

PROOF-OF-STAKE CONSENSUS METHOD FOR UPCOMING BLOCKCHAIN NETWORKS

Sridharan Krishnan, ArjunVikram Thiruvengavaradan Koperundevi, Bharathiraja Jayasundarapandiyam*, and Jeevanraj Sampath

Received: March 15, 2023; Revised: June 25, 2023; Accepted: June 28, 2023

Abstract

Currency transaction is a major part that had to be made secured. So rather than making usual currency transactions, there is a secured way of currency transactions by using cryptocurrency which has the concept of blockchain. In today's world, the advancement of cryptocurrency facilitates every individual to make use of cryptocurrency for investing savings and transactions. Hence, we can witness the huge number of transactions occurring per second. Therefore, it is transforming the way of understanding the currency in a digitalized manner. It invokes interposer to interlope in the particulars of the transactions. To make an ensured transaction, we are using APC (ALPHA COIN) cryptocurrency. This APC cryptocurrency transaction is protected with the support of blockchain so that every user utilizing the APC for their transactions, can be more confident in doing their currency operations. The biggest demand of every user is securing their transaction details regarding the usage of cryptocurrency. Therefore, by using the hashing algorithm we are converting the values of the user's transactions details into hash values. The transaction details are validated using a validator and the validations are fact-checked by the administration, with the implementation of the modal concept of "proof of stake".

Keywords: Blockchain; consensus mechanisms; energy; game theory; mining process; proof-of-stake; proof-of-work; security

Introduction

Throughout the course of recent years, blockchain innovation has been declared by quite a few people as the most critical technological breakthrough since the creation of the Web. A blockchain is a disseminated information base of records divided between network members. With the assistance of cryptographic hash capabilities, computerized marks, and conveyed agreement systems, when a record enters the data set, it can't be modified

without the agreement of the other organization members. Subsequently, information put away in a blockchain can be ordinarily checked even in a decentralized climate, which prompts various blockchain applications. Cryptographic (Aitzhan and Svetinovic, 2016) forms of money, the most well-known blockchain applications, have a complete market capitalization of more than \$200 billion when this article is composed, with in excess

Department of Information Technology, Panimalar Engineering College, Chennai 600123, Tamil Nadu, India. E-mail: sridharank.p@gmail.com; vikramarjun21@gmail.com; bharathiraja1415r@gmail.com; jeevanrajsr282@gmail.com

* Corresponding author

DOI: <https://doi.org/10.55766/sujst-2023-04-e0775>

Suranaree J. Sci. Technol. 30(4):030129(1-5)

Materials and Methods

In the proposed system, when a user confidently makes transactions in our APC cryptocurrency, we must assure the security of every detail concerning their transactions. So during the operation of transactions, the more confidential and sensitive details should be verified and protected. Here a validator with a smart contract will validate the correctness of the transactions. Thus, for each validation, the validator acquires the respective APC benefits. Even fact-checking is required to verify the validated details given by the validator to ensure the rectitude of the details given during the validation. The fact-checking process is by using the concept of proof of stake (Figure 1). Further, the validated particulars are encrypted and the encrypted details are further turned into hashed values using the algorithm named SHA-384 (SECURE HASH ALGORITHM) (Miller *et al.*, 2014) is used to hash the data in the Blockchain so that the details cannot be accessed by any person other than the user. By providing the twofold stratum of security using both encryption and exclusively hashing (Figure 3(b)) our APC cryptocurrency transactions are more trustworthy and advance the potency of the transaction process

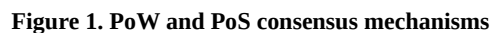


Figure 3. (a) Validator, (b) Hashing process

from both the user and receiver side who are availing our APC cryptocurrency (Li *et al.*, 2017).

Merits

Unlike traditional cloud storage, blockchain data storage solution breaks users' data into small portions. After doing so, it adds a security layer and distributes it throughout the network. If anyone tries to hack it, then they will get encrypted data first. At a later stage, they will get only a fragment of the data and not the whole file/block. Whenever a miner tries to fetch or access the data, all the fragments of data are first validated. The participant only gets a fragment of data and hence all sensitive information is protected from other miners. Moreover, each of these fragments of data is stored in a decentralized location.

Module Description

User

This module (Figure 2) gives the login and registration page where the users can register for the cryptocurrency transaction and cryptocurrency conversion. The registration page holds the username, email id, unique identification number, and password. Once the user has registered, after the approval of administration they can log in to their page. After logging in the session has been created which holds the user details. In the user module, there is an APC wallet where the user can view the amount details including the APC value. In this submodule, users can send their APC to another user's wallet with the name of the receiver and wallet id with transaction pin and APC. In this, the user can perform two types of conversion where can convert the user's currency to APC and vice-versa. Then in account info submodule, initially gives the registration form to the user to register the bank account to transfer the currency to APC and vice-versa. Once the registration has been completed, the account details will be displayed on this submodule. In the APC transaction submodule, it displays the table that has the APC transaction details where the APC is sent and received by the current user. In another submodule of currency transaction, which has the table that displays the currency conversion transaction details which have two types of currency to APC and vice-versa. And finally, the logout submodule is used to delete the session details of the particular user.

Validator

In validator module (Figure 2), it has the login and registration page where the validator can register for the validation process. After the

approval for login from the administration, the validator (Figure 3(a)) needs to register the account and needs to make a smart contract to become a validator. In the wallet, the submodule validator can transfer the APC to another APC wallet and also can convert the currency to APC and vice-versa. The validate queue submodule gives the table which shows the transaction details to be validated and that will be displayed to all validators where the current validator can accept the transaction details for validation which will be displayed in the submodule in the form of table structure. In that submodule, the validator can validate the particular transaction details. The transaction submodule shows the transaction with the validator account and the wallet. Finally, the logout submodule is used for deleting the session details of a validator (Figure 3(a)).

Repository

This module gives out the login page where the repository in-charge person can log in through this page to get the page to be redirected to the repository page. After the login process, the session has been created for the repository person. It has the submodule of transactions which displays the table with transaction details which are passed from the fact-checking (Miller *et al.*, 2015) process. In that, the encryption process is carried out by the repository in charge. Once the encryption process is completed then the encrypted value with the key will be displayed in the encrypted data submodule. In the encrypted data submodule, the table will display the encrypted data where the in-charge can hash the encrypted data and add that data in the blockchain, and store it in the ledger. And also the hashed data are stored in different cloud storage which satisfies the blockchain in the cloud concept. Ledger is a submodule which display the hashed data in the ledger with the individual validator. Furthermore, cloud storage submodule has multiple cloud bases and it displays the hashed data in blockchain stored in the multiple cloud bases (Kopp *et al.*, 2016).

Administration

The administration (Figure 2) module displays the login page where an admin can log in to get the page to be redirected to the admin page. User wallet submodule shows registration details of the user which will be approved by the admin. And in validator submodule shows the registration details of the validator where the admin can approve a particular validator. The allotment submodule displays the table has all types of transaction details that need to be validated by the validator. It also shows the status of the validation process which

is validated by the validator. The fact check submodule is used to make the fact-checking process for the validation. Admin will be fact-check the validation process and if the process is valid then some amount of APC will be credited to the respective validator's wallet (Figure 3(a)). If the process is not valid then according to the smart contract some of the APC will be debited from the respective validators.

Secure Hash Algorithm

SHA-384 (Secure Hash Algorithm 384) is a cryptographic hash function that generates a 384-bit message digest. It is one of the members of the SHA-2 family of hash functions, which also includes SHA-256, SHA-512, and several other variants. The SHA-384 (Shoker, 2017) algorithm operates on messages up to 2^{128} bits in length and produces a fixed-size 384-bit output. Like other hash functions, it is designed to be a one-way function, meaning that it is infeasible to compute the original message from its hash value, or to find two different messages that produce the same hash value.

The algorithm operates by breaking the input message into blocks and processing each block through a series of mathematical operations to produce a message digest. The final message digest is a combination of the results of all the individual block operations. SHA-384 provides a high level of security, making it suitable for use in a variety of applications, including digital signatures, message authentication, and password storage. However, it has been largely superseded by the newer SHA-3 family of hash functions, which were designed to address some of the vulnerabilities and weaknesses of the SHA-2 (Wang *et al.*, 2019) family. Basically it is an software based project so, SHA-3 (Tschorsch and Scheuermann, 2016) family is slower only in software based system.

Secure Hash Algorithm SHA-384

It is a cryptographic hash function that generates a 384-bit message digest.

Algorithm

```
import hashlib
def sha384(message):
    # Convert message to bytes
    message = message.encode('utf-8')
    # Hash the message using SHA-384
    sha384_hash = hashlib.sha384(message)
```

```
# Get the hexadecimal representation of the hash
hex_digest = sha384_hash.hexdigest()
return hex_digest
```

Security Issues

The ongoing plans of the PoS (Figure 1) conventions are confronting a few security issues. First and foremost, since the block age consumes insignificant assets, reasonable members might attempt to make various blocks or forks, i.e., nothing in question assaults. Besides, the foe might attempt to pay off the pioneer, i.e., pay off assaults, to perform twofold spending assaults. To relieve these assaults, the conventions can take a pioneer's store in the event of pernicious ways of behaving. In the convention where there is no punishment component, the nothing in question assault can be moderated by having precisely one forerunner in each round. Notwithstanding, without a punishment instrument, it is challenging to forestall pay off assaults.

One more sort of assault that explicitly focuses on the PoS (Figure 1) conventions utilizing casting a ballot systems is a long-range assault. For casting a ballot based PoS conventions, the board individuals might sell their stakes quickly toward the start of the age they are chosen. They are then unaffected by the motivating force system yet still have casting a ballot rights. Subsequently, they might act malignantly without being impacted by the punishment. A few conventions manage such goes after by locking the stake of the board of trustees part for a predefined time frame after the age finished. By utilizing a council to decide in favor of each and every block, when a block is added to the chain it is concluded. In this manner, the exchange history can't be changed, and every one of the referenced assaults are moderated.

Result and Discussion

The outputs are the hash values which are added in the blockchain by using the hash functions. Comparatively SHA-384 algorithm is 50% faster than SHA-256 and SHA-512 in 64bit machines which are used widely every where in industries.

Conclusions

We are implementing a blockchain that guarantees the security of the transactions made by the user who wants their particulars to be confident. Thus when a validator validates this transaction process and the

fact-checking operation will happen through validator. Here the showstopper is accuracy of QR scanner, limitations of blockchain explorer, compatibility with newer cryptocurrencies. The main advantages are while using 64 bit machines SHA-384 will be more faster than SHA family.

Acknowledgement

The authors are grateful for technical assistance and guidance from the faculty of Panimalar Engineering College.

References

- Aitzhan, N.Z. and Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, 15(5):840-852. <https://doi.org/10.1109/TDSC.2016.2616861>
- Ball, M., Rosen, A., Sabin, M., and Vasudevan, P.N. (2017). Proofs of Useful Work. *IACR Cryptology ePrint Archive*, 203p.
- Daian, P., Eyal, I., Juels, A., and Sirer, E.G. (2017). (Short Paper) PieceWork: generalized outsourcing control for proofs of work. In: Brenner, M., et al. *Financial Cryptography and Data Security. FC 2017. Lecture Notes in Computer Science*, Springer, Cham., p. 182-190. https://doi.org/10.1007/978-3-319-70278-0_11
- Kopp, H., Bosch, C., and Kargl, F. (2016). KopperCoin - A distributed file storage with financial incentives. In: Bao, F., Chen, L., Deng, R., and Wang, G. (eds) *Information Security Practice and Experience. ISPEC 2016. Lecture Notes in Computer Science*, Springer, Cham., p. 79-93. https://doi.org/10.1007/978-3-319-49151-6_6
- Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., and Zhang, Y. (2017). Consortium Blockchain for secure energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(8):3690-3700. <https://doi.org/10.1109/TII.2017.2786307>
- Miller, A., Juels, A., Shi, E., Parno, B., and Katz, J. (2014). Permacoin: Repurposing bitcoin work for data preservation. In: *2014 IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, 2014, p. 475-490. <https://doi.org/10.1109/SP.2014.37>
- Miller, A., Kosba, A., Katz, J., and Shi, E. (2015). Non outsourceable scratchoff puzzles to discourage bitcoin mining coalitions. In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS 15*, 2015, p. 680-691. <https://doi.org/10.1145/2810103.2813621>
- Shoker, A. (2017). Sustainable blockchain through proof of exercise. In: *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)*, Cambridge, MA, USA, p. 1-9, <https://doi.org/10.1109/NCA.2017.8171383>
- Tschorsch, F. and Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, 18(3):2084-2123. <https://doi.org/10.1109/COMST.2016.2535718>
- Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., and Kim, D.I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access*, 7:22328-22370. <https://doi.org/10.1109/ACCESS.2019.2896108>