Blockchain Technology – Transaction Processing, Challenges and Trends

Bach Dong Nam
NACENLAS, National Center for Technological Progress, Hanoi, Vietnam
Email: namdongbach@gmail.com

Abstract: Blockchain technology, one of the top 10 strategic technology trends for recent years, has shown its applications in a variety of industries, many salient advantages, also some disadvantages. Based on the advanced algorithms and P2P (Peer-to-Peer) network protocols, Blockchain technology focuses on processing and storing value transactions on a decentralized database that operates as a distributed digital ledger in a distributed high-secure and fair interaction environment. Therefore, Blockchain technology reduces transaction cost, execution time and has been researched and developed in many developed countries by top world technological corporations. Unfortunately, there has been no blockchain model for all applications so far. Normally, processing and storing procedures are context-relevantly designed to increase processing speed. The core algorithms such as randomization, cryptography, hash function, edge computing, offline associated processing, etc are also used for higher security. The combination of DApp (Decentralized Application), AI (Artificial Intelligence), IoT (Internet of Things) and blockchain also brings up many wonderful features.

Keywords: Blockchain technology, transaction, hash function, P2P network, DApps, AI, IoT.

Blockchain technology (BT), one of the top 10 strategic technology trends for recent years[1], has developed over the last decade into one of today's biggest ground-breaking technologies with the potential to impact every industry from financial to manufacturing and to educational institutions. Blockchain has provided the answer to digital trust because it records important information in a public, time-stamped and decentralized space and doesn't allow anyone to remove or change it. BT is a relatively new concept and rapidly growing.

1. Transaction Processing

Fig. 1 illustrates key definitions and concepts to understand the basic architecture, operations, features, and application areas of this revolutionary technology. The blockchain can be technically explained as a system comprised of core components like transactions, an immutable chain of blocks, decentralized P2P network, encryption processes, consensus mechanisms, and optional smart contracts.

- **Blockchain Transaction**

Transaction is simply an exchange, agreement, business deal or interaction between people or parties such as commercial, real estate, enterprise, financial transactions [2,3].

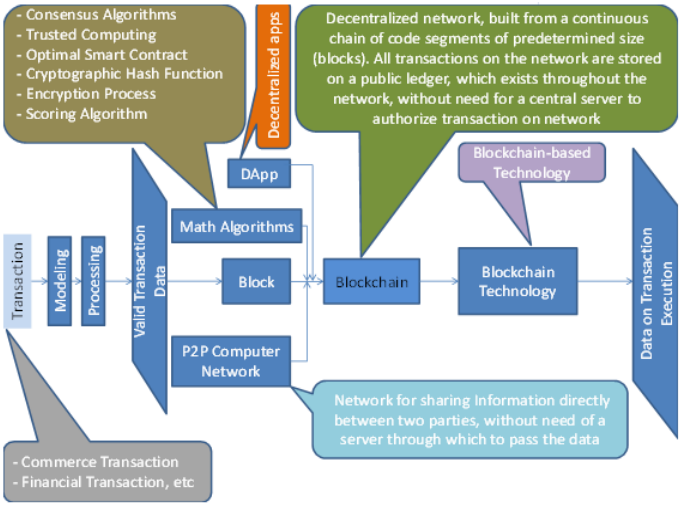

Fig 1: Logic Flowchart of Blockchain

- **Block**

Block is made up at least of information about:

- A transaction includes the date, time, exchange amount and the associated metadata. Batches of valid transactions are hashed and encoded into a Merkle tree.

- Who is participating in the transaction using a digital signature, sort of the like a username?

- Information that distinguishes it from other locks: The cryptographic hash of its own and of the most recent block added.

Each block is identified via a cryptographic hash and timestamp. A newly created block is appended to an existing chain of blocks. Each block is unique and can only be created once. The blocks represent transactions made within the network,

displayed on a public ledger. A single block on the blockchain can actually store up to 1 MB of data. Depending on the size of the transactions, a block can house a few thousand transactions.

- **Peer-to-Peer Computer Network**

It is one for sharing information on the network directly between two parties without a server that manages how the data is transferred between the users, and there is no central database where the data is kept, and for Dapp to run. The decentralized interactions happen between at least two parties. For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network, collectively adhering to a protocol for inter-node communication and validating new blocks (Fig. 2).

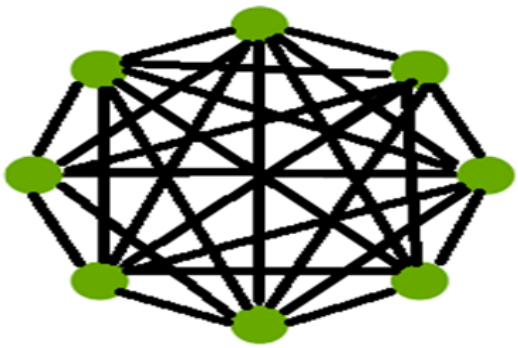

Fig 2: P2P Computer Network

- **Node**

A computer connected to the blockchain network is referred to as a node. A full node has a program that can fully validate transactions and blocks. The node can operate a copy of the blockchain ledger. Blockchain uses P2P protocol which allows all the network participants to hold an identical copy of transactions, enabling the approval through a machine consensus.

- **Encryption Algorithm**

RSA, an asymmetry cryptosystem, has an ample staying power. It is widely used for digital signatures and public-key encryption to encrypt messages in secure data transmission. The messages encrypted with the public key can only be decrypted in a reasonable amount of time by using a private key. All blocks are encrypted in this way. For better security, the required key lengths and cryptographic algorithms are advanced, table 1 [4].

Table 1: Standard Security in Comparision with the Quantum Computing based Security

Algorithm	Key Length	Security	In Comparison with Quantum-based Security
RSA-256	256	40	0
RSA-1024	1024	80	0
RSA-2048	2048	112	0
ECC-256	256	128	0
ECC-512	512	256	0
AES-128	128	128	64
AES-256	256	256	128

- **Hash Function**

It is an algorithm that can be used to map data of arbitrary size to fixed-size value or to create a unified form, that is called hash value, hash code or hash - the data for identifying blocks of code by converting the stored information on these blocks into a string of numbers and letters of a fixed size.

The hash is used to identify the block, confirm coin transactions on the blockchain, validate the integrate the set of all blockchain parameters, etc. The function SHA 256 is used as the basis for bitcoin's proof of work system. Cryptographic hash functions, such as SHA-512, have very strong uniformity guarantees and thus can provide very good general-purpose hashing functions. Generally, good randomization is the choice for the good hash function.

- **Consensus algorithm**

A consensus algorithm is defined as the mechanism through which a blockchain network reaches consensus for maintaining the integrity and security of this distributed system, e.g. agreeing on the validity of transactions or on which version of the blockchain is the real one.

It assures that the protocol rules are being followed and guarantees that all transactions occur in a trustful way. It allows the creation of blockchain system with high resistance to attack, such as the 51% attack (the so-called majority attack). In other words, once recorded, the data in any given block cannot be retroactively altered without the alteration of all subsequent blocks, which requires a consensus of the network majority.

There are several types of consensus algorithms such as Proof of Work, Proof of Stake, Proof of

Elapsed Time, Proof of Activity, Proof of Capacity, Proof of Burn, Proof of Importance…..

- **Smart Contract**

An algorithm which uses blockchain technology to automatically execute a certain contract. When the terms of a smart contract, as a set of instructions in a computer language, are met, it is automatically executed by a computing system such as a suitable distributed ledger system, with the participating parties being rewarded according to the contract's terms. The smart contract, also described as a digital self-executing agreement, is stored within the block and used in many cases (Fig. 3).

Fig 3: Smart Contract Use Cases

The smart contract works following three steps:

1. Coding what the parties want it to do;
2. The code is then encrypted and sent out to other computers via a distributed network of ledgers, i.e. Blockchain. If this is done via public permissionless blockchain, the contract is sent out;
3. Once the computers in this network of distributed ledgers receive the code, they each come to an individual agreement. The network then updates the individual ledgers.

- **Wallet**

A designated storage location for digital assets has an address used for sending and receiving funds to and from the wallet. The wallet can be online, offline, or on a physical device. A hot wallet is one that directly connected to the internet at all times. For this reason, hot wallets are considered to have lower security than a cold storage system or hardware wallet.

- **Blockchain Creation**

Fig. 4 illustrates the flowchart of a blockchain network's creation, using high-level programming languages or the blockchain platform.

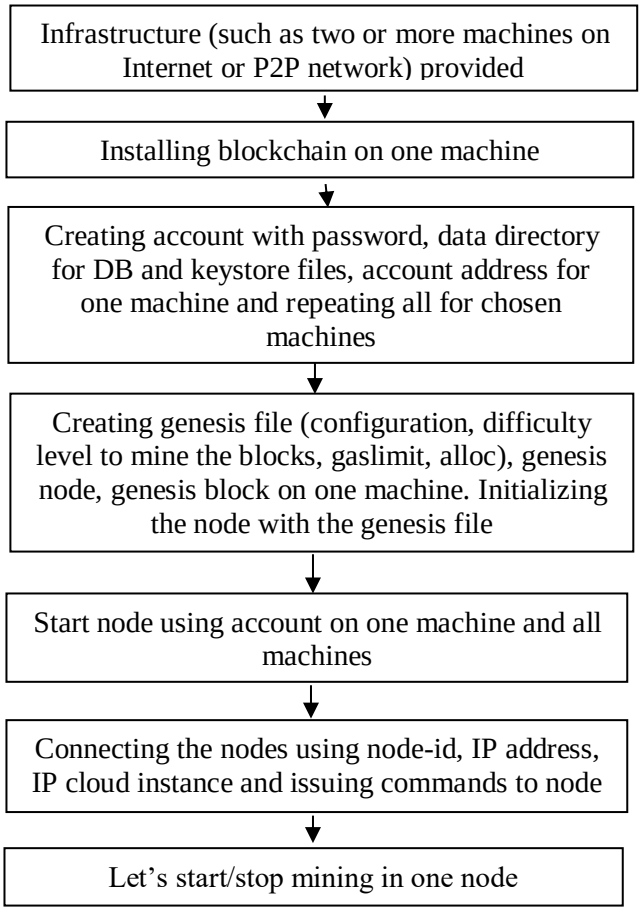

Fig. 4: Flowchart of Blockchain Creation

When a new block is formed, it will contain its hash and the hash of the previous block. Thus, blocks can form a chronologically ordered chain from the first block (genesis block). This process is repeated over-and-over again to grow and maintain the network (Fig. 5, 6).

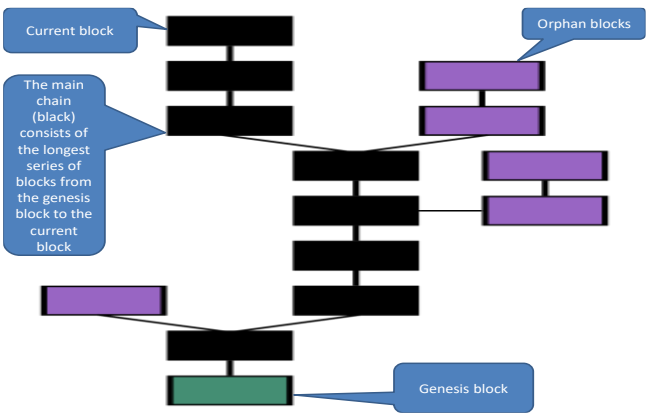

Fig. 5: Blockchain Formation

The initial block of any such list is a genesis block. The genesis block is a special block that is numbered "zero" and is hard-coded in the blockchain application. Each other block links to some previously existing block. Hence, a blockchain grows by appending new blocks to the existing chain. It takes about 10 minutes for a new block. The blockchain's operation and the application are also controlled by the command-line interface using a great API library developed for the following core categories: General utilities; Managing wallet addresses; Working with non-wallet addresses; Permissions management; Asset management; Querying wallet balances and transactions; Sending one-way payments; Stream management; Querying subscribed assets; Querying subscribed streams; Controlling off-chain data; Managing wallet unspent outputs; Working with raw transactions; Peer-to-peer connections; Messaging signing and verification; Querying the blockchain; Binary cache; Advanced wallet control; Smart filters and upgrades; Advanced node control,....

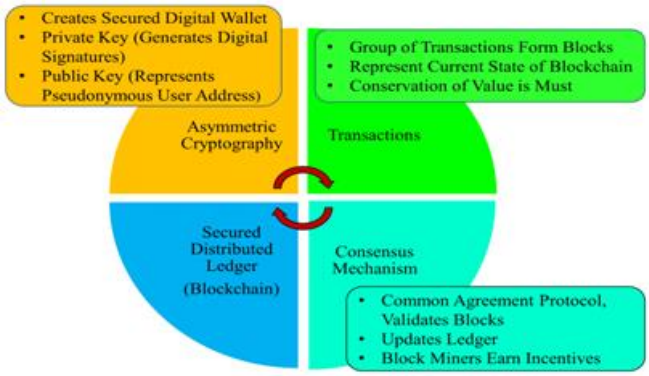

Fig. 6: Core Components of Blockchain

The transaction processing looks like the path of 6 steps (Fig. 7).

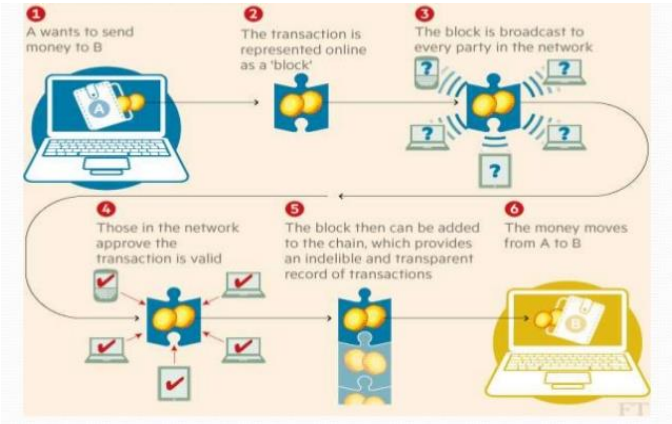

Fig. 7: Steps of a transaction processing

- **Changing the data of a block**

Once recorded, the transaction history data in any given block cannot be retroactively altered without the alteration of all subsequent blocks, which requires a consensus of the network majority. To change the transaction history data – say, if someone were trying to hack it – the ledger would have to be changed in the majority of participants, who own all subsequent blocks. With the number of people already using these, that's near impossible. The transaction can only be built, not changed and is documented and verified, therefore offers greater cybersecurity. The vital characteristics, potential benefits, advantages, disadvantages, classification, and applications of blockchain are summarized in Figs 8 to 13.

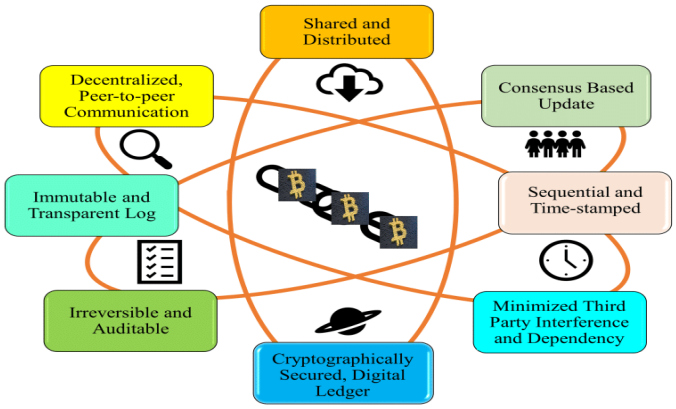

Fig. 8: Vital Blockchain Characteristics

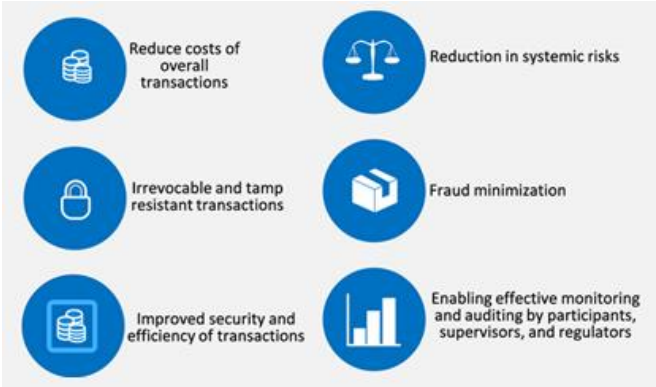

Fig. 9: Potential Blockchain Benefits

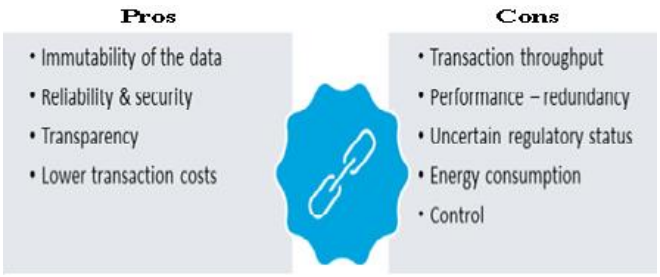

Fig. 10: Pros & Cons of Blockchain

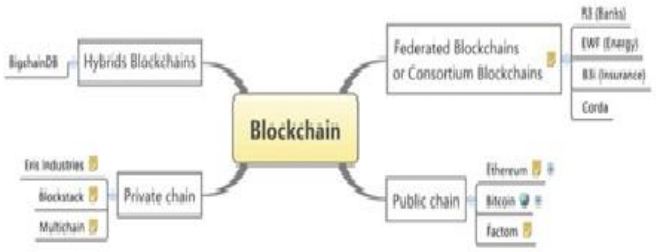

Fig.11: Classification of Blockchain

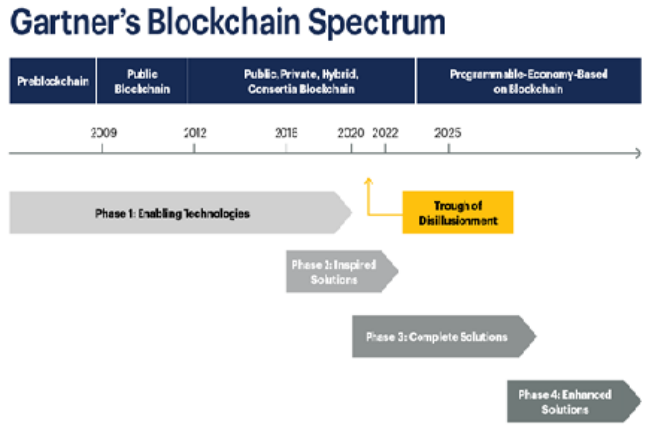

Fig. 12: Blockchain Spectrum

Fig. 13: Application Areas of Blockchain

2. Challenges and Trends

Blockchain has been developed in accordance with the global strategic technology trends (Fig. 14).

Fig. 14: Gartner's Top 10 Strategic Technology Trends for 2019

- **Blockchain 1.0:** Corrency

The first blockchain's application is for cryptocurrencies, that allows financial transactions to be executed at the most prominent level as a digital payment system.

- **Blockchain 2.0:** Smart Contracts

Smart contracts, automatically execute with beforehand defined conditions, reduce the cost of verification, execution, arbitration, prevent fraud and allow transparent contract.

- **Blockchain 3.0:** DApps

Dapps are programs that use blockchain to create an application that runs on a decentralized network. The third decentralized application combines data storage, smart contracts, cloud nodes, open-chain networks, and paves the way for sharing between back-end code and front-end code to new applications on decentralized systems.

- **Blockchain 4.0:** Making blockchain usable in industry 4.0.

The industrial revolution 4.0, meaning automation, enterprise resource planning, and integration of different execution systems, demands an increasing degree of trust and privacy protection. Therefore, it is required blockchain 3.0 usable in real-life business scenarios and make blockchain come to life.

Critics have stated out 9 blockchain's challenges:

1. Nascent technology

2. Uncertain regulatory status

3. Great consumption energy requirement to process and store transactions

4. Control, security, and privacy

5. Integration concerns

6. Cultural adoption

7. Cost from the expensive resources required to process and store bigger amounts of data

8. Challenges associated with the audit, taxes, and compliance

9. Scalability - The most serious challenge.

Despite skepticism and challenges, blockchain technology is developing and many companies see a bright future in its implementation. The currently relevant blockchain trends can be listed as follows:

1. In the 2020s, the BT will implement smart contracts and deliver the full value proposition of blockchain including decentralization and tokenization. Smart contracts will have real autonomy and advanced technologies will enable to execute exchanges and transactions that are not currently possible. Decentralized Autonomous Organizations (DAO) and microtransactions will be performed by machines.

2. Blockchain will need quantum computing for high computing power, advanced cryptographic algorithms and thus high transaction and block verification speed.

3. Blockchain in the IoT system will be used for the communications network to coordinate driverless vehicles without the need for a central server for protecting autonomous cars from being hacked. The built-in blockchain can help maintain a continuously growing list of cryptographically secured data records for protection against alteration and modification. For instance, when an IoT connected (e.g. RFID) asset with sensitive information moves along various points in a warehouse or in a smart home, its information could be updated on a blockchain. This permits all involved parties to share data and status of the package as it moves among different gatherings to guarantee the terms of an agreement are met.

4. The combination of blockchain and AI:

Both blockchain and AI can benefit from each other, and help one another. The integration of machine learning and AI into a blockchain and vice versa can enhance blockchain's underlying architecture and boost AI's potential. AI impacts blockchain through deep learning and blockchain benefits AI through using of smart contracts in AI.

Conclusion

1. Blockchain, a shared, replicated and decentralized ledger using advanced cryptography for the secure identity and integration of data, can open up a fair business network by taking out cost, improving efficiencies and increasing accessibility.

2. Blockchain addresses an exciting and topical set of challenges, which pave the way for many innovative solutions from Smart Contract, Dapp, tokenization…to DAO and microtransactions performed by machines.

3. The combination of blockchain, AI and IoT will have a huge impact on both the global economy and the way we live in the future. The new digital technologies will bring significant positives along with new challenges, particularly in the social economy.

REFERENCES

[1] David W. Cearley, Brian Burke (2018), "Top 10 Strategic Technology Trends for 2019", *Gartner Research*, October 15, ID: G00374252.

[2] Suyash Gupta and Mohammad Sadoghi, *Blockchain Transaction Processing,* Department of Computer Science, University of California, Davis, CA, USA.

[3] Jean de Maillard (1999), *Un mond sans loi, La criminalite financiere en images.* Editions Stock, Page 28.

[4] Nguyen Quoc Toan (2019), *Development of Cryptographic System in Quantum Computing Area,* Information Security Journal, Vietnam, 2-2019,