International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 5, July-August 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Expanding Beyond Cryptocurrency in the Digital World using Blockchain Technology

Anirvan Vinod

Anna University, Information Technology, Saranathan College of Engineering, Tiruchirappalli, Tamil Nadu, India

ABSTRACT

A blockchain is principally a distributed database of records or public ledger of all transactions or digital events that are executed and shared among the participating parties. Once entered, information can never be erased. The blockchain encompasses a precise and supportable record of each solo transaction ever made in the history of all the transactions. Bitcoin, the decentralized digital currency, is that the most well-liked example that uses blockchain technology. The digital currency bitcoin itself is extremely controversial but the underlying blockchain technology has worked flawlessly and located a good range of applications in both the financial and nonfinancial world.

KEYWORDS: *Blockchain, Bitcoins, Peers, Decentralized, Transactions, Cryptocurrencies*

How to cite this paper: Anirvan Vinod "Expanding Beyond Cryptocurrency in the Digital World using Blockchain Technology" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-5, August 2021, pp.624-629, URL: www.ijtsrd.com/papers/ijtsrd43871.pdf

IJTSRD43871

I. INTRODUCTION

The key premise of blockchain technology is that the blockchain launches the system of fashioning a distributed accord in the digital online world. This permits the contribution of entities to know for certain that a digital event happened by creating an irrefutable record in a public ledger. 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. Bitcoin works on eliminating the middle man concept of having bank control and view the transactions which are being made throughout the world. Once the middle man is eliminated transactions become more secure and confidential. Nevertheless, blockchain technology itself is non-controversial and has worked impeccably, and is being positively applied to both financial and non-financial world claims and applications. Last year, Marc Andreessen, the doyen of Silicon Valley's capitalists, listed the blockchain distributed consensus models as the most important invention since the Internet itself. The bitcoin's blockchain, the software that permits the digital currency to execute should be measured as a development that has the potential to transform the world of finance and beyond. 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 sad fact is that third-party foundations can be extremely compromised. This is where blockchain technology comes in handy. It has the potential to revolutionize the digital world by enabling a distributed consensus where each and every online transaction, past and present, involving digital assets can be verified at any time in the future. This technology has the power to do this without negotiating the concealment of the digital assets and the various different parties involved. The distributed accord and anonymity are the key factors involved with the blockchain technology.

A brief history of bitcoins - 1998 – 2009

Although it was an established cryptocurrency, there had been previous attempts at creating online currencies with ledgers secured by encryption. Two

examples of these were B-Money and Bit Gold, which were formulated but never fully developed.

2008 – Satoshi Nakamoto, the Mystery Man

A paper called Bitcoin – A Peer to Peer Electronic Cash System was posted to a mailing list discussion on cryptography. It was posted by someone calling themselves Satoshi Nakamoto, whose real identity remains a mystery to this day.

2009 – Bitcoin begins

The Bitcoin software is made available to the public for the first time and mining – the process through which new Bitcoins are created and transactions are recorded and verified on the blockchain – begins.

The popularity of the Bitcoin has never ceased to increase since then. The underlying Blockchain technology is now finding new range of applications beyond finance.

II. METHODOLOGY

HOW DOES BLOCKCHAIN WORK?

Internet commerce is exclusively tied to the financial institutions serving as the trusted third party who process and mediate any electronic transaction. The role of trusted third party is to validate, safeguard and preserve transactions. A certain percentage of fraud is unavoidable in online transactions and that needs mediation by financial transactions. This results in high transaction costs. Bitcoin uses cryptographic proof instead of the trust in the third party for two willing parties to execute an online transaction over the Internet. Each transaction is protected through a digital signature. Each transaction is sent to the "public key" of the receiver digitally signed using the "private key" of the sender. In order to spend money, owner of the cryptocurrency needs to prove the ownership of the "private key". The entity receiving the digital currency verifies the digital signature.

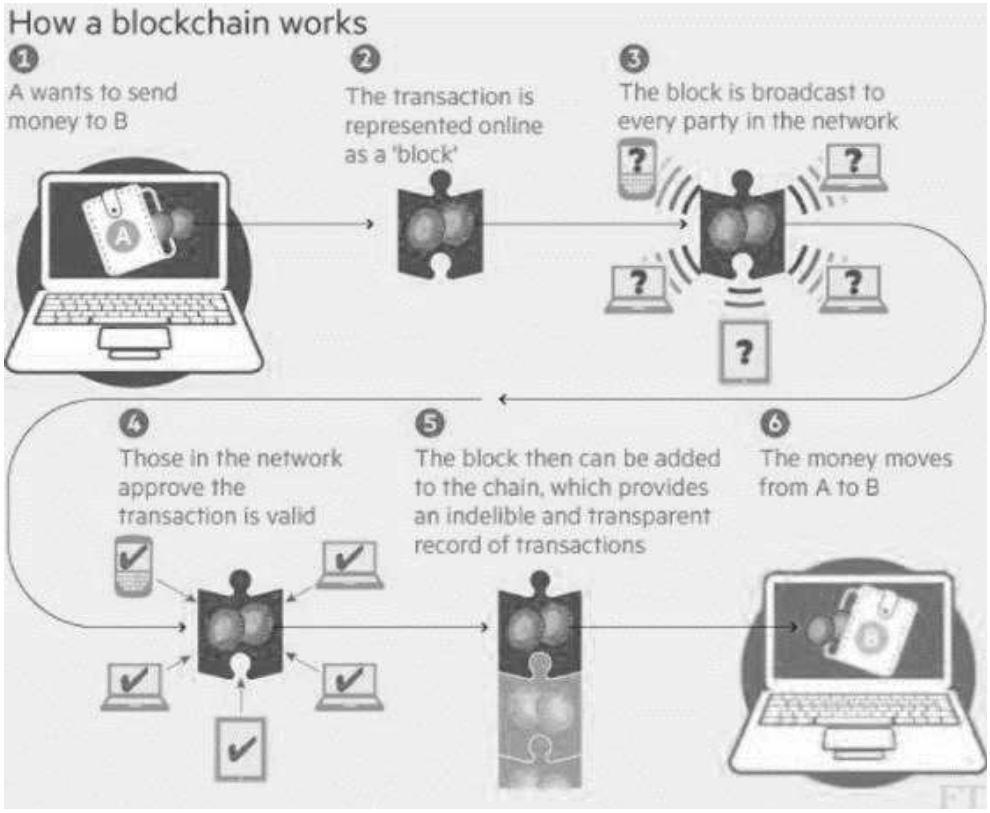

Figure 1: Working of a blockchain.

Thus, the ownership of corresponding "private key" on the transaction using the "public key" of the sender. Each transaction is broadcast to every node in the Bitcoin network and is then recorded in a public ledger after verification.

Every single transaction needs to be verified for validity before it is recorded in the public ledger. Verifying node needs to ensure two things before recording any transaction:

1. Spender owns the cryptocurrency—digital signature verification on the transaction.
2. Spender has sufficient cryptocurrency in his/her account: checking every transaction against spender's account ("public key") in the ledger to make sure that he/she has sufficient balance in his/her account.

THE CURRENT SCENARIO

Blockchain technology is finding applications in both financial and non-financial areas that traditionally relied on a third trusted online entity to validate and safeguard online transactions of digital assets. There was another application "Smart Contracts" that was invented in year 1994 by Nick Szabo. It was a great idea to automatically

execute contracts between participating parties. However, it did not find usage until the notion of crypto currencies or programmable payments came into existence. Now two programs blockchain and smart contract can work together to trigger payments when a preprogrammed condition of a contractual agreement is triggered. Smart Contracts are really the killer application of the cryptocurrency world. Smart contracts are contracts which are automatically enforced by computer protocols. Using blockchain technology it has become much easier to register, verify and execute Smart Contracts. Open-source companies like Ethereum and Codius are enabling Smart Contracts using blockchain technology. Many companies which operate on bitcoin and blockchain technologies are supporting Smart Contracts. Many cases where assets are transferred only on meeting certain conditions which require Lawyers to create a contract and Banks to provide Escrow service can be replaced by Smart Contracts. Ethereum has created lot of excitement for its programmable platform capabilities. Ethereum allows anyone to create their own cryptocurrency and use that to execute, pay for smart contracts. Ethereum itself has its own cryptocurrency (ether) which is used to pay for the services. Ethereum is already powering wide range of early applications in areas such as Governance, autonomous banks, keyless access, crowdfunding, financial derivatives trading and settlement using smart contracts. Also, there are a number of blockchains in existence to support wide range of applications - not just cryptocurrency. Currently there are three approaches in Industry to support other applications and also to overcome perceived limitations of Bitcoin blockchain: Alternative Blockchains is a system of using the blockchain algorithm to achieve distributed consensus on a particular digital asset. They may share miners with a parent network such as Bitcoin's- this is called merged mining. They have been suggested to implement applications such as DNS, SSL certification authority, file storage and voting. Colored Coins is an open-source protocol that describes class of methods for developers to create digital assets on top of Bitcoin blockchain by using its functionalities beyond digital currency. Sidechains are alternative blockchains which are backed by Bitcoins via Bitcoin contract- just as dollars and pounds used to be backed by Gold. One can possibly have a thousand of sidechains "pegged" to Bitcoin, all with different characteristics and purposes- all of them taking advantage of scarcity and resilience guaranteed by the Bitcoin blockchain. The Bitcoin blockchain can in turn iterate to support additional features for the experimental sidechains - once they have been tried and tested. Companies such as IBM, Samsung, Overstock, Amazon, UBS, Citi, Ebay, Verizon Wireless to name a few are all exploring alternative and novel uses of the blockchain for their own applications. Nine of the world's biggest banks including Barclays and Goldman Sachs have recently (Sept. 5 15, 2015) joined forces with the New York based financial technology firm R3 to create a framework for using the blockchain technology in the financial market. This is the first-time banks have come to work together to find applications of blockchain technology. Banks like JPMorgan, State Street, UBS, Royal Bank of Scotland, Credit Suisse, BBVA and Commonwealth Bank of Australia have joined this initiative.

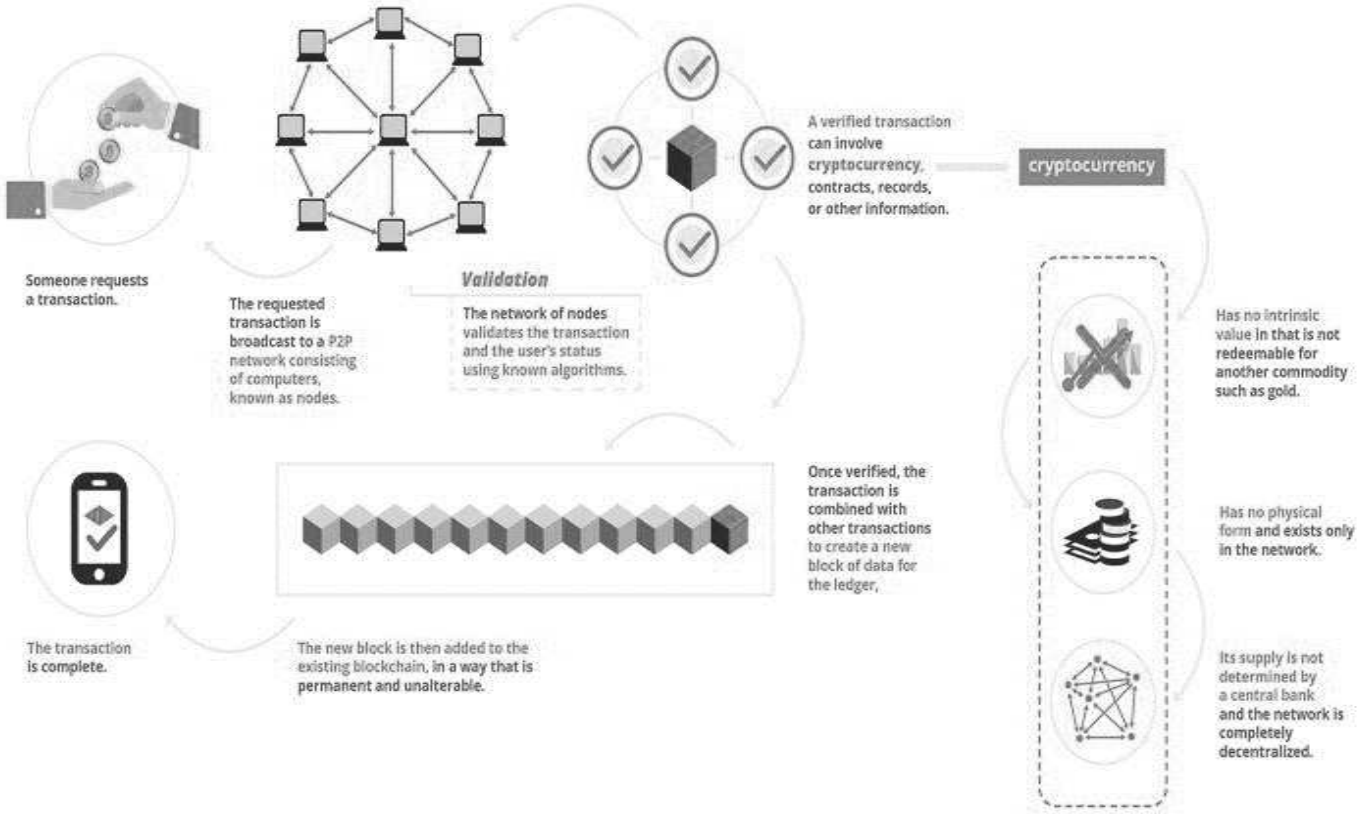

Figure 2: Validation Process

III. MODELING AND ANALYSIS APPLICATIONS OF BLOCKCHAIN IN BOTH FINANCIAL AND NON-FINANCIAL MARKETS

FINANCIAL APPLICATIONS

PRIVATE SECTOR 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. It is now theoretically possible for companies to 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. A few examples are:

NASDAQ launched its Private Equity Exchange in 2014. This is meant to provide the key functionalities like Cap table and investor relationship management for the pre-IPO or private companies. The current process of trading stocks in this exchange is inefficient and slow due to involvement of multiple 3rd parties. NASDAQ has joined hands with a San Francisco based Start-up called chain.com to implement private equity exchange on top of Blockchain. Chain.com is implementing Blockchain based smart contracts to implement exchange functionality. This product is expected to be fast, traceable and efficient.

Medici is being developed as a securities exchange that uses the Counterparty implementations of Bitcoin 2.0. The goal here is to create a cutting-edge stock market. Counterparty is a protocol that implements traditional financial instruments as the self-executing smart contracts. These smart contracts facilitate, verify or enforce the negotiation of contract and eliminate the need for a physical document. This eliminates the need for an intermediary, such as broker, exchange or bank.

Blockstream is an open-source project with focus on sidechains- interoperable blockchains- to avoid fragmentation, security and other issues related to alternative crypto-currencies. Uses can range from registering securities, such as stocks, bonds and derivatives, to securing bank balances and mortgages.

INSURANCE

Everledger is a company which creates permanent ledger of diamond certification and the transaction history of the diamond using blockchain. The characteristics which uniquely identify the diamond such as height, width, weight, depth, color etc. are hashed and registered in the ledger. The verification of diamonds can be done by insurance companies, law enforcement agencies, owners and claimants. Everledger provides a simple to use web service API for looking at a diamond, create/read/update claims (by insurance companies) and create/read/update police reports on diamonds.

NON-FINANCIAL APPLICATIONS

Applications of Blockchain in the Music Industry

The music industry has gone a big change in last decade due to the growth of Internet and availability of a number of streaming services over the Internet. It is impacting everyone in the music industry-artists, labels, publishers, songwriters and streaming service providers. The process by which music royalties are determined has always been convoluted one, but the rise of the Internet has made it even more complex giving rise to the demand of transparency in the royalty payments by artists and songwriters.

Decentralized proof of existence of documents

Validating the existence or the possession of signed documents is very important in any legal solution. The traditional document validation models rely on central authorities for storing and validating the documents, which present some obvious security challenges. These models become even more difficult as the documents become older. 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. Proof of existence is a simple service that allows one to anonymously and securely store online proof of existence of any document. This service simply stores the cryptographic digest of the file, linked to the time in which a user submits his/her document. It is to be noted here that cryptographic digest or fingerprint- not the actual document- is stored in blockchain, so user need not be worried about the privacy aspect.

Decentralized Storage

Cloud file storage solutions such as Dropbox, Google Drive or One Drive are growing in popularity to store documents, photos, video and music files. Despite their popularity, 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 peer-to-peer distributed cloud storage platform (see Appendix for detailed description) 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. Absence of a central control eliminates most traditional data failures and outages, as well as significantly increasing security, privacy and data control. Storj platform depends upon a challenge algorithm to offer incentivization for users to properly participate in this network. In this way, Storj platform can periodically cryptographically check the integrity and availability of a file, and offer direct rewards to those maintaining the file. Here, bitcoin-based micropayments serve as both an incentive and payment while a separate blockchain is used as a data store for file metadata.

Internet Applications

Namecoin is an alternative blockchain technology (with small variations) that is used to implement decentralized version of Domain Name Server (DNS) that is resilient to censorship. Current DNS servers are controlled by governments and large corporations, and could abuse their power to censor, hijack, or spy on your Internet usage. Use of Blockchain technology means since DNS or phonebook of the Internet is maintained in a decentralized manner and every user can have the same phone book data on their computer. Public Key Infrastructure (PKI) technology is widely used for centralized distribution and management of digital certificates. Every device needs to have root certificate of the Certification Authority (CA) to verify digital signature. While PKI have been widely deployed and incredibly successful, dependence on a CA makes scalability an issue.

IV. RESULTS AND DISCUSSION

ADVANTAGES OF BLOCKCHAIN TECHNOLOGY

1. Root Users

Users are in complete control of all their information and transactions.

2. High Quality Data

Blockchain data is complete, consistent, timely, accurate, and widely available.

3. Durability, Integrity and Longevity

Due to the decentralized networks which are present blockchain does not have a central point of failure and is better able to withstand malicious attacks.

4. Transparency and Immutability

Changes to public blockchains are publicly viewable by all parties creating transparency, and all transactions are immutable, meaning they cannot be altered or deleted.

5. Faster Transactions

Interbank transactions can potentially take days for clearing and final settlement, especially outside of working hours.

DISADVANTAGES OF BLOCKCHAIN TECHNOLOGY

1. Signature verification

Every blockchain transaction must be digitally signed using a public-private cryptography scheme such as ECDSA. This is necessary because transactions propagate between nodes in a peer-to-peer fashion, so their source cannot otherwise be proven.

2. Redundancy

This isn't about the performance of an individual node, but the total amount of computation that a blockchain requires. Whereas centralized databases process transactions once (or twice), in a blockchain they must be processed independently by every node in the network. So lots more work is being done for the same end result.

3. Nascent Technology

Resolving challenges such as transaction speed, the verification process, and data limits will be crucial in making blockchain widely applicable.

4. Control, Security, and Privacy

While solutions exist, including private or permissioned blockchains and strong encryption, there are still cyber security concerns that need to be addressed before the general public will entrust their personal data to a blockchain solution.

5. Cost

Blockchain offers tremendous savings in transaction costs and time but the high initial capital costs could be a deterrent.

TYPES OF CRYPTOCURRENCIES

Figure 3: Types of Cryptocurrencies

V. CONCLUSION

The entire process of Blockchain technology has been discussed in detail and how blockchain can be applied in many other fields apart from just implementing in the world of cryptocurrency. Blockchain technology is a powerful technology and nurturing it with the proper additional tuning, it can be applied in the digital world to create wonderful revolutions enhancing the quality of human life to a great extent. Blockchain technology can be embedded into the

field where there can be an elimination of middle man technology to ease in the entire process and save energy and time thus improving the quality of life. It also propagates a methodology of being highly secure since every transaction made gets an entry on the distributed ledger thus creating a permanent record. This further drives it to be extremely transparent and error free making it way more trust worthy than the traditional systems which are in play in the current digital world. Blockchain technology is on the rise in various industries and many adaptations are being done to the current traditional models. In conclusion, when the technology is implemented in the right manner, various industries in the digital world can be revolutionized enabling humanity to lead a higher quality of life.

VI. REFERENCES

[1] Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman Sutardja Center for Entrepreneurship & Technology Technical Report Berkeley University of California

[2] https://blockchaintechnologycom.wordpress.com/201 6/11/21/advantages-disadvantages/

[3] https://www.allerin.com/blog/wp-content/uploads/2016/06/Blockchain-Technology.png

[4] https://en.wikipedia.org/wiki/Blockchain

[5] https://en.wikipedia.org/wiki/Cryptocurrency

[6] https://www.munichre.com/us-life/en/perspectives/underwriting/blockchain-implications-insurance-industry.html

[7] Adhami S, Giudici G, Martinazzi S (2018) Why do businesses go crypto? An empirical analysis of initial coin offerings. J Econ Bus 100:64–75

[8] Chen Z, Li Y, Wu Y, Luo J (2017) The transition from traditional banking to mobile internet finance: an organizational innovation perspective - a comparative study of Citibank and ICBC. Financial Innovation 3(1):12