

A Novel Approach for Cross Xchange in Blockchain Technologies using Secure Authentication Protocol

Madhuri Surisetty¹, Nagalakshmi Vadlamani² and Bhargava Ganthi³

¹Research Scholar, Department of Computer Science, Gitam (Deemed to be University), Visakhapatnam, Andhra Pradesh, India

Email: Surisettymadhuri1@gmail.com

²Professor, Department of Computer Science, Gitam (Deemed to be University), Visakhapatnam, Andhra Pradesh, India

Email: nvadlama@gitam.edu

³Data Architect, Synergy Machines, Visakhapatnam, Andhra Pradesh, India

Email: bhargavaganthi@gmail.com

Abstract—Cybersecurity is the application of technologies, processes, and controls to secure systems, networks, programs, devices, and data from cyber threats. Cybersecurity aims to protect information from being stolen or compromised. We have 3 fundamental goals of security i.e., CIA Triad (Confidentiality, Integrity, Availability). It is said that Blockchain will alter the Cybersecurity of any business, making it possible to record the information without the possibility of damage, theft, or data loss. Blockchain is a decentralized technology containing information about all the actions performed through peer-to-peer networks. Many Cryptocurrencies like Bitcoin, Ethereum, Litecoin, etc., are using Blockchain technology for a decentralized network. Cryptocurrency is a digital currency that there is no central authority to control. The Cross-Chain transaction is the exchange between different Cryptocurrencies among multiple Blockchains. For a Cross-Chain transaction to happen, a third party must be involved. Our proposed work is to remove the third party in the middle and let the Cross-Chain transaction happen between only the participants for better authentication. This paper proposes an Authentication protocol to perform the Cross-Chain transaction without the involvement of a third-party.

Index Terms— Blockchain, Cross-Chain, Cryptocurrency, Third-party, Authentication.

I. INTRODUCTION

Blockchain is a decentralized network that stores information about all actions or transactions that are performed through the peer-to-peer network. Many Cryptocurrencies like Bitcoin and Ethereum are using this Blockchain Network as a decentralized registry. In Blockchain, every transaction is stored in the form of blocks.

In Cross-Chain transaction is one in which the different Cryptocurrencies exchange among multiple blockchains. Assume that two parties are exchanging their cryptocurrency from different blockchains. That transaction is done with the involvement of a third party.

The third party which is in the middle of the transaction of both parties will verify all the details of both parties whether they are authentic or not and process the Cross-chain transaction. Through this process, the third party is getting some benefit. Fig. 2(a) represents a cross-chain transaction in which 'H' is sending 3 Ethers to 'P' and 'P' is sending 2 Bitcoins with 'J'. In return 'J' is sending 3 Ethers to 'P' and 'P' is sending 3 Ethers to 'H'. It is

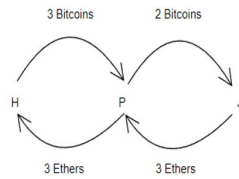


Fig.2 (a)-CC transaction

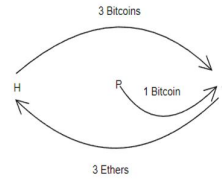


Fig.2 (b)-CC Transaction Showing P as a third party

representing a Cross-Chain transaction between ‘H’ and ‘J’ where they are exchanging Bitcoins and Ethers. Here ‘P’ is the third party. Fig. 2(b) represents ‘P’ as a third party.

Our proposed work is removing the third party and making the Cross-Chain transaction much stronger without any involvement of any unauthorized person in the transaction.

Authentication is a procedure for recognizing the end-user’s identity. Authentication elements can be divided into three groups “a password or a personal identification number”, “a token like a bank card” and “biometrics like fingerprints”.

Authorization is a method of permitting to do or have something. It is a security mechanism that is used to determine user rights or access levels to system resources, along with computer programs, files, services, data, and application characteristics. Authorization is before Authentication.

Authentication and Authorization play an important role in any transaction.

II. LITERATURE REVIEW

In 2017, Muhammad et.al [1], explained the use of blockchain bitcoin in the transactions zone on the growth of today’s emerging in the financial zone of the blockchain bitcoin transaction. They discussed how a Bitcoin Blockchain transaction works, and how the base58check encoding works. They also discussed the sending transaction process, transaction status, transaction record process, and transaction confirmation.

In 2017, Luon-Chang Lin et.al [2], has discussed Blockchain, and how it works. The structure of blockchain, proof of work, proof of stake, and types of blockchains. They also gave the applications of Blockchain technology like Bitcoin, Ethereum smart contract, Hyperledger, other applications, and also the Security issues and challenges.

In 2018, Jameela Al-Jaroodi et.al [3], has surveyed Blockchain technologies. They discussed the opportunities, benefits, and challenges of including the blockchain in various industry applications and also the different industrial applications and domains where the working of Blockchain technologies has been proposed like Financial Industry, Healthcare Industry, Logistics Industry, Manufacturing Industry, Energy Industry, etc., are analyzed.

In 2018, Suman Ghimire et.al [4], has discussed some topics of Bitcoin such as Blocks, Blockchains, the mining process, and the proof-of-work. They described the working of Bitcoin, mining, and Rewards. They compared the Hardware mining rate and Hardware power. They also gave the mining difficulty of Bitcoin over time.

In 2019, Varun Amruthiya et.al [5], have introduced a novel process to make secure authentication even safer. Their work does not need any third party between the applicant and verifier for authentication purposes. The functionalities of 2FA are as follows:

- User authentication.
- System Administration
- Saving secure access tokens
- Granting access to the system
- Abrogating access to the system in case of several incorrect attempts

In 2020, Sandhya Pasala et.al [6], gave a structure of security and insurance of blockchain. They described the security characteristics that are maintained as the fundamental requirements, building discourages of Bitcoin such as advanced cash structures, drawn by describing the advanced security and insurance properties that are used in various blockchain applications. They also discussed the security and assurance systems for fulfilling the security characteristics in Blockchain-based structures.

In 2020, Narges Shadab et.al [7], has proposed a 3-phase protocol that includes the following three steps:

Step-1: Contract creation

Step-2: Secret Release and propagation

Step-3: Secret Replay and propagation

Their work includes a Hash-time-lock protocol that is used to generate a contract connecting the Cross-Chain participants and this contract is locked with a secret hash value created by them by using a Hash function.

In 2020, Xiaohui Yang et.al [8], have exploited smart contracts and zero-knowledge proof (ZKP) algorithms to enhance the available claim identity method in blockchain model to notice the identity unlinkability, effectively preventing the revelation of the ownership of the attributes. They carried out a protocol "BZDIMS" which is including a challenge-response protocol that permits the end-users to acknowledge their ownership of attributes to service providers to safeguard user behavior privacy.

In 2020, Daniel Maldonado-Ruiz et.al [9], have implemented a framework named "Three Blockchains Identity Management with Elliptic curve Cryptography (3BI-ECC)". It is a decentralized identity management system in which the end-users identities are self-created without any third party involved in it. Their framework involves CoreBlockchain initialization, Identity storage, Identity Revocation, and Identity searching.

In 2020, Liang Zhang et al. [10], has proposed a framework for signing and verifying the contract for a transaction without the involvement of a third party. A fair contract signing scheme is implemented which is said to be a "Verifiable Encrypted Signature" (VES). VES is a fair exchange method used for digital signatures, where the sender creates a Signature and adds it to the contract, and sends the contract to the receiver. The receiver can extract the Signature of the Sender using the Verification mechanism. They proposed a robust Authentication mechanism for transactions.

III. PROPOSED METHODOLOGY

We are proposing a model with an Authentication protocol for a strong and secure Cross-chain transaction without the involvement of any outside party in the transaction. The previous works of Cross-Chain transactions are including the third party to make the transaction happen. But involving a third party in the transaction is not a safe part. For a more secure and safe transaction of Cross-Chain exchange, the third party must be removed and the transaction must be held by involving only the sender and the receiver with an Authentication protocol that proves the sender and the receiver as authorized persons.

Identity will be created for the sender and the receiver among themselves and those identities can be used later on for any cross-chain transaction. After the identity is created, the Transaction will take place through the contract.

IV. AUTHENTICATION PROTOCOL

Our Proposed Authentication Protocol Consists Of the following processes:

A. Signature process

In the Signature process, the parties willing to do the transaction will have to create a signature by themselves which is verified by the other party who is transacting with them. This Signing and verification process is done to prove themselves Authorized. The Signing process consists of:

- 1) *Key pair generation*: In which the Key pair for the parties is generated.
- 2) *Creating verifiable form*: In which a Verifiable form is created which includes a VF-ID (Verifiable form ID) which is used to create the Signature.
- 3) *Signature Creation*: Using the VF-ID created above, a Signature is created.

B. Announcement

In this process, the Announcement of the transaction is made. After the Announcement is done, the one who is willing to participate in the Crypto Exchange will be accepting it.

C. Verification

In this process, the parties whoever is exchanging the cryptocurrency will be verifying the Signature by themselves and will be creating a CC-ID themselves to prove themselves Authorized for a Cross-Chain transaction. i.e., Party A will be verifying Party B's Signature and create a CC-ID for the Party B and Party B will be verifying Party A's Signature and creating a CC-ID for Party A.

D. Transaction

The transaction process is done in two steps: They are:

- 1) *Contract locking*: Contract locking is done to lock the Cryptocurrency within the contract using the

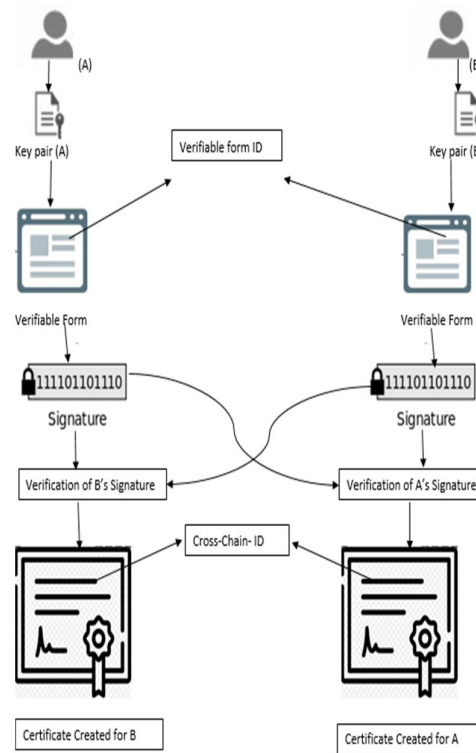


Figure 1-Cross-Chain ID Creation

- Hash of the CC-ID of the other party and send thatContract to them.
- 2) *Contract unlocking*: Contract unlocking is done to unlock the Cryptocurrency using the Hash of their CC-ID and the transaction is done.

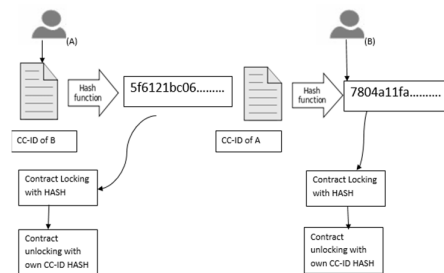


Figure 2- Transaction

V. CONCLUSION

A brief study on Blockchain technologies and Cross-Chain transactions is made. The Cross-Chain transactions are based on a third party, which acts as a representative of the whole transaction. Trusting a third party in a Crypto Currency exchange is not secure. So we proposed an Authentication protocol to make the Cross-Chain transaction safe and secure without the need of a third party to enter into the transaction.

REFERENCES

- [1] Fauzi, M. R. R., Nasution, S. M., & Paryasto, M. W. (2017). Implementation and Analysis of the use of Blockchain Transactions on the Workings of the Bitcoin. IOP Conference Series: Materials Science and Engineering, 260, 012003. <https://doi.org/10.1088/1757-899X/260/1/012003>
- [2] Lin, I.-C., & Liao, T.-C. (n.d.). A Survey of Blockchain Security Issues and Challenges. 7.

- [3] Al-Jaroodi, J., & Mohamed, N. (2019). Blockchain in Industries: A Survey. *IEEE Access*, 7, 36500–36515. <https://doi.org/10.1109/ACCESS.2019.2903554>
- [4] Ghimire, S., & Selvaraj, H. (2018). A Survey on Bitcoin Cryptocurrency and its Mining. 2018 26th International Conference on Systems Engineering (ICSEng), 1–6. <https://doi.org/10.1109/ICSENG.2018.8638208>
- [5] Amrutiya, V., Jhamb, S., Priyadarshi, P., & Bhatia, A. (2019). Trustless Two-Factor Authentication Using Smart Contracts in Blockchains. 2019 International Conference on Information Networking (ICOIN), 66–71. <https://doi.org/10.1109/ICOIN.2019.8718198>
- [6] Sandhya Pasala, V Pavani, G Vidya Lakshmi, & V Lakshman Narayana. (2020). Identification of attackers using blockchain transactions using cryptography methods. *Journal of Critical Reviews*, 7(06). <https://doi.org/10.31838/jcr.07.06.65>
- [7] Shadab, N., Houshmand, F., & Lesani, M. (2020). Cross-chain Transactions. 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 1–9. <https://doi.org/10.1109/ICBC48266.2020.9169477>
- [8] Yang, X., & Li, W. (2020). A zero-knowledge-proof-based digital identity management scheme in blockchain. *Computers & Security*, 99, 102050. <https://doi.org/10.1016/j.cose.2020.102050>
- [9] Maldonado-Ruiz, D., Torres, J., & El Madhoun, N. (2020). 3BI-ECC: A Decentralized Identity Framework Based on Blockchain Technology and Elliptic Curve Cryptography. 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 45–46. <https://doi.org/10.1109/BRAINS49436.2020.9223300>
- [10] Zhang, L., Zhang, H., Yu, J., & Xian, H. (2020). Blockchain-based two-party fair contract signing scheme. *Information Sciences*, 535, 142–155. <https://doi.org/10.1016/j.ins.2020.05.054>