Blockchain technology: A bibliographic study

2022 IEEE 3rd International Conference on Electronics, Control, Optimization and Computer Science (ICECOCS) | 978-1-6654-5723-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICECOCS55148.2022.9983286

Manal IZEM
Informatics department
IBN TOFAIL
Kenitra, Morocco
manal.izem@uit.ac.ma

Mohamed AMNAI
Informatics department
IBN TOFAIL
Kenitra, Morocco
mohamed.amnai@uit.ac.ma

***Abstract*—At the rate of breakthroughs and new technologies, the world is always changing and evolving. The "Economist" magazine's report on the blockchain at the end of 2015 helped the technology gain popularity. A virtual currency based on blockchain technology, Bitcoin, is becoming more and more popular in the media. This article seeks to educate readers by popularizing and demystifying how the blockchain works. Many industries, including the financial industry, starting with the banking system, could see their game rules altered by this technology. The goal of this new trust model is to eliminate the current trust intermediary and replace it with a decentralized, shared system. A brand-new era is beginning. In this work, we are interested in the use of Blockchain in different fields.**

Keywords*— *Blockchain, crypto-currency, Bitcoin, Litecoin, Ethereum, transaction, cryptocurrency, cryptography, internet of things.

I. INTRODUCTION

A term used in information technology is "Blockchain" It is simply a shared database, with the attributes "unfalsifiable," "trace left," "traceable," "open and transparent," and "collective maintenance" for the data or information kept there. Based on these traits, blockchain technology has built a strong foundation of "trust," establishing a trustworthy cooperation mechanism with a wide range of potential applications.

Trust is, in fact, a challenging concept. While blockchain technology does reduce specific, limited reliances on trust, it also necessitates alternative premises that may or may not be superior for particular use cases. Therefore, it is difficult to find talking points regarding the effectiveness, security, affordability, etc. of blockchain technology in a single line that are correct. It is obvious that a more nuanced conversation is necessary about this technology. The following three questions are commonly posed by corporate executives, government officials, investors, and researchers:

- What is blockchain technology, exactly?
- What functionalities does it offer?
- What are effective applications?

This article's objectives are to give comprehensive responses to these queries, a balanced introduction of blockchain technology that distinguishes hype from reality, and a helpful vocabulary for addressing blockchain-specific details in the future.

II. OVERVIEW OF BLOCKCHAIN

In the early 1990s, two American cryptologists Stuart Haber and W. Scott Stortnetta devised a computer system that anyone could write but that was impossible to erase and indestructible. Then in the 1991s, researchers came up with a solution that uses cryptographic security techniques to ensure that all files are secured by the blockchain. Later in 1992, the Markle Tree technology was also integrated into the system, allowing multiple documents to be stored simultaneously in the same block. It is a pity that this technology was then ignored and slowly abandoned. Unfortunately, this patent was cancelled in 2004 because it had not been updated, only four years before the Bitcoin boom. Hal Finney (Harold Thomas Finney II), a computer scientist and crypto campaigner, created a reusable proof-of-work system in 2004, called PoW (Proof of Work). The system receives irreplaceable hashcash[1] work tokens, which in turn create coins that can be transferred between users and signed by RSA[2].

PoW can be considered an early prototype of the blockchain, constituting an important first step in the encryption of currency history.

The end of 2008 saw the publication of a white paper on a peer-to-peer decentralized electronic payment system called Bitcoin on an encrypted mailing list by individuals or groups under the pseudonym Satoshi Nakamoto. Bitcoin is based on the Hashcash proof-of-work calculation. Compared to the highly reliable PoW operation, Bitcoin uses a decentralized point-to-point protocol to verify and track transactions to avoid double consumption. In short, Bitcoin "mines" using the mechanism of checking the work of each miner, then verified by decentralized nodes in the network.

On January 3, 2009, Satoshi Nakamoto mined and operated the first block of Bitcoins. He also received a bonus of 50 Bitcoins. On January 12, 2009, Hal Finney was the initial Bitcoin recipient and was given 10 Bitcoins by Satoshi Nakamoto. This was the first verified Bitcoin transaction ever.

In 2013, Bitcoin programmer and magazine co-founder Vitalik Buterin claimed that in order to develop decentralized applications, Bitcoin would need to write a scripting language. Unable to get support from the community, A new blockchain-based distributed computing platform called Ethereum is being developed by Vitalik, featuring scripting functions, also known as smart contracts [1].

[1] Hashcash: is a proof-of-work algorithm that has been employed in a number of systems as a denial-of-service defense mechanism.

[2] RSA: is a popular choice for secure data transfer and was one of the earliest public key cryptosystems.

A. *Definition*

A new technology, Blockchain, is seen as a possible game-changer with its unique trust-building mechanism, has become an important direction for the deep integration of finance and technology. But what is Blockchain and what is the potential of this technology for international trade [2]?

Blockchain is everywhere right now. But not everyone has yet understood what we are talking about, the evangelization phase is not over yet, here is a short explanation that can help you understand what it is and also explain it to others: Imagine a ledger or a digital record of transaction that everyone can read for free and freely, this ledger is decentralized, no entity controls the network and it is a distributed ledger. The records (users) are shared with all participants, without the need for a central authority and in which the transactions are stored in a highly secure, verifiable and permanent way, using various cryptographic techniques [3].

B. *Technical architecture of the blockchain*

After putting it into perspective and justifying its interest in the emergence of new use cases, this part describes the building blocks of the technology.

I will present the products at different stages of blockchain before concluding with an overview of technologies and tools.

In Figure 1, the basic division is made for 9 dimensions. Then, I analyze in detail the specific content of each module.

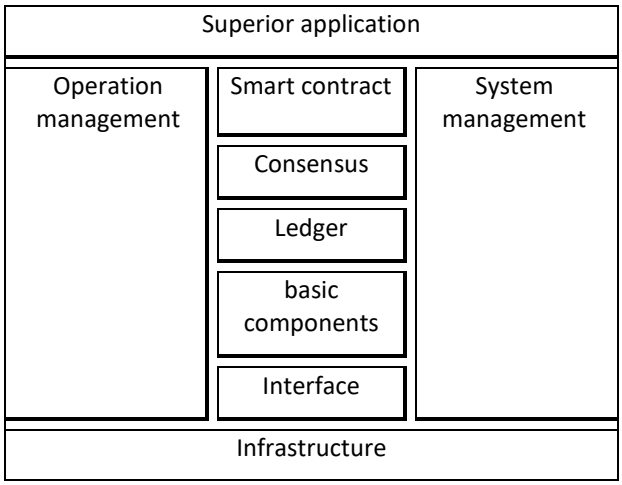

Figure 1: Technical architecture of blockchain technology

- The infrastructure layer provides the operating system and hardware facilities including physical servers, cloud hosts, etc. for the normal operation of the blockchain system.
- The core component layer implements the recording, verification and dissemination of information in the blockchain system. The blockchain is a distributed system, which means that all signed blocks are replicated across all nodes in the network. Like everyone else, you can, if you wish, use your computer to become a node. To do this, you need to download all the signed blocks so far. For Bitcoin, this is already more than 180 gigabytes.
- The ledger layer is responsible for storage. All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are only recorded once. The ledger layer incorporates the hash signature of the previous block into the next block to form a blockchain data structure. The ledger layer has two methods of recording data: asset-based and account-based.
- The consensus layer is responsible for coordinating and ensuring the consistency of each node's data records across the entire network, i.e., all nodes are competing to add the next block to the blockchain but only one of them will be selected to do so (and only it will be paid). This selection is random for each new block. This randomness is very important for the security of the blockchain; since nobody knows which miner will be selected. There are different ways to achieve this random selection of miners: these are the consensus mechanisms.
- The blockchain system's business logic must be implemented, assembled, and deployed as code by the smart contract layer in order to trigger situations, carry out automatic rule execution, and reduce the need for manual intervention.

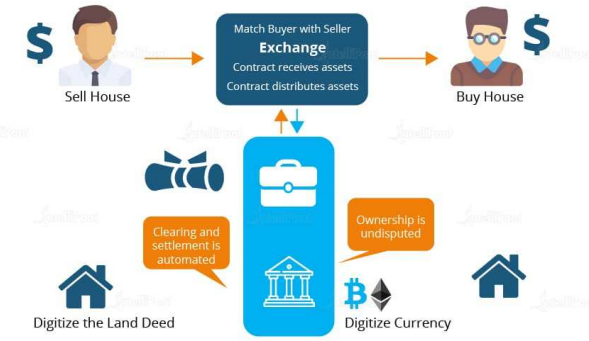

Figure 2: Smart contract operation

- Other components of the blockchain architecture, such as the two primary types of operations: node management and permission management, are managed by the system management layer. A crucial component of blockchain technology is entitlement management, particularly for authorization chains with increasingly stringent data access restrictions.
- The primary functions of the interface layer are to complete the encapsulation of functional modules and to provide the application layer with a straightforward calling method.
- The final component to be shown to the user is the application layer. Its primary purpose is to invoke the smart contract layer's interface in order to accommodate various blockchain application situations and provide consumers a variety of services and apps.
- The daily operation and maintenance of the blockchain system, including logging,

monitoring, administration, and growth, fall within the purview of the operation and maintenance layer. Traditional platforms' storage modules, data models, data structures, and programming languages differ from those of a unified architecture and sandbox[3] environment, etc., according to their own needs and locations.

C. *Field of application of blockchain*

Blockchain technology that reduces friction in business operations and improves efficiency is revolutionizing many industries. At the same time, reforms have also been implemented on a large scale, involving cooperative participants. In various fields such as finance, healthcare and government, blockchain has already contributed to industry reforms. Here are some of the endless possibilities of blockchain.

- Internet of Things
- Identifier management
- Supply chain management
- Financial Services
- Health care
- Insurance
- Government Agency
- Games
- Music
- Smart contracts

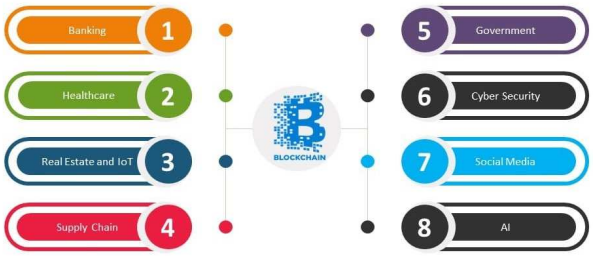

Figure 3: Applications of Blockchain

D. *Why use blockchain technology*

When individuals learn about blockchain, their next natural question is, "Why use blockchain?" Why would you use a distributed ledger? In an existing digital age, why not employ a conventional database or historical system of records?

- ✓ A blockchain is a highly decentralized system. This means that if two parties do not trust each other and want to share sensitive information without involving a third party, this is possible with a blockchain.
- ✓ Secure: No one can change or delete any data in the blockchain.

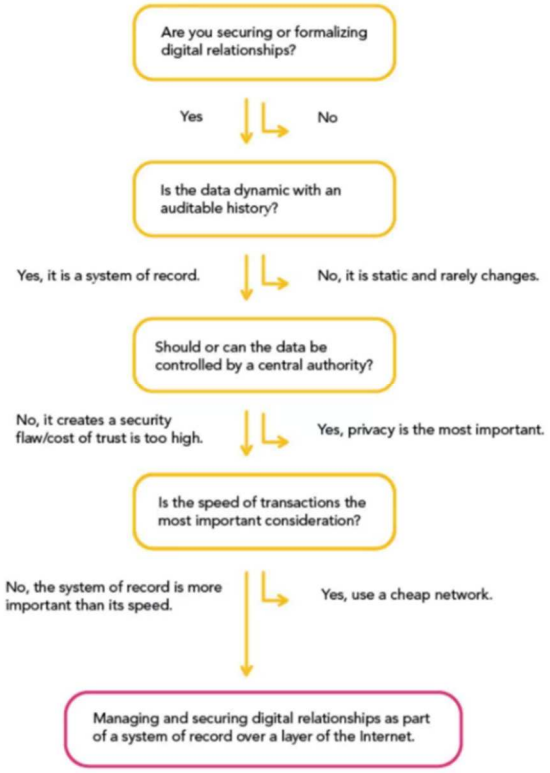

Figure 4: Why use Blockchain?

III. How Blockchain works

Let's make a simple definition and discuss Crypto-Currency [4] which uses the principles of cryptography to ensure the security of transactions and transaction control units to create a medium of exchange.

Just like banknotes commonly used in anti-counterfeiting designs, the anti-counterfeiting of crypto-currency is a new type of token that uses digital currency and virtual currency hashing, and is linked to smart contracts. In 2009, Bitcoin became the first decentralized multi-currency crypto-currency. Hereafter, the term refers to the crypto of these designs [5] . Since then, several similar crypto-currencies have been created often called altcoins[4] [6] [7]. Crypto-currency is based on a decentralized consensus mechanism [8], different from the financial banking system based on a centralized supervision system. You are first betting on a project, a promise and even a business model. To help you see this more clearly, I decided to explain the differences between the different series of crypto-currencies according to their most logical use [9] Cryptography is the most important component of the blockchain. It is a field of using mathematics to encrypt and decrypt data [10]. It allows you to store sensitive information or transmit it over unsecured networks like the internet so that it cannot be read by anyone except the intended recipient [11]. Cryptography has been around for over two thousand years. Now, it is the science of keeping things confidential by using encryption techniques. However, confidentiality is not the only goal. When it comes to cyber security, there are a number of things we are concerned about

[3] Sandbox: is a closed testing environment that enables users to execute files or run programs without altering the platform, system, or application they are operating on.

[4] The term "altcoins" refers to all crypto-currencies other than Bitcoin

when it comes to data. These include confidentiality, completeness, availability and non-repudiation Any information in the form of a text message can be called plaintext. The idea is to encrypt the plaintext using an encryption algorithm and a key that produces the ciphertext. The ciphertext can then be transmitted to the intended recipient, who decrypts it using the decryption algorithm and key to obtain the plaintext [12].

A. What are the differences between Bitcoin (BTC), Litecoin (LTC) and Ethereum (ETH)?

Bitcoin[5], Litecoin[6] and Ethereum[7] are the three main crypto-currencies. However, while they have much in common, they each have their own peculiarities. Therefore, we will see the difference between these three crypto-currencies [13].

a) The differences between Bitcoin and Litecoin

These are the two most similar currencies. Surprisingly, Litecoin is one of the first Bitcoin forks. It was developed by Charlie Lee and was initially released as open source on Github[8] on October 7, 2011. The token is designed as a faster and scalable alternative to Bitcoin. This token is very similar to the previous token, but there are many important differences. Since the token is designed as a "lighter" alternative to Bitcoin, it has been modified to improve its speed and usability [14].

Some differences between Litecoin and Bitcoin are:

- Reduced block generation time (from 10 minutes for Bitcoin to 2.5 minutes for Litecoin)
- Increased total token supply
- Different hashing algorithms (Scrypt instead of Bitcoin's Sha-256)
- Improved graphical user interface

Litecoin is often called the "silver" crypto-currency to match the "gold" status of Bitcoin's "gold" status.

The table below shows the main differences between Bitcoin and Litecoin [14]:

Table 1: The comparison between Bitcoin & Litecoin

	Bitcoin	Litecoin
Token Restriction	21 Millions	48 Millions
Algorithm	SHA-256	Scrypt
Concept	Digital money (Gold)	Digital money (Silver)
Average exit time	10 min	2,5 min
Block explorer	Blockchain.info	Block-explorer.com
Who made it	Satoshi Nakamoto	Charlie Lee
Date Of creation	January 3, 2009	October 7, 2009

b) The differences between Bitcoin and Ethereum

Ethereum and Bitcoin are two common crypto-currencies, but the most important thing is that the difference is huge. Here are the main ones between them [15]:

- The time it takes to generate a block. Although Bitcoin takes 10 minutes, Ethereum is much faster as it only takes 12 seconds.
- The algorithm used by the two crypto-currencies are different. In addition, Ethereum is more flexible and offers users more choice. Overall, with Ethereum, we can accomplish everything that Bitcoin can do, but we can also do other things.
- Finally, Ethereum is much more focused on its technology, of which Ether is just one component, whereas Bitcoin has primarily created a stable currency that is primarily intended for exchange.

c) The difference between Litecoin and Ethereum

Regarding Litecoin and Ethereum, we can note that the differences between Ethereum and Bitcoin are similar, but there are important differences between the two [13];

- The time needed to generate a block. The time needed to generate a block with Ethereum is less than the time needed to generate a block with Litecoin.
- Although Litecoin has been one of the most profitable crypto-currencies for miners, it is currently being overtaken by Ethereum.

In short, we can say this:

- Each of these three crypto-currencies has its own advantages and features.
- Despite the versatility of Ethereum and the appeal of Litecoin, Bitcoin is by far the most popular crypto-currency, not least because it is so stable
- Among the various crypto-currencies, Bitcoin serves as the benchmark and the others are compared to it
- You will find different types of crypto-currencies, which can allow you to pay anonymously, to mine, to find a good alternative to Bitcoin or which offer their own ecosystem.

B. What is cryptocurrency

Crypto-currency is a general term for currencies that use cryptography as a security measure and is synonymous with virtual currency [16].
It is characterized by the use of technology such as public key encryption, hashing or digital signatures to combine the two to improve the confidentiality of communications [17].
Virtual currency can be used as a reward for goods or services between an unlimited number of people and companies on the Internet. In the "fund settlement

[5] Bitcoin (₿, BTC) (from bit: unit of binary information and coin "coin") is a cryptocurrency otherwise known as cryptocurrency
[6] Litecoin (currency symbol: Ł; acronym: LTC) is a distributed electronic currency, Each Litecoin is divided into one hundred million smaller units, defined by eight decimal places.
[7] Ethereum: is a decentralized exchange system that enables users to create smart contracts using a language that is Turing-complete.
[8] GitHub: is a website and cloud service that aids programmers in managing, tracking, and controlling modifications to their code.

algorithm", the legal definition of crypto currency is as follows [18]:

- When purchasing the borrowing of goods or receiving services, an unidentified person can use these goods to pay for these expenses, and an unidentified person can buy as the other party. And the value of the property that can be sold.
- The value of the property that can be exchanged with an unidentified person as the other party of the party mentioned in the previous point, an electronic data processing organization can be used for the transfer.

C. *Cryptography*

Let's use an example where the "Sender" wishes to transmit a message (m) to the "Receiver". If he sends the message in its current form, any adversary may easily intercept it, compromising its confidentially. In order to create the encrypted message known as "cipher text," "Sender" want to encrypt the message using an encryption algorithm (E) and a secret key (k). To intercept the message, the adversary has to know both the algorithm (E) and the key (k). The more robust the algorithm and key, the more challenging it is to attack. Keep in mind that designing blockchain systems so that their security measures may change to accommodate various users is still desirable.

The following figure illustrates how to express the set of stages common to this approach:

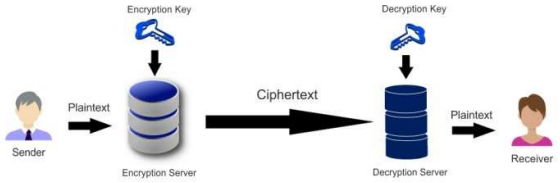

Figure 5: Cryptography working

D. *The different types of cryptography*

We look at the different forms of digital cryptography and how they can help us achieve the other three goals listed above. When we talk about digital cryptography, we usually refer to one of the following:

- Symmetric encryption.
- Asymmetric encryption.
- Hash functions.
- Digital signatures.

IV. Conclusion

In this article, we did explain the main lines without needing to be a computer expert to understand, we covered the evolution of blockchain, its history and definition, what are the benefits of the design and how it works, why is it so important with some relevant use cases. Then, we discussed the concept of cryptography.

The traditional goal of cryptography is to develop methods to exchange data securely. That's why modern cryptography addresses more generally the problems of communication security.

[1] E.GANNE, Can Blockchain revolutionize international trade?, Geneva: WorldTrade, 2018.

[2] M.ZAZA, L'impact des technologies de l'information et communication sur l'entreprise., Laayoune: Memoire online, 2016.

[3] «Blockchain - new opportunities for producers and consumers of electricity?,» [En ligne]. Available: https://www.pwc.ru/ru/publications/blockchain.html.

[4] «How much wealth do you know about cryptocurrency tycoons? "Forbes" list announced,» 17 February 2018. [En ligne]. Available: https://www.bbc.com/zhongwen/simp/business-43089926.

[5] L. O.Lakomski-Laguerre, L'alternative monétaire Bitcoin : une perspective institutionnaliste, open edition, 2015.

[6] J. Frankenfield, What investors need to know about altcoins, investopedia, 2021.

[7] «Qu'est-ce que la cryptomonnaie?,» [En ligne]. Available: https://finances-et-patrimoine.fr/bourse/la-crypto-monnaie/.

[8] «Crypto-monnaie : le guide complet,» [En ligne]. Available: https://crypto-monnaie.pro/quest-ce-que-la-crypto-monnaie/.

[9] G.Raymond, «Bitcoin, Ethereum, Ripple... L'avis de capital sur les cryptomonnaies qui comptent,» 22 March 2018. [En ligne]. Available: https://www.capital.fr/crypto/bitcoin-ethereum-ripple-lavis-de-capital-sur-les-cryptomonnaies-qui-comptent-1278913.

[10] G. Dubertret, initiation à la cryptographie, 2000.

[11] «Les fondements de la cryptographie,» [En ligne]. Available: https://www.clicours.com/les-fondements-de-la-cryptographie/.

[12] «Sécurité et Cryptographie,» 2013-2014. [En ligne]. Available: https://lipn.univ-paris13.fr/~poinsot/SEC/Chapitre_7_Printable.pdf.

[13] «Quelles differences entre Bitcoin (BTC), Litecoin (LTC) et Ethereum (ETH)?,» [En ligne]. Available: https://coin24.fr/crypto-monnaies/differences-btc-eth/.

[14] V.Flores, c'est quoi Litecoin (LTC)?, conseils crypto, 2018.

[15] R. Pomian-Bonnemaison, Bitcoin vs Ethereum : quelle est la différence ?, phoandroid, 2018.

[16] L. Rédaction, Cryptomonnaie : définition et synonymes, Journal du net, 2019.

[17] «Cryptomonnaie : qu'est ce que c'est?,» [En ligne]. Available: https://www.futura-sciences.com/tech/definitions/cryptomonnaies-cryptomonnaie-18278/.

[18] «What is crypto asset (virtual currency)?,» [En ligne]. Available: https://www.boj.or.jp/announcements/education/oshiete/money/c27.htm/.