

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Recent Trends in Blockchain Technology

R.Palaniyappan¹, Dr.P.Sivaprakasam²

Assistant Professor, Department of Computer Science, Sri Vasavi College, Erode, Tamilnadu, India ¹

Associate Professor, Sri Vasavi College, Erode, Tamilnadu, India ²

ABSTRACT: Block Chain is mainly used for Cryptocurrency that is Digital Currency which is used in substantiation and currency units of Fund transfer are autonomously operated without a central bank. Blockchain Technology had the majority force on our lifestyles in the final decade. A lot of people still confuse Blockchain with Bitcoin, but they are not the equivalent. Bit coin is an appliance that uses Blockchain technology. There is a large assortment of blockchain applications ranging from cryptocurrency, risk management, internet of things (IoT), financial services to public and social services. The major proposition is that the blockchain establishes a system of creating a dispersed consensus in the digital online world. Moreover, this paper also points out the recent aspects of blockchain technology.

KEYWORDS: Blockchain; Consensus; Platform; Tools; Protocols; Security; Privacy

I. INTRODUCTION

A. Block Chain

Block chain technology is an online ledger technology that provides information to a company and helps them record their communications easily. The ledger is encrypted, so the communication in this region can be done between the company and peer-to-peer network only when it is verified. The technology offers responsibility, as the transactions that are recorded are only throughout multiple-party verification, and no transaction in the ledger can be changed by the parties at a later stage.

B. Working Process of Block Chain

Every transaction that is made is verified by the parties implicated in the transaction. These transactions are also known as "blocks." Once the transaction is confirmed by each party, the transaction involved is solved through a mathematical puzzle and is entered in the ledger chain.

Once any entry of the transaction is made, no other person can make an adjustment to the entry. This makes the transaction safe and authentic. Blockchain was initially devised for digital currency such as Bitcoin, but it is now used for distributing digital information.

The blockchain technology is structured and very difficult to change the rules or its content without the compromise among the people who are using it. In blockchain newer blocks are linked to the older ones, forming a chain. It is totally public and open to everyone to view and access other can be closed to a select group of the approved user as a group of bank or government agencies.

Each transaction in a block is tagged by a specific timestamp. In the blockchain system, transaction details are stored in the form of blocks and each block relates to each other referring the hash value [1].The blocks are hashed, a hash pointer points to its before block, hence creating the chain. The mining process comes into the picture to authorize transactions and for eliminating the inappropriate data. The blockchain is a distributed network of computer devices used to maintain the source of information distribution among the nodes. Although, each node preserves security and information accuracy by keeping a wide-range distributed ledger with past transactions. The new block will be broadcasted to the entire blockchain network permitting all nodes to maintain the same ledger across the network. The works of blockchain is shown in Fig. 1.



18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

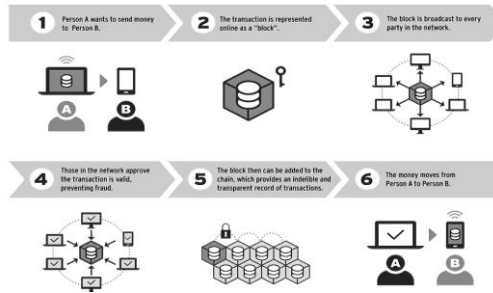


Fig. 1. Block Chain Working Process

II. STRUCTURE OF THE BLOCKCHAIN

Blockchain is a combination of computers linked to each other instead of a middle server, meaning that the entire network is decentralized. The blockchain technique allows digital information to be disseminated, rather than copied. This distributed ledger provides transparency, trust, and data security [2]. Basically, the following Fig. 2 blockchain sequence diagram is a connected list of records:

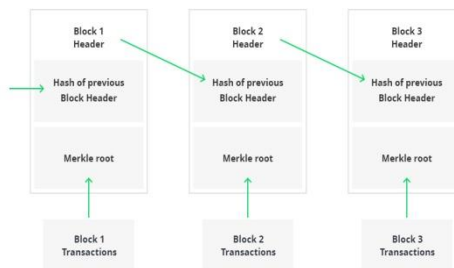


Fig. 2. Blockchain Structure

The block header consists of

- Nonce: a 4-byte field, which regularly starts with 0 and increases for every hash computation.
- Version: specifies which set of block justification rules to monitor.
- Merkle tree root hash: in a block, the hash value of all the transactions.
- Parent block hash: a hash value points to the previous block with a 256-bit hash value.
- Timestamp: shows the present timestamp as seconds since January 1, 1970.
- nBits: has a present hashing target threshold value in valid format.

A. Key factor of Block chain technology

1) Decentralized and Distributed: Conventional database in which data is stored in a middle data server, the data in a blockchain is stored in various computers across the network. Any valid updates made to data on one computer are distributed to the entire computer across the network. This makes it unfeasible for someone to damage or manipulate the data.

2) Secure: Each block of the blockchain is encrypted using highly developed encryption techniques. Each block is linked to the previous block making transaction tamper-proof. Blockchain can be permissioned or permissionless. The access level of each applicant in the blockchain network can be controlled.

3) Smart contracts: Smart contracts are rules that govern a transaction that participants can carry out in the blockchain. Smart contracts are stored on the blockchain and are executed automatically as a part of a transaction. The smart contract ensures that all parties adhere to the rules that are present on the blockchain.

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

4) **Consensus:** There must be an agreement between all appropriate parties before a transaction can be executed. The transaction is verified and dedicated to the ledger through various means of the consensus algorithm.

The familiar consensus algorithms are,

- Proof-of-Work (PoW)
- Proof-of-Stake (PoS)
- Practical Byzantine Fault Tolerance(PBFT)
- Delegated PoS (DPoS)

5) **Immutable:** Blockchain technology makes it an unfeasible transaction to tamper with transactions. The hash will not match with reference on the next block of the blockchain, if the tampered block is distributed to the blockchain network, the nodes on the network will identify this as a tampered block and will reject.

B. The Principle of Block chain

Block chain is a grouping of a variety of technologies. Hierarchical architecture of a blockchain consists of six layers from bottom to top: data layer, network layer, consensus layer, incentive layer, contract layer, and application layer.

- 1) The Data Layer: Encapsulates the data blocks, the data layer related to data encryption and time stamp [7].
- 2) The Network Layer: Included distributed networking mechanism, data circulation and verification mechanism [7].
- 3) Consensus Layer: Encapsulates consensus algorithm of the network node.
- 4) Incentive Layer: Integrate economic factors which are including economic incentive and distributed mechanism [7].
- 5) The Contract layer: The Contract layer is the main encapsulation algorithm and the smart contract, which is the basis of the blockchain programmable characteristic [7].
- 6) The application layer: Encapsulates the different applications [7] of the blockchain such as time-stamped blockchain, economic incentives depend on consensus computing.

III. TYPE OF BLOCKCHAIN

There are different kinds of blockchain architecture, each of them have different design and architecture.

A. Public Blockchain

In this type of blockchain, everyone in the network can authenticate the transaction and can take part in the process of attaining consensus. It ensures decentralization by setting up a block of peer-to-peer transactions. Each transaction is connected with the blockchain before it is written to the system. Hence, it can be established and synced with every node in the network. Anybody with a computer and internet connection can be enrolled as a node and can be provided with the complete blockchain history. It states that everyone can check the transaction and verify it, and also participate in the process of getting consensus. The benefit of the public network is the ambiguity of the user and full transparency of the ledger.

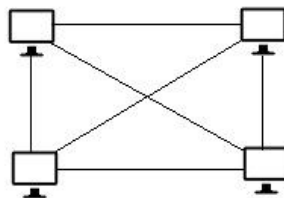


Fig 3. Public Blockchain

B. Private Blockchain

Node will be controlled, not every node can take part in this block chain, has strict authority administration on data access. Private block chains have a strict management with respect to the authority of the data access in the network. None of the nodes in the network can participate in the verification and validation of transactions. Instead, a company or association initiates, verifies and validates each transaction. This gives a higher level of efficiency in the verification and validation of transactions. The benefit of private blockchain is that a company can select the access rights to individuals and permit a higher level of privacy when compared with public blockchains. A private blockchain is related to a traditional and governance model based business. Using a privately-run version of blockchain can bring the

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

organization into the 21st century. Private block chains are more prone to acceptability by the private sector or government based companies as they allow a central authority to be present with a more secure, more efficient and faster technology.

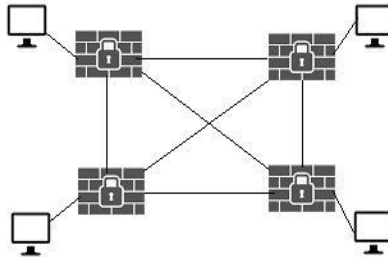


Fig 4. Private Blockchain

C. Consortium Blockchain

Consortium blockchain is a combination of public and private blockchain and can be interpreted as partly decentralized. These blockchains are open to public but not the entire data is available to all the participants. User rights vary and blocks are validated based on the predefined rules. Consortium blockchains are hence "partly decentralised". Consortium Blockchains are the ones in which the consensus process is controlled by a preselected set of trusted nodes. A block is added to the chain after consensus is achieved through the transaction validation by a group from the preselected set of nodes. In a consortium Blockchain, the right of reading the blockchain can be public or made restricted only to participants. In addition to this, consortium Blockchains are considered to be partially decentralized unlike private Blockchains. A consortium blockchain model is more appealing to corporate companies, because of the fact that it is decentralized unlike private Blockchains.

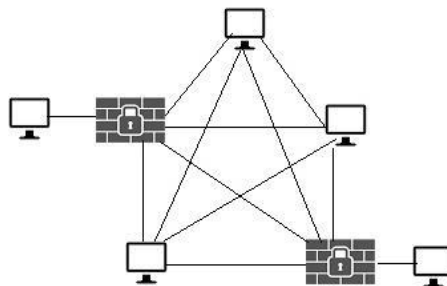


Fig 5. Consortium Blockchain

IV. PLATFORMS OF BLOCKCHAIN

A. Introduction of Black chain Platform

Blockchain platforms allow the development of blockchain-based applications. They can either be permissioned or permissionless. The blockchain platforms based on the slanted assessment of their ease of prototyping. On the other hand, if the project is transaction exhaustive, ensure to determine side-chain implications for security and evaluate network transaction fees.

B. Various Platforms of Block chain

The more popular platforms of blockchain as follows,

- 1) **BigchainDB**: BigchainDB is an open source system that “starts with a big data distributed database and then adds blockchain characteristics — decentralized control, immutability and the transfer of digital assets”.
- 2) **Chain Core** : Chain Core is a blockchain platform for issuing and transferring financial assets on a permissioned blockchain infrastructure. It runs on the open-source Chain Protocol.
- 3) **Corda**: Corda is an open-source distributed ledger platform with pluggable consensus — “it supports multiple consensus providers employing different algorithms on the same network”.

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

- 4) **Credits:** Credits is a development framework for building permissioned distributed ledgers.
- 5) **Elements Blockchain Platform:** Elements is an open source, protocol-level technology for extending the functionality of Bitcoin.
- 6) **Eris-db:** Eris-db is a permissioned distributed ledger client that executes Ethereum smart contracts on a permissioned virtual machine.
- 7) **Ethereum:** Ethereum is a decentralized platform that runs smart contracts on a custom built blockchain
- 8) **Hydra Chain:** Hydra Chain is an Ethereum extension for creating Permissioned Distributed Ledgers for private and consortium chains.
- 9) **Hyperledger Fabric:** Hyperledger Fabric supports the use of one or more networks, each managing different Assets, Agreements and Transactions between different sets of Member nodes.
- 10) **Hyperledger Iroha:** Hyperledger Iroha could be a “simple and modularized” distributed ledger system with emphasis on mobile application development.
- 11) **Hyperledger Saw tooth:** Hyperledger Saw tooth Lake could also be a modular blockchain suite that supports both permissioned and permissionless deployments. Transaction business logic in Hyperledger Saw tooth Lake is decoupled from the consensus layer..
- 12) **Multi Chain:** Multi chain is an open-source blockchain platform, based on bitcoin’s blockchain, for multi-asset financial transactions.
- 13) **Open chain:** Open chain is an open source distributed ledger system for issuing and managing digital assets
- 14) **Quorum:** Quorum us an open source distributed ledger and smart contract platform based on Ethereum
- 15) **Stellar:** Stellar is an open-source, distributed payments infrastructure that connects banks, payments systems, and people. Stellar enables building of mobile wallets, banking tools, smart devices.
- 16) **Tezos:** Tezos is a decentralized blockchain platform that is self-governing and establishes a true digital commonwealth. It is a platform linked to a digital token, called a Tezzie or Tez.
- 17) **Dragonchain:** Dragonchain’s Blockchain as a Service Platform is designed to provide developers and enterprises the useful resources required to develop blockchain applications in minutes. Dragonchain platform has been particularly designed for enterprises. It’s public/private hybrid blockchain platform offers ease of use and high performance to develop and deploy blockchain apps and micro service-based smart contracts.
- 18) **Hedera Hashgraph:** Hedera Hashgraph platform is lightning secure, fast and fair platform that does not need to compute a heavy proof of work algorithm.

V. TOOLS OF BLOCKCHAIN

Blockchain tools, simplify the process of blockchain development but also help to strengthen your knowledge of the domain. These tools are used to write, verify, test, and debug your blockchain code. The major 10 Blockchain Development Tools are as follows,

- 1) **Solidity:** Solidity is a contract-oriented, high-level language for implementing smart contracts.
- 2) **Geth:** Geth is an Ethereum node implementation built using the Go programming language.
- 3) **Mist:** Mist is the official Ethereum wallet developed by the creators of Ethereum.
- 4) **Solc:** Solc (Solidity Compiler) is a Solidity command-line compiler written in C++. Its primary purpose is to change Solidity scripts into a more readable format for the Ethereum Virtual Machine.



18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

- 5) **Remix:** Remix IDE is a browser-based Blockchain tool used for the creation and deployment of smart contracts.
- 6) **Metamask:** Metamask is a wallet designed to function that acts as a bridge between Ethereum Blockchain and a browser. Metamask offers a software platform that allows you to provide Ether and other ERC-20 resources while also letting you interact with Ethereum Dapps.
- 7) **Truffle:** Truffle is an Ethereum Blockchain framework intended to create a development environment for developing Ethereum-based apps.

VI. PROTOCOLS OF BLOCKCHAIN

A. Need for Block Chain Protocol

A protocol is the rules and guidelines are used to achieve a particular task. These rules are necessary to ensure that data can be transferred efficiently. This means that centralized authority is absent. The top 4 blockchain protocols as follow,

- 1) **Hyperledger:** Hyperledger is an open-source enterprise structure. It is managed by the Linux Foundation. It is an umbrella project which has loads of frameworks and protocols. As it is open-source, anyone with the right talent can supply to the project. Also, Hyperledger is all regarding permissioned blockchain.
- 2) **Quorum:** Quorum is yet another enterprise blockchain protocol that is aimed to solve finance sector problems. Quorum, presently like Hyperledger, is an open-source project.
- 3) **Corda:** R3 Corda is also a promising enterprise protocol that is built from scratch. It is handled by the R3 banking consortium and is best matched for banking and finance-related organizations. It utilizes distributed ledger software. It utilizes consensus algorithms to ensure transparency, traceability, and authenticate transactions.

Table 1: Data items extracted from the blockchain platforms

Category	#	Data Item	Description
Basic Information	1	Official Website	URL for the official website of the platform.
	2	Software Website	Online repository system that keeps track of the source code of the platform.
	3	Explorer Website	Special type of online website, "explorer," that keeps track of all the transactions for the platform. Note that, multiple explorers may exist for the platform which also serves as a cryptocurrency. In this case, we only list the "official" or the representative ones. Also, the living public websites do not exist for the non-cryptocurrency platforms, however, the "explorer" code may be available; in this case, we list the website of their "explorer" code instead.
	4	Main Reference	Main official white papers or the other types of articles discussing the platform.
Blockchain Technology	5	Real-World Application	Examples of the institutions or companies currently using the platform.
	6	Main Improvement over Bitcoin	Main technical difference from Bitcoin, the first distributed cryptocurrency.
	7	Network Permission	Permission mechanism of the blockchain network.
	8	Consensus Protocol	Core protocol used to create a consensus chain of blocks.
Public Cryptocurrency	9	Special Hardware Requirement	Special hardware (ie, besides a normal personal computer) needed to "mine" (ie, create) new blocks.
	10	Smart Contracts Support	Capability to support smart contracts/properties.
	11	Symbol	Short name for the cryptocurrency (eg, "BTC" for Bitcoin). ⁸⁰
	12	Mining for New Public Coins	Capability for participants to "mine" new coins to serve as public cryptocurrency.
	13	Anonymous Payment	Feature that prevents tracing the origin, destination and amount of the transactions.
	14	Rapid Payment	Support of the high-speed asset transferring.
	15	Coin Limit	Maximum amount of the coins that can be created for the cryptocurrency.
Application Programming	16	Coin Value	Value of the coin in U.S. dollars. ⁸¹
	17	Average Transaction per Second (TPS)	Average speed of transactions (data collected in December 2017). TPSs were averaged from values on October 5, November 5, and December 5 in 2017.
	18	Scripting Language	Supported blockchain scripting language (run instructions such as "freezing funds until a time in the future" ⁸²).
	19	Open Source	Availability of the source code.
	20	Main Implementation Languages	Programming languages used to implement the source code for the platform.
	21	Software License	Copyright license for the source code.

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

VII. APPLICATIONS OF BLOCKCHAIN

A. Finance: Financial services and Enterprise transformation:- blockchain systems such as Bitcoin has a tremendous collision on traditional financial and business services. Block chain and cryptocurrency technology can help POs to expand their simple roles with the provision of new financial and un-financial services.[3] Blockchain technology offers business opportunities for POs in identity services, device management, and supply chain management.

B. Internet of Things (IoT): Blockchains can also be used in the IoT field. The predictable utilization method is one where sensors, etc. predetermined processing tasks work independently without involving a central server. Distributed autonomous corporations (DAC) is basically obtained for coins and exchange sensor data without concerning any third party.

C. Healthcare: Healthcare is also ready to spend in blockchains as new business cases emerge. Several characteristics provided by the blockchain are of great thought to healthcare organizations: disintermediation, transparency, auditability, industry collaboration, and new business models [15].

D. Advertising: As a distributed, immutable, transparent ledger, the blockchain is a usual fit for the digital advertising supply chain. The core issues like Advertisements fraud, inefficiency, and lack of transparency of digital advertising have been need to be solved. With the help of blockchains significantly improve efficiency and transparency, reduce costs, and prevent fraud.

E. Energy: The trading of energy and commodities, even the simplest transactions, is often a impartial game of multi-parties. From the implementation to the conclusion of the transaction, both parties should organize and verify the transaction data.

G. China's Crypto Yuan: In April, after several years of work, the Chinese government announced the completion of two milestone initiatives involving blockchain and cryptographic technology. The first initiative pertains to the country's central bank digital currency, named DCEP, which is reportedly being tested in four local cities. The second development is related to Blockchain-based Service Network, or BSN, which is currently said to be fully operational. Meanwhile, China is also beginning a affected plan dubbed the "Chinese Standards of 2035," which outlines how the next generation of technology will be operated, including everything from telecommunications to artificial intelligence.

VIII. CHALLENGES OF BLOCKCHAIN

A challenge can be defined as an implicit demand for verification. Some of the most important challenges currently faced by blockchain technology are listed as below.

A. Scalability: a major concern in blockchain technology due to the validations for each transaction and change approval. The blockchain in various domains adopt an alternate strategic approach and possibly require less storage. The expected growth or size of data is 175 zetta bytes per year in 2025 for which the solution is yet to arrive if this could become a problem

B. Processing time: complicated to complete the verification of transactions in real time or in a short duration as quick decisions are required in the high speed environments.

C. Transaction cost: distributed data storage and cryptography operations are resource and time consuming. The user requires a special type of hardware and has high power consumptions.

D. Privacy leakage: The blockchain is mainly susceptible to transactional privacy leakage due to the fact that the details and balances of all public keys are visible to everyone in the network. The proposed solutions for accomplishing anonymity in blockchains can be expansively classified into mixing solution and anonymous solution. Mixing is a service that offers anonymity by transferring assets from numerous info delivers to various yield addresses. Anonymous is a service which unlinks the payment origins for a transaction to prevent transaction graph analysis as discussed in [8]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

E. Selfish Mining: Selfish mining is another challenge faced by blockchain. A block is susceptible to cheating if a small portion of hashing power is used. In selfish mining, the miners keep the mined blocks without broadcasting to the network and create a private branch which gets broadcast only after certain requirements are met. In this case, honest miners waste a lot of time and resources while the private chain is mined by selfish miners.

F. Personal identifiable information: Personal Identifiable Information (PII) is any information that can be used to remove an individual's identity. [10].

G. Lack of skills: yet to upgrade the skills of employees with blockchain to build decentralized applications or the organizations should be ready to pay high salary for the blockchain experts.

H. Energy consumption: Proof of Work is the mostly used consensus mechanism solves the complicated puzzles with more amount of energy.

IX. CONCLUSION & FUTURE SCOPE

The blockchain is a decentralized infrastructure and peer-to-peer environment. The different applications have been developed in blockchain technology due to its achievement and benefits. The main goal of blockchain technology is to offer safe data management for cloud and develop data security. This paper with complete survey provides insight into various concepts for enhancing the quality in maintenance of data with security; help the researchers and academicians to take forward their research. Blockchains have received much interest worldwide. In this work, can survey blockchain usage in different areas including Finance, healthcare, advertising, energy, and societal applications. In the paper presents a timely summary for entities with an interest in blockchains. Finally, the challenges and secure and privacy of blockchain technology are summarized.

The future scope can be focused with, the new consensus algorithm to develop scalability, processing time which helps to reduce the computation cost [13]. The new image code based algorithm to enhance the throughput of the transaction in cloud environment for block chain technology.

REFERENCES

- [1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008
- [2] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564.
- [3] Tian, F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In IEEE 13th International Conference on Service Systems and Service Management (ICSSSM). 1-6, 2016.
- [4] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," IEEE Communications Surveys & Tutorials, 2018.
- [5] T. McConaghy, R. Marques, A. Müller, D. De Jonghe, T. McConaghy, G. McMullen, et al., "BigchainDB: a scalable blockchain database," white paper, BigChainDB, 2016.
- [6] M. S. Sahoo and P. K. Baruah, "HBasechainDB—A Scalable Blockchain Framework on Hadoop Ecosystem," in Asian Conference on Supercomputing Frontiers, 2018, pp. 18-29.
- [7] Jiangsu and Nguyen Khoi Tran, "Application of Blockchain Technology in Sustainable Energy Systems: An Overview, 2 August 2018; Accepted: 26 August
- [8] Z.Zheng, S. Xie, H. Dai, X. Chen and H. Wang, An overview of blockchain technology:Architecture, consensus, and future trends, in Big Data (BigData Congress), 2017 IEEEInternational Congress on, IEEE, 2017, 557–564.
- [9] Y. Lu, "The blockchain: State-of-the-art and research challenges," Journal of Industrial Information Integration, 2019.
- [10] A.S.Elmaghraby and M. M. Losavio, Cyber security challenges in smart cities: Safety, security and privacy, Journal of Advanced Research, 5 (2014), 491–497
- [11] L. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018, pp. 1545-1550.
- [12] Ms. Ketki R. Ingole , Ms. Sheetal Yamde, " Blockchain Technology in Cloud Computing : A Systematic Review", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 04 | Apr-2018

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

- [13] Blockchan: Opportunities for Health Care https://www.healthit.gov/sites/default/files/4-37_hhs_blockchain_challenge_deloitte_consulting_llp.pdf
- [14] Wubing Chen, Zhiying Xu, Shuyu Shi, Yang Zhao, Jun Zhao, "A Survey of Blockchain Applications in Different Domains".
- [15] Merz, M. Potential of the blockchain technology in energy trading. Burgwinkel, Daniel. Blockchain Technology Introduction for Business and IT Managers. de Gruyter, 2016.
- [16] Dütsch, G, and Steinecke, N. Use cases for blockchain technology in energy and commodity trading. Snapshot of current developments of blockchain in the energy and commodity sector. pwc, 2017.
- [17] L. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, "Big data model of security sharing based on blockchain," in 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM), 2017, pp. 117-121.
- [18] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," Journal of Network and Computer Applications, 2018.
- [19] R. Yuan, Y.-B. Xia, H.-B. Chen, B.-Y. Zang, and J. Xie, "Shadoweth: Private smart contract on public blockchain," Journal of Computer Science and Technology, vol. 33, pp. 542-556, 2018.
- [20] T. McConaghy, R. Marques, A. Müller, D. De Jonghe, T. McConaghy, G. McMullen, et al., "BigchainDB: a scalable blockchain database," white paper, BigChainDB, 2016.
- [21] M. S. Sahoo and P. K. Baruah, "HBasechainDB—A Scalable Blockchain Framework on Hadoop Ecosystem," in Asian Conference on Supercomputing Frontiers, 2018, pp. 18-29.
- [22] <https://www.leewayhertz.com/blockchain-platforms-for-top-blockchain-companies/>
- [23] <https://medium.com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b>
- [24] <https://www.upgrad.com/blog/top-blockchain-tools/>
- [25] <https://www.codementor.io/learn/blockchain/development-tools>
- [26] <https://101blockchains.com/blockchain-protocol/>
- [27] <https://www.sciencedirect.com/science/article/pii/S240595951930164X>
- [28] <https://builtin.com/blockchain/blockchain-applications>
- [29] Dr Mark vanRijmenam, "7 Blockchain Challenges to be Solved before Large-Scale Deployment," medium.com, para. 3, Sep. 26, 2019. [Online]. Available: <https://medium.com/dataseries/7-blockchain-challenges-to-be-solved-before-large-scale-deployment-3e45b47eee6>. [Accessed Dec. 12, 2019].
- [30] L. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018, pp. 1545-1550.
- [31] A. V. Hazarika, G. J. S. R. Ram, and E. Jain, "Performance comparison of Hadoop and spark engine," in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017, pp. 671-674.
- [32] Ray S. Merkle trees. <https://hackernoon.com/merkle-trees-181cb4bc30b4>. Accessed December 1, 2018.
- [33] The Bitcoin Project. Bitcoin Developer Guide. <https://bitcoin.org/en/developer-guide>. Accessed December 1, 2018.
- [34] Oxford University Press. English Oxford Dictionaries. <https://en.oxforddictionaries.com/english>. Accessed July 1, 2017.
- [35] Nagpal R. 17 blockchain platforms—a brief introduction. Brave New Coin. April 17, 2017. <https://bravenewcoin.com/insights/17blockchainplatforms-a-brief-introduction>. Accessed July 1, 2017.
- [36] Purkayastha S. Eight blockchain platforms for rapid prototyping. Radio-Studio. <http://radiostud.io/eight-blockchain-platforms-comparison/>. Accessed July 1, 2017.
- [37] Kelsey J. Introduction to Blockchains. ONC/NIST Use of Blockchain in Healthcare and Research Workshop. Gaithersburg, MD: ONC/NIST; 2016.
- [38] The Bitcoin Project. Bitcoin. <https://bitcoin.org/en/>. Accessed July 1, 2017.
- [39] Zerocoin Electric Coin Company. Zcash. <https://z.cash/technology/index.html>. Accessed July 1, 2017.
- [40] Moser M. Anonymity of bitcoin transactions. In: Proceedings of Münster Bitcoin Conference. Münster, Germany; 2013: 17–8.
- [41] Biryukov A, Khovratovich D, Pustogarov I. Deanonymisation of clients in Bitcoin P2P network. In: 2014 ACM SIGSAC Conference on Computer and Communications Security. Scottsdale, AZ: ACM; 2014: 15–29.
- [42] Ludwin A. How anonymous is bitcoin? <https://coincenter.org/entry/how-anonymous-is-bitcoin>. Accessed July 1, 2017.

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

- [43] Abbas A. Understanding privacy: how anonymous can bitcoin payments be? <http://bitcoinist.com/understanding-privacy-anonymous-bitcoin/>. Accessed July 1, 2017.
- [44] Bowe S, Hornby T, Wilcox N. Zcash protocol specification. <https://github.com/zcash/zips/blob/master/protocol/protocol.pdf>. Accessed July 1, 2017.
- [45] Avi Mizrahi. Zcoin creates algorithm to avoid bitcoin's mining centralization problem. Finance Magnates Ltd. <https://www.financemagnates.com/cryptocurrency/innovation/zcoin-creates-algorithm-avoid-bitcoins-mining-centralization-problem/>. Accessed July 1, 2017.
- [46] The Litecoin Project. Litecoin—open source P2P digital currency. <https://litecoin.org/>. Accessed July 1, 2017.
- [47] Dash Core Group, Inc. What is dash? <https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146914/WhatIsDash>. Accessed July 1, 2017.
- [48] The Bitcoin Wiki. Bitcoin Script Examples. https://en.bitcoin.it/wiki/Script-Script_examples. Accessed July 1, 2017.
- [49] Ripple Labs Inc. Decentralized cryptocurrency blockchain daemon implementing the XRP Ledger in Cpp. <https://github.com/ripple/rippled>. Accessed July 1, 2017.
- [50] Cohen D, Schwartz D, Britt A. The XRP ledger consensus process. <https://ripple.com/build/xrp-ledger-consensus-process/>. Accessed July 1, 2017.
- [51] Schwartz D, Youngs N, Britto A. The ripple protocol consensus algorithm. 2014. https://ripple.com/files/ripple_consensus_whitepaper.pdf. Accessed July 1, 2017.
- [52] Karame GO, Androulaki E. Bitcoin and blockchain security artech house information security and privacy series. Artech House; 2016.
- [53] The Bitcoin Project. Some things you need to know. <https://bitcoin.org/en/you-need-to-know>. Accessed July 1, 2017.
- [54] Dash Core Group, Inc. How to use PrivateSend. <https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1867847/HowtoUsePrivateSend>. Accessed July 31, 2017.
- [55] Wood G. Ethereum: a secure decentralised generalised transaction ledger. <http://gavwood.com/paper.pdf>. Accessed July 31, 2017.
- [56] Kraken. Dash Instant-Send and InstantX. <https://support.kraken.com/hc/en-us/articles/115005481948-Dash-Instant-Send-and-InstantX>. Accessed July 1, 2017.
- [57] The Bitcoin Wiki. Controlled supply. https://en.bitcoin.it/wiki/Controlled_supply. Accessed July 1, 2017.
- [58] Buntinx JP. Ethereum not having a supply cap is not such a big deal. <http://www.fintechist.com/ethereum-not-supply-cap-not-big-deal/>. Accessed July 1, 2017.
- [59] Parker L. Zcash momentarily becomes the world's most valuable cryptocurrency. <https://bravenewcoin.com/insights/zcash-momentarily-becomes-the-worlds-most-valuable-cryptocurrency>. Accessed July 1, 2017.
- [60] The Dash Network. Dash (dash.org) - First Self-Funding Self-Governing Crypto Currency. <https://bitcointalk.org/index.php?topic%4421615.0>. Accessed July 1, 2017.
- [61] The Peercoin Developers and the Bitcoin Developers. Peercoin FAQ. <https://github.com/peercoin/peercoin/wiki/FAQ>. Accessed July 31, 2017.
- [62] Buntinx JP. Top 5 cryptocurrencies that can't be mined. <https://themerkle.com/top-5-cryptocurrencies-that-cant-be-mined/>. Accessed July 1, 2017.
- [63] Levy A. Bitcoin rival Ripple is suddenly sitting on billions of dollars worth of cryptocurrency. <https://www.cnn.com/2017/05/26/bitcoin-rival-ripple-is-sitting-on-many-billions-of-dollars-of-xrp.html>. Accessed July 1, 2017.
- [64] MoneroInfo.org. MoneroInfo. <https://moneroinfo.org/eng-about/>. Accessed July 1, 2017.
- [65] BitInfoChart. Bitcoin Transactions Historical Chart. <https://bitinfocharts.com/comparison/bitcoin-transactions.html#3m>. Accessed December 5, 2017.
- [66] Ripple Labs, Inc. XRP Charts - Network Metrics. <https://xrpcharts.ripple.com/#/metrics>. Accessed December 5, 2017.
- [67] GreenspanG.MultiChain, 1.0 beta 2 and 2.0 roadmap. Coin Sciences Ltd. <https://www.multichain.com/blog/2017/06/multichain-1-beta-2-roadmap/>. Accessed December 5, 2017.
- [68] Androulaki E. et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference. New York: Association for Computing Machinery; 2018.
- [69] The Ethereum Community. The Solidity Language. <https://github.com/ethereum/solidity>. Accessed July 1, 2017.



18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

- [70] The Ethereum Community. Ethereum: programming languages intro. <https://github.com/ethereum/wiki/wiki/Programming-languages-intro>. Accessed December 1, 2018.
- [71] Nakamoto S and the Bitcoin Core Developers. Zcash Script. <https://github.com/zcash/zcash/blob/master/src/script/script.cpp>. Accessed July 1, 2017.
- [72] Nakamoto S and the Bitcoin Core Developers. Litecoin Script. <https://n.github.com/litecoin-project/litecoin/blob/master/src/script/script.cpp>. Accessed July 1, 2017.
- [73] Nakamoto S and the Bitcoin Core Developers. Dash Script. <https://github.com/dashpay/dash/blob/master/src/script/script.cpp>. Accessed July 1, 2017.
- [74] Nakamoto S, the Bitcoin Core Developers, and the Peercoin Developers. Peercoin Script. <https://github.com/peercoin/peercoin/blob/master/src/script.cpp>. Accessed July 1, 2017.
- [75] Peercointalk. Peercoin's Potential. <https://talk.peercoin.net/t/peercoinspotential/3964>. Accessed July 1, 2017.
- [76] Codius. CODIUS - Where Smart Programs Live. <https://codius.org/>. Accessed July 1, 2017.
- [77] Coin Sciences Ltd. Native assets in MultiChain. <https://www.multichain.com/developers/native-assets/>. Accessed July 1, 2017.
- [78] Nakamoto S, the Bitcoin Core Developers, and Coin Sciences Ltd. Multi-Chain Script. <https://github.com/MultiChain/multichain/blob/master/src/script/script.cpp>. Accessed July 1, 2017.
- [79] The Linux Foundation. Hyperledger Architecture, Volume II: Smart Contracts. https://www.hyperledger.org/wpcontent/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf. Accessed December 1, 2018.
- [80] Wikipedia. List of Cryptocurrencies. https://en.wikipedia.org/wiki/List_of_cryptocurrencies. Accessed July 1, 2017.
- [81] CryptoCompare.com. Live cryptocurrency prices, trades, volumes, forums, wallets, mining equipment, and reviews. <https://www.cryptocompare.com/>. Accessed October 1, 2018.
- [82] The Bitcoin Wiki. Bitcoin Script Examples. https://en.bitcoin.it/wiki/Script-Script_examples. Accessed July 1, 2017.