technology is too complex and encompasses a huge operational cost since it requires high-end computing devices. With this judgment, more companies neglect to put into practice the use of blockchain technology. With the modification of hashing algorithm used by blockchain in its mining process, the suitability of using blockchain with low powered platforms are of great vertical extent. MSHA256 was designed as a lightweight hashing computation for off-chain transactions [5]. Hashing computation is used primarily for mining purposes to confirm a transaction on a block before it becomes a part on-chain. This has been the main reason why this paper seeks for solution on how blockchain can be part of business processes. The main contributions of this research are the following:

1. Design new consensus protocol using off-chain transactions.
2. Implement MSHA256 to authenticate and validate the transaction.
3. Discuss future extensions for this research and for

blockchain technology

3 CONTRIBUTION

A blockchain as to how it is defined is a shared ledger that is distributed and operated by a group of peers. All copies are on the distributed ledger with its link to all off-chain items. Thus, committed transactions on off-chain must be common and available for the mechanism of a distributed network to succeed. The fee of blockchain technologies varies based on the transaction published. This is in terms of the difficulties of the puzzle solves by the miners. The cost of various blockchain technology has the same calculation with regards the storage requirements. The charge per transaction in bitcoin is 1.30 USD as of November 2018. However, there is a likelihood of adjustment based on the current bitcoin cryptocurrency. These sample calculations add reasons to not participate in blockchain technology.

2.1 Smart Contracts

Smart contract will hold the program functions to be executed in a trustless and tamper-proof manner in an off-chain network [6]. This has defined conditions that will determine the results of valid transactions. For this research, the conditional logic is to check the hash value computed and authentication of the document before it executes the final hash value for storing off-chain.

2.2 The use of off-chain transactions

There are transactions on the blockchain network that do not require to be part of the chain, they just merely consume storage allocation. Documents, pictures, and alike should not be kept in an actual blockchain. With these, the design of off-chain or side DB storage is essential. One practice for off-chain transaction is known as content addressable pattern which uses virtual DB and the actual element is either deposited in the cloud storage. A hash value for the off-chain item is produced and should be stored in the blockchain so it is expected that the required storage for blockchain is reduce

3 METHODOLOGY

The objective for off-chain storage of item and use of modified SHA256 is to lessen operational cost and to overcome storage expenses. This can be done by moving data and computation outside the network of blockchain, for this research it makes the use of virtual disk as temporary data storage, the blockchain “footprints” perceptibly decreases. Doing so, the properties of blockchain technology has been transformed to some degree and might compromise the security but what should remain in the system is its “trustless” property

3.1 Design a consensus protocol

To address complexity of blockchain, MSHA256 was implemented to smart contract which will perform its task as a state channel. As a state channel, two individuals will trust the consensus of each party that is the off-chain consensus instead of global consensus on blockchain.

The consensus protocol follows:

1. Any transaction will not store an item.
2. Transaction is moved to virtual disk until validated.
3. Authentication is done using a logical condition that determine the hash value, signature, and authentication.
4. The hash value is generated using MSHA256.
5. Content-addressable pattern is used to store off-chain item.

Today, online data storages rely on trusted parties which runs documents and ensures protocols are followed [7]. However, these entities need to be trusted to not to perform any malicious act. The security of off-chain transaction is tightened by using MSHA256 applied to contract state in a smart contract.

2.2 Content-addressable patterns

The idea of off-chain network is to store data outside the blockchain network and to do this content-addressable pattern was applied and reference with consensus protocol through smart contract. This reference is the hash value generated using MSHA256 hashing algorithm. It can be retrieved by the user for referencing and to verify the correctness of the item stored. To simulate the implementation, the programmable smart contract follows the condition sets on the consensus protocol. The actual file and description are stored in cloud and the content-addressable storage was used to store hashes of the items. To reference the hash value it was also stored in the smart contract. Retrieval of the hash value can now be used to store item externally as well as to query the storage system.

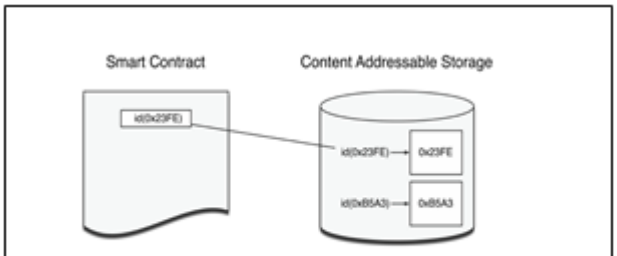

Fig. 1. Content-addressable Storage Pattern

The only way to securely and consistently sync off-chain storage and address all issues mentioned in this paper was to adopt a content-addressable pattern. It is intended to provide the necessary security in a shared environment for peer-to-peer blockchain network. Every time the item is accessed it must be verified using the hash value stored to prove that the same item was stored initially. For certainty that any loss in a node will not affect the whole chain and will not be a substantial loss to the network, each item should be stored in more than one data storage. Once a block joins a blockchain network, a mechanism to coordinate all items in the off-chain storage will balance the blockchain ecosystem. As mentioned, a content-addressable storage system requires a combination of smart contract. These technologies will implement MSHA256 hashing algorithm and will ensure availability and immutability of the blockchain. Figure 2 shows the paradigm of MSHA256 for Content addressable storage (CAS).

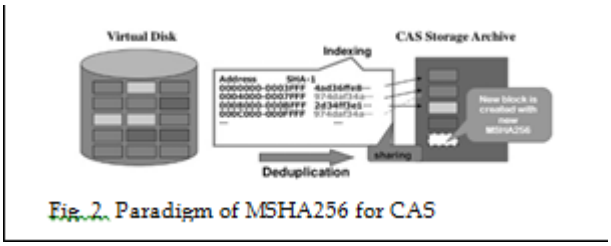

Fig. 2. Paradigm of MSHA256 for CAS

The use of virtual block device where the data is not addressed by its physical location. The data is addressed by a secure hash value derived from the content. The same hash are expressed by one original hash and others are addressed by indirect link. The generated MSHA256 hash value is concatenated with the signature for authentication and is controlled through indexing and deduplication. This is done to ensure that the generated hash value is not a redundant information before it will be part of an on-chain network

4 CONCLUSIONS

Any modification made in a distributed network is the same with third party intermediaries [8], therefore, off-chain transactions are similar to altering transaction using digital signature. This paper influences the need of off-chain transaction. The process of validating the transaction that involves tedious mining or solving cryptographic puzzles has been eliminated and move towards using signature to authenticate the transaction. Concatenation of all these elements is a generated hash value. Since the hash is secured, the transaction is secured.

5 FUTURE EXTENSIONS

New businesses today come from disruptive technologies. The availability of secured data storage should is significant. Therefore, these storages are encouraged to engaged into the blockchain revolutionary database. The re-engineering of business process opportunities often leads to blockchain-based application solution. Just like the payment scheme used in large scale businesses, they might enhance the procedure to dive into the benefit of the purpose of peer-to-peer mining practices [10]. Most of the payment transactions have long lived for decades, and using blockchain technology could be the significant transformation. This can also meet new standards in performance such as reliable and timely objectives. The design of the database storage are usually inaccurate especially in terms of relational models and join tables [11,12]. The keys on primary and secondary tables

6 ACKNOWLEDGMENT

The authors wish to thank International Research Conference in Computing, Engineering and Educational-Technology for the opportunity. This work was supported by a grant from FEU Institute of Technology.

7 REFERENCES

[1]. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https:// bitcoin.org/bitcoin.pdf [Accessed: 30 August 2017].
[2]. Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly, Sebastopol (2015)
[3]. K. Christidis, and M. Devetsiokiotis. Blockchains and Smart Contracts for the Internet of Things. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7467408
[4]. Smith, A. M. (2017). The blockchain challenge nobody is talking about. Available at: https:// usblogs.pwc.com/emerging-technology/the-blockchain-challenge/ [Accessed: 1 August 2017].
[5]. Perez, M.L., Gerardo, B and Medina, R. (2018). Modified SHA256 for securing online transactions based on Blockchain Mechanism. [Online]. Available: https://ieeexplore.ieee.org/document/8666341 DOI:10.1109/HNICEM.2018.8666341
[6]. N. Szabo. (1999). Smart contracts. [Online]. Available: http://szabo.best.vwh.net/smart.contracts.html
[7]. K. Korpela, K. Mikkonen, J. Hallikas, M. Pynnonen, Digital business ecosystem transformation - Towards cloud integration, in: Proceedings of the Annual Hawaii International Conference on System Sciences
[8]. C. Brenig, J. Schwarz, N. R¨uckesh¨auser, Value of Decentralized Consensus Systems - Evaluation Framework, ECIS 2016 Proceedings (2016) 1–18.
[9]. P. Forte, D. Romano, G. Schmid, Beyond Bitcoin Part I: A critical look at blockchain-based systems (2015) 1–34.
[10]. Gauravaram, Praveen 2007 Cryptographic Hash Functions: Cryptanalysis Design and Application. Ph.D. thesis, Information Security Institute, Faculty of Information Technology, Queensland University of Technology
[11]. Wilson, S. (2016). Blockchain: Almost Everything You Read Is Wrong. Available at: https://www. constellationr.com/blog-news/blockchain-almost-everything-you-read-wrong [Accessed: 16 July 2017].
[12]. Jeppsson and O. Olsson. Blockchains as a solution for traceability and transparency. In: (2017). URL: https://lup.lub.lu.se/student-papers/search/publication/8919957.
[13]. K. Korpela, J. Hallikas and T. Dahlberg. Digital Supply Chain Transformation toward Blockchain Integration. In: (2017), pp. 4182–4191. URL: http://hdl.handle.net/10125/41666.
[14]. A. Kosba et al. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts, In: Proceedings – 2016 IEEE Symposium on Security and Privacy, SP 2016 (May 2016), pp. 839–858.
[15]. Vitalik Buterin. [n.d.]. Ethereum's White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. ([n.d.]).