EXPLORING THE BLOCKCHAIN

Ms. Jalashree D. Trivedi[1], Prof. Karishma A. Chaudhary[2], Prof. Tushar.J Raval[3]

[1] Student ,Computer Engineering Department, L.D College of Engineering,Ahmedabad, Gujarat, India
[2] Professor, Computer Engineering Department, L.D College of Engineering,Ahmedabad, Gujarat, India
[3] Professor, Computer Engineering Department, L.D College of Engineering,Ahmedabad, Gujarat, India

ABSTRACT

A blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. Once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. Bitcoin, the decentralized peer-to-peer digital currency, is the most popular example that uses blockchain technology. The digital currency bitcoin itself is highly controversial but the underlying blockchain technology has worked flawlessly and found wide range of applications in both financial and non-financial world.

The main hypothesis is that the blockchain establishes a system of creating a distributed consensus in the digital online world. This allows participating entities to know for certain that a digital event happened by creating an irrefutable record in a public ledger. It opens the door for developing a democratic open and scalable digital economy from a centralized one. There are tremendous opportunities in this disruptive technology, and the revolution in this space has just begun.

This paper describes blockchain technology and some compelling specific applications in both financial and non-financial sector. We then look at the challenges ahead and business opportunities in this fundamental technology that is all set to revolutionize our digital world.

Keyword : - *Bitcoin , Blockchain*

1. Introduction

A blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. Once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. To use a basic analogy, it is easier to steal a cookie from a cookie jar, kept in a secluded place, than stealing the cookie from a cookie jar kept in a market place, being observed by thousands of people.

Bitcoin is the most popular example that is intrinsically tied to blockchain technology. It is also the most controversial one since it helps to enable a multibillion-dollar global market of anonymous transactions without any governmental control. Hence it has to deal with a number of regulatory issues involving national governments and financial institutions.

However, Blockchain technology itself is non-controversial and has worked flawlessly over the years and is being successfully applied to both financial and non-financial world applications. Last year, Marc Andreessen, the doyen of Silicon Valley's capitalists, listed the blockchain distributed consensus model as the most important invention since the Internet itself. Johann Palychata from BNP Paribas wrote in the Quintessence magazine that bitcoin's blockchain, the software that allows the digital currency to function should be considered as an invention like the steam or combustion engine that has the potential to transform the world of finance and beyond [1].

Current digital economy is based on the reliance on a certain trusted authority. All online transactions rely on trusting someone to tell us the truth— it can be an email service provider telling us that our email has been delivered; it can be a certification authority telling us that a certain digital certificate is trustworthy; or it can be a social network such as Facebook telling us that our posts regarding our life events have been shared only with our friends or it can be a bank telling us that our money has been delivered reliably to our dear ones in a remote country. The fact is that we live our life precariously in the digital world by relying on a third entity for the security and privacy of our digital assets. The fact remains that these third party sources can be hacked, manipulated or compromised.

This is where the blockchain technology comes handy. It has the potential to revolutionize the digital world by enabling a distributed consensus where each and every online transaction involving digital assets, past and present, can be verified at any time in the future. It does this without compromising the privacy of the digital assets and parties involved. The distributed consensus and anonymity are two important characteristics of blockchain technology.

The advantages of Blockchain technology outweigh the regulatory issues and technical challenges. One key emerging use case of blockchain technology involves "smart contracts". Smart contracts are basically computer programs that can automatically execute the terms of a contract. When a preconfigured condition in a smart contract among participating entities is met then the parties involved in a contractual agreement can be automatically made payments as per the contract in a transparent manner.

Smart Property is another related concept which is regarding controlling the ownership of a property or asset via blockchain using Smart Contracts. The property can be physical such as car, house or smartphone, or it can be non-physical such as shares of a company. It should be noted here that even Bitcoin is not really a currency: Bitcoin is all about controlling the ownership of money.

Blockchain technology is finding applications in wide range of areas; both financial and non-financial.

Financial institutions and banks no longer see blockchain technology as a threat to traditional business models. The world's biggest banks are in fact looking for opportunities in this area by doing research on innovative blockchain applications. In a recent interview Rain Lohmus of Estonia's LHV bank told that they found Blockchain to be the most tested and secure for some banking and finance related applications.

Non-Financial applications opportunities are also endless. We can envision putting proof of existence of all legal documents, health records, and loyalty payments in the music industry, notary, private securities and marriage licenses in the blockchain. By storing the fingerprint of the digital asset instead of storing the digital asset itself, the anonymity or privacy objective can be achieved.

1.1 Literature Survey

Blockchain attempts to solve one of the major problems- money transfers. Today, let's say, a say a person A wants to transfer money to person B maybe from India to Japan. This is typically done using a third trusted party in the following way (1) person A tells the third party to send money to person B. (2) this intermediate third party identifies the person B along with his bank account details (3) then it transfers the money after taking some fee. This typically takes some time.

Whereas, a blockchain enables (1) transaction of money without the trusted third entity; (2) complete the transfer immediately and (3) with much cheaper cost without actually paying the fee. [6]

A. Satoshi Nakamoto (2007)

According to a legend, Satoshi Nakamoto began working on the Bitcoin concept in the year 2007. While he is on record as living in Japan, it is speculated that Nakamoto may be a collective pseudonym for more than one person.

B. A patent application(August 15, 2008)

Neal Kin, Vladimir Oksman, and Charles Bry file an application for an encryption patent application. All three individuals deny a connection to Satoshi Nakamoto, the alleged originator of the Bitcoin concept

C. Bitcoin.org is registered (August 18, 2008)

Bitcoin.org was born. The domain was registered at anonymousspeech.com. It is a site that allows users to anonymously register domain names and it accepts bitcoins.[5]

D. The white paper is published (October 31, 2008)

Nakamoto publishes a design paper through a metzdowd.com cryptography mailing list that describes the Bitcoin currency and solves the problem of double spending so as to prevent the currency from being copied.

E. The Bitcoin Project hits SourceForge (November 9, 2008)

The Bitcoin project is registered on SourceForge.net, a community collaboration website focused on the development and distribution of open source software. [5]

F. The Genesis Block is mined (January 3, 2009)

Block 0, the genesis block, is established at 18:15:05 GMT.

G. Version 0.1 is released (January 9, 2009)

Version 0.1 of Bitcoin is released. It is compiled with Microsoft Visual Studio for Windows. It includes a Bitcoin generation system.

H. The first Bitcoin transaction (January 12, 2009)

The first transaction of Bitcoin currency, in block 170, took place between Satoshi and Hal Finney, a developer and cryptographic activist.

The popularity of the Bitcoin has never stopped to advance since then. The fundamental blockchain technology inspiring that is now finding new range of applications beyond finance.[7]

2. ARCHITECTURE

Blockchain Architecture Considerations: A few important design aspects that need to be discussed while examining blockchain architecture are –

1) The Blockchain platform.

2) The role of nodes in consisting the overall blockchain & the node discovery process.

3) Transactions that make up the blocks running in the Nodes.

4) Security implementation that generates the Blocks.

5) The process of adding newer blocks to the Chain.

The below architecture diagram Figure 1 broadly captures the 3 main layers of the Blockchain along with their roles.

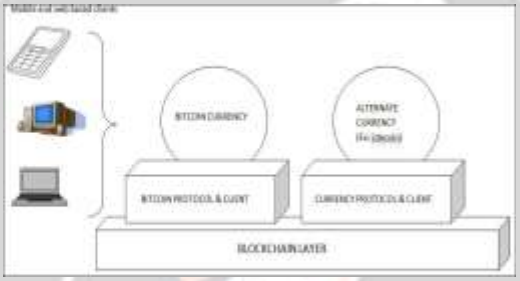
Mobile and web based clients
BITCOIN CURRENCY
ALTERNATE CURRENCY
BITCOIN PROTOCOL & CLIENT
CURRENCY PROTOCOL & CLIENT
BLOCKCHAIN LAYER

Fig -1:Layers of Blockchain Architecture

The blockchain layer provides shared ledger that store "chains of blocks". It stores all processed transactions in a chronological order. Bitcoin supports much type of clients: mobile, full and web depending on the client's needs to store bitcoin transactions. The blockchain is the global decentralized ledger which is overall technology platform. The blockchain is shared by all nodes and is updated by the miners. The blockchain maintains an ordered and time stamped ledger of all transactions. Cryptography ensures the constant integrity of the blockchain.

The currency layer provides the particular currency's peer to peer protocol along with the consensus rules and APIs that describes the semantics of the currency to the blockchain layer.

The blockchain explorer and the other tools provide a way to explore the contents of different blocks and to query & search them.

A. Blockchain Platform:

The Blockchain runs on a network of distributed servers. The core application of this platform is a transaction database modelled as a secure ledger that is shared by all nodes (servers) that run the full stack install.

While the Blockchain client uses Google's Level DB database to store metadata internally – the Blockchain data can be stored in a flat file or in a relational DB depending on user preferences.

B. Nodes in the Blockchain:

Blockchain is a peer to peer (P2P) network working on the IP protocol on the internet. [2] The nodes in the blockchain play the role of a Central Bank or a trusted third party. Every node maintains a fully replicated copy of a database that contains the payment history of every bitcoin ever created along with ownership information. As transactions happen using the currency, a mechanism essentially dictates how nodes agree on blockchain updates.Thus, there are 4 basic node types. It is to be noted that all of the node types discover and maintain connections with peers & also validate blocks.

Full nodes maintain a complete copy of the blockchain database and can verify any transaction without the need for an external lookup. Nodes that only store a subset of the blockchain database verify transactions using a method called Simplified Payment Verification (SPV).

Nodes of type Miners perform the core process by which transactions are confirmed & processed and eventually included in the blockchain. To be confirmed as valid, transactions are first packed in a data structure & format called a Block that has to satisfy strong cryptographic rules that are verified by the blockchain network. For applications like bitcoin, rollbacks currently are almost impossible in the vanilla blockchain architecture – which is a current limitation.

The miner node concept is unique to blockchain as it confers it a high level of security. An organized group of minor nodes create a block chain layer.

C. Network Protocol Stack:

Once nodes are booted up, they perform a peer discovery to contact any other valid node using a given port over TCP. The Blockchain Message Exchange specifies the handshake logic between nodes as well as the serialization format for messages exchanged over the wire.

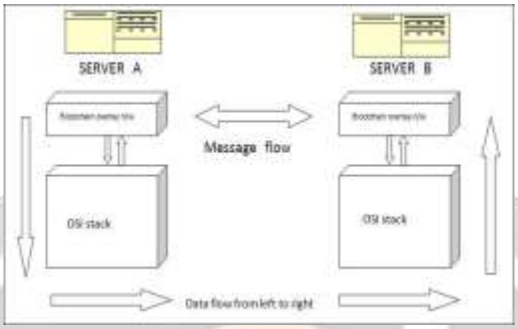

Fig. 2: Blockchain Network architecture

D. Transactions and Blocks:

Applications, the first among them being Bitcoin use blockchain to timestamp transactions. The blockchain implementation consists of two kinds of records: transactions and blocks.

Some features of transactions are –

1) Transactions can be created on the behalf of any client using a Mobile Wallet or any other client application

2) Transactions contain the actual business data to be stored in the blockchain

3) Blocks record the sequence of transactions in the blockchain. Transactions are journaled into the blockchain based on specific sequences

4) Miner nodes create blocks as discussed in the above section

2.1 Working of Blockchain

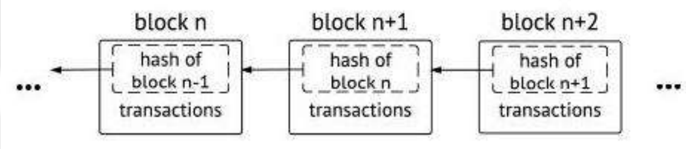

Fig. 3: Blocks in a transaction of a blockchain network

Each block shown in the above Figure 3 in the chain carries a list of a transactions and a hash to the previous block. The exception to this is the first block of the chain (not pictured), called genesis, which is common to all clients in a blockchain network and has no parent.[1]

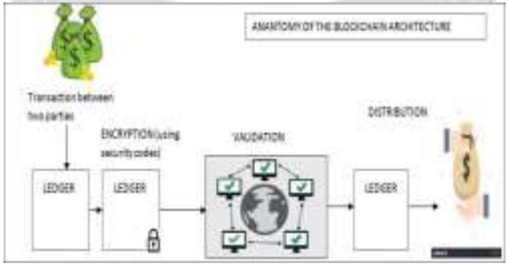
ANATOMY OF THE BLOCKCHAIN ARCHITECTURE
Transaction between two parties
ENCRYPTION(using security codes)
VALIDATION
DISTRIBUTION
LEDGER
LEDGER
LEDGER

Fig. 4: Working of BlockChain

The above Figure 4 shows the working of a blockchain. The transaction between two parties is added to an online transaction ledger encrypted with digital security code. The code of the transaction is sent to a large network where the authenticity of the code is confirmed without compromising private information and eliminating the need for a central authority for a central authority for confirming transactions. Once a transaction is confirmed and validated

by several parties, it exists on the ledger of each as a permanent and immutable record of the transaction. The transaction information is recorded in a public ledger and the transaction is completed. [2]
Example of a blockchain transaction: Person A wants to send money to Person B. The transaction is represented as a block online; this block will be broadcast over a network so that everybody in the network can validate the block. Once the approval is received from the network, (the parties present in the network) that the transaction being made is considered as a valid transaction, the transaction or the block is then added to the chain that is present which provides transparency in the whole process, also the money moves from Person A to Person B.[2][5]

2.2 Applications

A. Financial Applications:
1) Private Securities
It is very expensive to take a company public. A syndicate of banks must work to underwrite the deal and attract investors. The stock exchanges list company shares for secondary market to function securely with trades settling and clearing in a timely manner. Companies can directly issue the shares via the blockchain. These shares can then be purchased and sold in a secondary market that sits on top of the blockchain.[1]
2) Insurance
Assets like insurance which can be uniquely identified by one or more identifiers and that are difficult to destroy or replicate can be registered in blockchain. This can be used to verify ownership of an asset and also trace the transaction history. [5]
B. Non-Financial Applications:
1) Notary Public
Verifying authenticity of the document can be done using blockchain and eliminates the need for centralized authority. The document certification service helps in Proof of Ownership (who authored it), Proof of Existence (at a certain time) and Proof of Integrity (not tampered) of the documents. Using blockchain for notarization secures the privacy of the document and those who seek certification. It also eliminates the need for expensive notarization fees and ineffective ways of transferring documents.[5]
Stampery is a company which can stamp email or any files using blockchain. It simplifies certifying of emails by just emailing them to an email specifically created for each customer.
Viacoin is the one of the companies which uses clearinghouse protocol for notary service.
Block Notary is an iOS app which helps you to create proof of existence of any content (photo, files, any media) using Bitcoin network.
2) Applications of Blockchain in the Music Industry
The demand of transparency in the payment of artists and songwriters is where the blockchain can play a role by maintaining a consistent, accurate distributed database of music rights ownership information in a public ledger. [2][5]
3) Decentralized proof of existence of documents
Validating the existence or the possession of signed documents is very important in any legal solution. The blockchain technology provides an alternative model to proof-of-existence and possession of legal documents. By leveraging the blockchain, a user can simply store the signature and timestamp associated with a legal document in the blockchain and validate it anytime using native blockchain mechanisms.
4) Decentralized Storage
Cloud file storage solutions typically face challenges in areas such as security, privacy and data control. The major issue is that one has to trust a third party with one’s confidential files.
Storj provides a blockchain based distributed cloud storage platform that allows users to transfer and share data without relying on a third-party data provider. This allows people to share unused internet bandwidth and spare disk space in their personal computing devices to those looking to store large files in return for bitcoin based micropayments.[5]

3. FUTURE SCOPE

The blockchain is radically changing the future of transaction based industries. Some of them are shown in the Figure 5 below.

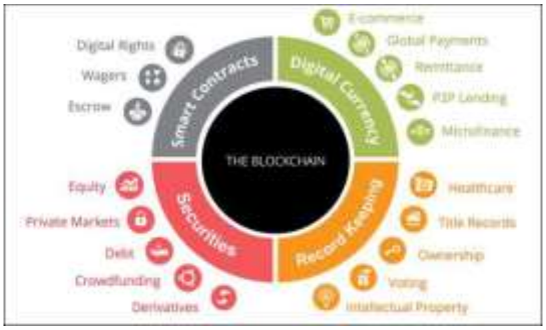

Fig. : Blockchain potential applications

The future of monetary support for organizations could be dominated by blockchain technologies. A traceable global currency complete along an efficient infrastructure will result in massive cost reduction for all market participants, along with it will change global banking. Bitcoin will do a tremendous change for payments similar to what email did for communication.

A. Control

New innovative technologies such as blockchain have the ability to diminish cyber risks by offering personality identification or authentication through a visible ledger. Automobile rental agencies could utilize smart contracts that automatically allow rentals when payments are received and insurance data is affirmed through a blockchain record. A cooler fitted with sensors and connected to the Internet could utilize blockchain to oversee automated communications with the external world-anything from ordering and paying for food to arranging for its own software upgrades and tracking its warranty. Small scale independent organizations could use blockchain for creating trusted trading platforms among themselves. Blockchain could conceivably assist to bring robustness and transparency to the trade environment. Example: A bank could pay the supplier instantly over the Internet.

B. Banks.

Blockchain will be embraced by centralized banks and cryptographically secured monetary forms will become widely used. Blockchain technology could be used to bypass today's centralized financial infrastructure completely. It could replace nationalized central banks though genuine risks remain for banks that choose to get involved with cryptographic currency firms.

Blockchain technology could reduce investments on infrastructure costs in cross-border payments, securities trading and administrative consistence. The quantity of applications inside and outside the banks could be reduced as the Blockchain transaction contains all relevant information for the successful transfer of assets and additionally related contracts.

C. Industries

Time and education will need to assume a part as other organizations are just realizing one of the core innovations of the blockchain is its ability to reduce or eliminate trusted parties in the transaction procedure. Blockchain can possibly make new industry openings and disturb existing advances and processes.

D. Governments

The future of finance in numerous nations could be dominated by Bitcoin and cryptographic forms of money. Blockchain technology could be utilized to distribute appropriate social welfare in developing nations. Example: Elections are nowadays an expensive and tedious. Because of blockchain tech they will soon be quick.

3.1 Risks of adoption

1) A technology beginning to display signs of future potential: Resolving challenges such as transaction speed, the verification process, and data limits will be crucial in making blockchain widely applicable.

2) Uncertain regulatory status: Even though modern currencies have always been created and regulated by national governments, blockchain and Bitcoin face a huge burden in widespread adoption by pre-existing financial institutions.[5]

3) Large energy consumption: Scaling of the current enormous services based on Blockchain faces a challenge.

4) Control, security, and privacy: While many solutions exist for enabling private blockchains with strong encryption, there are still huge cyber security concerns that need to be efficiently solved.

5) Integration concerns: Moving the existing contracts or business documents/frameworks to the new Blockchain based methodology presents a significant set of migration tasks that need to be executed.[1][2]

6) Cultural adoption: Blockchain represents a complete shift to a decentralized network which requires the buy-in of its users and operators. [2][5]
7) Cost: Blockchain offers huge savings in transaction costs and time but the high initial capital costs could be a discouragement for investment.[2]

4. CONCLUSIONS

Blockchain technology is almost significant to the development of the internet. If the internet brought us near instance digital communication, blockchain technology brings us near end digital asset transfer and security of data movement.

Blockchain technology has attracted interest of various industries from finance and health care to utilities, real estate and government sector. The blockchain empowers trustless networks, on the grounds that the parties can transact despite the fact that they don't believe each other. The absence of the third party enables speedier compromise in the transactions. Blockchain main characteristic is the high use of cryptography, which brings legitimacy in all the interactions in the network.

Smart contracts self-executing scripts that live on the blockchain incorporate these ideas and take into account appropriate, distributed, vigorously automated work processes. By permitting computerized data to be dispersed yet not replicated, blockchain technology made the foundation of another kind of web.

Blockchain is the technology backbone of Bitcoin. [2][5] It is called "digital gold," like the internet, you don't have to know how the blockchain works to utilize it. In any case, having a basic view of this new technology indicates why it's viewed as progressive.

5. REFERENCES

[1]. Konstantinos Christidis and Michael Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things” in SPECIAL SECTION ON THE PLETHORA OF RESEARCH IN INTERNET OF THINGS (iot), June 3, 2016.
[2]. Sanjana Panicker, Vaishnavi Patil Divya Kulkarni, “An Overview of Blockchain Architecture and it’s Applications “,International Journal of Innovative Research in Science, Engineering and Technology Vol. 5, Issue 11, November 2016
[3]. "A Gentle Introduction to Blockchain Technology". Bits on blocks. N.p., 2016. Web. 30 Oct. 2016.
[4]. Hassell, Jonathan. "What Is Blockchain And How Does It Work?". CIO. N.p., 2016. Web. 12 Nov. 2016.
[5]. Michael Crosby, Google Nachiappan, Yahoo Pradhan Pattanayak, Yahoo Sanjeev Verma, Samsung Research America Vignesh Kalyanaraman, Fairchild Semiconductor, “BlockChain Technology Beyond Bitcoin”, Sutardja Center for Entrepreneurship & Technology Technical Report, October 16, 2015
[6]. https://en.bitcoin.it/wiki/History
[7]. Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf
[8]. https://en.wikipedia.org/wiki/Blockchain