IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

STUDY OF BLOCKCHAIN FOUNDATION

Shrutika Sanjiv Padalkar
Department of IT
GMVCS Tala
University of Mumbai
shrutikapadalkar@gmail.com

Ashwini Dattatray Salunke
Department of IT
GMVCS Tala
University of Mumbai
ashwinisalunke2903@gmail.com

Kaustubh Pradip Mekde
Department of IT
GMVCS Tala
University of Mumbai
kaustubhmekde9@gmail.com

Prof Avni Anup Amburle.
Assistant professor GMVCS & GMVIT
University of Mumbai

Abstract :- Blockchain (or crypto) foundations are nonprofit organizations that supply public goods to a crypto-economy. The standard theory of crypto foundations is that they are like governments with respect to a national or regional economy, i.e. raising a public treasury and allocating resources to blockchain specific capital works, education, R&D, etc., to benefit the community and develop the ecosystem. We propose an alternative theory of what foundations do, namely that the treasury they manage is a moat to raise the cost of exit or forking because the benefit of the fund is only available to those who stay with the chain. Furthermore, building and maintaining a large treasury is a costly signal that only a high quality chain could afford to do (Spence 1973). We review these two models of the economic function of a blockchain foundation - (1) as a private government supplying local public goods, and (2) as a moat to raise the opportunity costs of exit.

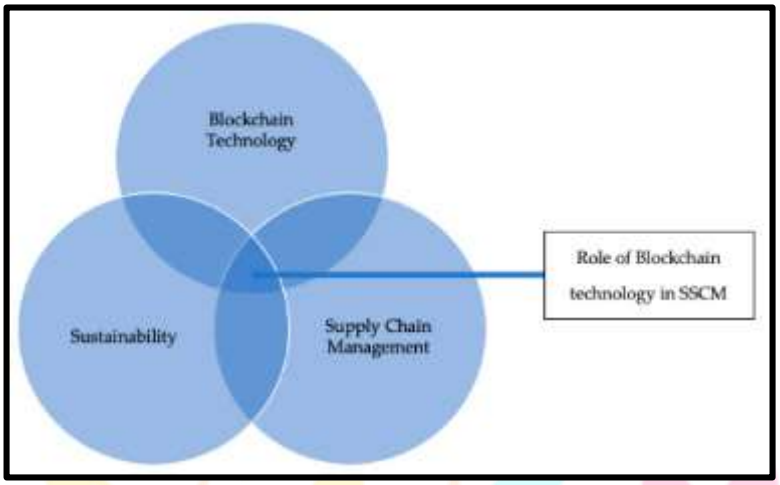
Keywords :- Laying The Blockchain Foundation, Cryptography, Properties Of Blockchain Solutions, Blockchain Transactions, Scaling Blockchain

INTRODUCTION

Blockchain is the new phenomenon to sweep the world of technology and moreover financial transactions. Many of us are drawn to it because of cryptocurrency. However, there is more to blockchain than cryptocurrency. Blockchain is a technology that can be used for carrying out financial transactions, creating applications as well as a database for your application. Blockchain has introduced a lot many new concepts as well as reused the existing ones in such an exemplary way that we are stunned by the sheer simplicity of the technology and awed by the possible scope of its applications. Blockchain technology has a lot of advantages like lowering the costs related to financial transactions, elimination of third parties, speed of transactions, reducing the risk of fraud and the flexibility to involve and be a part of the process.

❖ LAYING THE BLOCKCHAIN FOUNDATION

Blockchain is a combination of the concepts from cryptography, game theory, and computer science engineering, as shown below:



Traditional centralized systems allowed only one entity to maintain the history of transactions or modifications to ensure concurrency in a system. However, the issue with a single point of control was the complete trust on that single entity. If all the systems were given full control to modify the transactions then the problems would definitely increase because we never know what those systems might do. So, the trust issue now multiplies to the number of nodes with full control.

Blockchain uses cryptography, game theory and computer science concepts to solve the trust issues plaguing a trustless system with multiple entities.

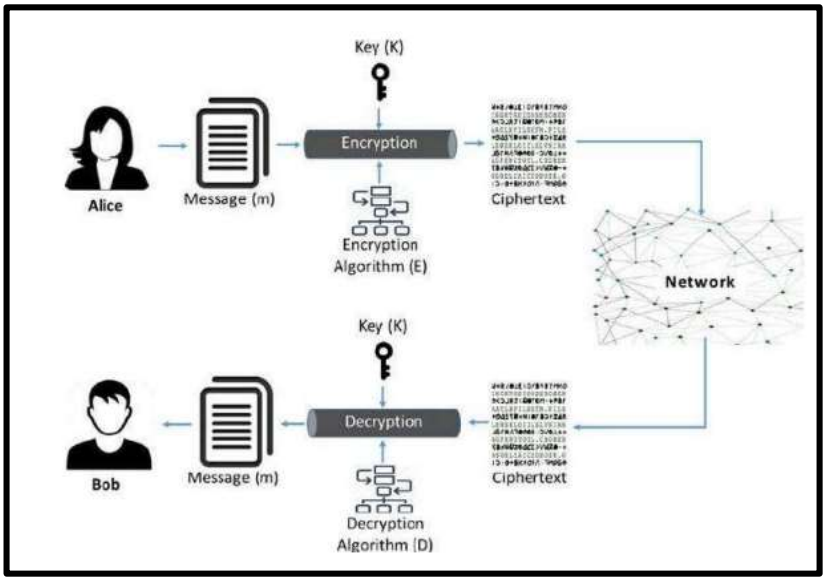
Cryptography can be used to check the validity of the user performing a particular transaction. However, it does not prevent a user from spending the same amount twice called as the double spend attack. The only way to thwart a double spend is to make all the nodes aware of all the transactions.

Computer science techniques incorporate cryptography and game theory concepts into an application and enables decentralized as well as distributed computing amongst the nodes using data structure and network communication components.

❖ CRYPTOGRAPHY

Cryptography is one of the most important components of blockchain. It plays an important part in validating users and securing transactions. Cryptography consists of many mathematical techniques that can be used to solve various issues in Blockchain.

Cryptography has been used from a long time ago for hiding information i.e. keeping the messages confidential. Cryptography has various applications likemaintaining the integrity of the message, verifying and validating a user,etc.



Confidentiality: Confidentiality means that only the intended recipient can access the message.

Data Integrity: Data Integrity allows us to check if the data has been altered or modified during transmission.

Authentication: The sender of a message is verified and validated using authentication. It checks whether a user is who he/she claims to be.

Non-repudiation: It ensures that the sender cannot deny sending a message. Plaintext: The actual information that needs to be sent is called plaintext.

Ciphertext: The information to be sent(plaintext) is converted to another form called ciphertext.

Encrypt: The process of converting plaintext to ciphertext is called Encryption or encoding. It usually consists of an algorithm and a key.

Decrypt: The process of recovering plaintext from ciphertext is called Decryption or Decoding. It usually consists of an algorithm and a key.

❖ PROPERTIES OF BLOCKCHAIN SOLUTIONS

1. Immutability : A blockchain transaction is irreversible. Once a transaction is recorded, it cannot be altered. The transactions are broadcast to the network so all the nodes have a copy of the blockchain. As the number of blocks increase so does the immutability of the blockchain. It is not feasible for someone to alter the data of so many blocks in a series. A transaction that gets logged in the system remains forever in the system.

2. Forgery Resistant : Blockchain is decentralized in nature. Hence, it is prone to attack and forgery. Cryptographic hash and digital signatures used in blockchain ensure the system is forgery resistant. The transactions are signed using a private key and a hash is calculated of the same. Hence, it is impossible for anyone to forge it thus ensuring integrity and authentication.

3. Democratic : Blockchain does not have a centralized controller. All the nodes are treated equally. Hence, every participant has equal rights in any situation, and decisions are made when the majority reaches a consensus. Thus it is democratic in nature.

4. **Consistent State of the Ledger :** The state of the blockchain should be consistent across all the nodes of the network. To ensure the stability of the system, a consensus mechanism is used in blockchains.

5. **Resilient :** The network should be resilient enough to withstand temporary node failures, unavailability of some computing nodes at times, network latency and packet drops, etc.

❖ BLOCKCHAIN TRANSACTIONS

Blockchain consists of blocks of transactions that are verified and then added to the block. Whenever an individual or an entity is making a transaction, they just have to broadcast it to the whole network. This transaction is validated by multiple nodes. Once validated, it is updated on all the nodes of the network as part of the blockchain. When the transactions happen every second, broadcasting individual transactions can become a costly affair. Hence, transactions are combined in blocks. It is also done to prevent a Sybil Attack. In a Sybil attack, people create replicas of their nodes to dominate the network.

Steps in blockchain transactions: Every new transaction gets broadcast to all the nodes on the network so that all the computing nodes are aware of all transactions

Every transaction undergoes validation and authentication checks by the nodes. If it is valid, it is accepted, else rejected. The nodes further group multiple transactions into blocks to share with the other nodes in the network. This is called proposing a block. Every node is given equal priority in the generation of new blocks. A consensus mechanism ensures that every node agrees upon a block. The blocks are time stamped in the order they arrive and get added to the blockchain.

Once the nodes in the network unanimously accept a block, then that block gets added to the blockchain by including the hash of the previous block. “Bloom filters” are widely used to test the membership of a transaction in a block.

❖ SCALING BLOCKCHAIN

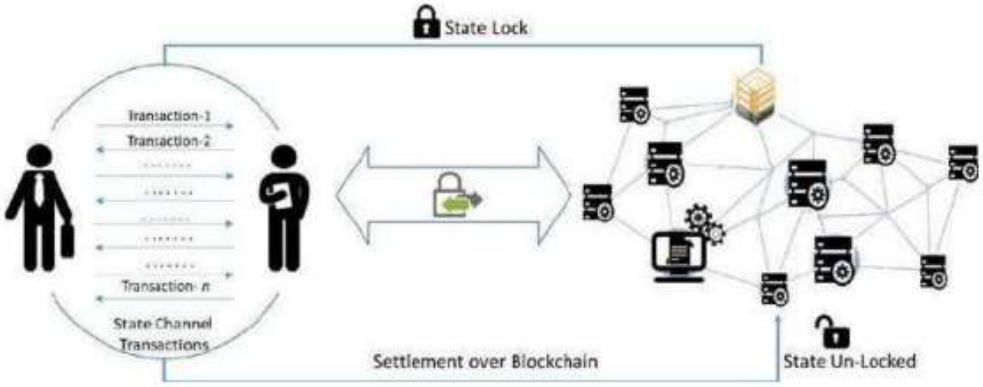
Blockchains are difficult to scale. Bitcoins are not a replacement to fiat currencies.It cannot be used for day to day monetary transactions which are carried out by our debit or credit card.

Consensus protocols are used for agreement between all the communicating nodes for stability of the system. In a blockchain network, every node maintains its own copy of the entire blockchain, validates all transactions and blocks, serves requests from other nodes in the network, etc. to achieve decentralization. This can lead to latency. Increase in the number of nodes provides stability however it also increases the number of transactions hence adding to the load of computing and storage requirements. This is a common cause for concern in public blockchains. Private blockchains on the other hand can be easily scaled because the controlling entities could define and set node specifications with high computation power and more bandwidth or use off-chain computations.

1. Off-Chain Computation

Off-chain computation is outsourcing the resource intensive operations and limiting only the storage of outcomes on blockchain nodes. There are different variants of off-chain computation depending on people as well as the computation needs and limitations of the nodes involved. It can be considered as a layer on top of the blockchain which is responsible for processing involved in a blockchain.

Let's assume Alice and Bob carry out a lot of transactions in a month. All these individual transactions would have their state information which will be maintained by all the nodes in a stateful blockchain. The concept of “state channels'' is introduced to address this challenge. The state channel is updated with utmost security using cryptography periodically or when a certain transaction threshold is reached. State channels are essentially a two-way communication channel between users, objects,or services.



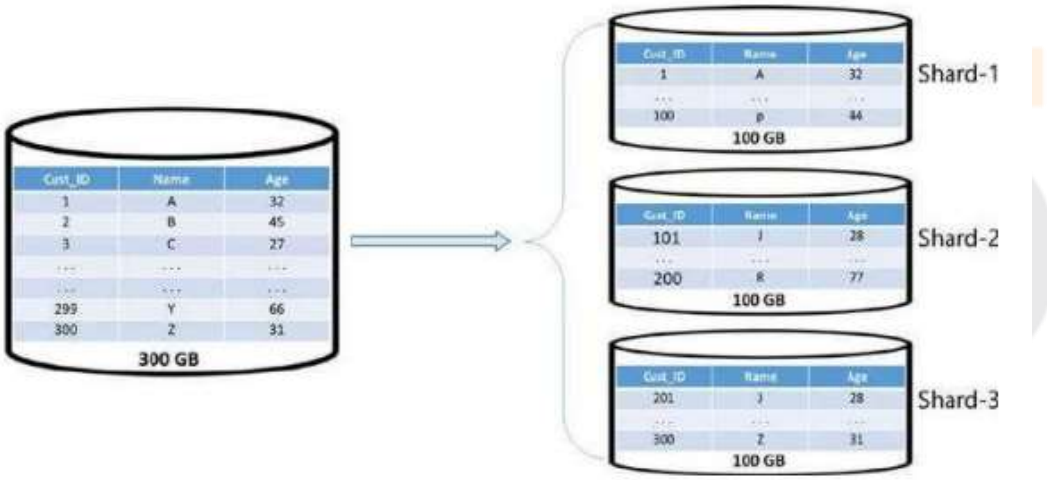
The off-chain state channels are private and confined to a group of participants. The state of blockchain for the participants is locked in the beginning by using MultiSig scheme or a smart contract-based locking. The participants make cryptographically secured transactions among each other.

Since the transactions are cryptographically signed, they can be verified and submitted to the blockchain. The state channels could have a predefined lifespan, or could be bound to the amount of transactions being carried out in terms of volume/quantity or any other quantifiable measure.

The final outcome of the transactions is saved on the blockchain and that unlocks the state as the final step.The Lightning Network is an Off-chain computation network for Bitcoin whereas the "Raiden Network" was designed for Ethereum blockchain.

2. Sharding Blockchain State

Sharding is a concept of slicing databases for easy processing. Operations like Disk read/write always lead to bottlenecks while dealing with huge data sets. The data is partitioned across multiple disks so that the read/ write could be performed in parallel leading to reduced latency. This technique is called sharding.



a300GB database table is partitioned into three shards of 100GB each and stored on separate server instances. The same concept can be applied for blockchain. The complete blockchain state is divided into different shards which contain their own substates i.e. a node need not store the entire blockchain, it can just store portions or shards relevant to it.

When a transaction occurs, it is routed to only specific nodes depending on which shards they affect. It is not mandatory for all the nodes to perform calculations and verifications for each and every transaction.

A mechanism or a protocol could be defined for communication between shards when multiple shards are needed to process transactions.

CONCLUSION

Hence we Had studied About Big data analytics and analytical theory and methods.

REFERENCES:-

Zhang, X., Bian, J., Zhou, X., & Sun, J. (2021). Understanding blockchain technology adoption in financial inclusion: