

AN ANALYTICAL STUDY OF BLOCKCHAIN TECHNOLOGIES AND ITS POTENTIAL APPLICATIONS

Mr.N.Ganapathiram¹, Dr.S.Karthikeyan², Dr. S. Dhinakaran³, Dr. D. Raj Balaji⁴

Assistant Professor, Department of Computer Science, Rathinam College Of Arts and
Science, Coimbatore¹,

Gmail-ganapathiram9800@gmail.com

Assistant Professor, Department of Computer Science, Rathinam College Of Arts and
Science, Coimbatore²

Gmail-s.karthics@gmail.com

Associate Professor, Department of Computer Science, Rathinam College Of Arts and
Science, Coimbatore³

Gmail- dhinakaran.cs@gmail.com

Assistant Professor, Department of Computer Science, Rathinam College Of Arts and
Science, Coimbatore⁴

Gmail- d.rajbalaji@gmail.com

Abstract:

The Blockchain is one among the automation which will have great effect on upcoming decades and it is making enormous changes in our current business platforms. Blockchain is well established, divided registry that easy out transaction recording process and pursue assets in a business network. It can make changes in our business perspective and can make a revolutionary impact on our economy. There are two types of assets one is tangible and another one is intangible. Tangible assets are easily portable such as cash, car and land intangible assets consist of copyrights, patent and intellectual property. Everything can be traded and tracked in the Blockchain network virtually so that it reduces cutting costs and reduces risk of all individuals using these technologies. Blockchain details will not be dejected or forgotten because it uses distributed and decentralized technology which aims in providing data security, integrity and transparency. Only few researchers are involved in complete utilization and exploration of bit coins but many current researchers focus only on Blockchain technology and view on its applications over crypto currencies like bit coins. Crypto currency is not one and only technology of Blockchain it has many other appliances in banking, finance, government, accounting and business management process. In this paper the overall aim of study is to explore concept, overview, characteristics types, merits and demerits of technologies opportunities based on investigation and how to resolve challenges in current and upcoming trends so that more secure and scalable Blockchain system for massive deployment can be done.

Keyword: Blockchain, Cryptocurrency, Distributed Ledger, Decentralized Applications.

Introduction:

In current trends one of the buzzword in recent time in industry as well as academics is crypto currency. The digital records and information storage on multiple nodes or multiple computers can be done using revolutionary computer protocol used in Blockchain technology. One of the

important components of the automation is ledger which is same as relational database Waldport. It consists of a block which holds list of encrypted transaction or digital records. With the assist of cryptographic signature every block has been chained to next block according to chronological linear order. Whenever last block is added last transaction copy has been stored in Blockchain. The distributed consensus algorithm has been deployed so that in asymmetric cryptography both ledger and user security can be provided. Anonymity, audit ability, decentralization are the major important characteristics used in Blockchain technology so it can reduce cost and efficiency can be improved. For the participants to validate, confirming transaction, need of removal of third party all their computers should be connected to a network so that block which has been shared is interconnected to all participants. Data can be distributed securely in unique new way using Blockchain. The radical shift to direct transactions among intermediary and non-intermediary service is happened in distributed network by central instance. Bitcoin is considered as one of most successful crypto currency. During the transaction of Bitcoin implication of network is completely avoided and important technology to create a bit coin is Blockchain which is done using specially designed data storage structure. With these availabilities block chin can easily reduce cost and improve efficiency. Once transaction is initialized into the bock chain it cannot be cancelled because it is immutable. It can be used to attract customers for the business which required high dependability and integrity. Single point of failure scenario is nullified in Blockchain because it is distributed. It is treated as important component in upcoming trend there are many technical issues. 1MB of block size is limited to bit coin for every 10 minutes of mining. Only 7 transactions can be made per second according to bit coin restriction so it is tough to deal with high trading frequency. In network lager blocks indicates huge storage place and slow transaction in network. Therefore it is very tough during exchange between security and block size. The result is huge concern in scalability. It is stated that larger revenue has been generated by minors than fair revenue because of mining strategy. Blockchain development is hindered because minors hide their mined blocks so that revenue can be gained by them in upcoming days or near future. There is leakage in privacy even though users make transaction via private and public key.

Overview & concept of Blockchain Technology

Blockchain functionality consists of blocks which hold groups of records to provide security functionality for network it is connected with cryptography. The transactions that happen here are immutable because it is designed in pattern that all block contains transaction data timestamp and cryptographic hash code of previous block. Nakamoto in 2008 revised concept of Blockchain technology which is shown in fig 1. DLT Blockchain or Distributed Ledger Technology is a distributed recording technology because it holds information about event or transactions. Transaction has been deposited in a decentralized secure, efficient and low cost way. There are many types of Blockchain some of the major Blockchain technologies are public Blockchain, private Blockchain and hybrid Blockchain. Each type consists of both merits and demerits according to applications. Figure 2 displays different types of Blockchain technologies.

Public Blockchain:

By using transparent and anonymous network anyone can make transaction via network transactions. The public coins are completely decentralized example Bitcoin. Based on consensus of the users the system gets operated. In this method centre part of failure is completely avoided. Here the system is vulnerable system has weakness in public Blockchain. For example without the detection of participants the attacker can recreate and completely chain all modified blocks in the chain.

Private Blockchain:

The secrecy has been maintained in transactions and there is no availability of data in private Blockchain. Without the invitation or permission the participants cannot write or read in private network. Large companies only use private Blockchain with access between various enterprise Blockchain stakeholders. For example with restricted access for private usage bank can have various stakeholders such as employer's customers and suppliers.

Hybrid Blockchain:

Hybrid Blockchain is also called as consortium Blockchain. Both private and public Blockchain blended together to form hybrid Blockchain. By selecting the model data can be shared among consortium participants like institutions, firm and banks so that private Blockchain can be accessed by institutions or enterprises.

Design Feature based on Blockchain

The main features of Blockchain based designs are evaluative to uniqueness and supremacy of the technology. Evaluative uniqueness and supremacy are main features of Blockchain design. The uncooperative amount of assets and vitality has been grounded for design features for the verification and settlement takes place.

Transaction Confirmation

As per posting precondition it is mandatory for the users to confirm Blockchain underpinned protocol so that validity of transaction is ensured.

Settlement Verification:

The Blockchain straight away verifies the pre-transaction proprietorship of assets which has been exchanged once transaction confirmation has been done by coordinates which allows assets settlement of complete transaction.

Permanent Timestamp:

An unchangeable sequence of record and timing of blocks in chain has been generated after the creation of blocks, addition of chains, accurately added pairs and timestamp.

Smart contract Automation:

Under specific needed requirements and conditions smart contract which works automatically is supported by Blockchain even though it is not inherent appliances of Blockchain.

Blockchain Technology Characteristics

The Blockchain characteristics contribute to one another in some way. The characteristics of Blockchain technologies have been clearly discussed in below table.

1) IMMUTABLE:

The Blockchain which remains stationary in an altered network is called as immutable Blockchain. With the assists of collection of nodes Blockchain functionality takes place. A copy or replica of digital ledger is stored in each and every node. Each and every nodes verify the validity of transaction and network is added to the transaction only if majority of node states that it is a valid transaction. This statement states that in ledger no transaction block is added unless the approval of majority nodes. The user available in network cannot delete, modify or change because valid records cannot be modified and they are irreversible

2) DISTRIBUTED

The entire system access, distributed ledger transaction details and verifying transaction pattern record can be done by all Blockchain users. It is completely decentralized, No availability of central authority and no trusted third party for transaction verification. Consensus between Blockchain confirms the data truth. Communication is not done via central node it is happened using direct peer communications.

3) PRIVACY:

There is no public identity of users because of inherent platform feature. The real identity of participants has not been revealed. Generated addresses have been used by the Blockchain using parties. Due to some in bon constraints complete safeguarding of privacy in Blockchain cannot be done.

4) AUDITABILITY:

With the assist of timestamp transactions which happens in Blockchain has been verified and recorded so it will be easy to trace and verify previous records so that transparent and traceable data storage can be maintained using Blockchain. To verify chronological and permanence order of recording computational algorithm has been used.

5) SECURITY:

The Blockchain is highly secured because of the powerful cryptography in Blockchain which gives authorization for users assets and selection of both public and private key. To eliminate and avoid identity theft there is no inter link or connection between the given address and users address. Additionally hashes have been linked by block modifying any data within given block would modify the connected blocks. So inside Blockchain technology user's transferable data's of business and information are secured in a proper way.

Merits of Blockchain Technology

1) Immutability and Data Integrity:

The regulatory compliance has been upgraded and strengthened for the participants to decrease fraud. The record which has been deposited in the ledger can be deleted only after completion of consensus

2) Security:

For every each and single transaction a unique alpha number signature 64 bit code is used so every transactions can be time stamped digitally with cryptographic hash code.

3) Accessibility and High Availability:

The Blockchain data's are complete one which time and accuracy because of the decentralized network.

4) Reliability:

Single point of failure is nullified in Blockchain technology because its not regulated by single point of control.

5) Decentralization:

Third party need has been removed by decreasing all over head cost and transaction fee so that transactions happen between peer-peer in decentralized way.

6) Consensus and Transparency:

The main source designation with time and date of transaction has been mentioned in the shared ledger. Subsequent audit can be done by counter party at anytime to show that

7) Automation:

Self executed command code named as smart contracts has been used by Blockchain technology so that the processing happening in blockchain can be stored and executed.

8) Time of processing:

The processing time can be reduced from two days to minutes or seconds in Blockchain technology for transactions processing and records.

Demerits of Blockchain Technology

1) High cost

It is mandatory for the users to pay for computational power and for transaction. It is decentralized there is no free of cost initial amount should be paid first itself.

2) Suppleness Issue In Data:

There is no guarantee provided by the signature for the ownership. Data suppleness issue takes place mainly during implementation of Blockchain. The transaction can be modified and changed by attacker at any time this can cause issues in confirmation of transaction.

3) Issues In Latency:

Because of complex verification process for massive transactions time factors the important critical issues in implementation of Blockchain.

4) Resource Wastage:

In a single day around 15million dollar energy has been spent for mining Bitcoin. Larger amount of resource and time is needed to mine Bitcoin.

5) Technological Immaturity:

Transform in organization, strategically including changes in structure of culture and process is needed because Blockchain basically is a new technology which represents complete transformation to decentralized network.

Conclusion:

From the conceptual point of view data integrity problems can be solved, transparency can be improved, security can be enhanced and emphasized privacy and trust can be built using Blockchain technologies. These technology can bring evolutionary changes in area of IOT, trading, E-government, health care finance and accounting. Along the technical innovation and applications innovative solutions can be created and implemented in all area with these technologies. But practically cost efficiency is very high for implementing Blockchain technologies in various industries and organization. Consequential investment amount is needed from the organization for resettle and pull up stakes in legacy system. In this starting phase to assist application of hybrid architecture, Blockchain incorporation it is important for organization to establish or situate 13 integrated platforms. Deeper understanding about technologies, opportunities, values and risk should be done by organizations. According to result system applications are applied only in small numbers. Therefore it takes some time for Blockchain technology to replace old system or legacy applications. In the upcoming new future new system development can be done by integration and incorporating application of Blockchain with legacy system. Through conclusion it is stated that to advance and improve maturity of this field it is mandatory to do many in-depth concerted research in this area. Many legal and technical issues must be resolved since it is the starting stage. This overview will provide and led be a starting point of themes related to future research for developing Blockchain applications.

References:

- [1] "State of blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016. [Online]. Available: <http://www.coindesk.com/state-of-blockchain-q1-2016/>
- [2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [3] G. W. Peters, E. Panayi, and A. Chapelle, "Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective," 2015. [Online]. Available: <http://dx.doi.org/10.2139/ssrn.2646618>.
- [4] G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain," 2015.
- [5] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.

- [6] B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy," 2013. [Online]. Available: <https://ssrn.com/abstract=2394738>
- [7] Y. Zhang and J. Wen, "An iot electric business model based on the protocol of bitcoin," in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp. 184–191.
- [8] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, France, 2015, pp. 490–496.
- [9] C. Noyes, "Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning," arXiv preprint arXiv:1601.01405, 2016.
- [10] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436–454.
- [11] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 15–29.
- [12] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.
- [13] NRI, "Survey on blockchain technologies and related services," Tech. Rep., 2015. [Online]. Available: <http://www.meti.go.jp/english/press/2016/pdf/053101f.pdf>
- [14] D. Lee Kuo Chuen, Ed., Handbook of Digital Currency, 1st ed. Elsevier, 2015. [Online]. Available: <http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170>
- [15] V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, 2014