Blockchain-Based Multimedia privacy protection: Survey

Dr Bashar M. Alesawy

Rihab I. Ajel and Amal H. Khaleel

Overview of blockchain

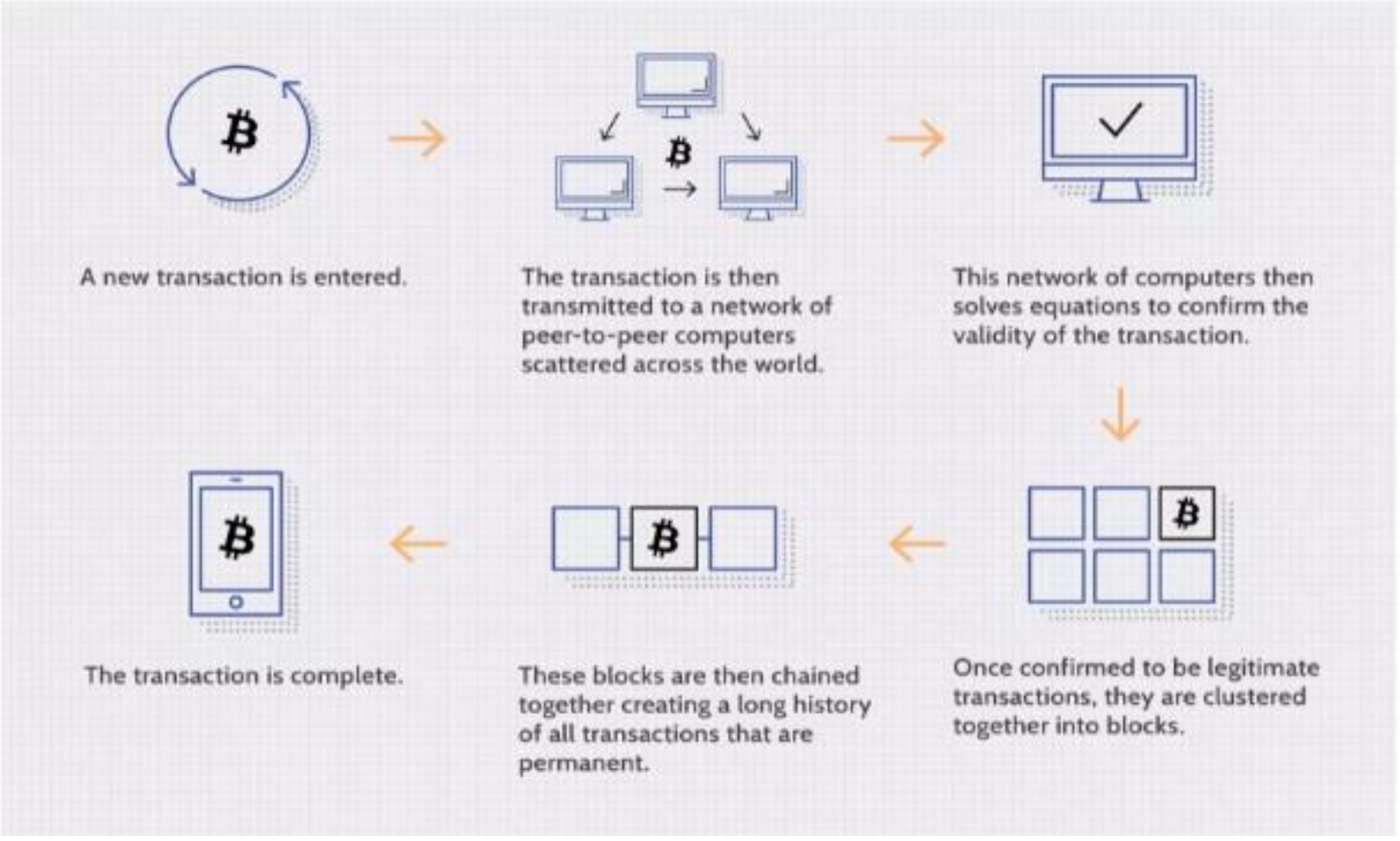
Blockchain published theoretically in 2008, and the first open source blockchain implementation was deployed in 2009 as an integral component of Bitcoin, as decentralized digital currency system. Blockchain technology is generally referred to as a distributed ledger, which was originally designed for the financial industry and records and replicates every transaction on every network node

Blockchain technology is a recent breakthrough in safe computing in an open network environment without centralized authority. It is a distributed chain of blocks that tracks an evolving list of transaction records by arranging them into a hierarchical chain. The block chain is created and maintained via a peer-to-peer overlay network, and it is secured by encryption that is both smart and decentralized.

In Fig. 1, A blockchain is a digital ledger that organizes data into groups called blocks, each of which contains a collection of data. Blocks have specific storage capacity, and when full, they are connected onto the preceding block, establishing a data chain known as a "blockchain." All additional information added after that newly added block is compiled into a new block, which is then added to the chain after it is filled.

A database organizes information into lists, but a blockchain organizes information into chunks (blocks) that are linked together. When implemented in a decentralized manner, this method creates an irreversible data timeline. When a block is filled, it becomes permanent and part of the chronology. When a block is added to the chain, it is assigned a precise timestamp.

In Fig. 1, Transaction Process



- **Joining a Blockchain Network:**

To join a blockchain network, a node will transmit a message confirming the user's identification to one existing node, a process known as seeding. If the node knows the user's network ID, it will broadcast it to the other nodes if the user chose to join the network, and after those nodes register the user's network ID, the user is added to the existing blockchain network.

- **Publishing new transaction:**

This is accomplished through the use of a basic broadcast technique. When a new transaction is announced to all nodes, it is added to the awaiting transaction array of each node.

Blockchain technology applications

1- Digital currency: Bitcoin Blockchain technology

2- Smart Contract: Ethereum

3- Hyperledger global commercial transactions

4- Additional Applications such as insurance, payments, IOT, protection of information in medical care, and online marketplaces

we can summarized some features of this technology:

- **Decentralized.** The fundamental characteristic of blockchain is that it no longer relies on centralized nodes
- **Transparent.** The blockchain system's data record is visible to each node, and it is also visible when updating the data.
- **Open source.** refers to the use of open the majority of blockchain systems are accessible to everyone, data can be checked openly.
- **Autonomy.** Because of the consensual foundation, any node on the public blockchain may safely transmit or change information; the goal is to trust from a single individual to the entire system, and no one can interfere.
- **Immutable**. Any records will be retained in perpetuity and cannot be altered until someone has control of more than 51 percent of the nodes at the same time.
- **Anonymity**. Blockchain technologies have handled the trust problem between nodesall that is required is the person's blockchain identity.

Blockchain structure

- **Generally, From bottom to top, the blockchain architecture consists of the, data layer network layer, consensus layer, incentive layer, contract layer, and application layer.**

Among these is the data layer, which wraps the blockchain design in the blockchain system and offers services such as non - symmetric encryption and data time stamping.

The network layer is a set of processes that allow the blockchain system to function, such as distributed networking mechanisms, data transfer and verification methods..

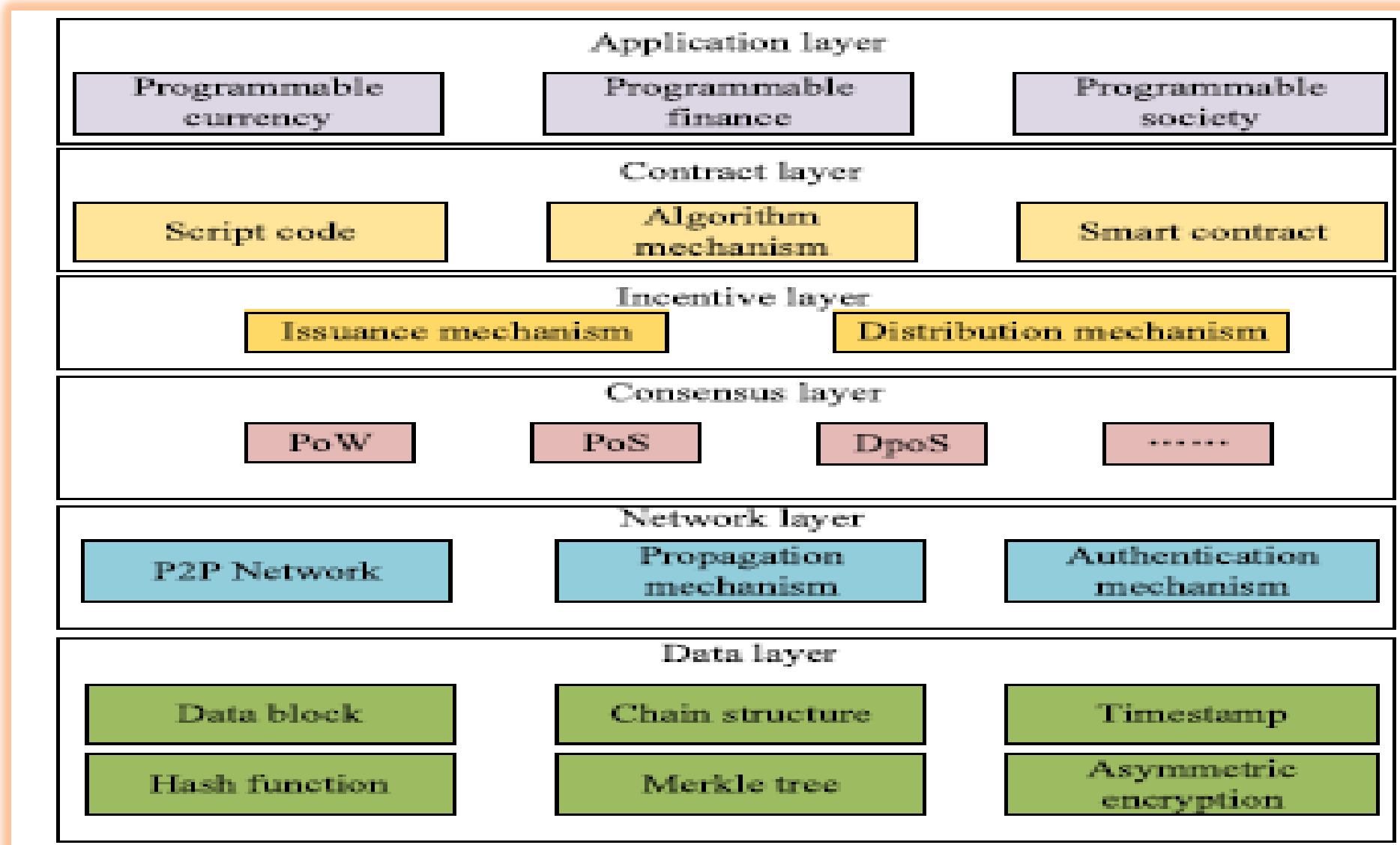
The consensus layer is the blockchain system's fundamental algorithm section, that sets the reporting subject and reporting technique.

To stimulate each node to engage in bookkeeping as much as possible, the incentive layer sends contract information in advance in addition to making contact with the transaction parties

Consensus algorithms

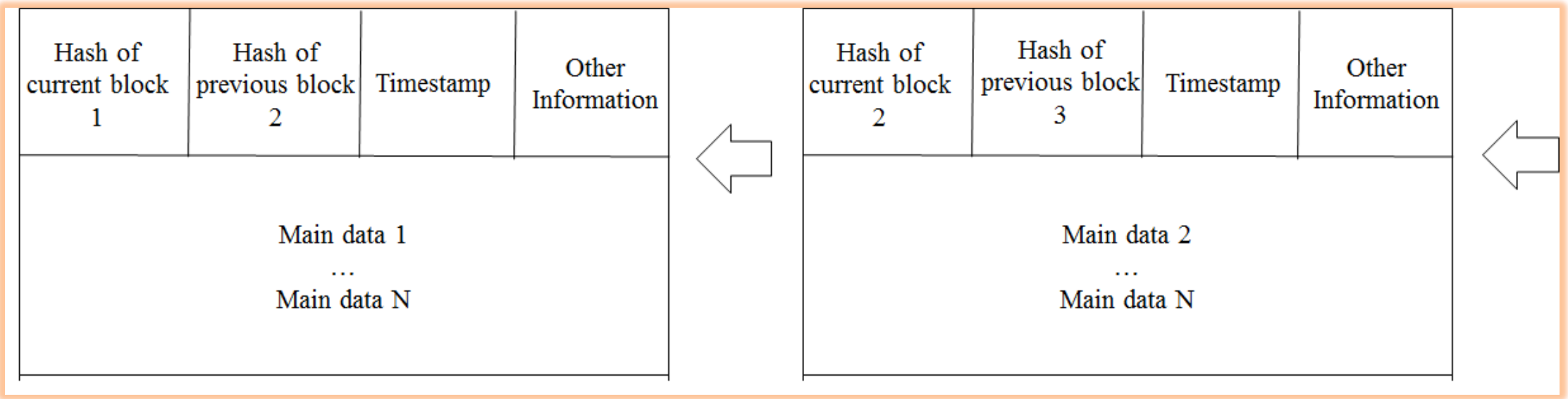
- (PoW): Proof of Work
- (PoS): Proof of Stake

Finger 2. The general structural framework of blockchain



In general, every block includes main data, a hash of the previous block, a hash of the current block, a timestamp, and additional metadata. Figure 3 shows the basic blockchain data structure, with each block:-

1. Main data.The most important information. depending on the service, for example, transaction records, bank clearance records, contract registers, or IOT data files etc..
2. Hash. When a transaction was completed successfully, it was hashed into a code and sent to all nodes.
3. Timestamp. The time when the block was created.
4. Additional Information. As an example, consider the block's signature, the Nonce value, or any other data that the user define.



Types of Blockchain

Three types of blockchain technology can be distinguished:-

- A public blockchain
- Private blockchain
- Consortium blockchains.

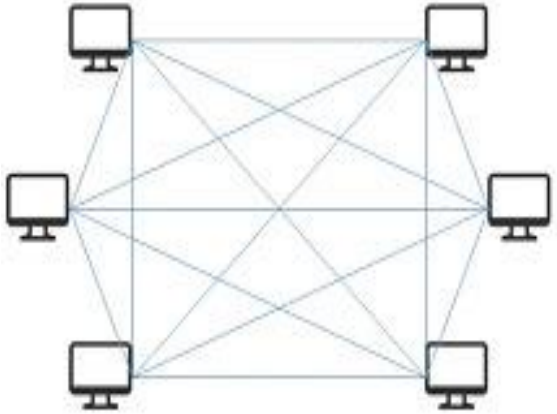


Figure 4: Public blockchain

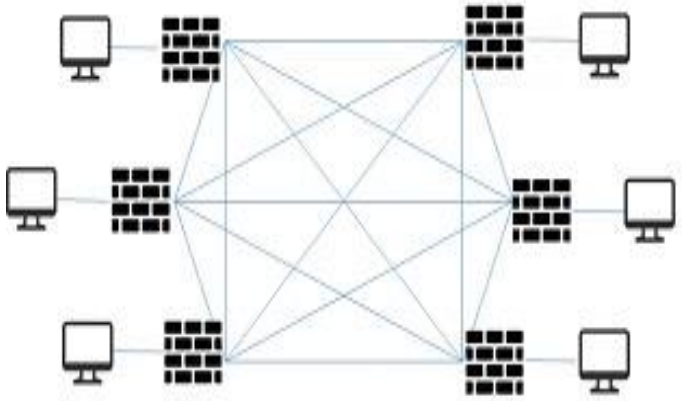


Figure 6: Consortium blockchain

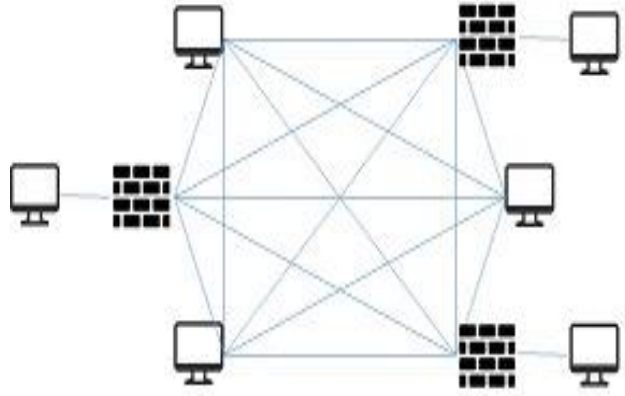


Figure 5: Private blockchain

Advantages and Disadvantages of Blockchain

Pros	Cons
• Improved accuracy by removing human involvement in verification	• Significant technology cost associated with mining bitcoin
• Cost reductions by eliminating third-party verification	• Low transactions per second
• Decentralization makes it harder to tamper with	• History of use in illicit activities
• Transactions are secure, private, and efficient	• Regulation
• Transparent technology	
• Provides a banking alternative and way to secure personal information for citizens of countries with unstable or underdeveloped governments	

3. Multimedia Protection

3.1 Encryption

Encryption symmetric (e.g., Advanced Encryption Standard (AES), Rivest Cipher (RC5), etc.); asymmetric (Rivest–Shamir–Adleman (RSA), Digital Signature Algorithm (DSA), etc.).

3.2 Digital watermarking

digital watermarking protects the multimedia material after it has been decoded by authorized users by concealing the identifying information (watermark) in the original content.

3.3 Fingerprinting

multimedia fingerprinting (also known as transaction tracking) may track down the identity of pirates (colluders) when an unauthorized copy is discovered.

3.4 Digital rights management (DRM)

DRM systems were created to allow for the safe transfer of digital material to an authorized recipient while imposing limits on the content's use after delivery

Discussion and Results

We noticed by reviewing previous research :

1. **Using blockchain technology with other technologies is better than using it alone.**
2. **Using it on text shows a better result than using it with video.**
3. **Frequent use of blockchain technology with encryption.**
4. **Ethereum Cryptocurrency has become more used than the Bitcoin**
5. **Common use of blockchain technology in multimedia is to protect the copyright of paid content.**

Conclusion

- **The success of this technology depends on various factors such as scalability and reliability.**
- **Blockchain technology has a good potential to be widely applied in copyright protection and management applications by allowing copyright holders and consumers to interact without costly intermediaries**