



AN OVERVIEW OF BLOCKCHAIN TECHNOLOGY IN MODERN ERA

¹ Priyanka B. Shingade, ² Babasaheb U. Shingade, ³ Pearly P. Kartha

¹ Assistant Professor, ² Librarian, ³ Assistant Professor

¹ Department of Mathematics,

¹ Dr.D.Y.Patil Arts, Commerce and Science College, Savitribai Phule Pune University Department of Mathematics, Sant Tukaram Nagar, Pimpri, Pune, Maharashtra-411018, India.

Abstract: Blockchain technology is an exceedingly modern approach in the field of information technologies. Blockchain, is the technology underlying cryptocurrency, which adopts a peer-to-peer network to authenticate transactions. This paper aims to explore the existing research in the field of blockchain-related studies and to discuss futuristic development in blockchain and cryptocurrency. Through the findings of this paper, we deliver a blockchain research which illuminates the possible research and provides implications for the future of cryptocurrency. We use distributed ledger technology to get to know more about blockchain, as blockchains are tamper evident and alter free digital ledgers implemented in a distributed fashion. This paper provides a summary of blockchain technology; it brings a blueprint of all the pivotal design features, attributes, and benefits of blockchain in cryptocurrency, Bitcoin and Ethereum are one of the major applications of cryptocurrency. Additionally, the paper discusses the enhancement that is needed in cryptocurrency. The originality of this paper is on the discussion of new approaches for cryptocurrency scanning by patterns in blockchain. Herein we have introduced one basic structure/model for a cryptocurrency for it to be traceable, which is a theoretical idea. This paper is meant to give a brief introduction to these topics.

Index Terms - blockchain; bitcoin; distributed ledger technology; cryptocurrency; advancement

I. INTRODUCTION

The Fundamentals of Blockchain Technology is how transactions are made on the Internet? Basically, Blockchain is a system of recording information which cannot be changed, hacked or duped. Let us understand in depth about the technology first. Suppose we want to purchase something which is authentic and not damaged or fake, for this we must ensure that we are buying real things and not some cheap local or in extreme case nothing in our delivery box at all. How we get the guarantee that the product indeed is the authentic or original one and we actually get it. The answer to the question is so simple, that is we need Information on the subject and we are able to verify the information in order to make a successful transaction. Blockchain Technology on the network works exactly like what we have stated when it comes to transactions. For each transaction the source must be reliable, authentic, verified and cannot get tampered. As we all know in the present cyber world everything that happens on the network it is difficult to secure such information without letting it get tampered with and maintain this authentic source of information for trusted transactions. Daily multiple attacks is attempted by hackers and cyber criminals which includes internet fraud, Malware, fake publicities, Bank fraud, Credit card fraud, and whatnot. It kind of became virtually impossible to make this even stopped. And here comes the solution to this virtual problem by a technology

called Blockchain Technology. Blockchain can be used as a trusted source of information that can be verified and cannot be tampered or changed in any way.

One scientific way to define blockchain- “Blockchain is an ever growing ledger that keeps a permanent record of all transactions that took place on the network in a secure and chronological order and cannot be tampered with.”

I. CHARACTERISTICS OF BLOCKCHAIN TECHNOLOGY

Let us understand blockchain technology deeply by gripping on the characteristics of blockchain.

- 1) Ever Growing ledger- Blockchain is just a file, which saves or stores the information of all the transactions that happened and that are going to happen in the future.
- 2) Permanent Record- All the information which is stored in blockchain is permanent and cannot be altered or deleted in any way
- 3) Secure Record- It uses every advanced cryptographic method to secure the data in the highest levels of security.
- 4) Chronological order- We are going to discuss this in detail about the idea in the paper. But, as of now the order based on time of transaction is the order we are interested in.

This basic characteristic underlines the feature and best understanding about the blockchain technology, helping the network to be tamper proof.

I. BACKGROUND ABOUT THE BLOCKCHAIN TECHNOLOGY

Before the Blockchain technology, the traditional way for network based transactions by Banks and Financial sectors was Client Server Model. So, what exactly is the Client Server Model? All the computers that is being used, run on Client Server Model. Client Server Model is a network created between the main server computer and the number of client computers which are connected to the Centralized main server. The main server computer stores all the information and data of a particular application. For example, In Banking applications, consider a bank situation where banks usually provide an internet banking facility to their customers through the internet. A bank has a main server computer that stores all the information or data of a customer. Each customer is provided with credentials from which they can login and do the respective transactions. The client server computer and main computer interact with each other and provide the customer accurate data and the transaction is made. There are thousands of client computers connected to the main service computer. This client server model is prone to hackers, attackers or viruses. They use extensive hacking techniques to get into the system and cause damage to the main server itself. They can access all sorts of data of all the customers once they are into the main server computer. So, to avoid this many organizations nowadays use Blockchains instead of the client server model. Unlike the Client server model, Blockchains are decentralized. Blockchain uses Nodes, nodes are individual computers that are broadened all over the world. All the nodes host and run the blockchain programme. As nodes provide real life solutions there is very less probability that a blockchain network fails or gets hacked. And as in blockchain networks the information or data is stored on thousands of nodes so even though one node fails the network will not fail. It fails only when all the nodes fail, and which is next to impossible, as the attacker needs to go through each node simultaneously without being detected. Information in the blockchain network cannot be changed, in the client server model any person who gets into the main server can access and hence can change the data easily. This type of security is one of the biggest successes for blockchain technology.

II. HISTORY OF A CRYPTOCURRENCY/ BITCOIN

Bitcoin is a peer to peer digital currency. In the early 90's, tampering of digital documents was one of the biggest security issues. Many people used others' information or data and published it in their names. Many programmers and researchers came up with an idea of Time stamping of digital documents. The idea was when a document is signed or changed or altered in any kind of way, a time stamp is generated. The idea of time stamping or data stamping technology is used in blockchain technology, allowing it to act as Digital ledger and store the data in such a way that no one can tamper with them. On 31st october 2008, **Satoshi Nakamoto** came with more secure time stamping technology. He proposed a white paper, outlining the function of his peer to peer virtual currency-Bitcoin. Bitcoin runs on a secure system that uses both digital signatures and actual time stamps of the transaction. All the time stamps or the transaction would be hash

into a chain which cannot be tampered or changed without changing the precious transaction which is impossible. Cryptocurrency runs on nodes instead of client server mode. Cryptocurrency is a digital asset which can be bought, sold and transferred securely between people all across the world through a network. Crptocurrency has no physical element like coin or paper form as it is totally different from rupees or dollars. Unlike other currencies Cryptocurrency needs no middleman, customers themselves do the transaction on their own easily, securely and instantly. The technology which makes this possible is Blockchain technology.

III. Components of Blockchain technology

Let us understand the components that help to build a blockchain.

A. Miners

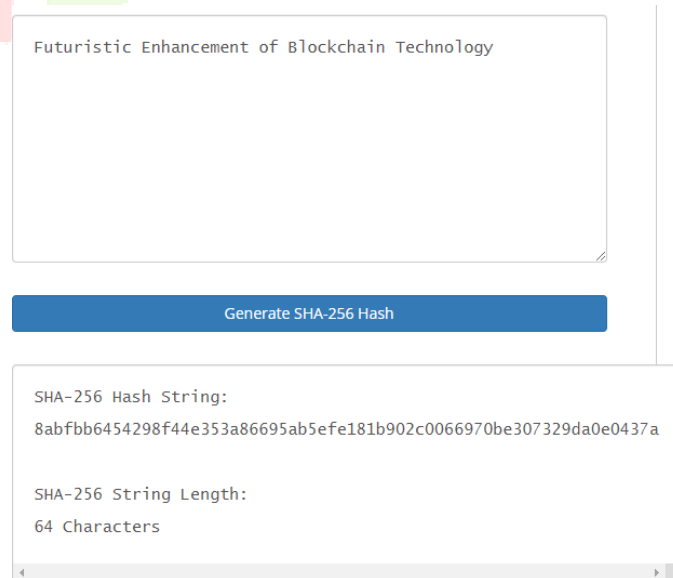
Cryptocurrency basically gets generated from Miners. Let us understand about Miners, Miners are the group of people all over the world that forms the blockchain network which in turn runs the Cryptocurrency ledger. The data of the network is hoarded in blocks. After every 10 minutes, a new block is created to the blockchain which contains all the information about the transactions that happened in that last 10 minutes, and as discussed data stored and the block generated are in chronological order this time stamp helps blocks to be in chronological order. Blockchain of bitcoin started all the way back from 3rd january 2009 on which the very first block transaction was made. This is called the Genesis block, from then all the transactions that happened on the network are stored in sizes of a block. Each block holds information about transactions that happened in the last 10 minutes of creating the block.

As new transactions happen they are added to blocks. Miners play a vital role in the blockchain network of bitcoin. Miners basically solve a cryptographic math problem and encode the transactions onto the network. For each encoding block is generated and miners get rewarded a bitcoin and this is how bitcoin is generated on the network.

B. Hash

Miners solve cryptographic math problem. A SHA256 hash function powers the cryptography of bitcoin Blockchain. SHA256 stands for a secure Hash Algorithm which has a fixed size of 256 bits. It is a part of the set of cryptographic functions developed by National Security Agencies. Hash is a digital fingerprint of a set of sets of data. It is a bunch of alpha-numeric characters that identify with a certain amount of data. We input some data into the Hash generator, it generates a hash for the particular input. i.e.; for the data we input we have a hash and even if we change a single character in the data, the hash changes completely.

We can generate a hash value for data of any size from a single character to the content of world's largest libraries together. The hash always has a fixed length i.e., 256 bits. Hash of the same data will always be the same. There is no way two different sets of data will have the same hash value. It is one directional i.e., we can change data into hash value but cannot change Hash value into data.



Futuristic Enhancement of Blockchain Technology

Generate SHA-256 Hash

SHA-256 Hash String:
8abfbb6454298f44e353a86695ab5efe181b902c0066970be307329da0e0437a

SHA-256 String Length:
64 Characters

Fig. 1 SHA256 Hash generator

C. Block

The very first block on blockchain is Genesis block. Let us understand the structure of elements of a block. Every block contains 6 elements.

- Understanding elements of block
 - 1) **Index:** Index is a serial number of that particular block. The very first block is Genesis block. In the next series of blocks, index will show the serial number of those particular blocks, like block #1, block #2, etc.
 - 2) **Time Stamp:** On every block of the blockchain, there will be a time stamp stating exactly when that particular block was created. As we know, every block follows the chronological order, so the time stamp helps maintain the chronological order.
 - 3) **Data:** This is the actual information of all the transactions that we want to store in the blockchain.
 - 4) **Hash:** It is a digital footprint of data that is stored in the data section.
 - 5) **Previous Hash:** As the name suggests, this section contains the Hash function from the previous blocks. For a genesis block there is no block prior to this block. So, the previous block is zero. But when the next block is created, we have the hash of the genesis block in the section of previous block in block #1.
 - 6) **Nonce:** Nonce stands for number used once. It is just a number that satisfies the validity of a block.

IV. Working of a Block

A block is valid if it contains three leading zeros in the hash. The task is to make a block valid. One needs to find out a way to generate a hash with three leading zeros' because only then we make sure that the block is valid with the help of nonce number.

We have to figure out the exact nonce number which generates a hash with three leading zero and make a block valid. And the way we figure out the exact nonce number is by mining the block.

When the miner clicks the mine button, the computer uses its processing power and runs all combinations of numbers from

one to millions to find the exact number to make the block reliable. The exact nonce number is found and generates a hash with three leading zeros and makes a block valid. If we change a little in data, hash changes and blocks become invalid even though we have the nonce. This is how SHA256 cryptography structures the validity of a particular block.

V. Understanding Blockchain technology and Cryptocurrency

Let us consider the number of blocks in blockchain; Block which has all the elements which makes all the blocks a valid one. Every block on the blockchain is cryptographically tied to the next block and this relation continues throughout the blockchain even when it has billions of blocks in it.

As we know in the genesis block the previous hash value is zero and in the block #1 and the block #2 has the previous hash which is hash of the block #1. And this makes immutable blocks. If anyone changes the content of any block, it breaks the validity of the block and not only that it breaks the validity of the next block and hence the next block and so on all the blocks next to it.

That is, a change in one block will not only make it invalid but it will also break down all the blocks that are created after that particular block as all the blocks on the blockchain are cryptographically tied together. But we can fix this by again giving it a nonce number which satisfies all the conditions and make a block valid one and we have to mine it. But not only for the first block but for all the blocks in that particular blockchain (mine all of the blocks). So, the cryptographic math problem is actually finding the nonce number. This entire system makes the network of blockchain secure and immutable. If any hacker or attacker tampers with any of the blocks, all the blocks from that particular block till the end becomes invalid. And if anyone wants to fix it like we discussed it, it becomes a huge task and which is next to impossible to be unidentified by the miners. They need at least 51% of control power of all the hashing power and they also need to complete it within 10 minutes, because new blocks get added to blockchain every 10 minutes.

- Structure of a Cryptocurrency -

There are four components of Cryptocurrency:

- 1) Software: Essentially Cryptocurrency is just software. The software defines what a Cryptocurrency is, how the Cryptocurrency is transferred from one person to another. Also defines the validity and invalidity of Cryptocurrency itself.
- 2) Cryptography: It is cryptocurrency. It depends on cryptography to regulate the transfer of Cryptocurrency between parties and also regulates new creation of Cryptocurrency.
- 3) Hardware: To run the software of Cryptocurrency it needs computer and processing units i.e. Miners run Cryptocurrency software. Cryptocurrency is running on thousands of computers all over the world forming the Hardware component of Cryptocurrency.
- 4) Motivation: All miners running software are doing so because they are rewarded in Cryptocurrency when they successfully encode a block onto a blockchain. The reward motivates them to mine the technology.

- Adding block onto blockchain

Various components of Cryptocurrency come together and form a blockchain network. In the process of Cryptocurrency, we first get into software which gives a cryptographic math problem every 10 min. The challenge is to find specific nonces which will help in finding the valid hash for a block, so that it can be added into a blockchain. Once this challenge is issued, miners get into the process. These miners run the hardware of Cryptocurrency. All the miners start to compete with each other to find the exact nonce that makes the hash and block valid and earns the Cryptocurrency. In the process, the computer actually has to deal with billions of possibilities of random numbers to find one nonce number that can satisfy the block.

During the process, one of the miners solve the cryptographic math problem and find a correct nonce number and all other miners take the responsibility to verify the validity of the block which has just been mined, which makes Cryptocurrency secure. Solution found by one miner is verified by the whole mining community. When the verification is completed and the block is declared valid by the whole network, the new block is added to the blockchain and this is how a block is generated every 10 minutes, which contains Data of all the transactions that happens in a network. Once this process is completed, the miner who solved it receives a reward which is 12.5 bitcoins now and this is how new bitcoins are created on the network. Cryptocurrency is more desirable as there is no middleman like other currencies on the internet. There are number of banking institutions or credit card companies that use processors like PayPal which acts as a middleman who controls the transfer of the money from one person to another. This middleman keeps a centralized record of all the transactions that happen through them, they hold authority and manage all monitoring processes. In Cryptocurrency, the middleman is eliminated. It is a peer-to-peer currency which replaces third party integration. As there is no single point of failure in Cryptocurrency, it is easy and powerful for the existence of bitcoin. Bitcoin is decentralized, the network takes care of itself.

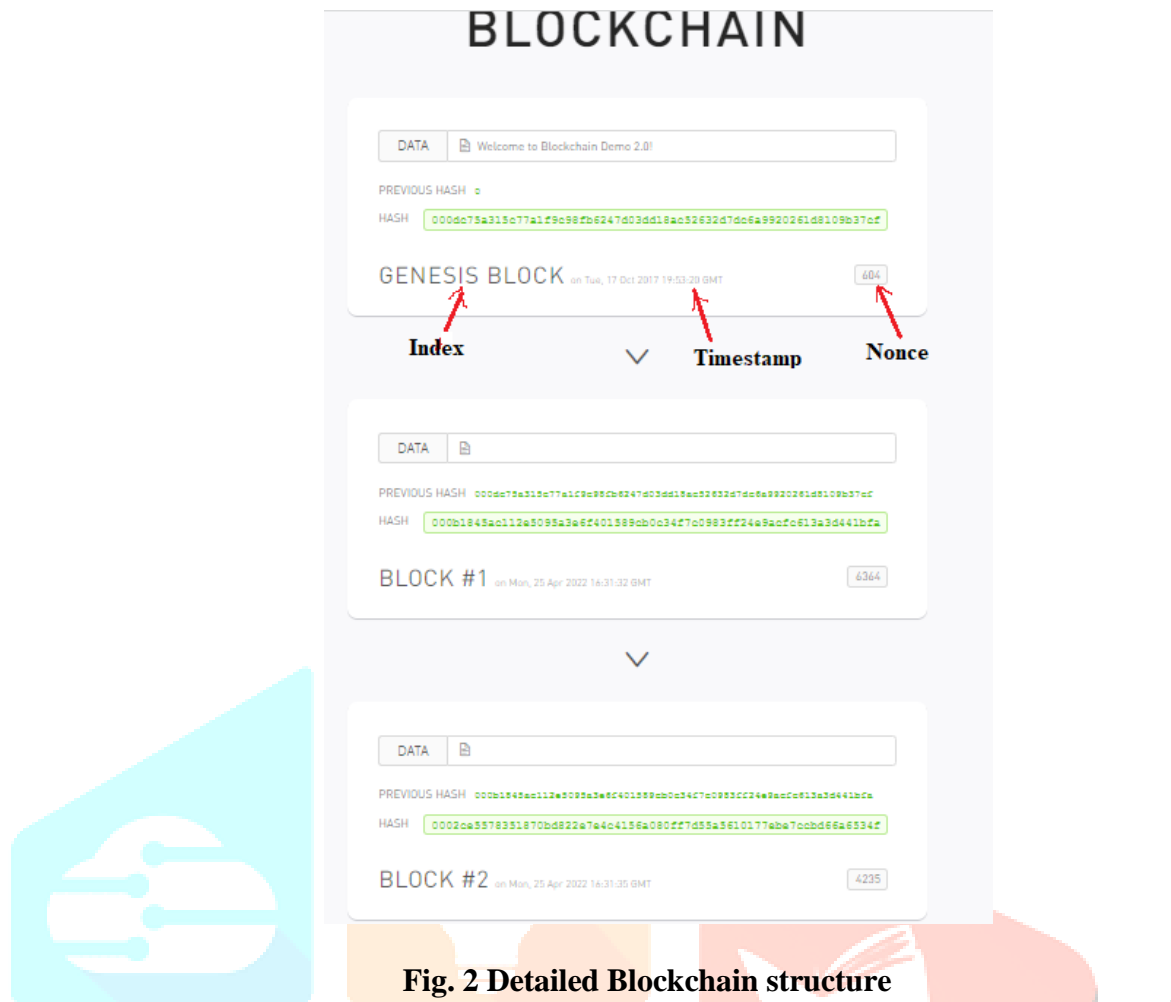


Fig. 2 Detailed Blockchain structure

Every transaction on the network is verified and enabled upon all the different nodes that are on the network. In the world of a Cryptocurrency, the first step in starting with Cryptocurrency is creating a wallet which is similar to an account. Wallet is something that you use to store Cryptocurrency. If you receive Cryptocurrency from someone, it is stored in the wallet, if you send Cryptocurrency to someone, it will be deducted from your wallet. Every wallet has an address which is similar to an account number. We can have multiple addresses to use for multiple purposes.

1) Mobile Wallets:

We can create a Mobile wallet on a smartphone with IOS, android, blackberries or windows. Download the app and transact in Cryptocurrency.

2) Desktop Wallets:

Operating systems like Windows, Mac, Linux, machines and start operating with Cryptocurrency.

3) Hardware Wallets:

Small Hardware system that is comparable with a valid series. There are other wallets that cost you money that is they are paid wallets. They are also called as Cold Storage of bitcoin and have the highest level of security that can be achieved while transacting a Cryptocurrency.

4) Web App Wallets:

Almost all Cryptocurrency wallet services provide you with a WebApp that we can use to store or send Cryptocurrency. Just need to create an account on the website and start using Cryptocurrency. Any number of Cryptocurrency wallets can be created and any number of addresses for different purposes. Each wallet is for different purposes. You can buy parts of Cryptocurrency, no need to buy whole Cryptocurrency. No one can reverse a Cryptocurrency transaction if you made a wrong transaction of money.

VI. Applications of Blockchain

After the enormous success of blockchain technology in Cryptocurrency, many programmers used blockchain in the business to improve cyber security as blockchain technology is smarter, simpler and more secure than the traditional client server system. Blockchain enables people to create a digital asset which can be transferred without any middleman unlike other systems. Blockchain is bigger than any cryptocurrencies and can be implemented on new applications. Apart from bitcoin, many other cryptocurrencies are coming to existence, like Altcoins, they differ from bitcoin since they have their own blockchain.

○ Bitcoin:

First cryptocurrency, biggest of all and has the highest market share.

○ Ethereum:

It is a Decentralized computer network that allows developers to build applications. The cryptocurrency that Ethereum uses is Ether.

○ Ripple:

It is a payment protocol which aims to support instant and cheap transactions. It is adopted by financial companies.

○ Smart Contracts:

Facilitate exchange of items of values on the internet without the need of a middleman and no escrow service. In service, blockchain acts as a bystander of the contract. When two parties are involved in a contract viz. a smart contract, the information that they both have provided turns into a block in the blockchain network. These blocks are visible to all the nodes on the network. Nonetheless, the identity and private information is anonymous. The technology of smart contracts led to the development of Ethereum. Ethereum is a decentralized, open source blockchain with smart contract functionality.

Vitalik Buterin, who works for bitcoin, created Ethereum. Then he got to know that the potential for blockchain technology is too large and he developed the platform for developers to just develop a blockchain instead of creating new ones.

VII. Defining the issue

As discussed, Blockchain and hence Cryptocurrencies are the future of Digital Transaction. As the blockchain technologies are non-fungible and more secure for transactions. The Problem exactly is that the transactions made are not as transparent as they should be. From the above all basics structure of blockchain technology let us discuss the problem that we want to find a solution of and the enhancement of blockchains in cryptocurrency.

The idea of this paper is to propose an idea for traceability of the transactions. Tracing a Cryptocurrency transaction is not impossible but a hectic procedure, although we get to know about the IP address from where the transaction happened and exact owner information is anonymous. As we know transactions are publicly recorded on blockchain, identifying users' information is not possible. During a transaction of cryptocurrency, the transaction made by which wallet to wallet is a mystery. And it does not give us the guarantee that we will be able to get detailed information about the transaction like from whom to whom the transaction happened. So, we basically proposed a Model to the legal authority that makes it traceable by first generating a verified and valid Wallet account detail which has traceable information about the owner and detail which is necessary for one to trace the transaction.

Let us understand the scenario step by step. Say, person A after mining into some blocks gets rewarded by cryptocurrency, so now he has a Wallet which has all of his cryptocurrency. There is now person B which does not have anything in his Wallet and now person A wants to transfer his one of the tokens from the Wallets. Initially person B has nothing in his wallet, now when the transfer happens it is untraceable as it has no information, just the authority of currency after transfer is from A to B.

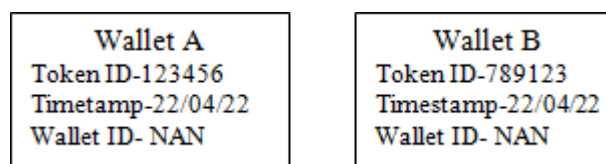


Fig.3 Block diagram with unlabeled information

But what if the mining community decides to take the detailed information, that is while creating or defining a block, the block itself embedded it in such a way that it becomes traceable and discoverable.

With the help of a reliable blockchain platform, we can customize these tokens for any asset which has more information about the sender and recipient.

Below is the chart which describes the characteristics of a detailed wallet token.

TABLE 1 ELEMENTS TO DEFINE A BLOCK

Sr. No.	Entities	Property
1)	Token ID	-Unique Id for a currency
2)	Data	-Detailed information about the transaction for a particular block
3)	Hash	-Unique string of characters generated for a block from the data defined
4)	Time Stamp	-Time when miner generates a Token
5)	Updated timestamp	-Time when Token is transferred to another person
6)	Wallet ID	-Unique Id for transaction -For miners it's NAN -After the transfer it's from the one who transferred it

Now, suppose we use traceable token/ wallet details. So, when transfer from person A to person B happens we get to know about every detail of the transaction that it is from person A to person B.

Wallet A	Wallet B
Token ID-123456 Timestamp-22/04/22 Wallet ID- NAN	Token ID-789123 Updated Timestamp-23/04/22 Time stamp-22/04/22 Wallet ID- Wallet A

Fig. 4 Block diagram with labeled information from Table 1

So, now because of the definition of wallet Token, it is now possible privately to trace the transaction. As knowledge of blockchain technology is still vague, there are misconceptions about blockchain technology and the cryptocurrencies. With the help of the above defined block (from fig.4) or token we can understand the transaction from the below figure.

Generating customized tokens requires technical computer knowledge. So, herein we just have an idea which helps government and legal authorities to track fraudulent activities that may have happened in the transactions.

Also, sometimes it may be, by mistake if anyone does the wrong transaction, and because of the nature and structure of blockchain technology it is not possible to reverse it.

Lack of developers is also one of the limitations of blockchain technology due to which legality of cryptocurrency is still an issue. As blockchain technology is tamper proof which makes transaction secure and cryptocurrencies like Bitcoin, Ethereum successful. Time for the process is also a huge constraint for blockchain technology. The miners find the nonce number and other miners validate the block, the process of validating the data on the blocks will be time consuming when there are numerous blocks.

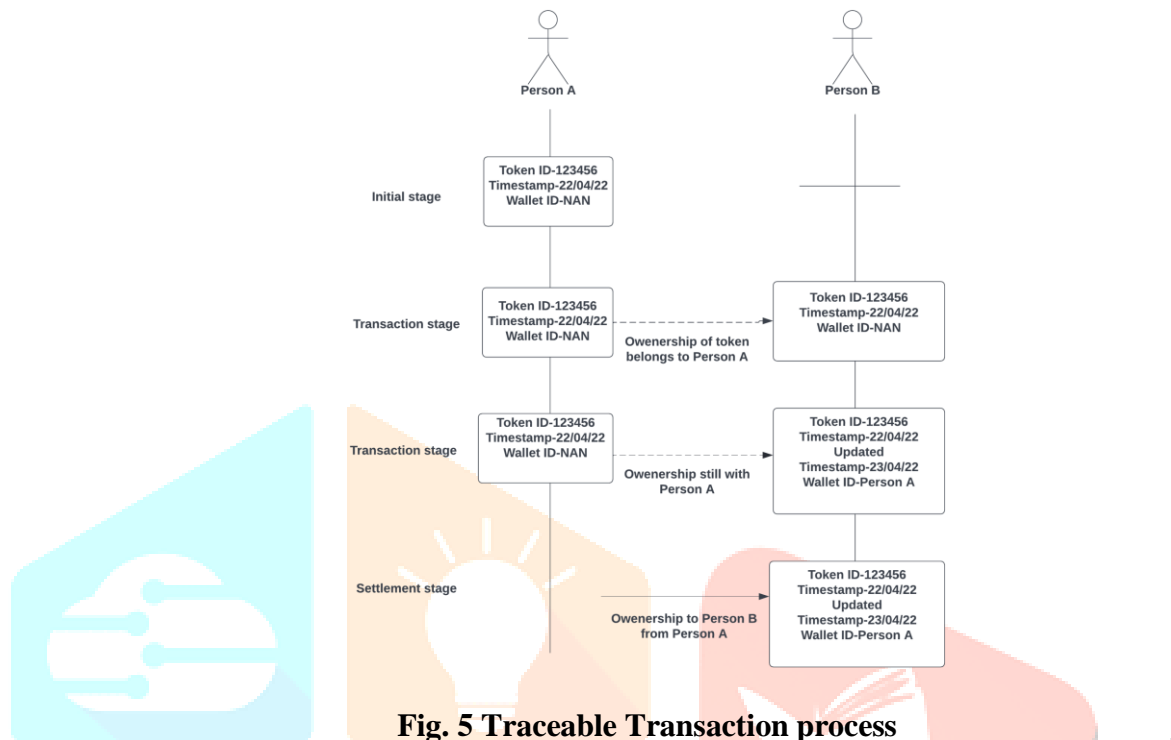


Fig. 5 Traceable Transaction process

VIII. CONCLUSIONS

Blockchain is a super growing technology and it will be moving ahead so fast. It is revolutionary in the finance industry through the implementation of Cryptocurrency, in Medical fields, in Telecommunication, in Retail, etc. As discussed in the paper Blockchains are made up of blocks which contain data and are linked together and Hash functions are used to encrypt these blocks. Theoretically it is possible to design such a block or wallet ID which are traceable, that is we can theoretically create blockchains that aren't anonymous which would be considered as private chains and would lead to more transparency, which can make cryptocurrency authorized and legal.

ACKNOWLEDGMENT

It gives me great pleasure and satisfaction in presenting this work on "Futuristic Enhancement in Cryptocurrency".

We are thankful to and fortunate enough to get constant encouragement, support and guidance from **Dr. Ranjit Patil**, which helped us in successfully completing our work. We would like to extend our sincere thanks to librarian **Dr. Babasaheb Shingade** for his timely support.

We would like to thank all those who have directly or indirectly helped for the completion of this paper.

Conflict of Interest Statement

The authors have no conflicts of interest to declare. All co-authors have seen and agree with the contents of the manuscript and there is no financial interest to report. We certify that the submission is original work and is not under review at any other publication.

REFERENCES

- [1] A. Reddy, A Beginner's Guide to Authentic Knowledge on Blockchain Technology and its Applications in 2018, [Online] Available
: <https://www.udemy.com/share/101uFY3@MDwnwUhj2CI0VNdWYhZ4mTXGD9oHRgAiksPcMOZtAyA9NXUDz3LQ0K1w71EAo5VcQ==/>
- [2] A. Hayes, “How to buy a Bitcoin, Strategy and Precautions” [Online] Available: <https://www.investopedia.com/articles/investing/082914/basics-buying-and-investing-bitcoin.asp>
- [3] “Difference between Blockchain Technology and Bitcoin”, [Online] Available: <https://www.euromoney.com/learning/blockchain-explained/the-difference-between-blockchain-and-bitcoin>
- [4] V. Buterin, “On public and private blockchains,” 2015. [Online]. Available: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>
- [5] “Bitshares - your share in the decentralized exchange.” [Online]. Available: <https://bitshares.org/>
- [6] “Structure of a blockchain” [Online] Available <https://blockchaindemo.io/>
- [7] “SHA256 Hash Generator” [Online] Available: <https://xorbin.com/tools/sha256-hash-calculator>
- [8] “Blockchain Basics” [Online] Available: <https://en.wikipedia.org/wiki/Blockchain>.

