ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Blockchain: Beyond CryptoCurrencies

Priyanshu[1], Gajendra Prasad KC[2]

U.G. Student, Department of Computer Science and Engineering, Sapthagiri College of Engineering, Hessarghatta, Bangalore India[1]

Assistant Professor, Department of Computer Science and Engineering, Sapthagiri College of Engineering, Hessarghatta, Bangalore India[2]

ABSTRACT: With the emergence of **Bitcoin crypto-currency**, world was also introduced to **Blockchain technology**. In this paper we will not only focus on security, and flaws of this technology, but also the validation process involved in the processing of transaction of Bitcoins. Understanding the validation process of Blockchain technology includes conception of new Blockchain features and it allows users to recognize all security risks. This paper aims to enlighten the fact that Blockchain technology can and should be implemented in different areas other than Bitcoin network such has banking, finance, land acquisition etc. Notice in the last three examples, there is always a requirement of a middle man. Blockchain eliminates the need of a middle man or a central authority. There is a direct connection between the stakeholders. They can develop a string of trust(sometimes anonymously) between them. This allows faster and efficient way of communication between the two parties. This paper is an extensive summary and survey of Blockchain technology. The data has been collected from throughout the internet and presented as one paper.

KEYWORDS: Blockchain, bitcoin, transaction, security, validation.

I. INTRODUCTION

The world is almost ready for the big change and the change is being brought by cryptocurrency and blockchain technology. It's been ages since the banking system was introduced. Banks have played the most important role in shaping the world's economy. They represent central authority and regulate the flow ofmoney. In this report, we have gathered data from all across the internet to present the overview of technology- Blockchain. The key principle behindblockchain is its distributed nature and lack of central authority. Blockchain technology brings new concept which embraces new technologicaldevelopments and shifts the power from one to many, or from central conceptto distributed one.Bitcoin, being the firstimplementation of blockchain technology, sets the standardfor the industry.Bitcoin showed for the first time, thatit is possible for two parties, who do not necessarily trust each other, to performtransactions without any central authority as intermediary. Both sender andreceiver trust only the underlying architecture which guarantees the security ofthe system. The data in the blockchain is divided into blocks.Each block is dependent on the previous one. The system in which a blockchainserves as the database comprises of nodes or workers. These workers are responsiblefor appending new blocks to the blockchain. A new block can only be appended after all nodes in the system agree thatthis block is legit and contains only valid transactions.

There are three main categories of blockchainapplications:

- Blockchain 1.0: Currency
- Blockchain 2.0: Smart contracts
- Blockchain 3.0: Areas in government, health, science etc.

Since each category has its own advantages and disadvantages on a broader concept, the description of each and every category is beyond the scope of this paper.

Blockchain in practice was first introduced in Bitcoins-world's first cryptocurrencies by SataoshiNakamoto. Bitcoin showed for the first time, that it is possible for two parties, who do not necessarily trust each other, to performtransactions without any central authority as intermediary. Both sender andreceiver trust only the underlying architecture which guarantees the security ofthe system.

The main parties in the Bitcoin protocol are:

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

- Sender: the one who initiates the transfer of currency.
- Receiver: the recipient of the transfer
- Miners: Independent nodes which verify and confirm the transactions, also sometimes called as workers. The security of the system is guaranteed by these nodes.
- Blockchain: Decentralised ledger shared among all miners where all transactions are stored (the complete history since the Bitcoin creation)

II. RELATED WORK

1. Blockchain as service for IoT

Blockchain can be efficiently implemented on IoT's.Ablockchain is a decentralized ledger that contains connected blocks of transactions. The ability to create/store/transfer digital assets in a distributed, decentralized and tamper-proof way is of great practical value for IoT systems. **A key challenge** in the deployment of Blockchain as a Service (BassS) for IoT is the hosting environment. Edge devices are often too constrained regarding computational resources and available bandwidth leading to *cloud or fog*[1] as potential hosts. This paper evaluates the use of the fog and the cloud as possible platforms. The performance analysis clearly indicates that the network latency is the dominant factor. Consequently, the fog outperforms the cloud. This paper overall asks the question- *"Where should the blockchain be hosted?"*

2. Blockchain: Future of Financial and Cyber security

Venture capital (VC) firms are betting big on Bitcoin and the Blockchain. CoinDesk'sBitcoin Venture Capital data shows that VC firms are investing heavily in bitcoinstartupprojects[2]. Blockchain can act as ledgers or record-keeper for billions of transactions generated by Internet of Things (IoT). The device cost is decreasing and computing power is increasing every day therefore Blockchain presents an immense possibility in Internet of Things (IoT) and providing security.

Bitcoin transactions are made using script which is stackbased and processed from left to right. The script contains list of instructions recorded with each transaction having description on how receiver can gain access to it. The transactions are valid if script returns true.

ifverify_signature(transaction.signature,transaction.input.public_key):
return True
else
return False

3. Blockchain Technology Innovations

Information technology has become a critical innovation in almost every industry. This paper discusses how institutions or teams that can use technology correctly and effectively play a major role in disrupting the status quo in a leadership position. The Blockchain technology as a catalyst for emerging use cases in the financial and nonfinancial industries such as industrial manufacturing, supply chain, and healthcare.[4] The research indicates Blockchain can play a pivotal role in transforming the digitization of industries and applications by enabling secure trust frameworks, creating agile value chain production, and tighter integration with technologies such as cloud computing, IoT, combined with a DevOps approach to iterative development and management, and integration of cyber security, distributed computing, and Block-chain technologies.

4. Increased Anonymity using Blockchain

There are advantages and disadvantages of being anonymous online. Increased anonymity may allow whole new uses of blockchain technologies. One of the more classical yet exciting use-cases would be the sharing of files in a more anonymous fashion than allowed by current P2P networks based on Bit torrent. While anonymity was sacrificed in the original design of Bitcoin in order to prevent double-spending, we expect this to be a fertile area for future applications that attempt to re-balance Bitcoin's original design [2]

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

5. Security and Privacy through blockchain

The blockchain has fueled one of the most enthusiastic bursts of activity in applied cryptography in years, but outstanding problems in security and privacy research must be solved for blockchain technologies to go beyond the hype and reach their full potential. The paper presents industry trends to analyse problems ranging from deploying newer cryptographic primitives on Bitcoin to enabling use cases like privacy-preserving file storage [3]. It overviews not only the larger problems the workshop has set out to tackle, but also outstanding unsolved issues that will require further cooperation between real world and the blockchain community.

III. BEYOND CRYPTOCURRENCIES

Almost since the introduction of Bitcoin and its underlying blockchain ledger, researchers began to explore other field where a blockchain technology might be of great use.

The nature of the blockchainnetworkhas the potential to enable the development of a wide range of different applicationsthat are decentralized. Decentralized applications are becoming moreand more important in recent years.

- **Non-Financial use cases of Blockchain**

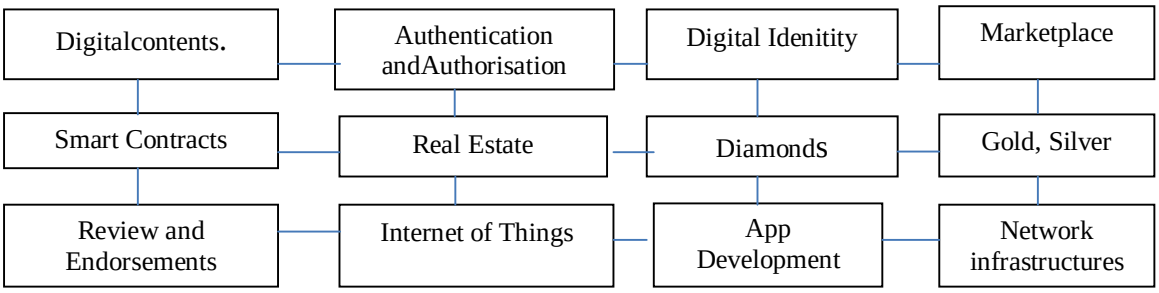


Figure 3.1: Non-Financial use cases of Blockchain

Digital Content: There are uncountable digital content on the internet. Digital content distribution using block chain uses decentralized peer-to-peer mechanism.There are some services which provides anonymity between the parties. Complete anonymity depends on the type of service.

Authentication and Authorisation: Blockchain technology can be used for lots of other exciting things. Think about the elections for example. A vote can be seen as a transaction in which you give your vote to a recipient candidate. Voters can validate the blockchain themselves and see for themselves their vote has been counted and the results are not tampered with.

Digital Identity: With the evolution of blockchain technology, usernames and passwords were the only accepted way to protect personally identifiable information. However, the username/password solution is becoming less and less feasible every day as individuals create hundreds of online accounts likely reusing username and password combinations across a multitude of sites. This inherently reduces the effectiveness of passwords. The IBM Hyperledger Foundation on Blockchain states that "blockchain is a shared, distributed ledger that facilitates the process of recording transactions and tracking assets in a network.

Marketplace: Theblockchain is a platform-like technology that consists of a decentralized ledger. Blockchain-baseddecentralized marketplaces connect consumers and sellers without any intermediaries.A decentralized marketplace connects three groups of users: producers, sellers, and consumers.

Smart Contracts: A smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. The smart contract code facilitates, verifies,

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

and enforces the negotiation or performance of an agreement or transaction. It is the simplest form of decentralized automation.

Real Estate: One of the biggest impacts of Blockchain on commercial real estate would be a smoother, faster contract management process. With smart contracts, every part of a lease or sale agreement is automated, and payments are received instantly – even outside of business hours.

Diamonds: Diamond is an insignificant commodity to invest; CEDEX (CErtifiedBlockchain based Diamond EXchange) has come up with a new online diamond exchange. It would connect main diamond supply sources – dealers and private holders to general investors and cryptocurrency holders.

- **Financial use cases of Blockchain:**

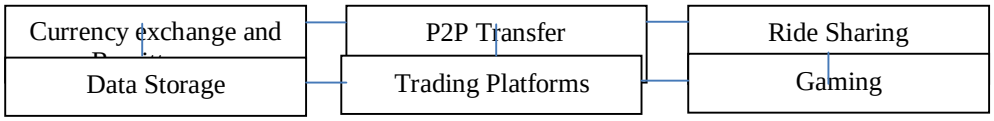


Figure 3.2: Financial use cases of Blockchain

Currency Exchange: Blockchainis giving a boom to Foreign exchange trading. Trading data is saved using block chain oriented technology.

P2P Transfer: Blockchain provides clear opportunities for P2P lending platforms. Companies will need to prioritise data transparency, create digital wallets to verify user identities and aggregate accounts, and work to mitigate the costs of operating this technology.

Ride Sharing: The proof-of-concept (PoC) is being developed in anticipation for the autonomous car future, where the average consumer won't own a car, but also, this provides utility now, allowing individual and fleet auto owners to lease their vehicles to trusted and identified riders.

Data Storage: There are a few ways that a Blockchain can be used in distributed storage software. One of the most common is to: Break up data into chunks; encrypt the data so that you are the only one with access to it; distribute files across a network in a way that means all your files are available, even if part of the network is down.

Trading Platforms: Cryptocurrency is based on knowledge sharing on a distributed platform. The entire transactional history is for everyone to see. One blockchain is one thread of transaction. One unit or one block stores many transactions. The data entered cannot be altered, nor can it be removed, enabling a system of complete transparency and trust. The entire money flow for the working model is beyond the traditional practices of controlling tax rates, credit usage, and money supply in the market.

Gaming: It could also be possible to have your character represent your real life form, using a combination of blockchain technology and information fed into the system such as photographs of your actual face. This new character will be different to every other character in the game, and impossible to completely replicate by any other player in the game.

IV. HOW BITCOIN WORKS

Following is the representation of howBlockchain algorithm works in Bitcoin:

- Step 0 - Retrieve the hash of the previous block from the network.
- Step 1 - Gather a list of potential transactions known as a "block". This list of transactions comes from the peer-to-peer bitcoin network.
- Step 2 - Calculate a hash for a block of potential transactions along with a random number.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

- Step 3 - If the hash is more than the currently set difficulty level, then you have mined that block. If not, start over from Step 1. Any additions to the list of transactions from step 1 along with change in the random number from Step 2 mean that there's a chance that the criterion will be met in the next go around

Hash

A hash is a function that converts data into a number within a certain range. The hash has the property that knowing its output is essentially unpredictable (within the given range). The specific hash function used for bitcoin mining is SHA256 applied twice.

Difficulty level

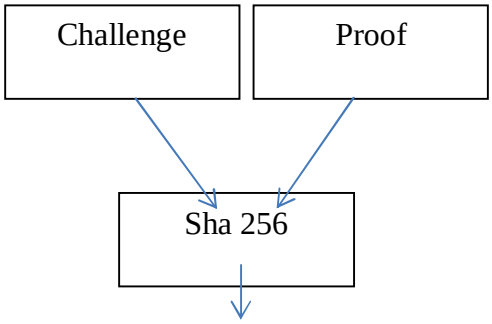
The unpredictable nature of the hash function means that putting in random data (the transaction + the random number) will essentially produce a random number within a certain range. This creates a way to probabilistically determine how often a solution will be found based on the number of times the algorithm can be run on the network.As the number of hashes per second across the entire network grows, the network automatically raises the difficulty such that a solution will be found within about 10 minutes.

Mining of Block

When a block is mined, the miner sends the block to all other miners on the network as evidence that it has found it. This block contains a list of transactions, the found hash, the specific random number, and a reference to the previous hash. As each miner receives the newly mined block, it removes all transactions that it is currently mining that exist within the block (because they've already been confirmed in the block chain) and broadcasts the block to other miners that do the same thing.

Proof of Work

Proof-of-Work is essentially a puzzle which consists of a challenge to which a proof has to be found. The proof-of-work puzzle is difficult to compute and easy to verify.TheBitcoin uses the following proof-of-work concept (shown in Figure 4.1): After the nodes compute the challenge, they need to find a proof (string) which when concatenated with a challenge and hashed using SHA-256 gives an output which has specific amount of leading 0s. This is very challenging problem because SHA-256, like other hash functions, has the property that it is impossible to compute the input for a given output, and also similar input strings have completely different hashes.



Hash with "predefined" properties

Figure 4.1: Proof of work using sha-256

V. CONCLUSION

A wide spectrum of use cases of the blockchainwas presented from all across the internet.Withcryptocurrencies like bitcoin, it was shown that it is the most prominent state which represents the blockchain technology. In recent years, people started building not only economic systems on top of the blockchain, but also other fields like diamond trading, gaming, real estate etc. This field is still pretty young, prone to problems and seemingly quite difficult to replace. Only time will tell how this turns out.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

REFERENCES

[1] Blockchain as Service for IoT http://ieeexplore.ieee.org/document/7917130/
[2] Blockchain: Future of financial security http://ieeexplore.ieee.org/document/7918009/
[3] Privacy and Security on Blockchain http://ieeexplore.ieee.org/document/7966963/
[4] Blockchain Technology Innovations ieeexplore.ieee.org/document/7998367
[5]Bitcoin transaction: From the creation to validation, a protocol overviewhttp://ieeexplore.ieee.org/document/8241988/
[6]https://bitcoin.stackexchange.com/questions/12603/the-bitcoin-mining-algorithm-from-a-programmers-viewpoint
[7] Blockchain: Technology and Applications, a report by Christian Mueller and DalmirHasic
[8] https://betterdiamondinitiative.org/blockchain-technology-making-diamond-exchange-transparent/
[9]https://www.theblockchainacademy.com/blog/blockchain-and-foreign-exchange-trading
[10] https://internationalbanker.com/technology/blockchain-technology-p2p-platforms-natural-allies/
[11] https://jaxenter.com/driving-future-blockchain-ride-sharing-136675.html
[12] http://www.dataversity.net/blockchain-can-used-secure-sensitive-data-storage/
[13] https://www.quantinsti.com/blog/top-9-cryptocurrency-trading-platforms/
[14] https://plarium.com/en/mmo-games/blockchain-games/
[15] https://productcoalition.com/blockchain-the-future-of-securing-your-digital-identity-6a78b846642c
[16]https://rubygarage.org/blog/how-blockchain-impacts-marketplace
[17] https://blockchainhub.net/smart-contracts/
[18] https://www.theinvestor.jll/news/world/others/blockchain-reshaping-real-estate-industry/
[19] https://www.traxion.com/blockchain-the-next-authentication-provide