A Future Perspective of Blockchain Technology, It's Design And Implementations

Ch.Venkata Ramana [#1], **M.V.Rajesh** [*2], **B.Preethi Devi** [#3]
Faculty of Department of Information Technology, Pragati Engineering College
Surampalem, India
[1]ramana.ch@pragati.ac.in
[2]rajesh.mv@pragati.ac.in
[3]preethidevi.b@pragati.ac.in

Abstract: ***Bitcoin is the predecessor for the blockchain technolog that has gain more attention in recent times.Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner. Blockchain applications are numerous including Internet of Things (IoT), eliminating trusted third parties, digital advertisement and so on. However there are some problems still arise with this technology which slowdown the growth of this like security and scalability. This paper presents blockchain technology architectures, algorithms and latest trends and it's future involvement in its growth and technical challenges.***

Keywords—Blockchain, decentralization, scalability, security, Internet of Things

I. INTRODUCTION

In current situation cryptocurrency has become a buzzword in both industry and academia and Bitcoin was the most popular and successful cryptocurrency with a huge capital market of 10 billion dollors in 2016[1]. This network can eliminate any third party and the Building block for this bitcoin is Blockchain.Blockchain could be regarded as a public ledger and all committed transactions are stored in a list of blocks.This chaingrows as new blocks are appended to it continuously.cryptography and distributed algorithms have been implemented for user security and ledger consistency. Blockchain allows the users to do payment [3],[4] without any intervention of bank , financial institutions or any intermediary and it is used in various financial services like online payment[3] ,digital assets. It can also be usede in Internet of Things (IoT) [7] and public services [9].Blockchain is immutable. Transaction cannot be tampered once it is packed into the blockchain. Businesses that require high reliability and honesty can use blockchain to attract customers. Besides, blockchain is distributed and can avoid the single point of failure situation. Although blockchain has more potentiality over future internet growth, it has some limits like scalability where Bitcoin block size is 1 MB, subsequently bitcoin network is restricted to have only seven transactinons oer second which is incapable in dealing with frequency trading. However larger blocks mean larger storage space and reduced movement in the network. Miners could also have larger revenue than their actual fair through selfish mining strategy [10]. So solutions for these problems need to be put forward to fix them. Current algorithms like proof of work or proof of stake are facing some serious problems, There is a lot of literature on blockchain from various sources, such as blogs, wikis, forum posts, codes, conference proceedings and journal articles. Tschorsch et al. [12] made a technical survey about decentralized digital currencies including Bitcoin. Compared to [12], our paper focuses on blockchain technology

instead of digital currencies. Nomura Research Institute made a technical report about blockchain [13]. Contrast to [13], our paper focuses on state-of-art blockchain researches including recent advances and future trends. This paper is organized as follows. Section II contains blockchain architectures, Section III shows some algorithms used in blockchain, section IV summarizes its challenges. Section V includes future trends and section VI concludes the paper.

II. BLOCKCHAIN ARCHITECTURE

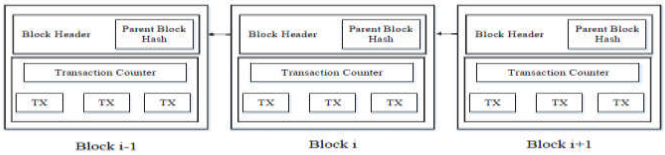

Fig. 1: An example of blockchain which consists of a continuous sequence of blocks.

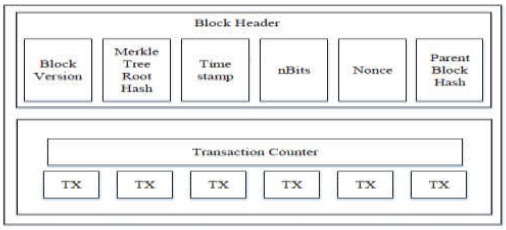

Fig. 2: Block structure

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger [14]. Figure 1 illustrates an example of a blockchain. With a previous block hash contained in the block header, a block has only one parent block. It is worth noting that uncle blocks (children of the block's ancestors) hashes would also be stored in ethereum blockchain [15]. The first block of a blockchain is called genesis block which has no parent block. We then explain the internals of blockchain in details.

A. Block A block consists of the block header and the block body as shown in Figure 2. In particular, the block header includes :(i) Block version: indicates which set of block validation rules to follow. (ii) Merkle tree root hash: the hash value of all the transactions in the block. (iii) Timestamp: current time as seconds in universal time since January 1, 1970. (iv) nBits: target threshold of a valid block hash. (v) Nonce: an 4-byte field, which usually starts with 0 and increases for every hash calculation (will be explained in details in Section III). (vi) Parent block hash: a 256-bit hash values that point to the previous block. The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions [13]. Digital signature based on asymmetric cryptography is used in an untrustworthy environment. We next briefly illustrate digital signature.

B. Digital Signature Each user owns a pair of private key and public key. The private key that shall be kept in confidentiality is used to sign the transactions. The digital signed transactions are broadcasted throughout the whole network. The typical digital signature is involved with two phases: signing phase and verification phase. For instance, an user Alice wants to send another user Bob a message. (1) In the signing phase, Alice encrypts her data with her private key and sends Bob the encrypted result and original data. (2) In the verification phase, Bob validates the value with Alice's public key. In that way, Bob could easily check if the data has been tampered or not. The typical digital signature algorithm used in blockchains is the elliptic curve digital signature algorithm (ECDSA) [16].

C. Key Characteristics of Blockchain In summary, blockchain has following key characteristics.

• *Decentralization.* In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank), inevitably resulting to the cost and the performance bottlenecks at the central servers. Contrast to the centralized mode, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain data consistency in distributed network.

• *Persistency.* Transactions can be validated quickly and invalid transactions would not be admitted by honest miners. It is nearly impossible to delete or rollback transactions once they are included in the blockchain. Blocks that contain invalid transactions could be discovered immediately.

• *Anonymity.* Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user. Note that blockchain cannot guarantee the perfect privacy preservation due to the intrinsic constraint.

III. BLOCKCHAIN ALGORITHMS

In blockchain, how to reach consensus among the untrustworthy nodes is a transformation of the Byzantine Generals (BG) Problem, which was raised in [20]. In BG problem, a group of generals who command a portion of Byzantine army circle the city. Some generals prefer to attack while other generals prefer to retreat. However, the attack would fail if only part of the generals attack the city. Thus, they have to reach an agreement to attack or retreat. How to reach a consensus in distributed environment is a challenge. It is also a challenge for blockchain as the blockchain network is distributed. In blockchain, there is no central node that ensures ledgers on distributed nodes are all the same. Some protocols are needed to ensure ledgers in different nodes are consistent. We next present several common approaches to reach a consensus in blockchain.

Approaches to consensus PoW (Proof of work) is a consensus strategy used in the Bitcoin network [2]. In a decentralized network, someone has to be selected to record the transactions. The easiest way is random selection. However, random selection is vulnerable to attacks. So if a node wants to publish a block of transactions, a lot of work

has to be done to prove that the node is not likely to attack the network. Generally the work means computer calculat ions

TABLE II: Typical Consensus Algorithms Comparison

Property	PoW	PoS	PBFT	DPOS	Ripple	Tendermint
Node Identity management	open	open	permissioned	open	open	permissioned
Energy saving	no	partial	yes	partial	yes	yes
Tolerated power of adversary	< 25% computing power	< 51% stake	< 33.3% faulty replicas	< 51% validators	< 20% faulty nodes in UNL	< 33.3% byzantine voting power
Example	Bitcoin [2]	Peercoin [21]	Hyperledger Fabric [18]	Bitshares [22]	Ripple [23]	Tendermint [24]

richest person is bound to be dominant in the network. As a result, many solutions are proposed with the combination of the stake size to decide which one to forge the next block. In particular, Blackcoin [26] uses randomization to predict the next generator. It uses a formula that looks for the lowest hash value in combination with the size of the stake. Peercoin [21] favors coin age based selection. In Peercoin, older and larger sets of coins

have a greater probability of mining the next block. Compared to PoW, PoS saves more energy and is more effective. Unfortunately, as the mining cost is nearly zero, attacks might come as a consequence. Many blockchains adopt PoW at the beginning and transform to PoS gradually. For instance, ethereum is planing to move from Ethash (a kind of PoW) [27] to Casper (a kind of PoS) [28]. PBFT (Practical byzantine fault tolerance) is a replication algorithm to tolerate byzantine faults [29]. Hyperledger Fabric [18] utilizes the PBFT as its consensus algorithm since PBFT could handle up to 1/3 malicious byzantine replicas. A new block is determined in a round. In each round, a primary would be selected according to some rules. And it is responsible for ordering the transaction. The whole process could be divided into three phase: pre-prepared, prepared and commit. In each phase, a node would enter next phase if it has received votes from over 2/3 of all nodes. So PBFT requires that every node is known to the network. Like PBFT, Stellar Consensus Protocol (SCP) [30] is also a Byzantine greement protocol. In PBFT, each node has to query other nodes while SCP gives participants the right to choose which set of other participants to believe. Based on PBFT, Antshares [31] has implemented their dBFT (delegated byzantine fault tolerance). In dBFT, some professional nodes are voted to record the transactions. DPOS (Delegated proof of stake). The major difference between PoS and DPOS is that PoS is direct democratic while DPOS is representative democratic. Stakeholders elect their delegates to generate and validate blocks. With significantly fewer nodes to validate the block, the block could be confirmed quickly, leading to the quick confirmation of transactions. Meanwhile, the In the network, nodes are divided into two types: server for participating consensus process and client for only transferring funds. Each server has an Unique Node List (UNL). UNL is important to the server. When determining whether to put a transaction into the ledger, the server would query the nodes in UNL and if the received agreements have reached 80%, the transaction would be packed into the ledger. For a node, the ledger will remain correct as long as the percentage of faulty nodes in UNL is less than 20%. Tendermint [24] is a byzantine consensus algorithm. A new block is determined in a round. A proposer would be selected to broadcast an unconfirmed block in this round. It could be divided into three steps: 1) Prevote step. Validators choose whether to broadcast a prevote for the proposed block. 2) Precommit step. If the node has received more than 2/3 of prevotes on the proposed block, it broadcasts a precommit for that block. If the node has received over 2/3 of precommits, it enters the commit step. 3) Commit step. The node validates the block and broadcasts a commit for that block. If the node has received 2/3 of the commits, it accepts the block. Contrast to PBFT, nodes has to lock their coins to become validators. Once a validator is found to be dishonest, it would be punished. B. Consensus algorithms comparison Different consensus algorithms have different advantages and disadvantages. Table II gives a comparison between different consensus algorithms and we use the properties given by [32].

• Node identity management.

• Energy saving.

• Tolerated power of adversary.

IV. CHALLENGES

Therer are many challenges which limits the usage of blockchainBlockchain enables new ways of exchanging value securely while ensuring a reliable transaction. It enables people to meter excess capacity and facilitates non-traditional ways of generating income. Despite all the benefits, there are some challenges that the technology needs to address. . Some major challenges and recent advances as follows.

- Because of all the hype surrounding Bitcoin and other digital currencies, blockchain started appearing like a pyramid scheme.
- The technology is yet to mature and is susceptible to capacity problems, system failure, unanticipated bugs, and perhaps most damaging, the huge disappointment of technically unsophisticated users.
- The bitcoin blockchain lacks transactional capacity. Some suggest that the way to mitigate this is by using other consensus algorithms. Another way is to use a sidechain which is a fork of a larger blockchain like bitcoin, while using the parent blockchain's infrastructure.
- Transactions on the blockchain are immutable which creates a system that is a bit sociopathic. Immutability is a double edged sword.
- Much work needs to be done in basic interface and experience. A bitcoin address is an alphanumeric code. You don't type an IP address to access a website, why would you then type an alphanumeric code to access a bitcoin wallet.
- There is a rule of thumb: for every dollar a computer burns electricity, it needs fifty cents to cool down. The bitcoin network consumes vast amounts of energy. Many argue that this computation and energy could be diverted to much nobler pursuits like curing cancer or solving world hunger. Beyond a point, the energy consumption will be unsustainable. To manage this, we will have to move away from proof of work or hardware would improve. Access to renewable energy could also mitigate this.
- In the short run, it'll cut jobs. In the long run, it'll put Uber out of a job.
- If everything is recorded, it leaves no room for serendipity.
- Blockchain after all is a tool and can be used for nefarious purposes. Closed blockchains which are secure and essentially unhackable could bring us back to the problem of lack of transparency and trust in institutions. It might fall into the same trap of concentration of power that the internet did.

V. POSSIBLE FUTURE ADVANCEMENTS

The future of finance could be dominated by blockchain technologies. A traceable global currency complete with an efficient infrastructure will not only result in massive cost reduction for all market participants, it will change global banking. Bitcoin will do for payments what email did for communication.

What is changing?

- Blockchain will be adopted by central banks and cryptographically secured currencies will become widely used.
- Nasdaq will launch blockchain-enabled digital ledger technology that will be used to expand and enhance the equity management capabilities offered by its Nasdaq Private Market platform.
- The settlement of currency, equity and fixed income trades almost instantaneously through permissioned distributed ledgers creates a significant opportunity for banks to drive efficiency and potentially create new asset classes.

Control

New technologies such as blockchain have the potential to reduce cyber risks by offering identity authentication through a visible ledger.There is no reason why requirements for numbering, maintaining and indexing records and

communicating information provided in records could not be met through an electronic ledger system.Car rental agencies could use smart contracts that automatically allow rentals when payment's received and insurance information is confirmed through a blockchain record.A refrigerator equipped with sensors and connected to the Internet could use blockchain to manage automated interactions with the external world-anything from ordering and paying for food to arranging for its own software upgrades and tracking its warranty.Small businesses could use blockchain to create trusted trading platforms among themselves.Blockchain could potentially help bring robustness and transparency to the post-trade environment.New technologies such as blockchain have the potential to reduce cyber risks by offering identity authentication through a visible ledger.A bank could pay the supplier instantly over the Internet.

Crime

A new blockchain startup has claimed its software could help track down criminals faster and cheaper than ever.Connecticut are warning parents that a new Darknet cryptocurrency called Bitcoin could be to blame for helping underage drinkers to get buzzed.Implications

Banks.

Blockchain will be adopted by central banks and cryptographically secured currencies will become widely used.Blockchain could replace central banks.Real risks remain for banks that choose to get involved with cryptocurrency firms.Blockchain technology could reduce the UBS's infrastructure costs in cross-border payments, securities trading and regulatory compliance by as much as $20 billion a year by 2022.The number of applications within and outside the banks could be reduced as the Blockchain transaction contains all relevant information for the successful transfer of assets and/or related contracts.Deutsche bank's economist sees blockchain as a threat because of the lack of the IT infrastructure to support the technology involved.Ethereum is much more general purpose than bitcoin and could be useful for banks.The future of finance in many nations could be dominated by Bitcoin and cryptocurrencies.A private blockchain run by banks could end up as just "another cartel" and function as poorly as the payments consortium.Banks could become the "custodians of cryptographic keys".The blockchain could save lenders up to $20 billion annually in settlement. Blockchain technology could be used to bypass today's centralised financial infrastructure entirely.

VI Conclusion

Blockchain has shown its potential for transforming traditional industry with its key characteristics: decentralization, persistency, anonymity and auditability. In this paper, we present a comprehensive overview on blockchain. We first give an overview of blockchain technologies including blockchain architecture and key characteristics of blockchain. We then discuss the typical algorithms used in blockchain. Furthermore, we listed some challenges and problems that would hinder blockchain development and summarized some existing approaches for solving these problems. Some possible future directions are also proposed.

References

1. *https://ieeexplore.ieee.org/document/8029379/*
2. *"State Of Blockchain Q1 2016: Blockchain Funding Overtakes Bitcoin," 2016. [Online]. Available: Http://Www.Coindesk.Com/ State-Of-Blockchain- Q1-2016/*

3 S. Nakamoto, "Bitcoin: A Peer-To-Peer Electronic Cash System," 2008. [Online]. Available: Https://Bitcoin.Org/Bitcoin.Pdf

4.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

5 G. Foroglou And A.-L. Tsilidou, "Further Applications Of The Blockchain,"2015.

6. 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.

7. 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

8. 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.

9. 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.

10 C. Noyes, "Bitav: Fast Anti-Malware By Distributed Blockchain Consensus And Feedforward Scanning," Arxiv Preprint Arxiv:1601.01405, 2016.

11 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.

12 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.

13 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.

14 Nri, "Survey On Blockchain Technologies And Related Services," Tech. Rep., 2015. [Online]. Available: Http://Www.Meti.Go.Jp/English/Press/ 2016/Pdf/0531 01f.Pdf

15 D. Lee Kuo Chuen, Ed., Handbook Of Digital Currency, 1st Ed. Elsevier, 2015. [Online]. Available: Http://Econpapers.Repec.Org/Repec: Eee:Monogr:9780128021170

16 V. Buterin, "A Next-Generation Smart Contract And Decentralized Application Platform," White Paper, 2014.

17 D. Johnson, A. Menezes, And S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (Ecdsa)," International Journal Of Information Security, Vol. 1, No. 1, Pp. 36–63, 2001.

18 V. Buterin, "On Public And Private Blockchains," 2015. [Online]. Available: Https://Blog.Ethereum.Org/2015/08/07/ On-Public-And-Private-Blockchains/

19 "Hyperledger Project," 2015. [Online]. Available: Https://Www. Hyperledger.Org/

20 "Consortium Chain Development." [Online]. Available: Https://Github. Com/Ethereum/Wiki/Wiki/Consortium-Chain-Development

21 L. Lamport, R. Shostak, And M. Pease, "The Byzantine Generals Problem," Acm Transactions On Programming Languages And Systems (Toplas), Vol. 4, No. 3, Pp. 382–401, 1982.

22 S. King And S. Nadal, "Ppcoin: Peer-To-Peer Crypto-Currency With Proofof- Stake," Self-Published Paper, August, Vol. 19, 2012.

23 "Bitshares - Your Share In The Decentralized Exchange." [Online]. Available: Https://Bitshares.Org/

24 D. Schwartz, N. Youngs, And A. Britto, "The Ripple Protocol Consensus Algorithm," Ripple Labs Inc White Paper, Vol. 5, 2014.

25. *J. Kwon, "Tendermint: Consensus Without Mining," Url Http://Tendermint. Com/Docs/Tendermint { } V04. Pdf, 2014.*

26 *S. King, "Primecoin: Cryptocurrency With Prime Number Proof-Of -Work," July 7th, 2013.*

27. *Blockchain Revolution By Alex Tapscott And Don Tapscott*

28. *Who Owns The Future? By Jaron Lanier*

29. *Smart Cities: Big Data, Civic Hackers, And The Quest For A New Utopia By Anthony M. Townsend*

30. *The Laws Of Simplicity By John Maeda*

31. *How The Blockchain Is Changing Money And Business By Don Tapscott (Ted Talk)*

32. *How The Blockchain Will Radically Transform The Economy By Bettina Warburg (Ted Talk)*

33. *Https://Www.Shapingtomorrow.Com/Home/Alert/665529-Future-Of--Blockchain*

Author(s) Profile

CH VENKATA RAMANA received the M Tech degree from JNTUK, Jawaharlal Nehru Technological University, Kakinada in 2013, Currently he is working as Assistant Professor in PRAGATI Engineering College, Surampalem, Andhra Pradesh, India. He has five years of experience in teaching and five years of experience in software industry. His research interests include object oriented programming, cloud computing, parallel programming, Internet of Things, Deep Learning.

M V RAJESH received the M Tech degree from JNTUCE,K,Jawaharlal Nehru Technological University, Hyderabad in 2006. Currently he is working as Associate Professor in PRAGATI Engineering College, Surampalem, Andhra Pradesh, India. He has nine years of experience in teaching and five years of experience in software industry. Previously he has worked with SIEMENS Information Systems Ltd, as Associate Consultant in the role of Software Developer in the HealthCare domain. His research interests include cloud computing, parallel programming and Data mining.

B PREETHI DEVI received the M Tech degree from JNTUK, Jawaharlal Nehru Technological University, Kakinada in 2015, and Currently She is working as Assistant Professor in PRAGATI Engineering College, Surampalem, Andhra Pradesh, India. She has three years of experience in teaching. Her research interests include object oriented programming, cloud computing, Artificial Intelligence.