ISSN No:-2456-2165

Kronocoin (KNC) – Peer-To-Peer Transactionusing Blockchain

Siddharth Shukla, Yash Wadhawe, Neha Ganeshe, Dr. Dilip Motwani
Vidyalankar Institute of Technology

Abstract:- A peer-to-peer version of electronic cash would allow online payments to be sent from one party to the other without contacting the financial institutions. We use the blockchain paradigm with cryptographically secured transactions. Here we are considering Bitcoin, the largest owned cryptocurrency in the market. We will tackle this by taking inspiration from previous cryptocurrency problems and providing a helpful solution to satisfy the requirements.

Our currency's name is Krono Coin, and it works on the algorithm of "Proof of Work." It uses blockchain to tackle real work problems and business application solutions.

Our objective is to build a platform where people would beable to mine cryptocurrency. Once hitting the desired mark, people would be able to use this coin as a means of transaction in real life.

We implement a wallet system for people to store their currency. This, if implemented with other wallets, will help people exchange, trade, and buy/sell other currencies.

Keywords:- *peer-to-peer, transactions, blockchain, cryptocurrency, proof of work.*

I. INTRODUCTION

Cryptocurrencies, often known as virtual currencies, are digital transactions that encrypt data. The word "crypto" comes from the Greek word "kryptós," which means "hidden" or "secret." There are numerous advantages to a digital currency established and utilized by private persons or organizations. We use the same blockchain method to deliversolutions to the most recent currency fluctuations.

Krono Coin is a decentralized currency. It is a blockchain- powered cryptocurrency that any user would be able to mine on his/her system. If the crypto is recognized in the market, users will be able to trade this currency with another form of currency. It is only possible when the currency gets a certain value to it in the later future. We use a proof-of-work algorithm to run our system. This algorithm maintains the security of the transaction by checking if the user has mined or not. Later about this algorithm in other pages. We use a proof-of-work algorithm to run our system. This algorithm maintains the security of the transaction by Ease of Use.

II. PROBLEM STATEMENT

Cryptocurrency is one of the latest trends in the market, which will be excessively big shortly. It is just like the internet back in the early 2000s. In today's world, each transaction we do can be tracked. This can leak out information that we do not want. A question of privacy and transparency comes into the picture. Lots of international transaction takes days/weeks to be executed. Not to forget, there is a central authority for every currency which governs the money. The government could track any transaction if it wanted to. Hence, there is a need for a decentralized, transparent, and fast currency in the transaction.

III. LITERATURE SURVEYED

A. SURVEY OF EXISTING OR SIMILAR SYSTEM

a) S. Nakamoto: Bitcoin, A peer-to-peer electronic cash system:
FEATURES - This paper talks about how the other cryptocurrency in the market face issue in their algorithm. This paper solves the gap that other cryptos have by implementing a "Proof of work" algorithm. This paper alsotalks about how the blockchain works in Bitcoin.

b) Vujicic, D., Jagodic, D., & Randic, S. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview:
FEATURES - This paper talks about how Ethereum works.Ethereum works on another algorithm known as "Proof of Stake," completely different from what bitcoin does. Ethereum solves the problem where Bitcoin falls short. They encrypt by SHA-256 for creating blocks. This paper also talked about the foundation of cryptocurrency and helped state how a cryptocurrency works.

B. LITERATURE SURVEY CONCLUSION

So, considering everything, we have decided to build our system/software. We will have improved scalability with less transaction time as per previous cryptocurrencies. Our project willalso be available for worldwide use.

C. LIMITATION EXISTING/SIMILAR SYSTEM

- Wallets Can Be Lost - Bitcoins are effectively "lost" ifa hard drive crashes, a virus corrupts data and the wallet file. There is not anything that can be done to get it back. These coins will remain orphaned in the system indefinitely. This has the potential to bankrupta wealthy Bitcoin investment in a matter of seconds, with no way of recovering. The investor's coins will be permanently orphaned as well.

- No Buyer Protection - When things are purchased with Bitcoins, and the seller fails to deliver the products promised, there is no way to reverse the transaction. This difficulty can be remedied by employing a third-party escrow service like ClearCoin; however, escrow services would take on banks' functions, making Bitcoins more liketraditional currencies.

IV. PROBLEM SOLUTION

The proposed solution introduces a new currency to the market. We use blockchain technology for decentralization. The currency is transparent and has a wallet feature. We use problems the problem solution provided in the research paper we skimmed across and generated our cryptocurrency. This currency can be mined and stored in the wallet for later tradingwith different users.

V. PROPOSED SYSTEM

We will try to explain the system using a simple block diagram:

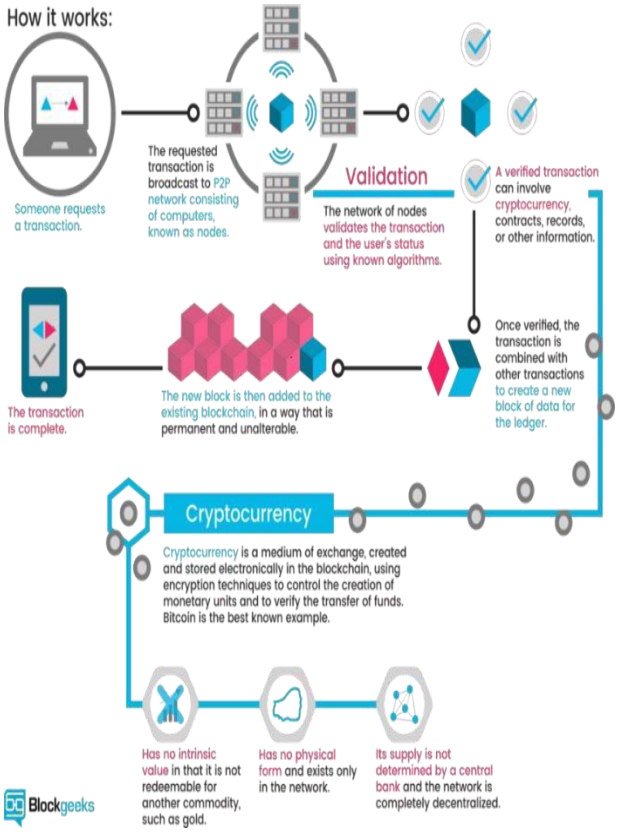

Fig. 1

A. OBJECTIVE OF THE PROPOSED SYSTEM

The objective of our current system is to implement decentralized currency for users. This will keep their transaction secured and private.

Our objectives are to learn the fundamentals of a new topic called the blockchain. We understand what cryptocurrency is by looking at examples such as Bitcoin, Ethereum, etc. There are many cryptocurrencies, but not all have an objective behind them. We come with an objective that provides "*Unique blockchain-centric solutions to real work problems and business applications*." We use JavaScript to code most ofour applications. We understand how mining works and make users be able to mine data and store it in their wallets.

We deploy the entire application on Heroku for the wide use of the public.

B. FEATURES OF THE PROPOSED SYSTEM

- OBSCURITY - Each transaction conducted is linked to the user's ID, whether the user is an individual or a company. The transactions are attached to a string of numbers which makes them unique. The Supply and demand cycle is proportional to the popularity of the cryptocurrency. Tracking the individual or company through a string of numbers is practically impossible. This subsequently makes the transactions done using Krono-coin extremely secure.
- ABSENCE OF SUPERVISION - The taxes and restrictions that are normally imposed by a governing body are eliminated in this case as there is no supervision by centrally authorized bodies. The fiscal and financial institutions cannot regulate the flow of Krono coin transactions, which can prove highly advantageous to the users. This removes the possibility of unfavourable fees and taxes.
- WALLET - Krono coin is equipped in a systematic way to ensure security. This is done through digital wallets, which areencrypted and can only be opened by a private key available tothe particular user. Only the person who mines the transactions will have access to the virtual rewards of the transaction provided to them. To further propagate security, Krono-coin miners should encrypt their storage devices.
- DECENTRALISATION - Like every efficient cryptocurrency system, Krono-coin is decentralized as it employs the blockchain method. Authorities do not have control over the transaction flow and rewards. The trading and transaction records address is not limited to a single location; it is spread throughout. After any infiltration attempt, there is no disruption of the transactions. The data is divided throughout the network as different miners and users extract it.

C. ALGORITHM

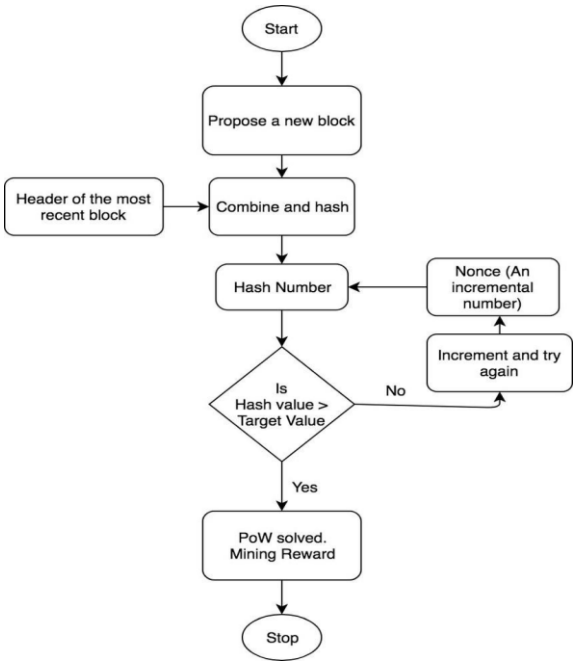

Fig 1: flowchart for proof of work

EXPLANATION: The algorithm generates a new block for the chain. It checks the header of the most recent block and combines the newly generated block with its hash value.

VI. METHODOLOGY

The proof of work algorithm is the main algorithm that would help build a new currency. We code a full-on backend for our crypto with test-driven development.

- Test driver approach for back end testing
- Building blockchain in OOP style
- Designing front end using ReactJS
- Deploy application on server using Redis
- Creating an API around the blockchain
- Use PubNub or PubSub to create real-timenetworking
- PoW algorithm for mining
- Using SHA-256 and digital signatures for validity
- To make a transaction pool accessible to users tocalculate the risk of invalid data.

VII. IMPLEMENTATION BY AES

A. ALGORITHM –

proof of work (pow) describes a system that requires a not-insignificant but feasible amount of effort to deter frivolous or malicious uses of computing power, such as sending spam emails or launching denial of service attacks. The concept was subsequently adapted to securing digital money by Hal Finney in 2004 through the idea of "reusable proof of work" using the SHA-256 hashing algorithm.

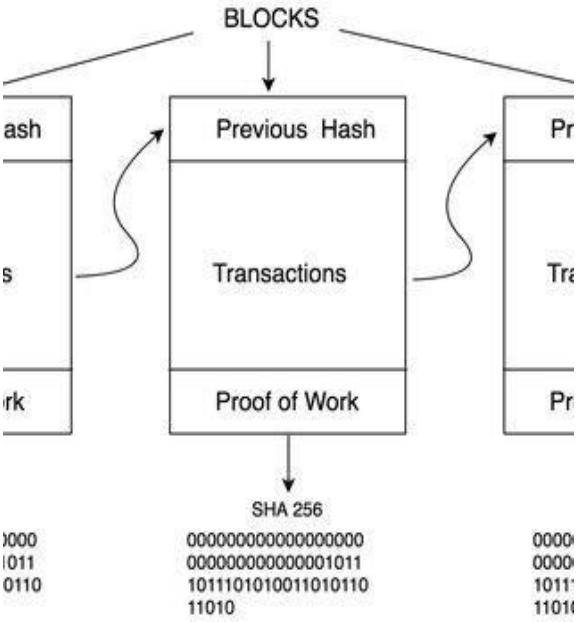

Fig. 2: Key size and Key Expansion in AES

B. SOCIAL IMPACT

The impact done by this initiative on society, in general, is huge. The investments related to the social aspects will open to more diverse and efficient funding as private establishments such as solar industries will cave into public funding. This will be analogous to crowdfunding but with digital and smart pay- outs to the stakeholders of the profit acquiring companies. the delivery of renewable energy will become efficient with the introduction of localized and decentralized currency

General citizens of the country will be in control of their data. The data of important organizations will be stored privately and securely on decentralized systems such as Krono-coin. This data will be efficiently transferred to financial and fiscal institutions, insurance companies, or health professionals.

The ability to harness and process big data by remaining within the boundaries of privacy will revolutionize the information-gaining sectors spread throughout the country. As we exponentially grow our ability to collect and process big data while retaining privacy, information generation will be revolutionized across all sectors and industries. Immediate transactions done to charitable institutions by Krono coin currency will induce faster and higher response rates.

VIII. CONCLUSION

Krono Coin will have its value if mined enough, using it as a trading method. It can trade different currencies such as USD, INR, BTC, ETH, etc. This only depends upon the value of the coin and the number of coins v/s the demand. This currency can help people do successful transactions across any international currency transparently. Most importantly,the decentralization makes sure that no central governing authority guides this currency. This could be India's first cryptocurrency. If the software picks up space, improved scalability and a faster transaction process would be

improved. A need for change in the algorithm will also happen.

ACKNOWLEDGEMENT

We thank our Head of Department, Principal, and our college staff for permitting us to use computers in the lab as and when required. We would also like to thank our project coordinator for providing us with all the proper facilities and support. We would also like to thank the staff members and lab assistants. Finally, we would like to thank everyone who has helped us directly or indirectly with our project.

REFERENCES

[1.] Vujicic, D., Jagodic, D., & Randic, S. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)
[2.] Ron, D., & Shamir, A. (2013). Quantitative Analysis of the Full Bitcoin Transaction Graph. Lecture Notes in Computer Science, 6–24
[3.] DR. GAVIN WOOD, ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER EIP-150 REVISION (a04ea02 - 2017-09-30)
[4.] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183–187
[5.] Nakov et al 2020 IOP Conf. Ser.: Mater. Sci. Eng. 1002 012020
[6.] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008
[7.] https://www.gqrgm.com/cryptocurrency-pros-cons/
[8.] Xu, Min Chen, Xingtong Kou, Gang 20192019/07/04 A systematic review of blockchain Financial Innovation
[9.] DeVries, Peter. (2016). An Analysis of Cryptocurrency, Bitcoin, and the Future. International Journal of Business Management andCommerce. Vol. 1. Pages 1-9.
[10.] https://www.ssrn.com/index.cfm/en/cryptocurrency/