National School Of Engineering Of Tunis

Year-end project report 1

Blockchain and Cryptomonnaies

Presented by :

Mayssa Somrani

Adam Sakly

Supervised by :

Mrs. Saoussen Ben Gamra

1st Year Industrial Engineering

Academic Year: 2022/2023

Dedication

We would like to express our sincere gratitude to Mrs. Saoussen Ben Gamra, our dedicated and attentive supervisor, whose invaluable guidance, encouragement, and expert insights have been instrumental in the successful completion of this bibliographical project. Her unwavering support and constant feedback have truly made a difference, and we are deeply grateful for the time and effort she has invested in us.

We would also like to extend our heartfelt thanks to the entire academic and administrative staff of ENIT for their unwavering support throughout our academic journey.

Finally, we would like to acknowledge and thank all those who have contributed in any way to the realization of this project. Without their assistance and encouragement, this work would not have been possible.

Contents

List of Figures

Acronyms

Crypto Cryptocurrency

P2P peer-to-peer

DigiCash Digital currency

B-MONEY Digital currency precursor

Bitgold Digital Gold Currency

Mt. Gox Bitcoin exchange bankruptcy

Doge Dogecoin

dApp decentralized application

BTC Bitcoin

ETH Ether

BNB Binance Coin

SOL Solana

USDC USD coin

AVAX Avalanche

DKE Double Key Encryption

MIP Microsoft Information Protection

LDAP Lightweight Directory Access Protocol

UPN User Principal Name

HYOK Hold Your Own Key

SHA-256 Secure Hash Algorithm 256-bit

SSL Secure Sockets Layer

TLS Transport Layer Security

DNS Domain Name System

NTP Network Time Protocol

DAO DAO

BFX Bitfinex

2FA Two-factor authentication

DHT Distributed Hash Table

IoT Internet of things

General Introduction

Cryptocurrencies have been making headlines in recent years as a revolutionary new form of currency that is decentralized, secure, and anonymous. Cryptocurrencies are digital or virtual currencies that use cryptography for security and operate independently of a central bank. The most famous cryptocurrency, Bitcoin, was created in 2009 and has since sparked a wave of innovation and competition in the digital currency space.

This document explores the history and evolution of cryptocurrencies, with a focus on their underlying technology, blockchain. The first chapter provides a comprehensive overview of cryptocurrency, including definitions, types, market developments, and the technological innovations that enable their creation and management.

The second chapter delves into blockchain technology, exploring what it is, how it works, and its relationship to cryptocurrencies. Specifically, it examines the role of blockchain in facilitating the creation, storage, and transfer of cryptocurrency assets. This chapter also explores the challenges and risks associated with blockchain and cryptocurrencies, such as scalability, security, and regulatory issues.

The third chapter provides a detailed analysis of the facts and figures related to the adoption of blockchain and cryptocurrencies around the world, with a focus on the case of Tunisia. It also examines the industry's response to past crises, such as the 2018 market crash, and the current challenges facing the industry.

Ultimately, this document aims to provide a comprehensive and insightful overview of the emergence and evolution of cryptocurrencies and blockchain technology. By exploring the technological, economic, and social dimensions of this transformative phenomenon, we hope to equip readers with the knowledge and insights necessary to navigate this exciting and rapidly evolving field.

Chapter 1

The Genesis Of Cryptocurrency

Introduction to chapter 1

Cryptocurrency is a type of digital currency that is decentralized and operates outside the control of central banks and governments. It all started with the creation of Bitcoin in 2009 by an unknown individual or group using the pseudonym Satoshi Nakamoto. Bitcoin was the first cryptocurrency to utilize blockchain technology, which is a secure and transparent digital ledger. It quickly gained popularity among technology enthusiasts and investors. Since then, numerous other cryptocurrencies have emerged, each with its own unique features and advantages. However, the long-term viability of cryptocurrencies and their potential impact on traditional financial systems continue to be controversial topics of debate.
In chapter one, we explored the world of cryptocurrencies, starting with their definition, history, and various forms. We also delved into the workings of the cryptocurrency market, including how it functions and the various exchange platforms available. Furthermore, we looked at the technological innovations that underlie cryptocurrencies, including decentralized databases, double-key encryption, and cryptographic protocols . Overall, the chapter provides a comprehensive overview of the foundations of cryptocurrencies and the technologies that make them possible.

1.1 Definition

Cryptocurrency, sometimes called Crypto is a system of digital payment that does not rely on banks to check the transactions.

It's a sharing system P2P (peer-to-peer), allowing everybody to send and receive payments anywhere. it's not physical money transported nor exchanged in the real world:

the payments in cryptocurrency are purely virtual realized in a database online

and relative to a certain particular transactions. When you transfer funds in cryptocurrency, the transactions are registered in a public registry. The crypto-currencies are stored in digital wallets.

The crypto-currencies were appointed because they use encryption to verify the transactions.

In other words, they integrate a complex coding system to transfer crypto money data from wallets to public registers The encryption aims to ensure security.

1.2 Cryptocurrency history

The Godfather of cryptography, David Chaum, wrote a paper in 1983 titled "Blind signatures for untraceable payments." that discussed a new sort of encryption that would give digital money the advantages of anonymity, proof of payment, and fund freezing.

To profit from this theatrical effort in digital currency, Chaun created DigiCash in Amsterdam in 1989, but this firm was unable to capitalize on its early accomplishments.

Previous attempts to establish online currencies with ledgers secured by encryption, such as B-MONEY and Bitgold , were made in 1998, but they were never completely developed.

Using the alias "Satoshi Nakamoto," which first appeared on the original 2008 Bitcoin white paper that first described the blockchain system that would serve as the backbone of the entire Cryptocurrency market, a person or group of people created bitcoin in 2009, during the global financial crises, at a time when disbandment of backs in the United States and central governments was at its height.

A year later, when someone chose to sell his cryptocurrencies, exchanging 10,000 of them for two prizes, Bitcoin was priced for the first time. At today's prices, the buyer's bitcoins would be worth more than $100 million if they had been kept.

In 2013, the price started to fall dramatically. Many investors at this time would have lost money as the price fell to about $300; it would take more than two years before it rose above $1,000 once more.

Unsurprisingly, Bitcoin has proven to be a popular and profitable target for thieves in 2014, given that it was created with anonymity and a lack of control in mind.

The largest Bitcoin exchange in the world, Mt. Gox , shut down in January, and the owners of 850,000 bitcoin never saw them again.

Whatever the case, someone dishonestly obtained a haul that was worth 450 million dollars at the time. Investigations are still ongoing to determine precisely what happened. Those lost coins would be worth $4,4 billion at today's values.

A year later, when someone chose to sell his cryptocurrencies, exchanging 10,000 of them for two prizes, Bitcoin was priced for the first time

At today's prices, the buyer's bitcoins would be worth more than $100 million if they had been kept.

The price of bitcoin steadily increased, year after year, passing from $434 in January 2016 to $998 in January 2017.

In July 2017, a bitcoin software update aimed at improving its adaptability and supporting the Lightning Network was approved.

One week after the update was activated in August, bitcoin traded around $2 700 and in 17 December 2017 , it reached an astronomical historical record a little less than $20 000

During this period, a new blockchain project called Ethereum was talked about in the cryptocurrency community and occupied the second place in the ranking of crypto on the market.

Bitcoin was unable to maintain its historic peak, Ethereum, which hit its own high peak in January 2018 for a value approximately 1400 dollars, also followed the trajectory of its predecessor.

Financial regulations and the security issues due to incessant hacks of platforms contributed to this decline, which by the end of 2018 had fallen to around 3700 dollars.

Prices didn't stay down, and since the end of 2018, bitcoin, as well as most other cryptocurrencies, Ethereum included, have bounced back. [2]

1.3 Types of cryptocurrency

In general, crypto money can be grouped into two distinct categories:

1.3.1 Coins (pieces) and Altcoins

Coins means any crypto money that use its own independent blockchain.For example, bitcoin is a coin because it works on its own infrastructure.In the same way, Ether works on the Ethereum blockchain.The word: Altcoin means all the coins other than bitcoin. Many altcoins work as well as bitcoin. Nevertheless, some, like Dogecoin, are quite different.

The Doge offer an unlimited number of coins .While for bitcoin, the number of bitcoins that can be created was capped at 21 millions.

1.3.2 Tokens

Tokens are also digital assets which can be bought and sold.However, they are non-native assets, which means that they use blockchain infrastructure that is not theirs.This includes, Tether which is hosted on Ethereum blockchain and others.Especially, TerraUSD ,Chainlink , UniSwap and Polygon.

1.4 The cryptocurrency market

While crypto-currencies appear to be similar to real currencies, they actually have a very different way of working than other currencies, influenced by banking systems. Indeed, Bitcoin, Ethereum, Dash and Litecoin are crypto-currencies whose value changes regularly. In a few years, their value has multiplied and some are even becoming more valuable than real currencies.

How do the crypto-currency markets work? What is the value of Bitcoin, or Ether, based on?

1.4.1 Principle of crypto-currency markets

Crypto-currencies are decentralized currencies, entirely controlled by cryptography. Since crypto-currencies never go through banks or financial institutions, they have no connection to the banking community and therefore their market cannot directly evolve according to banking policies or investments made by these institutions. They exist in limited numbers, but are constantly produced by the mining system that allows new units to be introduced into the market every day.

The principle of the crypto-currency market therefore has similarities to that of precious metals, of which there is a limited quantity, but from which new units are extracted by mining. As in the case of a rare metal, the minable quantity being reduced, the value of it will depend on the demand. The price of a crypto-currency is therefore entirely based on the law of supply and demand.For example, when the supply of Bitcoins exceeds the demand, then the value of the Bitcoin drops. On the other hand, if there are more demanders than sellers, then the price skyrockets.

1.4.2 Market developments

Bitcoin and Ethereum have demonstrated through the evolution of their respective markets, the instability of their values. Indeed, if in periods of high demand, the value of Bitcoin swells to peaks, the market goes through moments of strong instability, sometimes falling violently by several billion dollars.

The case of Ethereum is interesting because the crypto-currency only serves here as a basis for a system selling decentralized application possibilities. As decentralized applications are a promising solution for many developers, demand seems to be smoothing out and increasing in a steady upward trend.

Since Ether is used to buy the "gas" needed by dApp developers to run their decentralized applications, the demand for Ether remains constant despite the fluctuations of the market. However, this operating system seems to have its limits in that it dangerously links the crypto-currency market to the real currency market.

In fact, companies buying Ether according to economic conditions will have to reduce their demand for Ether in case of a crisis or bankruptcy, thus making the value of the crypto-currency fall and making it more difficult for miners to sell Ether. A stock market crisis could therefore indirectly influence the crypto-currency markets, which are decentralized and independent of the classic financial systems.[3]

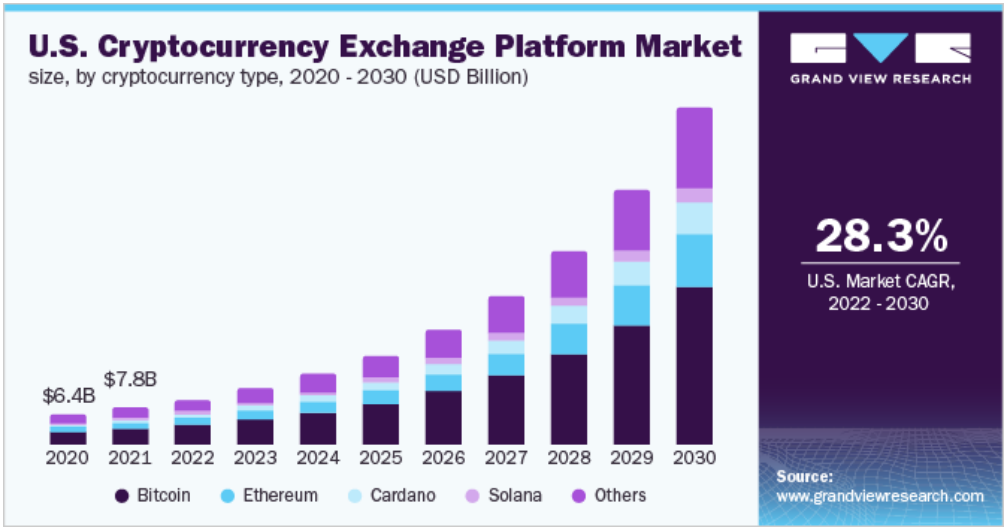


Figure 1.1: Cryptocurrency Exchange Platform Market size report, 2030

1.4.3 The 9 top cryptomoney most known and how they work

-Bitcoin(BTC)

Bitcoin is the first invented cryptomoney and it stay the most known one. It works on its own blockchain with verified transactions by an army of decentralized miners. In January 2022, it was the highest market capitalization with 896 billions USD.

-Ether(ETH)

Ether is a cryptomoney based in Ethereum blockchain and it's not capped, which means theoretically, there is an unlimited number of coins that can be created. Also, Ethereum allows the creation of smart contracts (programs which reside in blockchain Ethereum and which are executed automatically when certain conditions are united.

-Binance Coin (BNB)

Binance is the largest trading cryptomoney platform in the world in 2022. The transaction fees for the exchange have been reduced to encourage the adoption of Binance Coin. To ensure the stability of its value, Binance destroys a fixed percentage of coins in circulation.

-Tether(USDT)

Tether is a "stablecoin" type, designed to counter the problem of price volatility by being attached to an external assert. Every coin is actually backed by an equivalent amount in dollars US, which allows it to avoid price variations that undergo the others cryptomoney. Nevertheless, there is some disagreement regarding its real backing to dollar.

-Solana(SOL)

Solana is the native coin of Solana platform.Solana's network can run the impressive amount of 50 000 transactions per second, which makes this platform particularly attractive for investors who looking to trade quickly.

-XRP

XRP uses the ripple network. It has been described as "the cryptomoney for banks" because it was created in order to respond to the financial services sector's needs.Designed to facilitate international payments, XRP acts like a bridge between the currencies in order to offer cheaper and faster transfers all over the world.

-Cardano(ADA)

ADA is the cardano's blockchain coin. It is called "a third-generation cryptocurrency."Cardano divides its blockchain into two layers in order to increase transaction speed.It implements a native token to ensure a better experience for ADA crypto holders.

-USD Coin (USDC)

Like Tether, l'USD coin is a stablecoin attached to dollar US, which cannot be mined. Unlike Tether, USD coin benefits a more a more transparent funds and a better audit processes. The goal is to eliminate some cryptoccurencie's risks. Indeed, the users can always remove their coins and receive the corresponding amount in the chosen currency.

-Avalanche(AVAX)

AVAX is the Avalanche platform's native coin (the fastest smart contract platform).It is used to pay the costs of transactions on the platform. A vanche platform allows developers to create new custom blockchains as " subnets". The platform is compatible with Solidity (the Ethereum blockchain's programming language).

1.5 Cryptocurrency An innovation based on a combination of prevalent techniques

Cryptocurrencies are usually built using blockchain technology. Blockchain describes the way transactions are recorded into "blocks" and time stamped. It allows a person to safely send money to another person without going through a bank or financial services provider. Many in the financial services industry refer to blockchain technology as distributed ledger technology. And some see blockchain as a more reliable database than their existing databases.

1.5.1 Database decentralazed

1.5.1.1 Definition

A decentralized database system allows for multiple users to access the same data without having to share information with each other, which makes it an ideal solution for businesses that need to keep sensitive information confidential [1] .

1.5.1.2 The 4 properties of a Decentralized Database

There are certain factors that influence what makes a decentralized system function the way it does. Each factor makes up for different properties that run the system and here some properties that make it a stable system :

-Offline first

Offline first reduces the levels of network dependency, allowing you to create a "fork" by leaving the system at any point in time.

-Sharing

'*Offline first*' makes a file decentralized but is insufficient to act as a system. To do so, instance or node needs to communicate with other nodes or individual actors in the system.Different models of sharing are used as a part of decentralized database systems.

-Fault-tolerant

A decentralized software can often assume the appearance and disappearance of nodes without warning.that's way decentralized systems design methods for handling this type of activity from other nodes with usually maintain some sort of list of active nodes. Moreover, decentralized systems usually maintaining history so nodes coming online can synchronize to the correct state.

-Trustless

The trustless feature can tackle malicious or rogue nodes that may corrupt the entire system. A decentralized system means that you will not have control of all nodes. To prevent breaches, using cryptography can help make the system more secure and identify users who may not be a part of the database.

1.5.1.3 Decentralized databases Models

Decentralized databases are a new approach to data management that are gaining popularity due to their ability to provide increased security, transparency, and fault tolerance. Unlike traditional databases, where data is stored on a centralized server, decentralized databases distribute data across multiple nodes or servers, making it more resistant to tampering and hacking. Here are introductions to three popular decentralized database models:

-Blockchain

Blockchain is a distributed ledger that records transactions and stores data in a way that is resistant to modification and tampering. Each block in the chain contains a record of several transactions, and once a block is added to the chain, it cannot be altered or deleted. Blockchain is maintained by a network of nodes, rather than a single central authority, which makes it more secure and transparent than traditional databases. It is often used in financial applications, such as cryptocurrency, because it provides a secure and transparent way to record transactions without the need for a trusted intermediary.[2]

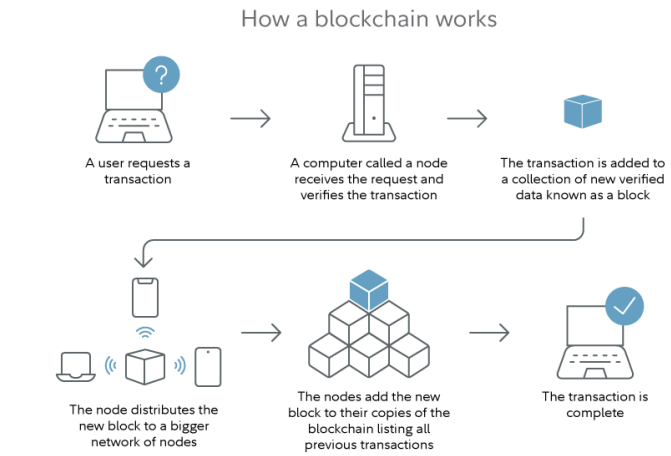


Figure 1.2: Decentralized Trust: A Visual Guide to Blockchain Technology
Source : fidelity investments

-Peer-to-peer(P2P) Network

A peer-to-peer (P2P) network is a decentralized database model where each node in the network stores a copy of the data, and changes made by one node are propagated to the others. P2P networks are often used for file sharing and distribution, as they can handle large amounts of data and are more resistant to failures than centralized systems. They can also be used for messaging and other communication applications, as they do not rely on a centralized server for routing messages.[3]

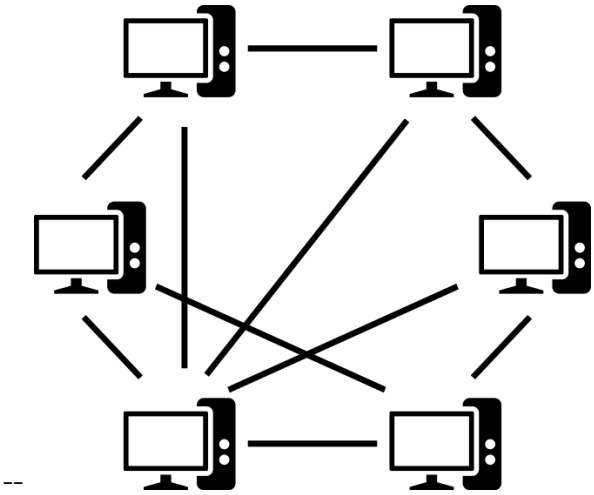
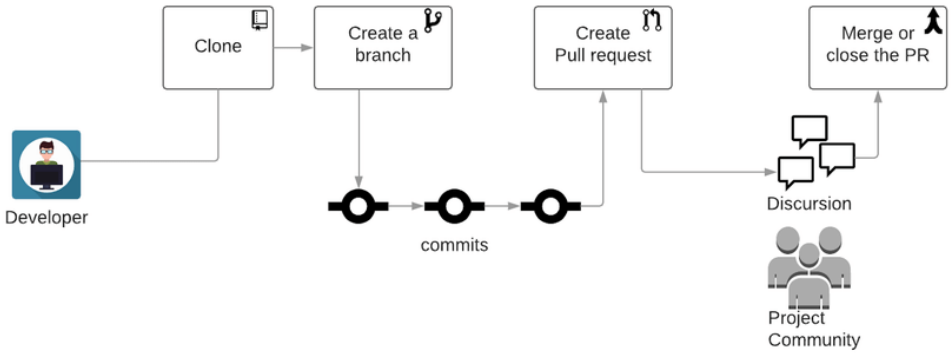


Figure 1.3: Peer-to-Peer Networking: Decentralizing Digital Connections
Source : Wikipédia

-Distributed Hash Table (DHT)

A distributed hash table (DHT) is a decentralized database model that is used for storing and retrieving key-value pairs. Each node in the network stores a subset of the data, and queries for a specific key are routed to the node that is responsible for that key. DHTs are often used in distributed applications, such as peer-to-peer file sharing, content distribution networks, and distributed databases. They provide a scalable and fault-tolerant way to store and retrieve data, as well as a mechanism for load balancing across the network.[4]



--

Figure 1.4: The Magic of Git: A Visual Guide to Version Control
Source : Github platform

1.5.1.4 Decentralized Database Options

Decentralized database options are becoming increasingly popular as they offer several benefits over traditional centralized databases. Decentralized databases distribute data across multiple nodes, which provides increased security, transparency, and fault tolerance. Additionally, they can handle large amounts of data and provide a more efficient way to store and manage information. Here is an introduction to some popular decentralized database options:

- BigchainDB

BigchainDB is a scalable blockchain database that allows users to store and manage large amounts of data. It combines the security and transparency of blockchain technology with the high throughput and low latency of traditional

databases. BigchainDB supports a range of data types, including structured, semi-structured, and unstructured data, and is suitable for applications such as supply chain management, identity verification, and IoT data management.

- Holochain

Holochain is a distributed computing platform that allows users to build decentralized applications using a peer-to-peer network. It uses a different architecture than blockchain, which allows for faster processing and greater scalability. Holochain supports a wide range of applications, including social networks, collaborative applications, and financial services.

- Apache Cassandra

Apache Cassandra is a distributed database that provides high scalability and fault tolerance. It is designed to handle large amounts of data across multiple nodes, making it suitable for applications that require high availability and low latency. Cassandra supports both structured and unstructured data and provides features such as automatic partitioning and replication, which can help improve performance and reduce the risk of data loss.

1.5.2 Double key encryption

1.5.2.1 Definition

Double Key Encryption (DKE) is a new option offered by Microsoft Information Protection (MIP), a cloud-based data classification and protection software.
Indeed, Given that many customers are worried to start their journey to the cloud because of data protection concerns, Microsoft implemented a new option to protect unstructured data (documents, files) against unauthorized access, wherever the document or file is stored AND against the cloud provider itself [5].

1.5.2.2 How does it work ?

Double Key Encryption enables you to protect your highly sensitive data while keeping full control of your encryption key. It uses two keys to protect your data—one key in your control, and a second key is stored securely in Microsoft Azure. Viewing data protected with Double Key Encryption requires access to both keys. Since Microsoft can access only one of these keys, your protected data remains inaccessible to Microsoft, ensuring that you have full control over its privacy and security.

Currently DKE demo server allows two ways to authorize users and both require Lightweight Directory Access Protocol (LDAP) access to Active Directory:

- LDAP group membership
- Emails addresses (based on the user's UPN)

1.5.2.3 The difference between Double key encrypton (DKE) and Hold your own key (HYOK) solution

Double Key Encryption encrypts your data with two keys. Your encryption key is in your control and the second key is stored in Microsoft Azure, allowing you to move your encrypted data to the cloud while HYOK protects your content with only one key and the key is always on premises.

1.5.3 Cryptographic hashing

Cryptographic hashing has been an integral part of the cybersecurity spectrum. In fact, it is widely used in different technologies including Bitcoin and other cryptocurrency protocols.

1.5.3.1 Definition

In simple terms, hashing means taking an input string of any length and giving out an output of a fixed length. In the context of cryptocurrencies like bitcoin, the transactions are taken as input and run through a hashing algorithm (bitcoin uses SHA-256) which gives an output of a fixed length.

1.5.3.2 Cryptographic hash functions

Cryptographic hash is mostly utilized for mining purposes. So, in Bitcoin, mining is a process of verifying SHA-256 hashing functions. This means that hashing can be used to write new transactions, reference them back to the previous block, and timestamp them.
For cryptographic hash, there are plenty of algorithms used. This includes the following:

-Message Direct (MD5)
-Secure Hash Function (SHA1)
-Secure Hash Function (SHA-256)

Now, let's take a look at an example of a cryptographic hash function.We are going to use the online available "SHA-256 tools". Now, if you type 101Blockchains as input, it will give the following output.

-Input 101Blockchains.com

-Output fbffd63a60374a31aa9811cbc80b577e23925a5874e86a17f712bab874f33ac9

1.5.4 Cryptographic protocols

A cryptographic system is a collection of software and hardware that can encrypt or decrypt information. A typical cryptographic system is the combination of a desktop computer, a web browser, a remote web server and the computer on which the web server is running. A cryptographic protocol, by contrast, describes how information moves throughout the cryptographic system. In our examples, the web browser and the remote web server communicate using the Secure Sockets Layer (SSL) cryptographic protocol.

1.5.4.1 Definition

Cryptographic protocols provide secure connections, enabling two parties to communicate with privacy and data integrity.The Transport Layer Security (TLS) protocol evolved from that of the Secure Sockets Layer (SSL). The primary goals of both protocols is to provide confidentiality, (sometimes referred to as privacy), data integrity, identification, and authentication using digital certificates.

1.5.4.2 Cryptographic protocols

- " SSL " and **" TLS "**

The SSL and TLS protocols enable two parties to identify and authenticate each other and communicate with confidentiality and data integrity. Indeed,The SSL or TLS handshake enables the SSL or TLS client and server to establish the secret keys with which they communicate.

- " SSL "

SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol. It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern TLS encryption used today.
SSL Cryptography uses Public Key Cryptography which requires asymmetric keys to encrypt and decrypt data sent between a server and a client—typically a website and a browser, or a mail server and a mail client, like Microsoft Outlook.

- " TLS"

TLS is a cryptographic protocol that provides end-to-end security of data sent between applications over the Internet. It is mostly familiar to users through its

use in secure web browsing, and in particular the padlock icon that appears in web browsers when a secure session is established. However, it can and indeed should also be used for other applications such as e-mail, file transfers, video/audioconferencing, instant messaging and voice-over-IP, as well as Internet services such as DNS and NTP.

TLS uses a combination of symmetric and asymmetric cryptography, as this provides a good compromise between performance and security when transmitting data securely.

Conclusion to chapter 1

In summary, the creation of Bitcoin in 2009 marked the genesis of cryptocurrency, introducing the world to the concept of decentralized digital currency. Bitcoin's use of blockchain technology paved the way for the development of numerous other cryptocurrencies, each with its own unique features and benefits. Cryptocurrencies have the potential to disrupt the traditional financial industry by providing a secure, decentralized, and transparent alternative to traditional financial systems. However, their long-term viability and impact on the traditional financial system remain uncertain and subject to ongoing scrutiny. Nonetheless, the genesis of cryptocurrency has opened up new possibilities and opportunities for innovation in the financial industry, and its evolution continues to shape the future of finance.

Chapter 2

Blockchain technology and Cryptocurrencies

Introduction to chapter 2

Blockchain technology is a decentralized digital ledger that records transactions in a transparent and secure manner. It was first introduced in 2008 as a way to enable secure and transparent transactions without the need for intermediaries. Since then, it has become a trendy topic in the world of finance and technology, with potential applications ranging from finance and banking to supply chain management and voting systems. Blockchain technology is unique in that it allows for the creation of tamper-proof records that are stored on a distributed network of computers, making it virtually impossible to alter or falsify transaction records. This has the potential to revolutionize the way we conduct transactions and manage data, providing increased transparency, security, and efficiency. In this way, blockchain technology represents a new era of trust and transparency in digital transactions.

Chapter two provided an in-depth analysis of blockchain technology and its relationship with cryptocurrencies. We started with a definition of blockchain, how it works, and the various types of blockchains. Then, we explored the relationship between blockchain and cryptocurrencies, including the creation of a chain of transactions in cryptocurrencies, the creation of a cryptocurrency wallet, and the payment of cryptocurrencies on the blockchain. Finally, we discussed the potential risks and challenges associated with the use of blockchain technology in the cryptocurrency market. Overall, the chapter offered a comprehensive overview of blockchain technology and its impact on the world of cryptocurrencies.

2.1 What is blockchain ?

2.1.1 Blockchain definition

Blockchain is a digital ledger technology that enables secure, transparent, and decentralized storage and transmission of information. It is a distributed database that allows multiple parties to have simultaneous access to the same information, and any changes made to the information are immediately recorded and verified by the network of computers that are part of the blockchain.

In a blockchain, information is stored in blocks that are linked together in a chronological order, forming a chain. Each block contains a record of transactions, and once a block is added to the chain, it cannot be altered or deleted. This makes the blockchain tamper-resistant and reliable, as all parties can trust that the information stored on it is accurate and immutable.

2.1.2 The functioning of blockchain

Blockchain is a decentralized digital ledger that is designed to facilitate secure, transparent, and immutable transactions. The functioning of blockchain can be explained in the following steps:

- Participants in the network make a transaction, which is a transfer of digital assets such as cryptocurrency, digital identities, or other data.

- The transaction is broadcasted to all the nodes in the network.

- The nodes verify the transaction and validate it using complex algorithms and consensus mechanisms. Once the transaction is validated, it is added to a block.

- The block is then added to the chain of blocks, forming a sequential and unalterable record of all the transactions in the network.

- Each block contains a unique cryptographic hash, which is a mathematical function that converts the transaction data into a fixed-length string of characters. This hash is used to link the blocks together in the chain, making it impossible to alter or tamper with any previous transactions without invalidating the entire chain.

- The blockchain is maintained by a network of decentralized nodes, which are responsible for validating transactions, adding new blocks to the chain, and ensuring the integrity and security of the network.

Overall, the functioning of blockchain is based on its decentralized, consensus-driven, and cryptographic nature, which allows for secure and transparent transactions without the need for intermediaries or centralized authorities.

2.1.3 Blockchain types

There are several types of blockchains, each with its unique characteristics and use cases. Here are some of the most common types of blockchains:

- Public Blockchain: A public blockchain is open to anyone, and anyone can participate in the network by becoming a node. Bitcoin and Ethereum are examples of public blockchains. Transactions on a public blockchain are transparent and immutable, and the consensus is achieved through a proof-of-work or proof-of-stake mechanism [6].

- Private Blockchain: A private blockchain is restricted to a particular group or organization, and only authorized participants can become nodes. Private blockchains are often used for enterprise applications and allow for more control and privacy. The consensus is achieved through a centralized authority or a pre-approved set of nodes[7].

- Consortium Blockchain: A consortium blockchain is a hybrid between public and private blockchains, where a group of organizations come together to form a network. Consortium blockchains are often used for industries such as finance, where multiple parties need to share data and collaborate in a secure and transparent manner.

- Permissionless Blockchain: A permissionless blockchain allows anyone to participate in the network without any restrictions. Bitcoin and Ethereum are examples of permissionless blockchains.

- Permissioned Blockchain: A permissioned blockchain allows only authorized participants to access the network and participate in the consensus process. Permissioned blockchains are often used in enterprise applications where access control and privacy are critical.

Overall, the type of blockchain used depends on the specific use case and requirements of the application. Public blockchains are often used for applications that require decentralization and transparency, while private and permissioned blockchains are used for applications that require privacy and control.

2.2 The relationship between blockchain and cryptocurrencies

Blockchain and cryptocurrency are two interrelated concepts that have revolutionized the world of finance and technology. Blockchain is a decentralized digital ledger technology that allows for secure and transparent data storage, while cryptocurrency is a digital currency that uses cryptography for security and operates independently of a central bank.

Cryptocurrency relies on blockchain technology for its underlying structure, as each transaction is recorded on a distributed ledger that cannot be altered or deleted. Blockchain ensures the integrity and security of the cryptocurrency system, while cryptocurrency facilitates peer-to-peer transactions without the need for intermediaries. Therefore, the relationship between blockchain and cryptocurrency is symbiotic, as blockchain provides the technological framework for the creation and maintenance of cryptocurrencies, and cryptocurrencies demonstrate the real-world applications and benefits of blockchain technology[8].

2.2.1 The Chain of Transactions of Cryptocurrency

A chain of transactions in cryptocurrency, also known as a blockchain, is a fundamental aspect of the cryptocurrency system. It is a distributed ledger that records all transactions made within the network in a chronological and immutable manner.Each transaction is verified by a network of users through a process known as consensus, which ensures the integrity and security of the system. The chain of transactions is linked through cryptographic algorithms that generate a unique digital signature for each block of transactions, making it nearly impossible for any individual or entity to alter the data on the blockchain[9].

The chain of transactions is critical to the functioning of cryptocurrency, as it provides a transparent and decentralized way to verify and record transactions, without the need for intermediaries such as banks or financial institutions. Furthermore, the transparency and immutability of the blockchain ensure that the system is resistant to fraud and hacking, making it a secure and reliable way to conduct transactions. In summary, the chain of transactions in cryptocurrency plays a central role in the functioning and security of the cryptocurrency system.

2.2.2 The Creation of Cryptocurrency Wallets

The creation of cryptocurrency wallets is a crucial step for anyone interested in using cryptocurrencies. A cryptocurrency wallet is a digital tool that allows individuals to store, manage, and transact cryptocurrencies securely. The process of creating a cryptocurrency wallet varies depending on the type of wallet chosen, but the general steps include selecting a wallet provider, downloading the wallet application, and setting up an account[10]. Wallets are typically classified as hot or cold, depending on whether they are connected to the internet or not:

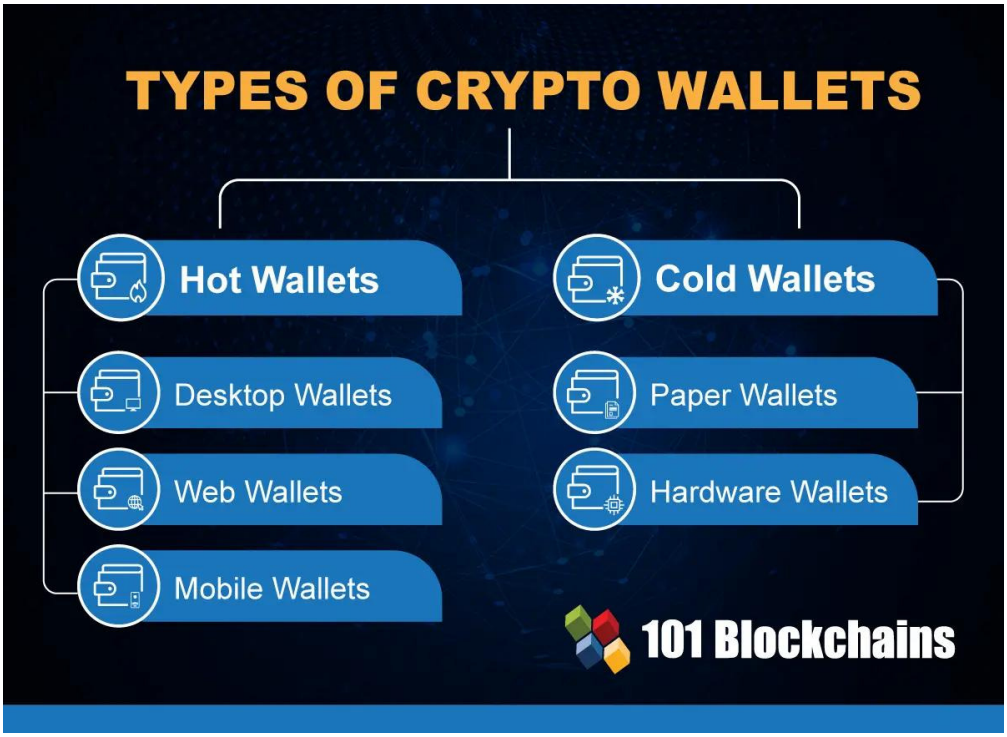
-Hot wallets are typically used for day-to-day transactions.

-Cold wallets are used for long-term storage of cryptocurrencies.

When creating a wallet, users are usually given a unique private key or seed phrase, which is a combination of words that acts as a password to access the wallet. It is essential to keep this private key or seed phrase secure, as it is the

only way to access the wallet and its contents. The creation of cryptocurrency wallets is an important aspect of using cryptocurrencies, as it provides users with a secure and convenient way to manage their digital assets. It is essential to choose a reputable wallet provider and follow best practices for securing and backing up wallet data to ensure the safety of one's funds.

There are several types of cryptocurrency wallets available, each with its unique features, security levels, and usability. The most common types of cryptocurrency wallets include software wallets, hardware wallets, paper wallets, and web wallets:



--

Figure 2.1: Types of crypto-wallets

- Software wallets are applications that are installed on a computer or mobile device, allowing users to store and manage cryptocurrencies on their devices.

- Hardware wallets are physical devices that store cryptocurrencies offline, making them highly secure against hacking and other cyber threats.

-Paper wallets, as the name suggests, involve printing out the public and private keys on a piece of paper, which can then be stored in a secure location. Paper wallets are the most secure type of wallet as they are entirely offline and not susceptible to cyber threats.

-Web wallets are online platforms that allow users to store and manage their cryptocurrencies through a web browser, making them accessible from anywhere.

web wallets are considered less secure than other types of wallets as they are connected to the internet and susceptible to hacking and other cyber threats [11].

Choosing the right type of cryptocurrency wallet depends on an individual's specific needs and preferences, including their level of security and convenience. It is essential to research and choose a reputable wallet provider and follow best practices for securing and backing up wallet data to ensure the safety of one's funds.[5]

2.2.3 Payment of Cryptocurrency in Blockchain

The payment of cryptocurrency in blockchain is a process that involves the transfer of digital currency from one user to another on a decentralized ledger known as the blockchain. Unlike traditional payment systems that rely on intermediaries such as banks, cryptocurrency payments on the blockchain are processed through a peer-to-peer network of users without the need for intermediaries. Transactions are verified through a consensus mechanism that involves a network of nodes working together to confirm the authenticity and validity of each transaction. Once a transaction is confirmed, it is recorded on the blockchain as a block, forming an unbreakable chain of information that cannot be altered or deleted.[4]

--

Figure 2.2: Blockchain payment
Source : Internetofbuisness platform

Cryptocurrency payments on the blockchain are highly secure, transparent, and efficient, as they are processed in real-time without the need for intermediaries. However, it is important to note that the value of cryptocurrencies is volatile and

subject to fluctuations, making it essential to monitor the value of the currency being transacted. In summary, the payment of cryptocurrency in blockchain is a secure and decentralized way of processing transactions without the need for intermediaries, providing users with greater control over their funds and fostering financial inclusivity

2.3 The challenges and risks of blockchain in the cryptocurrency market

Blockchain technology has revolutionized the way we think about trust and transparency in financial transactions. However, the cryptocurrency market, which relies heavily on blockchain, faces several challenges and risks that need to be addressed. Here are some of the key challenges and risks associated with blockchain in the cryptocurrency market:

- Scalability, The scalability of blockchain technology is still a challenge, particularly when it comes to processing large volumes of transactions. This can result in slow transaction times, which can be a barrier to the adoption of cryptocurrencies.

- Security, While blockchain technology is inherently secure, there have been instances of hacks and thefts in the cryptocurrency market. These attacks can result in the loss of millions of dollars in cryptocurrencies.

- Regulation, The lack of regulation in the cryptocurrency market is a major challenge, as it can result in fraud, market manipulation, and other illegal activities.

- Volatility, Cryptocurrencies are known for their high volatility, which can be a barrier to their adoption as a means of payment.

- Adoption, Despite the growing interest in cryptocurrencies, adoption is still relatively low. This can be attributed to a lack of understanding of the technology, as well as concerns over security and volatility.

In general, the challenges and risks associated with blockchain in the cryptocurrency market need to be addressed in order to promote wider adoption and acceptance of cryptocurrencies as a legitimate means of payment and investment. This can be achieved through increased regulation, improved security measures, and greater education and awareness about the technology.

Conclusion to chapter 2

In conclusion, blockchain technology has the potential to transform the way we conduct transactions and manage data, providing a more secure and transparent system. Its decentralized nature makes it virtually impossible to tamper with transaction records, which could greatly benefit industries such as finance, supply

chain management, and voting systems. The potential applications of blockchain technology are vast, and as it continues to be developed and implemented, it is likely that we will see even more innovative solutions to current challenges in various industries. With increased transparency, security, and efficiency, blockchain technology represents a new era of trust and transparency in digital transactions.

Chapter 3

Blockchain and Cryptocurrencies: facts and figures

Introduction to chapter 3

Blockchain technology has emerged as a disruptive force in recent years, transforming the way we store, manage, and transfer data. At the core of this technology is a decentralized system that enables secure, transparent, and immutable transactions. While originally developed as the underlying technology for cryptocurrencies, blockchain has since found applications in a range of industries, including finance, healthcare, logistics, and more. This technology has the potential to revolutionize the way we conduct business, interact with one another, and even govern our societies.

However, as with any new technology, the blockchain industry has faced its fair share of challenges and crises. From high-profile hacks and scams to regulatory uncertainty and market volatility, the blockchain and cryptocurrency industry has had to navigate numerous obstacles. In this chapter, we will explore some of the current crises in the blockchain and cryptocurrency industry, as well as how this industry has responded to past crises. We will also examine the potential of blockchain and cryptocurrencies in Tunisia, a country that has shown a growing interest in this technology in recent years.

3.1 Blockchain in the world and its contribution to cryptocurrencies

3.1.1 Current Crises in the Blockchain and Cryptocurrency Industry

Cryptocurrencies are currently experiencing a crisis due to various factors such as concerns over rising inflation and the ensuing increases in interest rates by central banks. Bitcoin, the world's biggest cryptocurrency, has plummeted about 65% so far this year. The cryptocurrency TerraUSD, a stablecoin that is supposed to keep its value at $1, fell below its fixed value, triggering a selloff. The banking turmoil of the last week is fueling worries that cryptocurrencies will be walled off from traditional finance. However, despite the current crisis, cryptocurrencies are not going to disappear, and blockchain technology is still being developed and used in various industries.

The lack of inherent value in most cryptocurrencies is also a significant risk. The extreme volatility in unregulated markets and the era of cheap money have contributed to the crypto crisis. The collapse of some so-called stablecoins, which are supposed to be less volatile, is also a cause for concern. The failure of the terra/luna stablecoin sparked the beginning of the latest crisis in crypto. The stunning implosion of FTX, one of the biggest and most powerful players in the industry, has also contributed to the crisis. The lack of regulations in the crypto industry is another risk factor.

Rising interest rates generally mean a lower appetite for high-risk/high-return assets such as cryptocurrencies. When interest rates rise, there's a shrinkage of the money supply, a shrinking of the Fed's balance sheet, and a price increase for individual cryptocurrencies. However, the impact of rising interest rates on cryptocurrencies is not straightforward, and other factors such as market sentiment, regulations, and technological advancements also play a role. Cryptocurrencies have been affected by rising interest rates in the past, and concerns over rising inflation and the ensuing increases in interest rates by central banks have affected Bitcoin and other cryptocurrencies. With the stock market also reacting badly to recent rate hikes and the crypto market becoming increasingly correlated to stocks, crypto could be in for a continued bearish year because of the bearish macroeconomic outlook.

However, it is essential to remember that such high volatility is not unprecedented for this asset class. Outside of the crisis period, there is no clear evidence of any inflation hedging capacity of Bitcoin or Ethereum during times of increasing forward inflation. Cryptocurrencies have historically performed well during periods of low-interest rates, but their performance during periods of rising interest rates is

less clear. It is worth noting that Bitcoin was born from the ashes of the 2007/08 financial crisis, and its network launched in January 2009, which means that, for most of its existence, the world's biggest cryptocurrency has benefited from an era of ultra-low interest rates. Overall, the impact of rising interest rates on cryptocurrencies is difficult to predict, and other factors such as market sentiment, regulations, and technological advancements also play a role .

3.1.2 How has the blockchain and cryptocurrency industry responded to past crises?

The blockchain and cryptocurrency industry has responded to past crises in various ways. Here are some examples:

- In 2014, Mt. Gox, which was one of the largest cryptocurrency exchanges at the time, suffered a massive hack resulting in the loss of around 850,000 bitcoins, worth about $450 million at that time. This incident is considered one of the biggest crises in the history of the blockchain and cryptocurrency industry.

After the hack, Mt. Gox declared bankruptcy and went through a lengthy legal process, which lasted several years. Eventually, some of the customers received partial compensation for their lost funds. This crisis highlighted the need for better security measures on cryptocurrency exchanges, and it also raised concerns about the lack of regulations and oversight in the industry.

In response to the Mt. Gox hack, many cryptocurrency exchanges have implemented stricter security measures, such as multi-factor authentication, cold storage, and regular security audits, to protect their customers' funds. The incident also brought attention to the importance of education and awareness among cryptocurrency users regarding the security risks associated with trading and storing digital assets.

Overall, the Mt. Gox hack was a turning point for the blockchain and cryptocurrency industry, leading to increased awareness of security risks and the need for better safeguards to protect against similar incidents in the future.

- In June 2016, the DAO (Decentralized Autonomous Organization), which was built on the Ethereum blockchain, suffered a massive hack resulting in the loss of around 3.6 million Ether, worth approximately $50 million at that time. This incident is considered one of the significant crises in the history of the blockchain and cryptocurrency industry.

In response to the DAO hack, the Ethereum community faced a difficult decision regarding how to address the stolen funds. Ultimately, they decided to implement a hard fork, which effectively reversed the transaction and recovered the stolen funds. This decision was controversial, as some members of the community argued that it went against the decentralized nature of the blockchain and could set a

precedent for centralized decision-making.

The hard fork led to the creation of Ethereum Classic, which maintained the original blockchain without the reversal of the DAO hack. Ethereum Classic was created by a group of developers who disagreed with the decision to implement the hard fork, believing that it was against the principles of immutability and decentralization.

The DAO hack and subsequent hard fork highlighted the complexities and challenges involved in managing a decentralized ecosystem. It raised questions about the role of community consensus in decision-making and the trade-offs between security and decentralization.

In summary, the DAO hack and the subsequent hard fork demonstrated the importance of proactive security measures, such as smart contract auditing, to prevent similar incidents in the future. It also sparked important debates about the philosophical and practical implications of decentralization in the blockchain and cryptocurrency industry.

- The Bitfinex hack was one of the largest cryptocurrency exchange hacks in history, with approximately 120,000 bitcoins stolen from the exchange in August 2016. In response to the hack, Bitfinex issued a new token called BFX to its customers to compensate for their losses[12].

The BFX token was issued on a 1:1 basis to Bitfinex users who had lost bitcoins in the hack, and it could be redeemed for shares in the exchange's parent company, iFinex, or for repayment of the funds lost in the hack. This compensation process was praised by many in the cryptocurrency community for its transparency and fairness.

In addition to compensation, Bitfinex also implemented new security measures to prevent similar incidents from happening in the future. These measures included the introduction of multi-signature wallets and mandatory two-factor authentication for all users. Bitfinex also enhanced its auditing and compliance procedures, which helped to restore confidence in the exchange.

The Bitfinex hack was a significant event in the history of cryptocurrency exchanges, but the response by Bitfinex demonstrated the industry's commitment to protecting customer funds and preventing future incidents. The use of a token as a means of compensation was innovative, and the introduction of new security measures was an important step forward for the industry as a whole.

- Tether Controversy: The Tether controversy is ongoing, and the investigation by the New York Attorney General's office is still ongoing. Tether and Bitfinex have denied any wrongdoing, and Tether has continued to maintain that it has enough reserves to back all of its tokens[13].

Tether is a cryptocurrency that is pegged to the US dollar and is designed to maintain a stable value. Tether tokens are widely used in the cryptocurrency

industry, as they allow traders to move funds between exchanges without having to convert back to fiat currencies.

However, there have been concerns about the transparency of Tether's operations and whether it has enough reserves to back all of its tokens. In 2018, the New York Attorney General's office launched an investigation into Tether and its parent company, Bitfinex, over allegations that Tether had been used to manipulate the cryptocurrency market.

Tether and Bitfinex have denied any wrongdoing and have maintained that they have enough reserves to back all of their tokens. However, the investigation is ongoing, and the controversy has raised questions about the stability of the cryptocurrency market as a whole.

The controversy has also led to increased scrutiny of stablecoins, which are designed to maintain a stable value and are widely used in the cryptocurrency industry. Some regulators and industry experts have called for more transparency and oversight of stablecoins to prevent similar controversies in the future.

In generally, the Tether controversy highlights the need for greater transparency and oversight in the cryptocurrency industry to ensure the stability and integrity of the market. The ongoing investigation by the New York Attorney General's office will be closely watched by industry participants and regulators alike.

- Cryptocurrency exchanges have become attractive targets for hackers due to the large amounts of funds they hold in cryptocurrencies. In response to past hacking incidents, many exchanges have taken steps to improve their security measures.

Two-factor authentication (2FA) is one security measure that has become more widely adopted by cryptocurrency exchanges. This adds an additional layer of security by requiring users to enter a second factor, such as a code generated by an app on their smartphone, in addition to their password when logging in [14].

Cold storage is another security measure that some exchanges have implemented. This involves storing cryptocurrency funds offline in a secure location that is not connected to the internet. This greatly reduces the risk of theft by hackers, as they would need physical access to the storage device to steal the funds.

Regular security audits are also being conducted by many exchanges to identify and fix vulnerabilities in their systems. These audits are typically carried out by third-party security firms that specialize in blockchain and cryptocurrency security.

In addition to these security measures, some exchanges have also implemented insurance policies to cover any losses due to hacking incidents. These policies typically cover losses up to a certain amount and can provide users with additional peace of mind when trading on the exchange.

On the whole, these measures demonstrate the commitment of cryptocurrency exchanges to improving their security and protecting their users' funds. While no security measure can provide 100% protection against hacking, the implementation

of these measures can greatly reduce the risk and provide users with a more secure trading environment.[1]

--

Figure 3.1: Cryptocurrencies: A store of value for the Covid crisis
Source : GIS reports

3.2 Case of Tunisia

Blockchain technology and cryptocurrencies are gaining popularity in Tunisia, with the government and private sector showing interest in exploring their potential benefits. Here are some developments in Tunisia related to blockchain and cryptocurrency:

- In 2018, the Central Bank of Tunisia announced that it was exploring the possibility of issuing a digital currency based on blockchain technology.
- In 2019, the Tunisian government signed a memorandum of understanding with the Swiss-based blockchain firm Tejori to explore the use of blockchain technology in various sectors, including finance, healthcare, and energy. The government committed to a $10 million investment over 5 years to support blockchain projects.
- The Tunisian startup DigitUS has developed a blockchain-based platform for managing land ownership and property registration, which aims to address issues related to property disputes and fraud. Over 13,000 land plots have been registered using their platform.
- In 2020, the Tunisian Ministry of Justice announced a partnership with the blockchain firm Universa to develop a blockchain-based platform for the management of notarial acts.

- The Tunisian Ministry of Communication Technologies and Digital Economy is working on a national blockchain strategy to promote the use of blockchain technology in various sectors, including finance, healthcare, and supply chain management.
- The Tunisian cryptocurrency exchange DigitX is one of the leading cryptocurrency exchanges in North Africa, offering trading in several cryptocurrencies including Bitcoin, Ethereum, and Litecoin.

Despite the potential benefits of blockchain and cryptocurrencies in Tunisia, there are several challenges that need to be addressed in order to ensure their successful adoption and integration into the economy. Some of the main challenges are: - Regulatory uncertainty: There is currently no clear legal framework for blockchain and cryptocurrency in Tunisia, which can create uncertainty for investors and businesses. The government needs to establish clear regulations to protect investors and ensure the stability of the financial system.
- Lack of awareness and education: Many Tunisians are not familiar with blockchain and cryptocurrency, which can create barriers to adoption. Efforts need to be made to educate the public about the potential benefits and risks of these technologies.
- Cybersecurity risks: Blockchain and cryptocurrency are vulnerable to cyber attacks, which can result in theft and loss of funds. The government and businesses need to invest in robust cybersecurity measures to protect against these risks.
- Lack of infrastructure: The development of blockchain and cryptocurrency requires significant investment in infrastructure, such as high-speed internet and data centers. Tunisia will need to invest in these areas to attract businesses and investors.

Despite these challenges, the future of blockchain and cryptocurrency in Tunisia looks promising. The government and private sector are showing interest in exploring the potential of these technologies, and there is a growing community of blockchain and cryptocurrency enthusiasts in the country. If Tunisia can overcome the challenges of regulation, education, cybersecurity, and infrastructure, blockchain and cryptocurrency could play an important role in driving economic growth and innovation in the country.[15]

Conclusion to chapter 3

The blockchain and cryptocurrency industry has come a long way since its inception, and it has gone through its fair share of ups and downs. Despite the current crises faced by the industry, it is important to acknowledge that the industry has shown remarkable resilience and adaptability in response to these challenges.

The industry has taken significant strides in addressing the issues that have led to past crises, and it has implemented measures to mitigate potential risks. Moreover, the development of new technologies and innovative solutions has allowed

the industry to evolve and become more robust.

With more countries, including Tunisia, embracing the potential benefits of blockchain and cryptocurrencies, there is a growing sense of optimism about the industry's future. The adoption of blockchain technology in Tunisia has the potential to transform the way business is conducted and has the potential to drive economic growth.

In conclusion, the blockchain and cryptocurrency industry may have had its fair share of challenges, but it has also demonstrated resilience and innovation in addressing these challenges. As more countries embrace this new technology, we can expect to see further advancements and potential benefits in the years to come.

General conclusion

In conclusion, the rise of cryptocurrency and blockchain technology has brought about significant changes to the financial world. The Genesis of Cryptocurrency, as discussed in this document, highlights the history, types, and market of cryptocurrencies. It is evident that cryptocurrencies are an innovation based on a combination of prevalent techniques, including database decentralization, double key encryption, cryptographic hashing, and cryptographic protocols.

The relationship between blockchain technology and cryptocurrencies, as discussed in section two, illustrates the functioning of blockchain, its types, and the challenges and risks it poses in the cryptocurrency market. It is essential to note that blockchain technology plays a critical role in the creation of cryptocurrency wallets, payment of cryptocurrency, and the chain of transactions of cryptocurrency.

Chapter three provides facts and figures on the use of blockchain technology in the world, its contribution to cryptocurrencies, and the case of Tunisia. The document highlights the current crises in the blockchain and cryptocurrency industry, how the industry has responded to past crises, and the potential of blockchain technology in countries such as Tunisia.

Overall, the use of cryptocurrencies and blockchain technology has brought about significant changes in the financial world, offering an alternative to traditional financial systems. As the world continues to adopt these technologies, it is essential to address the challenges and risks they pose and take measures to ensure their security and stability.

Bibliography

[1] "The Bitcoin Standard" by Saifedean Ammous

[2] "Digital Gold" by Nathaniel Popper

[3] "Cryptocurrency Investing for Dummies" by Kiana Danial

[4] "Blockchain Revolution" by Don Tapscott and Alex Tapscott

[5] "Mastering Bitcoin: Unlocking Digital Cryptocurrencies" by Andreas M. Antonopoulos

Webography

[1] Hybrid SQL and NoSQL Database https://harperdb.io/.

[2] Blockchain : https://www.blockchain.com/learning-portal/blockchain-technology.

[3] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.: https://bitcoin.org/bitcoin.pdf.

[4] Git : https://git-scm.com/about.

[5] Double Key Encryption : https://docs.microsoft.com/en-us/microsoft-365/compliance/double-key-encryption?view=o365-worldwide.

[6] "Public blockchain" IBM, : https://www.ibm.com/topics/public-blockchain..

[7] "Private blockchain" IBM, : https://www.investopedia.com/terms/p/private-blockchain.asp.

[8] "Blockchain and Cryptocurrency: What's the Connection?" : https://www.investopedia.com/articles/investing/031416/blockchain-and-cryptocurrency-whats-connection.asp.

[9] "Chain of transactions" IBM, : https://www.ibm.com/topics/chain-of-transactions.

[10] "cryptocurrency wallet" : https://coinrivet.com/what-is-a-cryptocurrency-wallet.

[11] "Types of Cryptocurrency Wallets and Their Overall Security Aspect" : https://techbullion.com/types-of-cryptocurrency-wallets-and-their-overall-security-aspect.

[12] "Bitfinex" : https://www.bitfinex.com.

[13] "tether" : https://tether.to.

[14] "Two-factor authentication" : : https://en.wikipedia.org/wiki/Multi-factor_authentication.

[15] "Case of Tunisia" : https://www.bloomberg.com/news/articles/2022-03-22/tunisia-joins-bitcoin-bull-run-as-currency-crisis-deepens.