ISSN No:-2456-2165

Designing a Cryptocurrency from Scratch

Raman Kumar [#1], Rahul Sivaselvam [#2], Prabhakaran R[#3]
[#] SCOPE, VIT Chennai
Chennai, Tamil Nadu, India

Abstract:- Cryptocurrencies have started garnering attention and worldwide usage. While various cryptocurrencies like Bitcoin and Ethereum have emerged as dominant players, there remains a growing interest in developing new, innovative cryptocurrencies that address specific shortcomings and requirements. This paper deals with exploring the key challenges faced by developers while designing a decentralized cryptocurrency from scratch.

I. INTRODUCTION

The word cryptocurrency is combination of crypto (cryptography) and currency. Cryptocurrency explained in the simplest terms is a digital currency. Knowing the working and limitation of traditional currencies helps in development of a cryptocurrency. Currency came into existence as it provided a medium of exchange for goods or services. The earliest usage of currency dates back to 600BCE, which was in the form of metal coinage[1]. Later on, paper notes were introduced which is currently the widest use form of fiat currencies. Currencies helped the solved the problem of alignment of needs associated with the barter system.

The fiat currencies around the world are controlled by some central authorities, which in almost all the cases is the respective country's government. If a person has to make an online transaction using fiat currency, then some third-party or central authority has to get involved to validate and regulate the transaction. This is dependency of fiat currencies on central authorities fuelled the need for a decentralized currency.

Since a decentralized currency does not depend on a central authority for validation of transactions, it must rely on some other means for validation of transactions such as cryptography. The cryptographic electronic money *ecash* developed by David Chaum in 1990 is one such example of usage of cryptography in payment systems.

Bitcoin, the first cryptocurrency, developed by Satoshi Nakamoto in 2008 proved to be a revolution in the field of decentralized finance. Currently it is the most valuable cryptocurrency in the world with market capitalization of around $666 billion. The cryptographic algorithms used by bitcoin includes SHA-256, ECDSA (Elliptic curve digital signature algorithm), RIPEMD-160, etc. This heavy use of cryptography provides the security against forgery. Bitcoin users can see all the transactions on the blockchain which is a distributed ledger. Users connect as nodes to the decentralized bitcoin network for making transactions or for listening to other user's transactions. To ensure that every node has the same copy of the blockchain, consensus algorithms for general agreement are used. Bitcoin uses of proof of work algorithm, which basically requires users to solve a mathematical puzzle in order to add a new block to the blockchain. This process of adding new blocks is called mining. The mining process creates new bitcoins.[2]

Though Bitcoin had many advantages like transparency and decentralization, its' limitations overshadow those advantages. Some of the major limitations include slow transaction speed, small block size and many more. These limitations eventually led to the creation of other cryptocurrencies. These new cryptocurrencies tried to improve upon the drawbacks of Bitcoin. That list includes Ethereum, Dogecoin, Solana and many other cryptocurrencies.

While designing a new cryptocurrency, the most important thing to consider is that this cryptocurrency should improve upon the features of most of the currently existing cryptocurrencies otherwise it would not be used by many people and the cryptocurrency will not be able to support itself.

II. RELATED WORKS

A literature survey on some related research and conference papers were performed. In the first journal paper by Mihail Mihaylov et al titled "NRGcoin: Virtual currency for trading of renewable energy in smart grids"[3], the researchers have built a decentralized digital currency titled NRGcoin for helping in trading renewable energy. Contrary to bitcoin, this cryptocurrency is generated by injecting energy in the smart grid rather than expending energy on solving hash puzzles. This paper conveys the fact the nowadays cryptocurrency for a specific purpose is also made. This whole cryptocurrency-energy trade system is carried out on the NRGcoin network. The system for which this cryptocurrency system is designed consists of three entities which are prosumers (those who have solar panels or any other renewable energy generators installed in their houses), consumers, and DSOs (the local power substations). A decentralized protocol determines how much NRGcoins a respective prosumer should get for injecting energy into the smart grid. The DSOs transfers the NRGcoins to the prosumer based on their production amount. New NRGcoins are generated by producing renewable energy.

Generating new coins is necessary to avert deflation. In the second paper, titled "Cryptocurrency Networks: A New P2P Paradigm", by Sergi Delgado-Segura, Cristina Pérez-Solà, Jordi Herrera-Joancomartí, Guillermo Navarro-Arribas and Joan Borrell, the distinctive features of peer-to-peer (P2P) networks in the realm of cryptocurrencies is investigated, with a focus on Bitcoin[4]. The study underscores the fundamental principles of decentralization, security, and synchronization in cryptocurrency networks. By examining properties such as node classifications, network subsets, and communication protocols, the paper reveals the unique nature of P2P networks within the cryptocurrency domain. Notably, the decentralized and nonstructured architecture of these networks, coupled with cryptographic techniques and information redundancy, ensures reliability and security. The research highlights the absence of traditional lookup protocols due to data replication in all nodes and emphasizes the critical role of propagation delay for network synchronization. The article concludes by outlining potential research avenues, including further analysis of pseudorandom mechanisms, and exploring integration possibilities with other distributed applications.

The third paper titled "Implementing a blockchain from scratch: why, how, and what we learned" by Fabian Knirsch et al. basically deals with implementation of a custom private and permissioned blockchain for trading of portions of photovoltaic plants by the users[5]. The nodes in their blockchain network are connected within a virtual private network. Java programming language and Raspberry Pi Model B were used for the implementing the nodes. The users of this blockchain network use a mobile application which is connected to the node for sending transactions and receiving confirmations. The app is also connected with a clearing server which has the task of retrieving data from the blockchain and sending the billing related information to the customers' app. After starting, the node reads the last persisted state stored in the disk and initializes the internal tree data structure that represents the blockchain, state table and other connected data structures. Then a watchdog for the server threads is initiated for listening to incoming messages from other nodes. Also, a mining thread is started which processes transactions that are unconfirmed and aggregates them into blocks. SQLite database is used for storing the state table.

Thus, from the survey of related works, it can be inferred that cryptocurrencies and blockchains are being made for real-world applications apart from finance.

III. SYSTEM DESIGN

Our blockchain and cryptocurrency system operate through a network of interconnected components, each serving a unique purpose. At the heart of the system lies the Blockchain, a decentralized ledger consisting of a series of Blocks, where each block contains a list of verified and secure Transactions. The integrity of these transactions is ensured through cryptographic hashing functions provided by the system.

When a new transaction is initiated, it enters the Transaction Pool, a temporary storage area (Fig 1.0). The Transaction Miner component validates transactions from the pool, ensuring their authenticity and compliance with the system's rules. Once a block is validated, it is added to the blockchain, making the transaction a permanent part of the ledger.

Users interact with the system through Wallets, creating new transactions and signing them with their private keys. These transactions are broadcasted to the network, picked up by the Transaction Pool, and subsequently included in the blockchain after validation.

The system also incorporates a Pubsub mechanism to facilitate communication between various components, ensuring seamless coordination among nodes in the network. Additionally, a transaction history, managed by the History component, is maintained, allowing users to track the flow of transactions over time.

This design establishes a robust and transparent ecosystem for cryptocurrency transactions, characterized by decentralized control, cryptographic security, and efficient validation processes. To enhance scalability, our system employs advanced consensus algorithms and optimized data structures. The decentralized nature of the Blockchain ensures that the network can scale horizontally, accommodating a growing number of transactions and users without compromising efficiency. Smart optimizations within the Transaction Pool and Transaction Miner components further streamline the validation process, allowing the system to handle a high volume of transactions in real-time.

Security is paramount in our design. The cryptographic techniques used not only secure individual transactions but also safeguard the entire network against tampering and unauthorized access. Public and private key cryptography mechanisms, integrated into Wallets and Transactions, guarantee secure peer-to-peer transactions. Additionally, regular updates and security audits are conducted to identify and mitigate potential vulnerabilities, ensuring the system's resilience against evolving threats.

In summary, our blockchain and cryptocurrency system combines cutting-edge technology with a user-friendly interface, creating a secure, scalable, and transparent environment for digital transactions.

ISSN No:-2456-2165

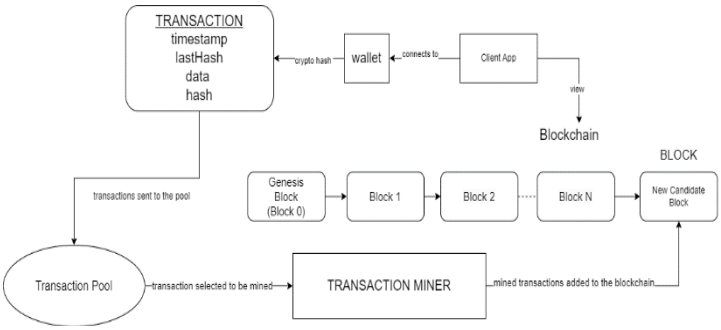

Fig 1.0 – Process Flow Diagram

IV. CONCLUSION

In conclusion, the blockchain cryptocurrency system is but a dip in the realm of digital finance, leveraging decentralized technologies to create a secure, transparent, and efficient ecosystem for financial transactions. By addressing the limitations of traditional fiat currencies, we have developed a robust infrastructure that fosters peer-to-peer transactions without the need for central authorities, ensuring financial sovereignty for users. Through meticulous attention to detail in system design, we have established a decentralized ledger, the Blockchain, propped up by the latest cryptographic techniques, guaranteeing the integrity and security of every transaction. The transaction pool and transaction miner components streamline transaction validation, which facilitates real-time processing and scalability to accommodate a growing user base. The system has been proven to support multiple instances at the same time on different peer applications. The privacy and security of the users are protected as nowhere in the system do we pass the private key value for any operation, just the public key.

V. FUTURE WORK

Our blockchain and cryptocurrency system lays a solid foundation for future innovations and expansions. One avenue that is necessary to be explored is the integration of smart contracts, enabling self-executing agreements without intermediaries. By incorporating a smart contract platform, our system could facilitate a wide array of decentralized applications, from automated financial services to secure voting systems. Exploring interoperability with other blockchain networks can enhance the ecosystem's functionality. Cross-chain communication protocols would enable seamless exchange of assets and data between different blockchain platforms, fostering a more interconnected and versatile digital economy. Additionally, ongoing research into consensus algorithms and scalability solutions will be crucial. New consensus mechanisms, such as Directed Acyclic Graphs (DAGs), could enhance energy efficiency and transaction throughput. Scalability solutions like sharding or off-chain protocols might further optimize the system's performance, ensuring it can handle an ever-increasing user base and transaction volume. Lastly, privacy-focused technologies such as zero-knowledge proofs and ring signatures could be integrated to enhance transaction privacy, addressing a critical concern in the cryptocurrency space. By continuously exploring these avenues and embracing emerging technologies, our blockchain and cryptocurrency system can evolve into a dynamic and versatile platform, catering to diverse user needs while maintaining the core principles of decentralization, security, and efficiency.

REFERENCES

[1]. Beattie, A. (2022, September 18). The history of money. Investopedia. https://www.investopedia.com/articles/07/roots_of_money.asp

[2]. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

[3]. M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril and A. Nowé, "NRGcoin: Virtual currency for trading of renewable energy in smart grids," 11th International Conference on the European Energy Market (EEM14), Krakow, Poland, 2014, pp. 1-6, doi:10.1109/EEM.2014.6861213.

[4]. Sergi Delgado-Segura, Cristina Pérez-Solà, Jordi Herrera-Joancomartí, Guillermo Navarro-Arribas, Joan Borrell, "Cryptocurrency Networks: A New P2P Paradigm", Mobile Information Systems, vol. 2018, Article ID 2159082, 16 pages, 2018. https://doi.org/10.1155/2018/2159082

[5]. Knirsch, F., Unterweger, A., & Engel, D. (2019). Implementing a blockchain from scratch: why, how, and what we learned. EURASIP Journal on Information Security, 2019(1). https://doi.org/10.1186/s13635-019-0085-3