# Title

Blockchain Challenges and Opportunities: A Survey

# Citation

Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Huaimin Wang

# Abstract

Author presents a comprehensive survey on blockchain technologies.

1. Provide an overview of blockchain technologies and a taxonomy of various blockchain systems.
2. Enumerate a number of both current and future blockchain applications.
3. Discuss the challenges in this promising area and discuss the future directions.

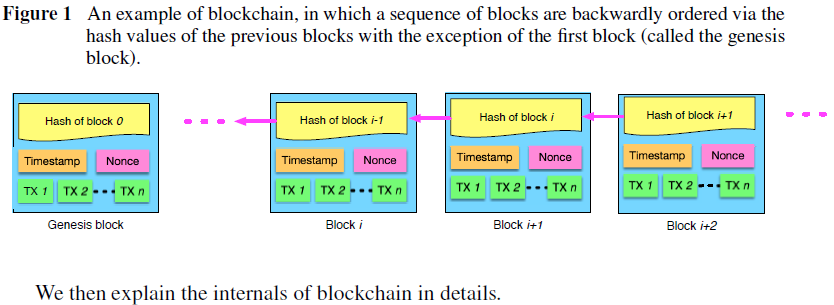
# Issues

## Overview of blockchain technologies

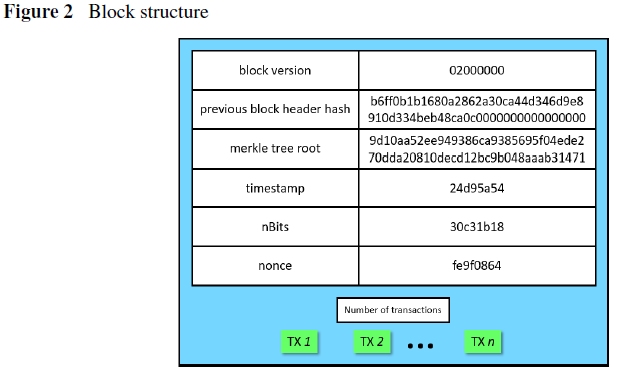
### Blockchain architecture

Blockchain is a sequence of blocks, which holds a complete list of transaction records like

conventional public ledger. Figure 1 illustrates an example.

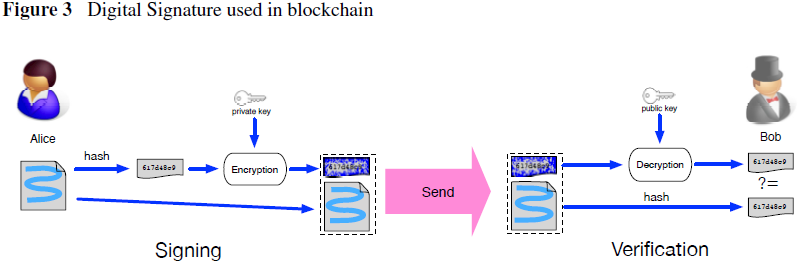


#### Block



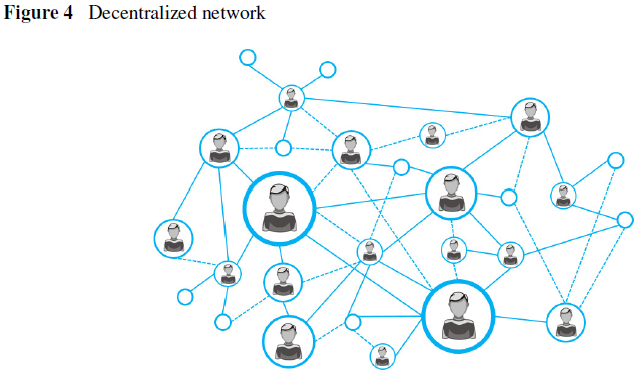
A block consists of the block header and the block body as shown in Figure 2. In particular, the block header includes: (i) block version, (ii) previous block header hash, (iii) merkle tree root hash, (iv) timestamp, (v) nBits, (vi) the nonce. The block body includes the number of transactions and the collection of transactions. A valid transaction is mainly composed of two individual parts: inputs and outputs. Transaction ids in inputs is a reference to the unspent transaction outputs (UTXO) of the sender while the sender has to specify the destination address and amount in outputs. Furthermore miners would check the signature in inputs to validate a transaction. Miners would check the signature in inputs to validate a transaction by using an asymmetric cryptography mechanism.

#### 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 spread throughout the whole network and then are accessed by public keys, which are visible to everyone in the network. Figure 3 shows an example of digital signature used in blockchain.

#### Decentralized Network



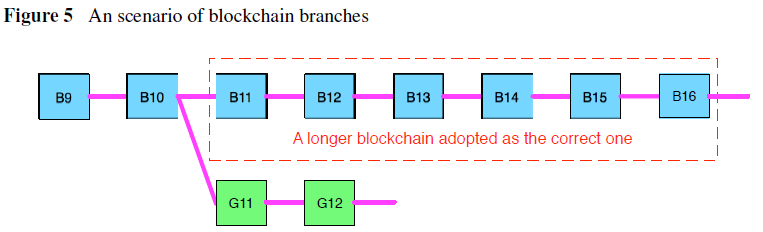
Each user interacts with the blockchain network via a dedicated node in which a blockchain client is installed. A large number of nodes across the whole network form a decentralized network as shown in Figure 4. Once a node receives data from another node, it verifies the authentication of the data. It then broadcasts the validated data to every other node connected to it. In this way, the data is spread across the whole network.

### Consensus on the network

Once the transactions have been created, they need to be verified by the network. However, there may exist a divergence of branches of a blockchain as shown in Figure 5 since each node may have a different view of the whole network state.

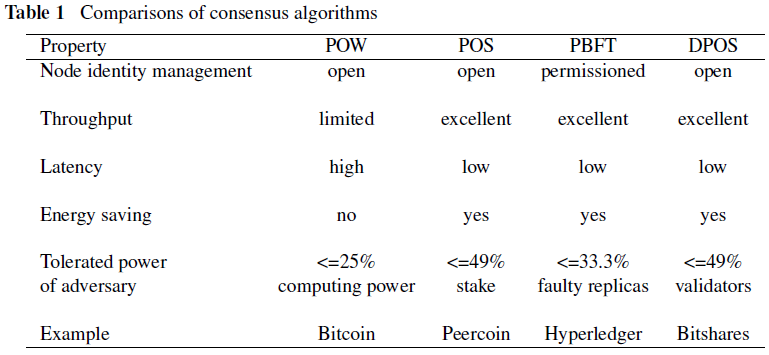
In the blockchain network, how to reach consensus on a transaction among the untrusted nodes is a transformation of Byzantine Generals (BG) Problem.

#### Approaches to consensus



1. POW (Proof of work)
   1. Used in Bitcoin network.
   2. Each node of the network is calculating a hash value of the constantly changing block header. Target is that, by testing the value of nonce from zero to infinity, calculated value must be equal to or smaller than a certain given value.
   3. When one node obtains the relevant value, all other nodes must mutually confirm the correctness of the value.
   4. After that, transactions in the new block would be validated in case of frauds.
   5. Then, the collection of transactions used for the calculations is approved to be the authenticated result, which is denoted by a new block in the blockchain.
   6. When multiple nodes find the suitable nonce nearly at the same time branches (or forks) may be generated as shown in Figure 5.
   7. In POW protocol, a chain that becomes longer thereafter is judged as the authentic one.
2. POS (Proof of stake)
   1. An energy-saving alternative to POW.
   2. POS requires people to prove the ownership of the amount of currency because it is believed that people with more currencies would be less likely to attack the network.
   3. Many solutions are proposed with the combination of the stake size to decide which one to forge the next block, like randomization and coin age.
   4. But the attacks might come as a consequence.
3. PBFT (Practical byzantine fault tolerance)
   1. A replication algorithm to tolerate byzantine faults.
   2. Used in Hyperledger since PBFT could handle up to 1/3 malicious byzantine replicas.
   3. A primary that is responsible for multicasting requests to other replicas is selected in a view.
   4. A service operation would be valid if it has received approvements from over 1/3 different replicas.
4. DPOS (Delegated proof of stake)
   1. Used in Bitshares.
   2. Similar to POS, miners get their priority to generate the blocks according to their stake.
   3. POS is a direct democratic while DPOS is representative democratic
   4. The dishonest delegates could be voted out easily.

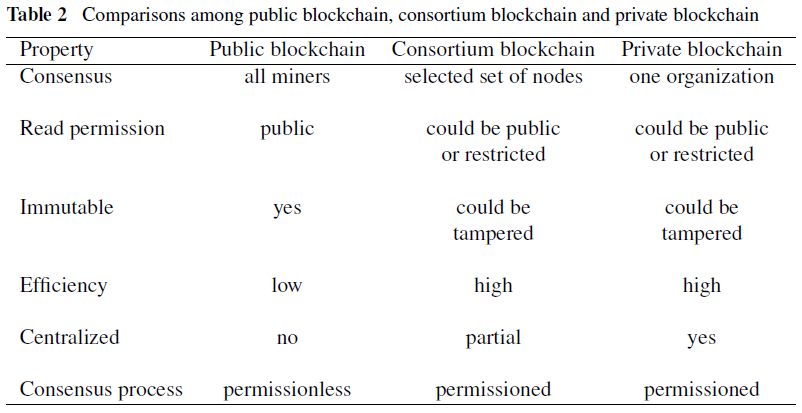
#### Comparisons of consensus approaches



### Key characteristics of blockchain

1. Decentralization.
2. Persistency.
3. Anonymity.
4. Auditability.

### Taxonomy of blockchain systems



## Applications of blockchain

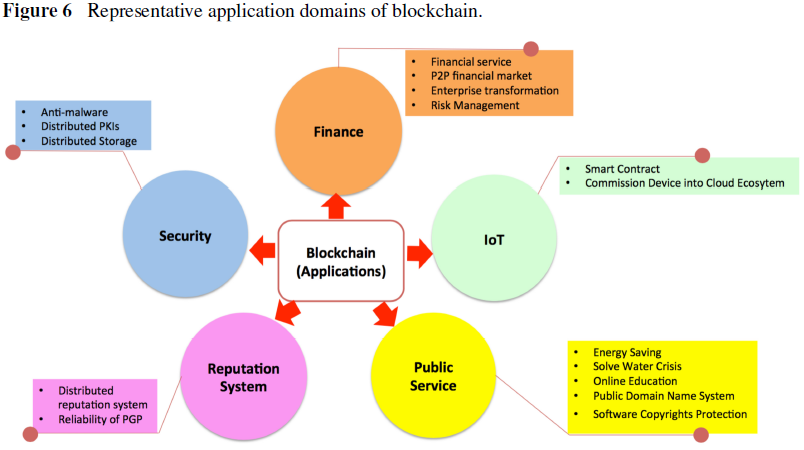


Figure 6 illustrates 6 representative application domains of blockchain.

### Financial and business services

The emergency of blockchain systems has brought a huge impact on traditional financial and business services, including remittance, smart contracts, automated banking ledgers and digital assets. Many researchers argue the suitability of blockchain technology due to the vulnerability to bugs and hacking of blockchain. On the other hand, many other researchers blockchain technologies will improve financial and business services instead of disrupting them.

In addition to the evolution of financial and business services, blockchain can help traditional organizations to complete the enterprise transformation smoothly, including postal operators (POs).

Risk management framework plays a significant role in financial technology (FinTech) and now it can be combined with blockchain to perform better.

### Internet of Things (IoT)

Blockchain technologies can potentially improve the IoT sector. a) Digital tokenized assets transfer; b) Smart contracts; c) A new E-business model.

Blockchain can also help in improving privacy in IoT applications. a) A privacy-preserving method for commissioning an IoT device into a cloud ecosystem; b) A new architecture was proposed in to help device to prove its manufacturing provenance without the authentication of third party; c) A system using blockchain technologies to build a distributed network of devices - a decentralized Internet of Things.

### Public services

Blockchains can also be widely used in public services. a) Land registration; b) Marriage registration; c) Patent management; d) Income taxation systems. Mobile devices with digital signature embedded may replace seals to be affixed on documents, which are submitted to administrative departments.

Blockchains can be used in green energy. a) Solarcoin; b) A study on the issue that crosses over between solar engineering, network engineering and finally blockchain development.

Blockchain also contributes to solve water crisis. a) Clean water coin; People who mine the clean water blockchain and make a new transaction with clean water coin will donate 1 percent of the coins to the charity wallet.

If we regard the learning and teaching process as the currency, blockchain technology can potentially be applied to the online educational market. a) Blockchain learning.

Blockchain can also be used in software copyright protection. a) Novel method aiming to reduce software piracy; b) Namecoin, used to secure DNS and identities.

### Reputation system

Blockchain can potentially solve this problem of cheating cases of personal reputation records falsification. a) A quantified reputation system, established on blockchain; b) A blockchain-based distributed system for educational record and reputation; c) A reputation model based on blockchain, in which a voucher will be signed if customer is satisfied with the service and would like to give a good feedback; d) a new reputation system that is practically applicable to multiple networks.

Blockchain can also be used to enhance the reliability of PGP (pretty good privacy). a) A distributed PGP key server that leverages the blockchain to store and retrieve the certificates.

### Security

Blockchain can potentially help to improve the security in distributed networks. a) A novel anti-malware environment named BitAV.

Blockchain has the potential to improve the security of privacy sensitive data. a) A decentralized personal data management system that ensures the user ownership of their data; b) A similar system based on blockchain technology to securely distribute sensitive data.

Blockchain technologies can also be used to improve the reliability of security infrastructure. a) A privacy-aware PKI, simultaneously improving the reliability of conventional PKIs.

Blockchain can also enhance the security and the reliability of decentralized systems, such as cloud systems and distributed databases. a) Metadisk project to improve the security and the efficiency of a peer-to-peer cloud storage system; b) BigchainDB project, used in creation and movement of digital assets; c) A blockchain-based system named ChainAnchor, which can commission IoT devices into a cloud system in a privacy-preserving manner; d) Use blockchain to serve as a software connector to improve security, privacy, scalability and sustainability of shared data storage systems.

## Challenges

### Challenges in blockchain

1. Scalability.
2. Vulnerability.
3. Deficiency of exisiting consensus algorithms.
4. Tendency to centralization.
5. Privacy Leakage.

### Recent advances

#### Improvements on scalability

1. Storage optimization of blockchain. a) A novel cryptocurrency scheme, in which the old transaction records are removed (or forgotten) by the network; b) VerSum, allowing lightweight clients to exist since they can outsource expensive computations over large inputs; c) A novel blockchain architecture, in which conventional blockchains are divided into two groups: one group of blockchains is used to store transactional information and another group is used to store account information.
2. Redesigning blockchain. a) Bitcoin-NG, to decouple conventional block into two parts: key block for leader election and microblock to store transactions.

#### Advances on consensus protocols

1. Consensus protocol. a) A new computationally-scalable Byzantine consensus protocol (named SCP) for blockchains; b) A new consensus protocol for peer-to-peer blockchain system, in which anyone who provides non-interactive proofs of retrievability for the past state snapshots is agreed to generate the block; c) a new consensus method to ensure that a block is generated in a relatively stable speed; d) A new consensus algorithm named proof of stake time (POST), which is a time-accepted nonlinear consensus algorithm; e) PeerCensus, to reduce the confirmation time of a transaction.
2. Performance analysis of blockchain consensus protocols.

#### Approaches to improve privacy and security

1. Improve the anonymity of blockchain. a) A solution based on the micro-payment channel to achieve anonymity and fairness, implemented by blind signature and smart contract; b) CoinParty, integrated of decryption mix networks (mixnets) with threshold signatures.
2. Enhancing the vulnerability of blockchain. a) A markov chain model to detect selfish miners; b) By two simplified mining games, propose some approaches; c) Proof of witness to eliminate block-withholding attacks; d) Miners failing to verify are vulnerable to attack and proposed a novel solution to this problem.

### Future directions

1. Application of blockchain in sharing economy.
2. Application of blockchain in healthcare.
3. Big data analytics in blockchain.

# References

1. [揭秘比特币和区块链（二）：什么是工作量证明？](http://www.infoq.com/cn/articles/bitcoin-and-block-chain-part02)
2. [Proof of Stake FAQ · ethereum/wiki Wiki](https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ)
3. [区块链核心技术：拜占庭共识算法之PBFT](http://blog.liqilei.com/bai-zhan-ting-gong-shi-suan-fa-zhi-pbftjie-xi/)