Blockchain Architecture and Consensus Mechanisms: Challenges, Innovations, and Future Trends

Nancy Sethi
Assistant Professor, CSE
Inderprastha Engineering College, Ghaziabad

ABSTRACT
Bitcoin's underlying era, blockchain, has attracted quite a few interests recently. Blockchain acts as an immutable ledger that permits decentralized transaction processing. A growing number of industries, consisting of monetary offerings, reputation management, and the internet of things (IoT), are relying on blockchain technology. Blockchain era still faces several boundaries, inclusive of scalability and security problems that want to be addressed. This paper presents an intensive introduction to blockchain technology. First, we provide a brief creation to blockchain architecture earlier than contrasting some not unusual consensus methods utilized in diverse blockchains. We also in short evaluate the technical difficulties and recent advances. We additionally define capability blockchain traits for the destiny.

Keywords
Scalability, decentralization, consensus, and blockchain

1. INTRODUCTION
The time period "cryptocurrency" has recently won reputation in each commercial enterprise and academia. Bitcoin is one of the maximum successful cryptocurrencies, with its capital market exceeding $10 billion in 2016 [1]. The key technology used to increase Bitcoin is the blockchain, which became first proposed in 2008 and delivered in 2009 [2]. With a particularly designed information storage shape, transactions on the Bitcoin network ought to take area without the involvement of a third celebration. All showed transactions are recorded in a listing of blocks on the blockchain, which can be concept of as a public ledger. This chain expands as new blocks are constantly introduced. For consumer safety and ledger consistency, uneven cryptography and distributed consensus algorithms have been used.

Blockchain can be used in a diffusion of financial offerings, including digital assets, remittances, and online payments, because it lets in payments to be processed without the use of a financial institution or different intermediary [3], [4]. It may also be used in other industries, such as clever contracts, public offerings, and the internet of things, recognition structures. These industries benefit from Blockchain in numerous methods. Blockchain is immutable, first. Once a transaction is saved in Blockchain, it cannot be changed. Blockchain may be utilized by agencies that want to be very dependable and honest so as to appeal to customers. Also, seeing that Blockchain is decentralized, it can save single points of failure. even though blockchain generation offers a good deal capability for the improvement of future net services, there are some of technical difficulties it must triumph over. initially, scalability is a major trouble. presently, a Bitcoin block can handiest be 1 MB in length, and a block is mined about every 10 minutes. As an end result, the Bitcoin community can simplest technique 7 transactions in line with 2d, making it not able to address high-frequency buying and selling. but larger blocks require extra garage space and propagate more slowly across the network. The increasing centralization that effects from fewer and fewer users looking to preserve one of these massive blockchain will reason this to appear. As an end result, it has tested hard to stability block length and safety. Second, it has been proven that egocentric mining strategies can cause miners making more money than is truthful [10] and be able to make more money in the future, miners conceal their extracted blocks. In this situation, forking could arise frequently, which would slow down the improvement of the blockchain. Consequently, a few treatments want to be proposed to solve this problem. Further, it's been shown that privateness leakage can occur in blockchain although users only use their public and private keys for transactions [11]. Further, there are numerous widespread problems with cutting-edge consensus techniques including proof of work and evidence of Stake. As an example, the proof of Stake consensus technique can also display the anomaly that the wealthy get richer, while proof of labor wastes excessive electricity.

Numerous resources, consisting of blogs, wikis, discussion board postings, codes, conference proceedings, and journal articles, have a wealth of information on blockchain. A technical study on decentralized digital currencies, which include Bitcoin, become performed through Tschorsch et al. [12]. It specializes in blockchain technology instead of digital currencies. A technical report on blockchain was published by way of the Nomura studies Institute [13]. It focused on blockchain research, encompassing present day advancements and rising traits.

The blockchain architecture is introduced in segment 2. The common consensus algorithms used in blockchain are displayed in segment 3. The technological difficulties and maximum recent traits in this discipline are summarized in section 4. The paper is concluded in segment 6 after phase 5 explores a few potential destiny instructions.

Numerous sources, including blogs, wikis, forum postings, codes, conference proceedings, and journal articles, have a wealth of information on blockchain. A technical study on decentralized digital currencies, such as Bitcoin, was conducted by Tschorsch et al. [12]. Our study differs from [12] in that it focuses on blockchain technology rather than virtual currencies. A technical report on blockchain was published by the Nomura Research Institute [13]. Study is focused on cutting-edge blockchain research, encompassing current advancements and emerging developments.

The blockchain architecture is introduced in Section 2. The common consensus algorithms used in blockchain are displayed in Section 3. The technological difficulties and most recent developments in this field are summarized in Section 4. The paper is concluded in section 7 after section 5 explores some prospective future directions.

2. BLOCKCHAIN ARCHITECTURE

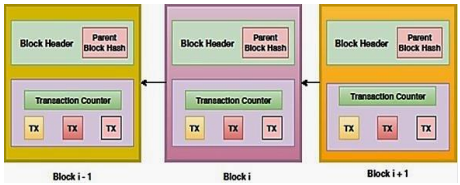

Fig. 1: An example of blockchain which consists of a continuous sequence of blocks.

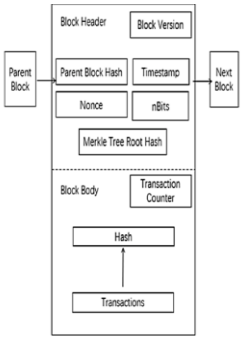

Fig. 2: Block internal structure

Blockchain is a series of blocks like a traditional public ledger, contains an exhaustive list of transaction records [14]. A blockchain is shown as an example in Figure 1. A block only has one parent block if the block header contains a preceding block hash. The internals of blockchain are then thoroughly explained.

2.1 Block

A block consists of the block header and the block body as proven in figure 2. particularly, the block header consists of:

(i) Block version: Specifies which set of block validation tips to use.

(ii) Merkle tree root hash: the sum of all the block's transactions.

(iii) Timestamp: the modern time expressed in seconds relative to the start of astronomical time

(iv) nBits: the preferred minimal length of a legitimate block hash.

(v) Nonce: a 4-byte subject that normally starts with 0 and rises with every hash computation (in addition records about as soon as is furnished in section III).

(vi) A 256-bit hash fee that refers to the previous block is the discern block hash.

A transaction counter and transactions make up the block frame. relying at the block length and the size of each transaction, a block can incorporate a maximum wide variety of transactions. Blockchain validates the authenticity of transactions via an asymmetric cryptography algorithm [13]. In an unreliable environment, asymmetrical virtual signatures are utilized. next, we give a short example of a virtual signature.

2.2 Digital Signature

Each user as a fixed of personal and public keys. The transactions are signed the use of a private key that need to be saved secret. The transactions which have been digitally signed are disseminated across the entire network. the two steps of an ordinary virtual signature are the signing segment and the verification phase. for example, consumer Alice wants to talk with consumer Bob.

(1) Alice uses her personal key to encrypt the statistics she desires to sign, then she offers Bob each the encrypted records and the authentic records.

(2) Bob verifies the cost within the verification stage the usage of Alice's public key. Bob may additionally then quickly decide if the data has been altered or no longer. The elliptic curve is the not unusual digital signature m approach utilized in blockchains is the elliptic curve digital signature set of rules (ECDSA) [16].

2.3 Key Characteristics of Blockchain

2.3.1 Decentralization*:* Blockchain operates on a distributed network where no single entity holds control. Instead of relying on a central authority, decisions are made collectively by all participating nodes, enhancing security and reducing the risk of centralized control or failures.

2.3.2 Persistency*:* Once a transaction is recorded on the blockchain, it is permanent and unchangeable. This ensures data integrity, as the records cannot be altered or deleted, making the system highly reliable for keeping historical information.

2.3.3 Anonymity*:* Blockchain allows users to conduct transactions without revealing their real identities. Participants are identified through cryptographic addresses, ensuring privacy while still maintaining trust in the system.

2.3.4 Auditability*:* The blockchain's transparent and chronological record of all transactions makes it easy to track and verify data. This auditability ensures that every transaction can be traced back to its origin, promoting transparency and trustworthiness in the network.

Table 1: Comparisons among public blockchain, consortium blockchain and private blockchain

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	One organization
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

2.4 Taxonomy of blockchain systems

Public blockchain, personal blockchain, and consortium blockchain are the three standard classes used to describe modern blockchain systems [17]. In a public blockchain, all of us may additionally get entry to all facts and take part in the consensus method. however, in a consortium blockchain, the consensus manner might handily involve a select few nodes. regarding personal blockchain, handiest nodes from a single enterprise might be permitted to participate within the consensus procedure.

A non-public blockchain is considered as a centralized network due to the fact handiest one organization has whole control over it. on account that just a small range of nodes might be selected to decide the consensus, the consortium blockchain constructed with the aid of several businesses is simplest partially centralized. The three distinct kinds of blockchains are as compared.

2.4.1 Consensus determination- every node on a public blockchain might take part in the consensus system. And with

consortium blockchain, simplest a delegated organization of nodes are in charge of validating the block. concerning personal chains, they are absolutely under the authority of 1 agency, which has the energy to pick out the closing consensus.

2.4.2 Read permission- in relation to a private blockchain or a consortium blockchain, it relies upon if transactions are visible to most of the people.

2.4.3 Immutability- Transactions in a public blockchain are almost not possible to adjust with due to the fact information are saved on a big number of participants. alternatively, because there are fewer members in a private blockchain or a consortium blockchain, transaction.

2.4.4 Efficiency- As there are numerous nodes within the public blockchain community, it takes a long term for blocks and transactions to spread. As an end result, there's low transaction throughput and excessive latency. personal blockchain and consortium blockchain may be greater powerful with fewer validators.

2.4.5 Centralized- Public blockchains are decentralized, consortium blockchains are in part centralized, and personal blockchains are absolutely centralized since they are managed through an unmarried entity. that is the major distinction among the three types of blockchains.

2.4.6 Process of consensus- The public blockchain's consensus method is open to participation from everybody in the globe. both consortium blockchain and personal blockchain are permissioned, not like public blockchain. Public blockchain can attract many customers and companies due to the fact it's miles handy to everybody inside the globe.

Since public blockchain is accessible to everyone, it can entice a big consumer base and vibrant communities. each day, new public blockchains are created. The consortium blockchain has numerous capacity enterprise makes use of. presently, Hyperledger [18] is creating blockchain frameworks for company consortiums. moreover, Ethereum has supplied equipment for developing consortium blockchains [19].

3. CONSENSUS ALGORITHMS

The **Byzantine Generals Problem** (BGP) illustrates the challenge of achieving consensus among distributed and potentially unreliable nodes[20]. In this scenario, a group of generals commanding different divisions of the Byzantine army must decide whether to attack a city or retreat. However, some generals may have conflicting opinions, and the success of their action relies on a coordinated decision: if not all loyal generals agree to attack, the attempt will fail.

This problem translates directly to blockchain technology, where nodes in a decentralized network must reach agreement on the state of the ledger without a central authority. The challenge is further complicated by the potential for unreliable or malicious nodes, which may attempt to disrupt the consensus process.

In a blockchain, ensuring that all nodes maintain identical ledgers is crucial. To achieve this, various consensus mechanisms have been developed to address the Byzantine Fault Tolerance (BFT) problem and ensure consistency across the network.

3.1 Approaches to consensus

3.1.1 Proof of Work (PoW): Miners compete to solve complex mathematical puzzles to validate transactions and create new blocks.

Pros: High security due to the computational effort required; widely tested and proven.

Cons:Energy-intensive and environmentally unfriendly; can lead to slower transaction times.

3.1.2 Proof of Stake (PoS): Validators are chosen to create new blocks based on the number of coins they hold and are willing to "stake" as collateral.

Pros: More energy-efficient compared to PoW; incentivizes users to hold onto their tokens.

Cons: Potential centralization if a few holders dominate the stake; "nothing at stake" problem.

3.1.3 Delegated Proof of Stake (DPoS): Token holders vote to elect a small number of delegates who are responsible for validating transactions and maintaining the network.

Pros: Faster transaction times; reduced energy consumption; allows for democratic governance.

Cons: Potential for centralization if a few delegates gain too much power; risks of "vote buying."

3.1.4 Practical Byzantine Fault Tolerance (PBFT): Designed for permissioned blockchains, PBFT allows nodes to reach consensus even if some nodes are unreliable, typically requiring a two-thirds majority for agreement.

Pros: High throughput and low latency; resilient against malicious nodes.

Cons: Requires a known set of participants; can become inefficient as the number of nodes increases.

3.1.5 Proof of Authority (PoA): A limited number of pre-approved validators are responsible for validating transactions and creating blocks.

Pros: Fast and efficient; low resource consumption; suitable for private and consortium blockchains.

Cons: Centralization risk; relies on the trustworthiness of the authorities.

3.1.6 Federated Byzantine Agreement (FBA): Nodes form "quorums" and reach consensus based on a pre-selected set of trusted nodes.

Pros: Flexibility in trust assumptions; can achieve consensus with fewer messages.

Cons: Requires participants to agree on the set of trusted nodes; potential for collusion.

Conclusion

The choice of consensus mechanism significantly affects the performance, security, and decentralization of a blockchain. Each approach has its strengths and weaknesses, and the selection often depends on the specific requirements of the blockchain application being developed.

TABLE 2: Consensus Algorithms Comparison

Consensus Algorithm	Node Identity Management	Energy Saving	Tolerated Power of Adversary	Example

Proof of Work (PoW)	Pseudonymous; no central manage	High energy consumption	< 50% adversarial nodes	Bitcoin
Proof of Stake (PoS)	Identified by stake in the network	Low energy consumption	Up to 1/3 adversarial nodes	Ethereum 2.0
Delegated Proof of Stake (DPoS)	Managed through elected delegates	More energy-efficient than PoW	Up to 1/3 adversarial nodes	EOS
Practical Byzantine Fault Tolerance (PBFT)	Known identities in permissioned networks	Efficient, varies by network size	Up to 1/3 adversarial nodes	Hyperledger Fabric
Proof of Authority (PoA)	Pre-approved validators;	Very low energy consumption	Depends on the number of authorities	VeChain
Federated Byzantine Agreement (FBA)	Trusted nodes with verified identities	Efficient in terms of energy	Up to 1/3 adversarial nodes	Stellar

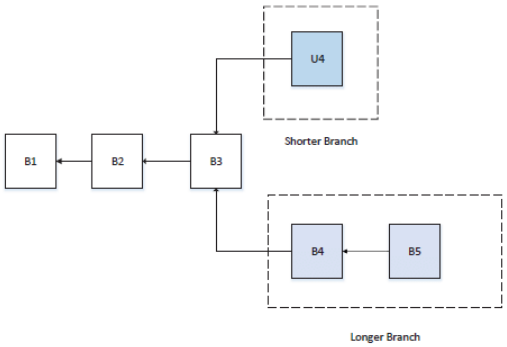

Fig. 3: Multiple Branches

Fig. 3: An example of a blockchain with multiple branches, where the longer department subsequently turns into the principle chain while the shorter department is dropped. A block header hash fee is decided by each node of the PoW community. The block header contains a nonce, which miners often modified to supply exceptional hash values. The consensus states that the predicted cost ought to be decrease than or equal to a particular given fee. the opposite nodes then need to mutually confirm that the hash value is accurate after receiving the block when a node reaches the desired price and proclaims it to all other nodes. If the block is validated, similarly miners will upload it to their individual blockchains. Miners are nodes that carry out hash calculations, and the PoW procedure is referred to as mining in Bitcoin.

In a decentralized network, legitimate blocks can be generated concurrently if numerous nodes discover the proper nonce nearly concurrently. therefore, branches much like the ones in figure three may end result. it's miles fantastic that opposing forks will generate the following block simultaneously. inside the PoW protocol, a chain that continues becoming longer is seemed as the real one. consider two forks that resulted from simultaneously validating U4 and B4 blocks. The mining process keeps till a longer branch is determined. considering that B4, B5 produces a longer chain, the miners on U4 might pass to the longer branch.

The several laptop calculations required through PoW miners devour too much system sources. so that it will lessen the loss, positive PoW protocols that allow some potential aspect-packages were created. for example, Primecoin [25] searches for specific prime wide variety sequences which can be beneficial for mathematical studies. PoS (evidence of stake) is a PoW replacement that uses less electricity. An evidence-of-stake mechanism requires miners to prove they are the rightful proprietors of the finances. its miles believed that folks who possess more currencies are less probable to attack the network. deciding on applicants primarily based entirely on account balance is extraordinarily unfair because the wealthiest candidate might inevitably dominate the community. therefore, a number of options are proven at the side of the stake quantity to choose which one can be utilized to create the following block. Black coin [26] uses unpredictability in particular to predict the destiny. It uses a component that searches for the hash value with the lowest price even as accounting for the stake amount. Peercoin prefers coin selection based totally on age [21]. Peercoin's coming near block is more likely to contain older and large corporations of currency. in comparison to PoW, PoS is greater powerful and makes use of less strength. unluckily, attacks may want to occur considering mining prices are so low. Many blockchains start out utilizing PoW and switch over to PoS over the years. As an illustration, Ethereum intends to replace from Ethash, (a sort of PoS) [28].

3.2 Advances on consensus algorithms

A terrific consensus algorithm manner efficiency, safety and comfort. these days, a number of endeavors were made to improve consensus algorithms in blockchain. New consensus algorithms are devised aiming to resolve some specific problems of blockchain. the principle concept of Peer Census [33] is to decouple block creation and transaction confirmation in order that the consensus speed may be significantly improved. except, Kraft [34] proposed a new consensus approach to make sure that a block is generated in a relatively stable speed. its miles recognized that excessive blocks generation charge compromise Bitcoin's safety. So, the greedy Heaviest-located Sub-Tree (GHOST) chain choice rule [35] is proposed to remedy this trouble. in preference to the longest branch scheme, GHOST weights the branches and miners ought to pick the higher one to comply with. Chepurnoy et al. [36] supplied a brand-new consensus set of rules for peer-to- peer blockchain structures wherein anyone who provides non- interactive proofs of retrievability for the beyond kingdom snapshots is agreed to generate the block. In this type of protocol, miners handiest must store vintage block headers as opposed to complete blocks.

4. CHALLENGES & RECENT ADVANCES

Despite the significant potential of blockchain, it encounters various challenges that constrain its widespread adoption. Some

key challenges and recent advances as follow:

4.1 Scalability

With the number of transactions increasing every day, the blockchain becomes cumbersome. each node has to shop all transactions to validate them on the blockchain due to the fact they have got to test if the source of the modern-day transaction is unspent or no longer. besides, because of the unique limit of block size and the time c programming language used to generate a brand-new block, the Bitcoin blockchain can most effective process nearly 7 transactions in step with 2d, which can't fulfill the requirement of processing thousands and thousands of transactions in real-time style. meanwhile, because the potential of blocks is very small, many small transactions is probably delayed considering miners choose those transactions with excessive transaction fee.

There are a number of efforts proposed to cope with the scalability problem of blockchain, which can be labeled into two types:

4.1.1 Storage optimization of blockchain-Consider that it's far harder for node to operate complete reproduction of ledger, Bruce proposed a unique cryptocurrency scheme, wherein the vintage transaction facts are eliminated (or forgotten) by way of the community [37]. A database named account tree is used to keep the balance of all non-empty addresses. except light-weight purchaser could also help fix this hassle. a unique scheme named Ver Sum [38] become proposed to provide every other way allowing lightweight customers to exist. Ver Sum lets in light-weight clients to outsource highly-priced computations over large inputs. It ensures the computation result is accurate via evaluating results from more than one server.

4.1.2 Redesigning blockchain: In [39], Bitcoin-NG (next Generation) turned into proposed. The principle concept of Bitcoin-NG is to decouple traditional block into elements: key block for leader election and micro block to shop transactions. The protocol divides time into epochs. In each epoch, miners should hash to generate a key block. as soon as the key block is generated, the node turns into the leader who's chargeable for producing micro blocks. Bitcoin-NG additionally extended the heaviest (longest) chain approach wherein micro blocks convey no weight. on this way, blockchain is redesigned and the tradeoff among block size and network security has been addressed.

4.2 Privacy Leakage

Blockchain can maintain a certain amount of privacy through the public key and private key. users transact with their non-public key and public key without any real identification exposure. however, it is proven in [40], [5] that blockchain cannot assure the transactional privateness since the values of all transactions and balances for every public key are publicly seen. except, the recent take a look at [41] has proven that a consumer's Bitcoin transactions can be connected to show person's records. moreover, Biryukov et al. [11] provided an approach to hyperlink consumer pseudonyms to IP addresses even when customers are in the back of community cope with Translation (NAT) or firewalls. In [11], every purchaser may be uniquely identified through a fixed of nodes it connects to. however, this set may be found out and used to find the beginning of a transaction. more than one strategy had been proposed to enhance anonymity of blockchain, which can be roughly categorized into two sorts:

4.2.1 Mixing [42]: In blockchain, user's addresses are pseudonym but it is nonetheless feasible to link addresses to person real identity as many customers make transactions with the equal address regularly. mixing service is a kind of provider which presents anonymity by means of moving funds from more than one enters addresses to a couple of output addresses. as an instance, consumer Alice with deal with A wants to ship a few prices range to Bob with address B. If Alice directly makes a transaction with enter cope with A and output cope with B, courting between Alice and Bob is probably discovered. So, Alice ought to send budget to a trusted intermediary Carol. Then Carol transfer price range to Bob with multiple inputs c1, c2, c3, etc., and multiple output d1, d2, B, d3, and so forth. Bob's cope with B is likewise contained inside the output addresses. So, it turns into tougher to show dating among Alice and Bob. but the middleman might be cheating and display Alice and Bob's private records on purpose. it is also feasible that Carol transfers Alice's funds to her own deal with in place of Bob's address. Mix coin [43] gives an easy method to keep away from cheating behaviors. The middleman encrypts users' requirements consisting of finances amount and switch date with its personal key. Then if the middleman did now not transfer the cash, anybody ought to affirm that the middleman cheated. but theft is detected but nevertheless no longer prevented. Coinjoin [44] relies upon on a significant blending server to shuffle output addresses to prevent theft.

***Anonymous*:** In Zerocoin [46], zero-knowledge proof is used. Miners are not required to authenticate a transaction through a digital signature; instead, their validation focuses on confirming that the coins involved belong to a recognized list of valid coins. Payment's origin is unlinked from transactions to prevent transaction graph analyses. However, it still discloses information about payment destinations and amounts. To tackle this issue, zero cash [47] was introduced. Zero cash utilizes zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs), which conceals transaction amounts and the values of coins held by users.

4.3 Selfish Mining

Blockchain is liable to assaults of colluding selfish miners. specifically, Eyal and Sirer [10] showed that the community is inclined despite the fact that simplest a small portion of the hashing energy is used to cheat. In selfish mining strategy, selfish miners maintain their mined blocks without broadcasting and the private branch might be found out to the public most effective if a few necessities are satisfied. because the non-public department is longer than the cutting-edge public chain, it could be admitted through all miners. earlier than the non-public blockchain publishment, sincere miners are losing their assets on a vain department while selfish miners are mining their non-public chain without competition. So selfish miners generally tend to get extra sales.

Primarily based on selfish mining, many different attacks have been proposed to expose that blockchain is not so cozy. In stubborn mining [48], miners should expand its advantage through non-trivially composing mining assaults with community-degree eclipse attacks. The path-stubbornness is one of the stubborn methods that miners still mine the blocks even though the personal chain is left behind. yet in some cases, it is able to bring about 13% gains in comparison with a non-path-cussed counterpart. [49] shows that there are selfish mining techniques that earn extra cash and are seasoned desk for smaller miners as compared to easy selfish mining. but the profits are rather small. furthermore, it suggests that attackers with much less than 25% of the

computational resources can nonetheless benefit from selfish mining. To assist fix the selfish mining problem, Heilman [50] supplied a novel approach for honest miners to select which department to observe. With random beacons and timestamps, honest miners would choose more clean blocks. but, [50] is prone to mining. But the gains are relatively small. Furthermore, it shows that attackers with less than 25% of the computational resources can still gain from selfish mining. To address the selfish mining problem, Heilman [50] introduced a novel approach to guide honest miners in choosing which branch to follow. By incorporating random beacons and timestamps, honest miners are inclined to select more recent blocks. However, [50] is vulnerable to forgeable timestamps. Zero Block [51] builds on the easy scheme: each block has to be generated and usual via the network within a most time interval. within Zero Block, selfish miners can't reap more than its expected praise.

5. POSSIBLE FUTURE DIRECTIONS

Blockchain has shown its capacity in both enterprise and academia. Future directions can be explored in four key areas: blockchain testing, addressing the tendency toward centralization, leveraging big data analytics, and enhancing blockchain applications. Each of these areas presents unique opportunities for innovation and improvement, which could significantly advance the technology and its adoption across various sectors. By focusing on these domains, stakeholders can contribute to a more robust and decentralized blockchain ecosystem.

5.1 Blockchain testing

Currently one-of-a-kind varieties of blockchains seem and over 700 cryptocurrencies are indexed in [52] thus far. but a few builders would possibly falsify their blockchain performance to attract investors driven by means of the big seasoned. except that, when customers want to mix blockchain into business, they must know which blockchain fits their necessities. So blockchain testing mechanism needs to be in vicinity to test one-of-a-kind blockchains.

Blockchain testing will be separated into two levels: standardization section and checking out segment. In standardization phase, all criteria ought to be made and agreed. whilst a blockchain is born, it can be tested with the agreed standards to valid if the blockchain works fine as developers claim. As for testing phase, blockchain checking out wishes to be done with distinctive criteria. as an instance, a consumer who's in charge of on-line retail commercial enterprise cares about the throughput of the blockchain, so the exam wishes to check the common time from a consumer send a transaction to the transaction is packed into the blockchain, capability for a blockchain block and many others.

5.2 Stop the tendency to centralization

Blockchain is designed as a decentralized device. but there's a fashion that miners are centralized within the mining pool. to date, the pinnacle five mining swimming pools collectively owns large than fifty-one% of the entire hash energy in the Bitcoin network [53]. apart from that, selfish mining method [10] showed that pools with over 25% of total computing power may want to get more sales than fair percentage. Rational miners would be attracted into the selfish pool and finally the pool may want to effortlessly exceed 51% of the overall electricity. because the blockchain isn't always supposed to serve some groups, some methods must be proposed to resolve this problem.

5.3 Big data analytics

Blockchain may be properly combined with massive information. here more or less categorized the mixture into kinds: information control and facts analytics. As for statistics management, blockchain may be used to keep critical records as it is allotted and relaxed. Blockchain could also ensure the statistics is authentic. as an example, if blockchain is used to store sufferers' fitness data, the facts could not be tampered and it is tough to stole the ones private facts. on the subject of facts analytics, transactions on blockchain can be used for massive data analytics. as an example, consumer trading patterns might be extracted. users can predict their capability companions' trading behaviors with the evaluation.

5.4 Blockchain applications

Currently maximum blockchains are used inside the financial domain, increasingly programs for unique fields are appearing. conventional industries ought to take blockchain into consideration and observe blockchain into their fields to decorate their systems. as an instance, consumer reputations could be saved on blockchain. at the identical time, the up-and-coming enterprise may want to make use of blockchain to enhance overall performance. for instance, Arcade town [51], a ridesharing startup offers an open market in which riders connect without delay with drivers with the aid of leveraging blockchain generation. drivers.

A clever settlement is an automated transaction protocol that executes the phrases of an agreement [54]. it's been proposed for long term and now this concept may be applied with blockchain. In blockchain, clever contract is a code fragment that would be completed with the aid of miners routinely. smart contract has transformative capacity in various fields like financial services and IoT.

6. LIMITATIONS

Writing a research paper on blockchain can be incredibly rewarding, but it also comes with several limitations and challenges:

6.1 Rapidly Evolving Technology

Blockchain technology is constantly changing. Keeping up with the latest developments can be difficult, leading to potential obsolescence of research.

6.2 Lack of Standardization

There are many different blockchain platforms and protocols, each with unique features and use cases. This diversity can complicate comparisons and analyses.

6.3 Limited Empirical Data

Depending on focus, there might be a shortage of real-world data and case studies, making it hard to support arguments with concrete evidence.

6.4 Interdisciplinary Nature

Blockchain intersects with various fields (e.g., computer science, law, economics), which can make it challenging to cover all relevant aspects comprehensively.

6.5 Complexity of Concepts

The underlying principles of blockchain (like cryptography and consensus mechanisms) can be complex, making it hard to explain these concepts clearly to a broader audience.

6.6 Regulatory and Legal Challenges

The legal landscape around blockchain and cryptocurrencies is still developing. This can create uncertainties in research

findings.

6.7 Bias and Misunderstandings

There is often a hype cycle surrounding blockchain, which can lead to biased interpretations of its potential. Avoiding sensationalism while remaining realistic is crucial.

6.8 Scalability Issues

Discussing scalability solutions and challenges can be difficult, as these are still hotly debated topics with ongoing research.

6.9 Ethical Considerations\

Issues like privacy, security, and the environmental impact of blockchain technologies need careful consideration, adding complexity to analysis.

6.10 Technical Language

The use of technical jargon can alienate readers who are not specialists in the field, making it necessary to strike a balance between technical accuracy and accessibility.

7. CONCLUSION

Blockchain has demonstrated its potential to transform traditional industries through its key characteristics: decentralization, persistency, anonymity, and auditability. This paper provided a comprehensive overview of blockchain technology, covering its architecture and essential features. Standard consensus algorithms were discussed, with an analysis and comparison of these protocols across various aspects.

Additionally, challenges that may impede blockchain development were identified, along with existing approaches to address these issues. Several future research directions were proposed. As blockchain-based applications continue to emerge, in-depth investigations into their implementations and impacts will be crucial for unlocking the full transformative potential of blockchain across various sectors.

8. 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 Sur- veys 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/0531 01f.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 appli- cation platform," white paper, 2014.

[16] 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.

[17] V. Buterin, "On public and private blockchains," 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/ on-public-and-private-blockchains/

[18] "Hyperledger project," 2015. [Online]. Available: https://www. hyperledger.org/

[19] "Consortium chain development." [Online]. Available: https://github. com/Ethereum/wiki/wiki/Consortium-Chain-Development

[20] L. Lamport, R. Shostak, and M. Pease, "The byzantine general's problem," ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.

[21] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof- of-stake," Self-Published Paper, August, vol. 19, 2012.

[22] "Bit shares - share in the decentralized exchange." [Online].Available: https://bitshares.org/

[23] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," Ripple Labs Inc White Paper, vol. 5, 2014.

[24] J. Kwon, "Tendermint: Consensus without mining," URL http://tendermint. com/docs/tendermint v04. pdf, 2014.

[25] S. King, "Primecoin: Cryptocurrency with prime number proof-of- work," July 7th, 2013.

[26] P. Vasin, "Blackcoins proof-of-stake protocol v2," 2014. [Online]. Avail- able: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

[27] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," Ethereum Project Yellow Paper, 2014.

[28] V. Zamfir, "Introducing Casper the friendly ghost," Ethereum Blog URL: https://blog. Ethereum. org/2015/08/01/introducing-Casper- friendly-ghost, 2015.

[29] C. Miguel and L. Barbara, "Practical byzantine fault tolerance," in Proceedings of the Third Symposium on Operating Systems Design and Implementation, vol. 99, New Orleans, USA, 1999, pp. 173–186.

[30] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," Stellar Development Foundation, 2015. "Antshares digital assets for everyone," 2016. [Online]. Available: https://www.antshares.org

[31] M. Vukolic´, "The quest for scalable blockchain fabric: Proof-of-work vs. bft replication," in International Workshop on Open Problems in Network Security, Zurich, Switzerland, 2015, pp. 112–125.

[32] C. Decker, J. Seidel, and R. Wattenhofer, "Bitcoin meets strong con- sistency," in Proceedings of the 17th International Conference on Dis- tributed Computing and Networking (ICDCN). Singapore, Singapore: ACM, 2016, p. 13.

[33] D. Kraft, "Difficulty control for blockchain-based consensus systems," Peer-to-Peer Networking and Applications, vol. 9, no. 2, pp. 397–413, 2016.

[34] Y. Sompolinsky and A. Zohar, "Accelerating bitcoin's transaction pro- cessing. fast money grows on trees, not chains." IACR Cryptology ePrint Archive, vol. 2013, no. 881, 2013.

[35] A. Chepurnoy, M. Larangeira, and A. Ojiganov, "A prunable blockchain consensus protocol based on non-interactive proofs of past states retriev- ability," arXiv preprint arXiv:1603.07926, 2016.

[36] J. Bruce, "The mini-blockchain scheme," July 2014. [Online]. Available: http://cryptonite.info/files/mbc-scheme-rev3.pdf

[37] J. van den Hooff, M. F. Kaashoek, and N. Zeldovich, "Versum: Verifiable computations over large public logs," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 1304–1316.

[38] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin- ng: A scalable blockchain protocol," in Proceedings of 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), Santa Clara, CA, USA, 2016, pp. 45–59.

[39] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: Characterizing payments among men with no names," in Proceedings of the 2013 Conference on Internet Measurement Conference (IMC'13), New York, NY, USA, 2013.

[40] J. Barcelo, "User privacy in the public bitcoin blockchain," 2014.

[41] M. Mo¨ser, "Anonymity of bitcoin transactions: An analysis of mixing services," in Proceedings of Munster Bitcoin Conference, Munster, Germany, 2013, pp. 17–18.

[42] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 486–504.

[43] G. Maxwell, "Coinjoin: Bitcoin privacy for the real world," in Post on Bitcoin Forum, 2013.

[44] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coinshuffle: Practical decentralized coin mixing for bitcoin," in Proceedings of European Symposium on Research in Computer Security, Cham, 2014, pp. 345– 364.

[45] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in Proceedings of IEEE Symposium Security and Privacy (SP), Berkeley, CA, USA, 2013, pp. 397–411.

[46] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in Proceedings of 2014 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2014, pp. 459–474.

[47] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generaliz- ing selfish mining and combining with an eclipse attack," in Proceedings of 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, Germany, 2016, pp. 305–320.

[48] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," arXiv preprint arXiv:1507.06183, 2015.

[49] S. Billah, "One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner," 2015.

[50] S. Solat and M. Potop-Butucaru, "ZeroBlock: Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin," Sorbonne Universities, UPMC University of Paris 6, Technical Report, May 2016. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01310088

[51] "Crypto-currency market capitalizations," 2017. [Online]. Available: https://coinmarketcap.com

[52] "The biggest mining pools." [Online]. Available: https:

[53] //bitcoinworldwide.com/mining/pools/N. Szabo, "The idea of smart contracts," 1997.