Module 1. Money to Crypto: A Journey through History, Bitcoin, and Blockchain Consensus

BARÇA INNOVATION HUB
Universitas

Welcome to the first module of our course on blockchain and cryptocurrencies. In this module, we will explore the fascinating journey of money, from the early days of barter trade to the emergence of classical economics. Understanding the evolution of money is crucial in comprehending the revolutionary impact that digital currencies, like bitcoin, have on our modern economic landscape.

For this course to provide maximum practical value, we suggest registering on the WhiteBIT cryptocurrency exchange and actively engaging with each module topic.

- To sign up, open the WhiteBIT exchange platform and set up your account. Provide your email address, create a robust password, agree to the user agreement, and follow the simple steps to complete the registration process.
- Verify your identity (KYC) to enable operations on the exchange. A step-by-step guide can be found in the video (WhiteBIT, 2023a) or on the WhiteBIT blog (WhiteBIT, 2023b).

Unit 1.1 History of money: from barter to classical economy

Chapter 1. History of money: from barter to classical economy

At the dawn of human civilisation, communities engaged in trade through a primitive system known as barter.

Barter trade is a system of exchange in which goods and services are directly swapped for one another without the use of a commonly accepted medium of exchange, such as money. In a barter transaction, two parties engage in a mutual exchange of commodities, with each participant providing what the other desires. The value of the goods or services being traded is determined by the subjective preferences and needs of the individuals involved. Barter trade was a prevalent method of commerce in early human societies before the establishment of more formalised systems of currency and exchange.

This kind of trade was prevalent in early economic relations for a substantial period, spanning thousands of years. It served as the

primary method of exchange in various ancient civilisations and early societies. The period during which barter trade dominated economic transactions can be broadly traced from the emergence of early human communities until the development of more sophisticated exchange systems.

The transition from barter trade began as societies encountered the challenges posed by the 'problem of double coincidence of needs.' As these challenges became more apparent, communities sought alternative solutions, leading to the gradual evolution of proto-money and the establishment of more efficient mediums of exchange.

Figure 1. Barter trade (M1-U1-1)

Source: created by the author for this course

Complexity of barter transactions

Barter transactions were fraught with complexity due to the need for a perfect alignment of wants between trading partners. If a farmer wanted to exchange bushels of wheat for a set of tools, they had to find a blacksmith or toolmaker, who not only required wheat, but also had the necessary quantity and quality of tools the farmer desired. The impracticality of this scenario limited the scope and efficiency of trade interactions, hindering the economic development of early societies.

Geographical limitations

The problem of double coincidence of needs was exacerbated by geographical factors. In a world in which communication and transportation were limited, finding individuals with perfectly aligned needs for mutual trade became even more challenging. The efficiency and scale of trade were thus constrained within the confines of local communities, preventing the broader economic interactions that are commonplace in modern societies.

Emergence of barter alternatives

Recognising the limitations of barter trade, communities began exploring alternative means of exchange. This quest for more efficient mediums marked the initial stages of the evolution of money, as societies sought solutions to the inherent challenges posed by the problem of double coincidence of needs.

Impact on economic growth

The problem of double coincidence of needs not only impeded the ease of trade, but also hindered economic growth. The lack of a standardised medium of exchange made transactions cumbersome and inhibited the specialisation of labour, which is a key driver of economic progress.

The rise of proto-money and the dilemma of collectibles

As human societies evolved, their methods of trade and wealth storage underwent significant transformations. This chapter explores the emergence of proto-money and the intricate decision-making process faced by early individuals as they sought to predict demand and gain advantages in trade.

The birth of proto-money

The development of proto-money represented a crucial shift in how individuals perceived and used certain collectibles. This evolution,

driven by the rarity and symbolic value of specific items, was also influenced by the cultural, social, and economic contexts of diverse communities.

Proto-money was not confined to a specific set of items; rather, diverse cultures globally employed a diverse array of objects with intrinsic value. Notable examples include shells, animal teeth, and flint, while other societies used precious stones, rare feathers, or intricately crafted artifacts as proto-money, illustrating the cultural diversity in the evolution of early forms of currency.

The transition of collectibles into proto-money was intertwined with cultural practices and beliefs, adding layers of complexity. These items often held cultural significance beyond their utilitarian or economic roles, becoming symbols of status, spirituality, or communal identity.

Beyond stores of value to mediums of exchange

Proto-money items served not only as stores of value, but also as mediums of exchange within palaeolithic societies. This allowed individuals to facilitate transactions, promoting a more efficient and standardised method of trade. This transition laid the groundwork for the eventual emergence of more sophisticated systems of currency.

As collectibles gained importance, early humans faced a crucial theoretical dilemma: what objects would others desire for trade? Correctly predicting future demand for specific collectibles became a strategic advantage, transforming certain societies and individuals into economic hubs capable of consistently providing desirable items for exchange.

Specialisation and trade advantage

Highlighting the adaptive nature of human societies, some Native American tribes, such as the Narragansett, specialised in creating collectibles specifically for their trade value. The ability to produce items with anticipated demand gave them a significant advantage in economic interactions. The earlier societies could predict the future demand for such goods, the greater the economic edge their owners gained.

Competition among stores of value

As human societies expanded and trade routes developed, the stores of value within individual communities began to compete. Merchants found themselves at a crossroads: whether to store their trade proceeds in their society's chosen medium, the medium of the society they traded with, or a combination of both.

Benefits of foreign stores of value

Merchants discovered the advantages of holding savings in foreign funds, facilitating trade with respective communities and accelerating the acceptance of foreign stores of value into their own societies. The infusion of diverse stores of value increased the purchasing power of their assets, fostering economic growth.

Global acceptance of gold

The culmination of these developments occurred in the 19th century, when most of the world embraced a single store of value—gold. This marked the zenith of the greatest trade boom in history. In settlements using the same store of value, the costs of trading with each other significantly reduced, and trade potential soared.

As we navigate the historical landscape of money, these early adaptations and decisions set the stage for evolving concepts of value and exchange, leading us to the modern era in which digital currencies and blockchain technology are poised to redefine how we perceive and transact with money.

CONTINUE

Unit 1.2 The evolution from classical economics to digital currencies

Chapter 2: The evolution from classical economics to digital currencies

The transition from classical economics to the era of digital currencies represents a profound evolution in the way societies conceptualise and engage with economic systems. This chapter delves into the historical roots of classical economics and explores the contemporary challenges that have paved the way for the emergence of digital currencies.

The transition from a gold-based economic system to classical economy involved a complex historical and economic evolution. Here is a simplified overview of the key phases.

Gold standard era

- Gold as currency: in the 19th century and early 20th century, many countries adopted the gold standard, in which the value of their

currency was linked to a specific quantity of gold.

- Stability and trade: the gold standard was seen as a stabilising force for economies, providing a fixed exchange rate and fostering international trade.

Challenges and economic shifts

- Post-World War I: the devastating impact of World War I led to economic challenges, and countries found it difficult to maintain the gold standard.
- Great Depression: the global economic downturn in the thirties, known as the Great Depression, prompted nations to reassess their economic policies.

Abandonment of gold standard

- Bretton Woods agreement (1944): the Bretton Woods agreement established a new international monetary system, in which currencies were pegged to the US dollar, and the US dollar was convertible to gold.
- Nixon Shocks (1971): in 1971, the US president, Richard Nixon, suspended the dollar's convertibility to gold, officially ending the

Bretton Woods system and severing the link between major world currencies and gold.

Rise of classical economy

- Shift to fiat money: with the abandonment of the gold standard, countries moved to fiat currencies, which are not backed by physical commodities, but derive their value from the trust and confidence in the issuing governments.

- Monetary policy: central banks gained more control over monetary policy, using tools like interest rates to manage inflation and economic stability.

Modern economic systems

- Globalisation: the latter half of the 20th century and the 21st century witnessed increased globalisation, technological advancements, and the rise of digital currencies.

- Diverse monetary systems: different countries adopted various monetary systems, including managed float, fixed exchange rates, and independent floating currencies.

The transition from the gold standard to classical economy was a dynamic process shaped by historical events, economic challenges, and shifts in global monetary policies. It marked a move toward more flexible and adaptable economic systems in response to the changing needs of the modern world.

However, as time passed, society began to recognise the limitations of classical economics in addressing evolving economic landscapes. The advent of new challenges necessitated a re-evaluation of traditional economic models. In particular, the physical forms of money, such as coins and banknotes, began to reveal their disadvantages and limitations in the digital age.

The digital age brought forth modern technologies and opportunities associated with the Internet and electronic payment systems. This shift fostered the development of the idea of digital currencies. These currencies, such as bitcoin and other cryptocurrencies, have introduced transformative possibilities for the way we interact with money and conduct financial transactions.

Fiat money and the rise of digital currencies

In the realm of monetary evolution, the term 'fiat money' comes to the forefront. The term 'fiat' originates from the Latin word, often translated as 'it shall be' or 'let it be done.' In the context of currencies, fiat refers to money that derives its value solely from government

regulation and decree. Unlike historical currencies, which were tied to valuable physical commodities like gold or silver, fiat money lacks intrinsic value and cannot be exchanged for a specific underlying commodity.

In the pre-fiat era, governments minted coins from precious metals or issued paper money redeemable for a set amount of such commodities. However, fiat currency is distinct in that it is inconvertible; there is no inherent commodity backing it. The value of fiat money relies entirely on the trust and confidence placed in the issuing government, marking a departure from traditional currency models based on tangible assets.

Fiat money, not tethered to physical reserves like a national stockpile of gold or silver, faces the inherent risk of losing value through inflation and, in extreme cases, becoming entirely worthless during hyperinflation. Historical instances, such as Hungary's post-WWII hyperinflation, reveal the staggering potential for inflation rates to double in a single day.

Moreover, if public confidence in a nation's currency wanes, the money can swiftly depreciate. This stands in stark contrast to a currency backed by gold, which derives intrinsic value from the demand for gold in various industries, including jewellery, decoration, electronic devices, computers, and aerospace vehicles. The tangible

utility of gold provides a stabilising factor absent in fiat currencies susceptible to fluctuations in public trust and economic conditions.

Key takeaways about fiat currencies

- Fiat money is a government-issued currency that is not backed by a commodity, such as gold.
- Fiat money gives central banks greater control over the economy because they can control how much money is printed.
- Most modern paper currencies, such as the US dollar, are fiat currencies.
- One danger of fiat money is that governments can print too much of it, resulting in hyperinflation.

The transition from traditional finances to digital currencies represents a significant paradigm shift in the world of finance, introducing novel concepts and transformative technologies. This transition is characterised by several key developments and trends.

Emergence of digital currencies

The rise of digital currencies, such as bitcoin, marked the beginning of the transition. These decentralised cryptocurrencies operate on blockchain technology, providing secure and transparent transactions without the need for intermediaries.

Blockchain technology

Blockchain, the underlying technology of many digital currencies, revolutionised the way financial transactions are recorded and verified. Its decentralised and tamper-resistant nature enhances security and transparency, reducing the risk of fraud and manipulation.

Decentralised finance ('DeFi')

The advent of DeFi platforms introduced decentralised financial services, such as lending, borrowing, and trading, without the need for traditional banking institutions. DeFi leverages smart contracts on blockchain to automate financial processes.

Central bank digital currencies (CBDCs)

Governments and central banks are exploring the concept of central bank digital currencies (CBDCs) as a digitised form of traditional

currency. CBDCs aim to combine the benefits of digital currencies with the stability of national fiat currencies.

Tokenisation of assets

Traditional assets, such as real estate, art, and securities, are being tokenised on blockchain platforms. This process transforms physical assets into digital tokens, making them more accessible, divisible, and tradable.

Digital payment systems

Digital payment systems, facilitated by fintech innovations, have become mainstream, offering efficient and convenient alternatives to traditional payment methods. Mobile wallets, contactless payments, and peer-to-peer transfers are gaining widespread acceptance.

In a noteworthy example, platforms like WhiteBIT for cryptocurrency exchange now enable users to leverage digital currencies for purchasing tickets to football events. It is possible thanks to Whitepay SaaS company providing cryptocurrency payment solutions. This approach allows enthusiasts to secure their seats with cryptocurrency a couple of days before the official start of ticket sales, showcasing the evolving integration of digital currencies into various aspects of everyday transactions.

Whitepay provides solutions for accepting cryptocurrency payments and donations. The company has developed a platform and POS terminal to accept cryptocurrency payments so that online and offline businesses can easily and quickly accept cryptocurrencies for payment. Whitepay already works successfully with major Ukrainian online and offline companies to help them accept crypto payments.

Institutional adoption

Institutional players, including banks and investment firms, are increasingly acknowledging the potential of digital currencies. Some institutions are integrating cryptocurrency services, offering clients exposure to this new asset class.

Regulatory developments

Governments and regulatory bodies are actively working to establish frameworks for the legal and regulated use of digital currencies. Regulatory clarity is essential to encourage responsible innovation while mitigating risks.

Public awareness and acceptance

Growing public awareness and acceptance of digital currencies contribute to their mainstream adoption. More individuals are

recognising the benefits of borderless, fast, and cost-effective transactions offered by digital currencies.

The ongoing transition from traditional finances to digital currencies reflects a dynamic and evolving landscape. As the financial ecosystem continues to embrace technological advancements, the integration of digital currencies is poised to reshape the way individuals and institutions engage with and perceive financial systems.

The genesis and significance of bitcoin

Bitcoin originated as a decentralised, open-source digital payment system aiming to address the vulnerabilities in centralised structures like banks and commercial financial institutions. Trusting these entities with funds often entails a lack of transparency and an inability to monitor their operations.

In contrast, bitcoin operates as a decentralised system, free from regulatory authority or central bank control. Users collectively build and maintain the network with public balances and concealed identities. The blockchain, an open and distributed ledger, records all transactions, and settlement on the network is facilitated using the bitcoin/Satoshi unit.

The core strength of bitcoin lies in its self-sufficiency, reliability, and decentralised nature. Despite being commonly referred to as a digital currency, its true value extends beyond, serving as the native coin for the network. The security and functionality of bitcoin are underpinned by cryptography.

Cryptography, the science of information security, ensures the confidentiality, integrity, and authentication of data. It transforms messages into an incomprehensible form, making them readable only to the sender and recipient. Historical roots of cryptography trace back to ancient civilisations, with significant development occurring during the era of radio communications in the twentieth century.

During World War II, the Enigma encryption machine was a pivotal point in cryptography history, with mathematician Alan Turing deciphering it. This breakthrough marked the organised emergence of cryptography as a science. Modern cryptographers now employ mathematical functions resistant to various attacks, intertwining with statistics, probability theory, and general algebra.

The scope of cryptography has evolved over decades, encompassing not only secret information transmission, but also verifying message integrity, authentication, digital signatures, and serving as the foundation for digital currencies. In the context of bitcoin, cryptography ensures the security and immutability of transactions, making it a cornerstone of the cryptocurrency revolution.

The genesis of bitcoin represents a convergence of decades of research in computer science and cryptography. Marc Andreessen, a pioneer in the development of the first graphical Internet browser, Mosaic, views bitcoin as a breakthrough that draws on twenty years of cryptographic currency research and forty years of global cryptography efforts.

The journey to bitcoin's creation includes significant milestones.

- **Early electronic cash protocols** (1983). In 1983, cryptographers David Chaum and Stefan Brands laid the groundwork for electronic cash protocols, marking an early attempt to envision a digital form of currency. Chaum's concept focused on the idea of providing privacy in transactions, a principle that would later become a crucial aspect of cryptocurrencies.

- **Hashcash and proof of work** (1997). In 1997, Adam Back introduced hashcash, a groundbreaking innovation designed to tackle spam and denial-of-service (DoS) attacks. Hashcash introduced the concept of proof of work, a mechanism requiring computational effort to deter abuse. This concept would later become a cornerstone of bitcoin's consensus algorithm, ensuring the security and integrity of the decentralised network.

- **B-money and bit-gold** (1998). In 1998, Wei Dai introduced the concept of ‘b-money’, an anonymous, distributed electronic cash system. Simultaneously, Nick Szabo proposed ‘bit-gold’, exploring

the idea of a decentralised system with a scarce and valuable digital commodity. These early conceptualisations contributed to the theoretical underpinnings of cryptocurrencies, contemplating the challenges of decentralised consensus, privacy, and scarcity.

- **The cypherpunk movement**. During this period, a community known as the cypherpunks emerged. Comprising cryptographers, privacy advocates, and tech enthusiasts, the cypherpunk movement played a crucial role in shaping the ideological foundations of cryptocurrencies. The movement emphasised the importance of privacy, cryptographic tools, and decentralised systems to counteract centralised control.

- **The mosaic browser and the dot-com boom.** In the 1990s, the development of the mosaic browser by Marc Andreessen marked a significant milestone in the evolution of the Internet. This era, characterised by the dot-com boom, laid the groundwork for the digitisation of various aspects of life, including financial transactions.

- **Bitcoin's genesis (2009)**. The convergence of these ideas and technological advancements culminated in the release of bitcoins in 2009 by an individual or group using the pseudonym Satoshi Nakamoto. Bitcoin combined cryptographic principles, decentralised consensus through proof of work, and the vision of a borderless, censorship-resistant currency. Its decentralised nature and the use of a blockchain for transparent and immutable transaction history set it apart from traditional forms of money. On January 3, 2009, the first block and fifty bitcoins were created, marking the genesis of

bitcoin. Just nine days later, on January 12, Satoshi Nakamoto sent ten bitcoins to Hal Finney, marking the first recorded bitcoin transfer. The pioneering exchange of bitcoins for national currency occurred in September 2009, when Martti Malmi sent 5050 bitcoins to a user named NewLibertyStandard, receiving $5.02 in his PayPal account. Notably, NewLibertyStandard proposed using the electricity cost of bitcoin generation as a valuation metric, adding a unique perspective to cryptocurrency economics. These early events laid the groundwork for the disruptive evolution of digital currencies.

In April 2011, Satoshi Nakamoto vanished, leaving behind a final message on the primary bitcoin forum, bitcointalk.org. Since this disappearance, the quest to unveil the creator's identity has persisted. Each year introduces new versions and theories, yet the community remains no closer to unravelling the mystery behind the pseudonym.

Persistent rumours suggest that the cryptographer and programmer Hal Finney could be the elusive creator. Notably, Finney was the recipient of the first bitcoin transaction from Satoshi Nakamoto, adding intrigue to the speculation surrounding his potential role in the creation of bitcoin. However, despite ongoing speculation, the identity behind the pseudonym continues to elude the community, maintaining an air of mystery around the enigmatic figure who birthed the revolutionary cryptocurrency.

Digital currencies vs. traditional financial means

Digital currencies represent electronic money operating exclusively within the digital realm, devoid of physical counterparts like banknotes or coins. Existing solely in electronic form, these currencies leverage blockchain technology, a decentralised transaction recording system. Using blockchain ensures both the security and transparency of transactions while affirming their authenticity without reliance on a central entity, be it a bank or government.

In the competition among various saving methods, distinctive and valuable properties come to the forefront, enabling an increase in demand over time. While numerous items served as means of savings or 'proto-money,' certain attributes emerged as particularly sought-after, giving these objects an edge over their competitors.

Table 1. Gold vs. fiat currencies vs. bitcoin

Characteristics	Gold	Fiat currencies	Bitco
Durability	Gold stands as the unparalleled champion of durability. Most of the gold ever mined or	In the realm of fiat currencies, the historical narrative reveals instances in which	Bitcoins, la central exhibit contingent functionali supporting Although

Characteristics	Gold	Fiat currencies	Bitco
	minted, including the treasures of ancient civilisations like the pharaohs, has not only endured through the ages, but is expected to persist for centuries to come. Gold coins, once used as currency in ancient times, maintain substantial value in the contemporary era, underscoring the enduring nature of this precious metal.	numerous governments have risen and fallen over the centuries, and their corresponding currencies have vanished along with them. Examples such as paper and rent stamps, or the Reichsmarks of the Weimar Republic, have lost their value precisely because the issuing institutions have ceased to exist. Drawing from history, it would be unwise to perceive fiat currencies as inherently	still in it stages, definitive statements lifespan pr there are indications. governmen attempts regulation numerous attacks, the persists, highlightin notable l 'antifragilit

Characteristics	Gold	Fiat currencies	Bitco
		long-term assets, with the US dollar and British pound standing as relative anomalies in this context.	
Mobility	Gold, being a dense and tangible substance, ranks as the least mobile of assets. It is unsurprising that most of the bullion remains stationary, with ownership often changing hands without the physical metal being transported. The transfer of physical gold over extended distances is	Fiat currencies, primarily digital in today's landscape, possess a degree of mobility. However, the mobility is constrained by government regulations and capital controls, often resulting in lengthy processing times for large transfers or, in some cases,	Bitcoins sta the most store of va used. Priva representin significant money, securely st compact U allowing effortless transportab Moreover, substantial amounts transferred instantly individuals at opposite the globe. currencies,

Characteristics	Gold	Fiat currencies	Bitco
	marked by excessive costs, substantial risks, and considerable time investment.	rendering them impossible. While physical cash can be employed to evade certain controls, this approach introduces heightened risks associated with storage and increased transportation costs.	predominar digital, s degree of the unp ease of tra and tra significant sets bitcoin terms of por
Fungibility	Gold has established the benchmark for fungibility. A molten ounce of gold is identical to any other ounce, and this uniformity has long been the basis for its trade in the market. In contrast, the fungibility of	While fiat bills are typically considered of equal value by merchants, instances exist where large and small denomination bills have been treated disparately. For instance, the Indian government,	Bitcoins are at the netw This mea every transferred treated across th network. since the er of bitcoins tracked blockchain, coin can b due to use trade,

Characteristics	Gold	Fiat currencies	Bitco
	fiat currencies is contingent on the extent permitted by the issuing institutions.	aiming to eliminate the gray market, underwent complete demonetisation of the 500- and 1000-rupee notes. Consequently, these bills have been traded below their nominal value.	merchants exchanges refuse to Without i the priva anonymity network bitcoin ca considered fungible as
Corroborability	In most cases, verifying the authenticity of gold is straightforward. However, gold is not immune to counterfeiting. In the past, crafty criminals employed gold-plated tungsten to deceive consumers.	While fiat currency, equipped with anti-counterfeiting features on banknotes, is easy to verify, the presence of counterfeit notes remains a potential risk for states and their citizens.	On the bitcoins verified mathemati certainty. cryptograph signatures, owner of can demonstrat ownership claimed coi

Characteristics	Gold	Fiat currencies	Bitc
Patribility	Although gold can be physically separated, making it divisible in theory, this attribute makes it less convenient and practical for everyday use.	Fiat currencies can be divided down to pocket money, offering flexibility in practice. However, the purchasing power of small denominations is often limited.	One bitcoir divided ir hundred pieces, allc transfers quantities. it is worth that netw can renc transfer c amounts bitcoin e inefficient.
Supply	While gold has maintained its scarcity for many centuries, it is not impervious to an increase in supply. The discovery of new, cost-effective methods for mining or acquiring gold, such as seabed or asteroid mining, could	Fiat currencies, despite being a recent invention, have exhibited a tendency toward an ever-expanding supply. States consistently show an inclination to inflate the money supply to address immediate	What sets apart from currencies is its e limited According original con total nur coins that be created at tw million. Thi feature bitcoin hc know in their perce the total co

Characteristics	Gold	Fiat currencies	Bitco
	potentially lead to a significant surge in the availability of this valuable metal.	political challenges. The ongoing inflationary trends employed by governments globally have instilled a perpetual sense of caution among fiat currency holders, who remain vigilant against potential declines in the value of their assets.	in the ma instance, individual ten bitcoir be aware more than 7 people on E than 0.03% world's pc could pos equivalent of coins.
Censorship resistance	While not issued by states, gold's physical nature makes it challenging to move, rendering the precious metal more susceptible to government	In a regulated economic system, governments oversee banks and financial institutions to prevent illicit uses of monetary	Bitcoin gair demand, in to its use illegal dru fostering misconcept its primary was its anonymity. However,

Characteristics	Gold	Fiat currencies	Bitco
	regulation than bitcoin. A case in point is the gold control act in India.	products, exemplified by capital controls. This regulatory framework can make it challenging for individuals, such as a wealthy millionaire, to transfer wealth to another country to escape a repressive regime.	transaction permanentl recorded public bl allowing analysis t fund flov coin's popu illicit activit not from anonymity, its 'permissions at the netw In the network, transaction without interventio embodying distributed peer inherently to censorsh

Source: own source.

NO currency boasts a history as extensive and enduring as gold, which has been revered throughout the annals of human civilisation. Coins

minted in ancient times continue to retain significant value in the contemporary era.

This contrasts sharply with fiat currencies, a recent anomaly in history. Since their introduction, they have displayed a propensity to depreciate. The use of inflation as a surreptitious form of taxation has proven to be a temptation that few states in history have resisted.

The lessons of the 20th century, during which fiat currencies began dominating the global monetary system, underscore the unreliability of fiat in the long or even medium term.

On the other hand, bitcoin, despite its brief existence, has weathered substantial trials in the market. This resilience suggests a high probability that bitcoin will persist as a store of value in the near future.

CONTINUE

Unit 1.3 Achieving consensus. Byzantine generals' problem at the core of blockchain solutions

Chapter 3: Achieving consensus. Byzantine generals' problem at the core of blockchain solutions

The two generals' problem

It is a thought experiment and a concept in computer science that illustrates the challenges of achieving consensus and coordination between two distributed entities in the presence of uncertainty and unreliable communication.

The scenario involves two generals, each commanding their armies and planning to launch a coordinated attack on a common enemy situated in a city. To be successful, the generals need to synchronise their actions and agree on a specific time to attack. However, the challenge arises due to the uncertainty in communication – the generals can only communicate through messengers, and there is a risk of messengers getting lost, delayed, or intercepted by the enemy.

The problem is framed as follows:

- the two generals, A and B, are situated with their armies on opposite sides of the enemy city.
- They need to decide on a common time to attack for the assault to be effective.
- Communication is only possible through messengers, and these messengers may be captured or delayed by the enemy.

The fundamental issue is that there is no guaranteed way for the generals to ensure that they both agree on the attack time. Even if one general sends a message to the other proposing a specific time, there is no certainty that the message will be received, leading to a situation in which one general might attack while the other holds back, resulting in failure.

In computer science, the two generals' problem is often used as an analogy for challenges in designing distributed systems, particularly in scenarios in which achieving consensus and reliable communication between different components or nodes is crucial. It highlights the difficulties of ensuring agreement between distributed

entities when faced with communication uncertainties and the potential for failures.

The Byzantine generals' problem

In 1982, Lamport, Szostak, and Pease introduced a problem involving multiple generals, some of whom might be traitors. This scenario expands on the classic two generals' problem, requiring more generals to agree on the time of attack. A complicating factor is the presence of potential traitors among the generals, capable of providing false information about their intentions.

The leader-follower paradigm from the two generals' problem transforms into a commander-subordinate dynamic. To achieve consensus in this setting, the commander and each subordinate must align on the same decision, whether to attack or retreat.

This scenario is known as the Byzantine generals' problem. The commanding general must issue an order to their n-1 subordinates with the following criteria:

- all loyal subordinate generals obey the same order.
- If the commanding general is loyal, all subordinates loyal to him obey his orders.

Notably, even if the commanding general is a traitor, consensus must still be reached. Consequently, all lieutenants must reach a majority vote.

The consensus algorithm, in this case, relies on the concept of most decisions perceived by subordinates.

This implies that the algorithm can attain consensus as long as two-thirds of the participants are honest. If more than one-third of the generals are traitors, consensus becomes unattainable, preventing the coordination of attacks between armies and resulting in victory for the enemy.

In summary, while the two generals' problem focuses on the challenges of achieving consensus between two entities with unreliable communication, the Byzantine generals' problem extends the scenario to involve multiple generals and introduces the complication of potential traitors among them.

How does this relate to blockchains? Blockchains, as decentralised ledgers, inherently lack a central authority, making them susceptible to attacks driven by economic incentives to exploit vulnerabilities. The value stored in blockchains creates a tempting target for attackers seeking to manipulate or disrupt the system. However, to ensure the

integrity and reliability of a blockchain, addressing the Byzantine generals' problem through Byzantine fault tolerance is imperative.

In the absence of Byzantine fault tolerance, malicious peers within a blockchain network can propagate and validate false transactions, undermining the trustworthiness of the entire ledger. Compounding the challenge is the absence of a central authority to assume responsibility and rectify the resulting damage.

The breakthrough innovation introduced with the creation of bitcoin lies in its ingenious solution to the Byzantine generals' problem, primarily through the implementation of a proof of work probabilistic consensus mechanism. This approach, meticulously detailed by Satoshi Nakamoto (2008a) in a seminal email, marked a pivotal moment in the development of decentralised systems.

By integrating Byzantine fault tolerance, blockchains enhance their resilience against malicious actors attempting to compromise the system. The proof of work mechanism, as exemplified in bitcoin, introduces a probabilistic solution that addresses the Byzantine generals' problem, establishing a decentralised consensus that withstands attempts at manipulation or misinformation. This innovative solution laid the foundation for the secure and trustworthy operation of blockchain networks, demonstrating the practical application of Byzantine fault tolerance in the realm of distributed ledger technology.

Consensus mechanisms form the backbone of blockchain networks, ensuring agreement among participants on the validity of transactions and the state of the distributed ledger. We will delve deeper into the topic in the following units, but let us mention the most prominent and original consensus mechanisms that serve as a basis for the evolution of the technology.

CONTINUE

Unit 1.4 Emission and value of cryptocurrency

Chapter 4: Emission and value of cryptocurrency

Currency issuance involves the creation and introduction of new units of a particular currency into circulation. This process is typically undertaken by the central bank or other authorised entities and can manifest through the printing of banknotes or the establishment of electronic accounting records.

The value of a currency is intricately tied to the interplay of supply and demand within the market. Numerous factors contribute to shaping the value of a currency, encompassing a nation's economic conditions, inflation rates, interest rates, political stability, and international relations. When demand for a currency surpasses its supply, its price tends to rise. Conversely, if the supply exceeds demand, the price may decrease.

The dynamics of currency value are influenced by the delicate balance between supply and demand, and a multitude of economic and geopolitical factors play a role in shaping the perceived worth of a particular currency in the global market.

How is the value of digital currencies formed? To evaluate risks associated with digital currencies, it is crucial to delve into the fundamental factors shaping their value. The price of any asset, including digital currencies like bitcoin, is fundamentally driven by the interplay of supply and demand dynamics an asset is valued at precisely what individuals are willing to pay for it. However, the complexity lies in understanding the multitude of factors influencing this demand.

The demand for digital currencies is intricately tied to several variables, such as investor confidence, the growth of supporting infrastructure, the expanding participant base, and overall market volume. The dynamics of supply and demand are, therefore, subject to a myriad of influences.

A critical principle underpinning the value of any asset is that it will not plummet to zero if there are at least two parties expressing interest in it. In the case of bitcoin, the widespread global interest and engagement from millions of individuals and thousands of companies make the sudden loss of interest highly improbable.

Moreover, the potential depreciation of an asset often arises when it faces destruction or deletion. For instance, if the database containing all transactions at the central bank is erased, the value of non-cash currency would effectively be reduced to nothing. However, decentralised cryptocurrencies, including bitcoin, present a unique

challenge to this scenario. If even one copy of the blockchain exists on any node worldwide, bitcoin retains its existence, albeit with diminished liquidity.

Considering these foundational principles, discussing the theoretical depreciation of bitcoin in the current landscape seems futile. The resilience of bitcoin stems from its widespread adoption and the decentralised nature of its blockchain.

However, exploring such hypothetical scenarios is not entirely without merit. A theoretical collapse of bitcoin would reverberate beyond its immediate impact on digital currencies. As a trendsetter and a primary liquidity provider in exchange trading, bitcoin's decline could have cascading effects, potentially impacting on 99% of other cryptocurrencies. This downturn would extend to the broader cryptocurrency industry, leading to the disruption of mining, staking, lending, and even affecting stablecoin issuers. The theoretical depreciation of bitcoin could entail the collapse of an entire sector within the emerging world economy.

What is halving, and when will all bitcoins be mined?

Figure 2. Bitcoin (M1-U1-2)

Source: created by the author for this course

Bitcoin

Bitcoin halving is an event programmed into the bitcoin protocol that occurs every four years, or after every 210,000 blocks are mined. During the halving, the reward that miners receive for adding a new block to the blockchain is cut in half. This reduction in the rate of new bitcoin creation serves as a built-in mechanism to control the overall supply of bitcoin.

The bitcoin halving has a significant impact on the economics of bitcoin mining. In the early days of bitcoin, the block reward was fifty bitcoins. The first halving in 2012 reduced it to twenty-five bitcoins, the second halving in 2016 reduced it to 12.5 bitcoins, and the third halving in 2020 further reduced it to 6.25 bitcoins.

The next Bitcoin halving will take place when the number of blocks reaches 840,000. This is expected to occur in April, 2024.

This decreasing block reward has implications for the total supply of bitcoin. The maximum supply of bitcoin is capped at twenty-one million, and the halving events play a crucial role in approaching and

eventually reaching this limit. Theoretically, the last bitcoin is expected to be mined in the year 2140.

Bitcoin halving events are closely monitored by the community, as they often have a significant impact on the market dynamics, influencing factors such as miners' profitability, supply and demand dynamics, and overall market sentiment.

What will happen when the last bitcoin is mined? When the last bitcoin is mined, it will mark the completion of the predetermined and limited supply of bitcoin. The maximum supply of bitcoin is capped at twenty-one million coins, a design choice embedded in the bitcoin protocol by its pseudonymous creator, Satoshi Nakamoto. The last bitcoin is expected to be mined in the year 2140.

Figure 3. Bitcoin mining (M1-U1-3)

Source: [untitled image of bitcoin mining], (n. d.), https://bit.ly/49443SW.

Several consequences and shifts in the bitcoin ecosystem are anticipated when this event occurs.

- Mining rewards: currently, miners are rewarded with newly minted bitcoins for successfully adding a new block to the blockchain. As the supply approaches its limit, the block reward will diminish, and miners will rely increasingly on transaction fees for their revenue.

- Economic dynamics: the transition from relying on block rewards to transaction fees may alter the economic incentives for miners. It could lead to changes in the cost structure of bitcoin transactions and the dynamics of transaction fee markets.

- Scarcity and demand: with a fixed supply and no possibility of additional mining, bitcoin's scarcity becomes absolute. This feature could potentially intensify its perception as a store of value, like precious metals such as gold, with the principle of scarcity driving demand.

- Market impact: the culmination of mining and the fixed supply could have implications for the broader cryptocurrency market. Investors, traders, and stakeholders in the cryptocurrency space are

likely to closely monitor this milestone for its potential effects on market dynamics and sentiment.

It is important to notice that these predictions are speculative, and the actual impact will depend on a variety of factors, including the state of the broader financial ecosystem, technological developments, regulatory considerations, and the ongoing evolution of the cryptocurrency space.

Wrapping up

In conclusion, our exploration of the history of money, from the early days of barter to the establishment of classical economic principles, has laid the groundwork for understanding the dynamic evolution towards digital currencies. In the second chapter, we witnessed the transition from classical economics to the era of digital currencies, exploring the self-regulating nature of classical economies, the rise of fiat money, and the groundbreaking significance of bitcoin in reshaping financial landscapes. Moving forward, the third chapter delved into the core challenge of achieving consensus in decentralised systems, unravelling the complexities of the Byzantine generals' problem and its direct relevance to the revolutionary concept of blockchain technology. Lastly, our journey concluded with a focus on the emission and value of cryptocurrency, addressing fundamental questions about the formation of digital currency

values, the intricacies of halving events, and the future implications when the last bitcoin is mined. This educational unit has equipped us with a comprehensive understanding of the historical, technological, and economic facets that shape the world of money, both traditional and digital.

CONTINUE

Unit 2.1 The introduction to blockchain essentials

Chapter 1: The introduction to blockchain essentials

In 2008, the global financial landscape underwent a seismic shift with the bankruptcy filing of Lehman Brothers Holdings Inc. This event, coupled with a widespread erosion of public trust in traditional banking institutions, paved the way for the emergence of a new category of assets that operate independently of formal banking structures. It was against this backdrop of financial upheaval that the first cryptocurrency, bitcoin, made its debut.

Bitcoin, introduced in 2008 by an enigmatic figure or group operating under the pseudonym Satoshi Nakamoto, marked a revolutionary departure from conventional currencies. The overarching goal was to create a decentralised, open-source digital currency that operated without the need for a central bank or administrative authority. The original white paper detailing the concept and mechanics of bitcoin can be found here (Nakamoto, 2008b).

In this part of the module 1, we will delve into the foundational principles governing cryptocurrencies, deciphering the basics of

blockchain technology.

Bitcoin ≠ blockchain

Blockchain stands as a unique and decentralised digital ledger, serving as a special database distributed across numerous computers globally. This innovative technology ensures the secure storage of data through a series of chronological blocks, each safeguarded by robust cryptographic mechanisms.

The roots of the blockchain concept trace back to the early 1990s, originating from the collaboration between computer scientist Stuart Haber and physicist W. Scott Stornetta. Their vision involved applying cryptography to the blockchain to safeguard digital documents against tampering, marking a pivotal moment in the evolution of secure data management.

The influence of Haber and Stornetta reverberated through the programming and cryptography communities, sparking inspiration that eventually birthed bitcoin. As the inaugural cryptocurrency leveraging blockchain technology, bitcoin emerged as a decentralised and trustless digital currency, disrupting traditional financial paradigms.

Since those early days, blockchain has transcended its initial application in cryptocurrency transactions. Its versatility extends to

recording several types of digital data and executing diverse tasks, making it a formidable force in the technological landscape. The widespread adoption of blockchain technology is evident in the steadily growing number of cryptocurrency users worldwide.

Beyond its association with cryptocurrencies, blockchain's decentralised nature and cryptographic security render it suitable for a myriad of applications. Whether recording financial transactions, ensuring the integrity of digital documents, or facilitating complex tasks, blockchain continues to evolve as a transformative force, promising innovation and security across diverse industries.

While commonly used interchangeably, bitcoin and blockchain are distinct concepts, and understanding their differences is crucial. Bitcoin is not merely a coin; it is a comprehensive protocol built on blockchain technology. A protocol defines the rules guiding communication among network participants. In the case of bitcoin, these rules regulate various aspects, such as the management of private and public keys, the process of mining to confirm transactions, and more. Notably, other cryptocurrencies like ethereum, waves, NEO, ripple, and several others share a protocol like bitcoin.

What is decentralisation in blockchain? Decentralisation within a blockchain framework is the distribution of control and decision-making authority across the network's users, as opposed to being concentrated in the hands of a singular entity, like a government or

corporation. This decentralised approach proves beneficial in scenarios in which users seek coordination with unfamiliar counterparts or prioritise safeguarding the security and integrity of their data.

Within a decentralised blockchain network, there exists no central authority or intermediary dictating the flow of data or transactions. Instead, the verification and recording of transactions are entrusted to a widely dispersed network of computers. This collaborative effort ensures the overall integrity of the network.

It is crucial to recognise that blockchain transcends its role as a mere database. Beyond its foundational function, it empowers a spectrum of services, including cryptocurrencies and non-fungible tokens (NFTs). This versatility allows users to engage in collaborative transactions without reliance on a centralised authority. The decentralised nature of blockchain not only upholds security, but also fosters an environment in which users can seamlessly interact and transact, establishing a trustless and peer-to-peer paradigm.

CONTINUE

Unit 2.2 The way blockchain works

Chapter 2: The way blockchain works

A blockchain serves as a secure digital ledger, recording transactions between parties and safeguarding this information against unauthorised access. The process involves a distributed network of specialised computers, known as nodes, located around the globe.

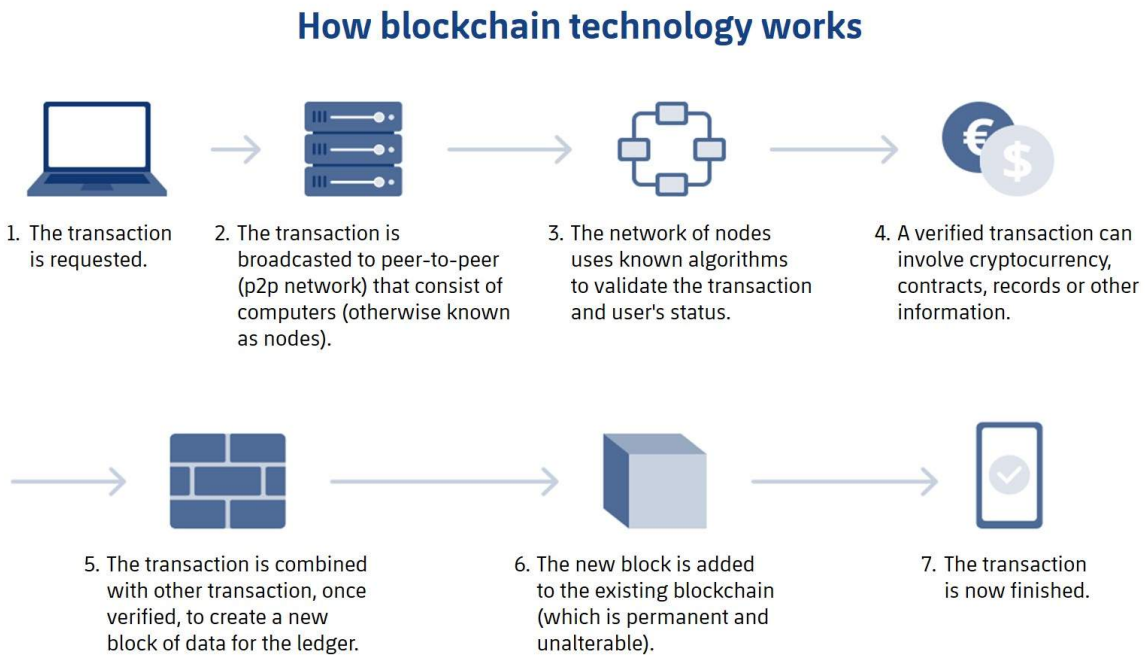
When a user initiates a transaction, such as transferring a specific amount of cryptocurrency, the details are broadcasted across the network. Each node plays a critical role in the verification process, scrutinising digital signatures and other transaction data to authenticate its legitimacy.

Once a transaction receives approval, it becomes part of a block, joined to other sanctioned transactions. These blocks are sequentially linked using cryptographic techniques, forming the immutable structure known as a blockchain. The validation and inclusion of transactions into the blockchain rely on a consensus mechanism, a set of rules guiding nodes to coordinate and reach agreement on the blockchain's state and transaction approval.

Cryptography plays a pivotal role in ensuring the security, transparency, and tamper resistance of transaction records within the blockchain. A fundamental cryptographic technique employed is hashing, a process that converts input data of variable sizes into a fixed-length string of characters.

Blockchain hash functions prioritise collision resistance, reducing the likelihood of finding two distinct pieces of data yielding the same result. Additionally, any alteration in the input data results in a complete change to the hashing outcome, further enhancing the integrity and security of the blockchain's transaction history.

Figure 4. The way blockchain technology works (M1-U2-4)



Source: created by the author for this course

A ledger and a digital signature

Imagine you and your friend, Alice, decide to keep track of shared expenses using a digital ledger and digital signatures. The ledger is like a shared digital notebook in which you both record all your shared expenses. Each 'page' of the notebook represents a block in the ledger, and every time you spend money or contribute to a shared expense, you write it down in a new block. The ledger is not stored in one place, but is duplicated and shared with both you and Alice, so both of you have an identical copy, and any changes are updated for everyone simultaneously.

Now, when you want to confirm your contributions to the ledger without the fear of someone else pretending to be you, you use a digital signature. Think of it like a unique, secret handshake that only you have. When you add an entry to the ledger, you sign it with your digital signature, which is based on your secret handshake (private key). Alice, and anyone else, can use your public handshake (public key) to check the signature and confirm that it was indeed you who made that entry. If the signature does not match or the ledger entry looks tampered with, they will know something is not right.

To put it all together, let us say you decide to buy groceries for $20 and add that to the ledger. You sign this entry with your digital

signature, indicating that you are the one who paid for it. The ledger updates for both you and Alice, showing the new entry with your signature. Later, when Alice checks the ledger, she sees your entry and verifies your digital signature using your public key. If the signature is valid, she knows you indeed paid for the groceries. This way, the ledger keeps a transparent record of shared expenses, and the digital signatures ensure the authenticity of each entry, preventing tampering and establishing trust between you and Alice in your shared financial dealings.

Ledger

- In the context of finance and transactions, a ledger is a record-keeping system that tracks and manages financial transactions. Traditionally, ledgers were physical books in which businesses recorded their debits and credits. In the digital age, ledgers have become electronic, and many are now decentralised and distributed across a network of computers.

- A blockchain, which is a type of decentralised ledger, is a sequential chain of blocks, each containing a list of transactions. It provides a transparent and secure way to record and verify transactions without the need for a central authority.

Digital signature

- A digital signature is a cryptographic technique used to verify the authenticity and integrity of digital messages or documents. It provides a way for the sender of a message to prove their identity and ensure that the message has not been altered during transmission.

- In the context of transactions, digital signatures are often used to sign electronic documents or confirm the origin of a digital message. They rely on a pair of cryptographic keys: a private key known only to the signer and a public key that others can use to verify the signature.

- The process involves creating a unique digital fingerprint (hash) of the document or message using the private key. This hash, along with the private key, forms the digital signature. The recipient can then use the sender's public key to verify the signature and confirm the document's authenticity.

In the realm of digital currencies and blockchain technology, ledgers and digital signatures play crucial roles in ensuring the security, transparency, and trustworthiness of transactions. Blockchain ledgers use cryptographic techniques, including digital signatures, to secure and validate the integrity of transactions within a decentralised network.

Hash function

Let us explore the concept of a cryptographic hash function, specifically the SHA-256 algorithm.

Imagine you want to secure a message you are sending to your friend, Bob, using a cryptographic hash function, in this case, SHA-256.

You write the message 'Hello, Bob!' and want to create a hash of it using SHA-256. The SHA-256 algorithm processes this message and generates a fixed-length string of characters, typically sixty-four characters long, known as the hash value. You send this hash value along with your message.

Now, Bob receives the message and the hash value. He runs the same SHA-256 algorithm on the received message, and if the hash value he computes matches the one you sent, he can be confident that the message has not been tampered with.

Definition: a cryptographic hash function, such as SHA-256 (secure hash algorithm 256-bit), is a mathematical algorithm that takes input data (like a message or file) and produces a fixed-size string of characters, which is typically a hexadecimal number.

The key properties of cryptographic hash functions include:

- deterministic. The same input will always produce the same output (hash value).
- Quick computation: the hash value is efficiently and quickly computed.
- Irreversibility: it should be computationally infeasible to reverse the process and derive the original input from the hash value.
- Collision resistance: it should be unlikely that two different inputs produce the same hash value.

In the case of SHA-256, it specifically produces a 256-bit (32-byte) hash value. This type of hash function is widely used in various security applications and forms a crucial component of blockchain technology, ensuring data integrity and authentication.

Types of blockchain networks

There are several types of blockchain networks, each with distinct characteristics and use cases. The primary types include:

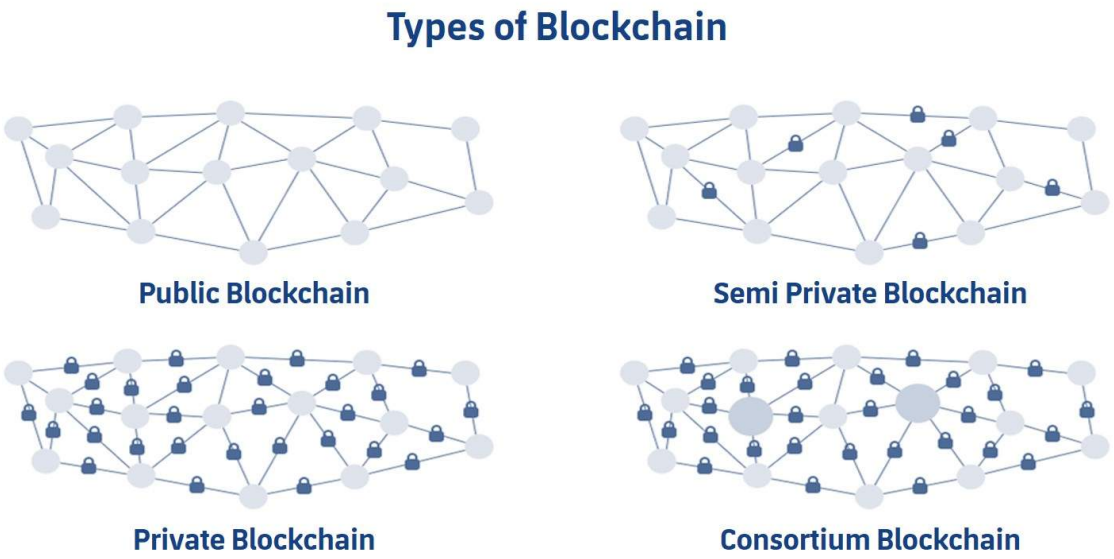
public blockchain. Open and decentralised networks accessible to anyone. Transactions are transparent, and the network operates on a trustless basis, allowing universal participation. Examples include bitcoin and ethereum.

Private blockchain: closed blockchain networks, typically controlled by a single organisation. Access is restricted, and rules are set by the controlling entity for transaction visibility and recording.

Consortium blockchain: a hybrid model combining elements of public and private blockchains. Multiple organisations collaboratively manage a shared blockchain network. It can be open or closed, depending on the consortium's objectives.

Hybrid blockchain: a combination of public and private blockchains, offering features of both. Certain aspects of the blockchain may be public for transparency, while others are private for restricted access.

Figure 5. Types of blockchain (M1-U2-5)



Source: created by the author for this course

Permissioned blockchain: similar to private blockchains, but with a predefined set of participants who have permission to access and validate transactions. Often used in enterprise settings in which a controlled environment is required.

Sidechain: a separate blockchain network connected to the main blockchain, allowing for the execution of specific functions without directly impacting on the main chain. It enhances scalability and functionality.

Multichain: a private or consortium blockchain platform that enables the creation of multiple, independent blockchains (sub-chains) within the same network. Each sub-chain can have its rules and permissions.

CONTINUE

Unit 2.3 Consensus mechanisms

Chapter 3: Consensus mechanisms

In our previous discussions, we explored the Byzantine generals' problem and its implications for distributed systems. To address the challenges posed by malicious actors and ensure consensus among network participants, various consensus mechanisms have been devised. These mechanisms serve as the cornerstone of blockchain technology, providing solutions to the Byzantine generals' problem and establishing a trustless and decentralised framework for validating transactions and maintaining the integrity of the distributed ledger. In this chapter, we will navigate through different consensus mechanisms, dissecting their unique approaches, strengths, and potential challenges.

Proof of work (PoW)

Proof of work (PoW) is a consensus mechanism used in blockchain networks to validate and confirm transactions. In a PoW system, participants, known as miners, compete to solve complex mathematical puzzles. The first miner to solve the puzzle gets the

opportunity to add a new block to the blockchain and is rewarded with newly created cryptocurrency and transaction fees. This process requires significant computational power and energy consumption.

Advantages

- Security: PoW is renowned for its robust security. The computational complexity of solving puzzles makes it computationally infeasible for a single participant or group to control most of the network, preventing malicious attacks.

- Decentralisation: PoW promotes decentralisation by allowing a diverse group of miners to participate in the consensus process. The distributed nature of mining helps to prevent the centralisation of control within the network.

- Fair distribution: the process of mining provides an opportunity for fair distribution of new cryptocurrency. Participants who invest in mining equipment and contribute computational power are rewarded for their efforts.

- Proven track record: PoW has a proven track record, especially in the case of bitcoin, which has been operational since 2009. The longevity of PoW networks contributes to their perceived reliability and trustworthiness.

- Resistance to Sybil attacks: PoW systems resist Sybil attacks, in which a single participant poses as multiple entities to gain control over the network. The cost and effort required for mining equipment act as a deterrent against Sybil attacks.

Challenges

- **Energy consumption:** one of the significant criticisms of PoW is its high-energy consumption. The process of solving complex puzzles requires substantial computational power, leading to concerns about the environmental impact and sustainability of PoW networks.

- **Centralisation of mining power:** over time, PoW networks have witnessed the centralisation of mining power, in which a few mining pools control a sizeable portion of the total computational capacity. This raises concerns about potential 51% attacks.

- **Limited scalability:** PoW networks face challenges related to scalability as the computational requirements increase with the growing size of the network. This can lead to slower transaction processing times and increased fees during network congestion.

- **Mining hardware arms race:** the competitive nature of mining has led to an arms race in the development of specialised hardware, such as application-specific integrated circuits (ASICs). This creates

a barrier to entry for individual miners and may contribute to centralisation.

- **Economic inefficiency:** critics argue that PoW is economically inefficient due to the high-energy consumption and the need for specialised hardware. This inefficiency contrasts with newer consensus mechanisms designed to address environmental concerns.

In summary, proof of work has demonstrated its effectiveness in providing security and decentralisation to blockchain networks. However, the challenges of energy consumption, centralisation, and scalability have led to ongoing debates about the sustainability and future viability of PoW in the rapidly evolving landscape of blockchain technology.

Proof of stake (PoS)

Proof of stake (PoS) is a consensus mechanism employed in blockchain networks to validate and confirm transactions. Unlike proof of work (PoW), in which participants (miners) compete to solve complex mathematical puzzles to add blocks to the blockchain, PoS relies on validators who are chosen to create new blocks and verify transactions based on the amount of cryptocurrency they hold or

'stake.' In PoS, the probability of being chosen to create a new block is proportional to the participant's stake in the network.

Advantages

- **Energy efficiency:** one of the key advantages of PoS is its energy efficiency compared to PoW. As it does not involve the resource-intensive process of solving complex puzzles, PoS consumes significantly less energy, making it an environmentally friendly alternative.

- **Security:** PoS systems are designed to discourage malicious behaviour by requiring participants to stake their own cryptocurrency. This economic incentive aligns the interests of participants with the security and stability of the network, as malicious actions would risk their own staked assets.

- **Decentralisation:** PoS promotes decentralisation by allowing a broader range of participants to engage in the consensus process. This contrasts with PoW, in which the process tends to be dominated by miners with significant computational power.

- **Reduced centralisation of mining power:** PoS mitigates the centralisation of mining power seen in PoW networks, in which a few entities may control most of the mining capacity. This helps prevent the risk of a 51% attack.

- **Scalability:** PoS is often considered more scalable than PoW. The absence of resource-intensive computations allows for faster transaction processing, contributing to improved scalability as the network grows.

Challenges

- Initial distribution: the effectiveness of PoS relies on a fair and broad distribution of cryptocurrency among participants. If a small number of entities hold a majority of the stake, it could lead to centralisation concerns.

- Nothing at stake problem: the 'nothing at stake' problem refers to the scenario in which validators have no cost associated with supporting multiple conflicting blockchain histories. This can potentially lead to a lack of consensus, as validators may choose multiple forks.

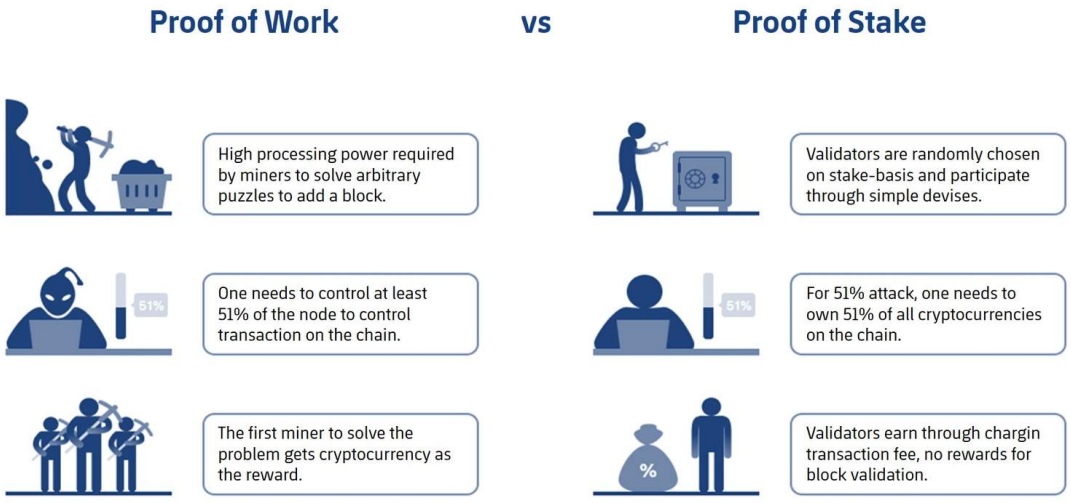
- Long-range attack: PoS networks are susceptible to long-range attacks, in which an attacker can create a fork from an earlier point in the blockchain and build a new chain. This challenge necessitates additional security measures.

- Censorship risk: in PoS, the ability to create new blocks is linked to the amount of cryptocurrency staked. This raises concerns about potential censorship, in which those with larger stakes might influence the consensus process to favour their interests.

- Staking centralisation: PoS networks may face challenges related to staking centralisation, in which a few large stakeholders dominate the consensus process. This could undermine the decentralisation goals of the system.

In conclusion, proof of stake offers notable advantages in terms of energy efficiency, security, and scalability. However, challenges such as initial distribution, the 'nothing at stake' problem, and the potential for staking centralisation must be carefully addressed to ensure the effectiveness and decentralisation of PoS-based blockchain networks.

Figure 6. POW and POS (M1-U2-6)



Source: created by the author for this course

CONTINUE

Unit 2.4 The future of blockchain technology. Application and use cases

Chapter 4: The future of blockchain technology. Application and use cases

What is blockchain technology used for? Blockchain technology is versatile and has found applications across various industries due to its unique features such as decentralisation, transparency, security, and immutability.

Cryptocurrency and blockchain technologies are bridging the gap between sports teams and their fans. They provide innovative solutions to traditional problems, providing a more inclusive and interactive experience for fans.

Let us learn how cryptocurrency enables a strong connection between teams and fans through the benefits of fan apps, digital memberships, and fan tokens.

Ticketing and fan engagement

Use case: the illicit black market has long plagued the sports industry, presenting a significant challenge. However, the integration of blockchain technology into ticketing systems offers a promising solution. Sports organisations embracing blockchain can effectively mitigate the risk of fraud, ensuring fans secure access to priced tickets. The innovative use of blockchain also facilitates easy verification of ticket authenticity, creating a trustworthy marketplace in which transactions are immediate, shared, and completely transparent. This not only bolsters the integrity of ticketing processes, but also enhances the overall fan experience by fostering a secure and reliable environment for ticket trading.

Let us consider the case of Ukraine's national football team that officially partners with WhiteBIT cryptocurrency exchange.

Home match tickets against Italy, Malta, and England were available for purchase with cryptocurrency. This option was made possible by the integration of the Whitepay service into the ticketing system. Whitepay, a crypto-acquiring service and part of the WhiteBIT ecosystem, facilitated this technical integration.

Crypto users enjoyed the advantage of early access to match tickets, gaining the opportunity to secure preferred seats several days before the official commencement of ticket sales. The ticket prices remained fixed in both crypto and fiat currency.

While fans opting for crypto purchases obtained tickets across all categories, there was a noticeable prevalence of tickets from more expensive categories. This trend highlighted the flexibility and appeal of using cryptocurrency for ticket acquisitions.

Authenticity of memorabilia

Use case: blockchain can be used to verify the authenticity of sports memorabilia. Each item can be assigned a unique digital token on the blockchain, providing a transparent and tamper-proof record of its origin and ownership.

Player contracts and transfers

Use case: blockchain simplifies and secures the management of player contracts, transfers, and payments. Smart contracts automate contract execution based on predefined conditions, reducing the risk of disputes and ensuring timely payments.

Anti-doping and health records

Use case: blockchain can be employed to secure and manage athletes' health records and anti-doping test results. This ensures the integrity of the data and provides athletes with more control over their personal information.

Supply chain for sports equipment

Use case: blockchain enhances transparency in the supply chain for sports equipment. It allows consumers to trace the origin and authenticity of sports gear, ensuring that they meet quality and safety standards.

Digital collectibles and NFTs

Use case: non-fungible tokens (NFTs) on the blockchain enable the creation and trading of digital collectibles, including moments from sports events, player highlights, and virtual merchandise. This provides a new revenue stream and fan engagement opportunities.

Fan tokenisation and voting

Use case: blockchain allows sports teams to issue fan tokens, providing fans with ownership stakes and voting rights on certain decisions. This fosters a sense of community and involvement among supporters.

Media rights and royalties

Use case: blockchain can streamline the management of media rights and royalties for athletes and teams. Smart contracts automate the

distribution of payments based on predefined agreements, reducing disputes and ensuring fair compensation.

Sports betting and integrity

Use case: blockchain enhances the transparency and integrity of sports betting. By recording and timestamping betting data on the blockchain, it becomes more resistant to manipulation, reducing the risk of match-fixing.

Decentralised sports platforms

Use case: blockchain facilitates the creation of decentralised sports platforms, enabling direct interactions between athletes, fans, and sponsors. This can lead to new business models, sponsorship opportunities, and content distribution channels.

Significant partnerships of the blockchain industry and professional sport

WhiteBIT cryptocurrency exchange, one of the biggest crypto exchanges in Europe, exemplifies the synergy of blockchain technology and professional sport.

As the official crypto-partner of the legendary football club Barcelona, WhiteBIT demonstrates a comprehensive and inclusive approach,

supporting not only the men's and women's football teams, but also cooperating with various sports branches of the club: the e-sports team in the League-of-Legends, as well as the basketball teams, ice hockey on roller skates, mini-football, and handball.

These partnerships highlight WhiteBIT's commitment to the enhancement and integration of traditional sports, e-sports and blockchain technology.

Moreover, WhiteBIT is a partner of the National Football Team of Ukraine, providing the necessary support and contribution to the wider development and promotion of football at the national level in Ukraine.

In addition, the cooperation with the Turkish football club Trabzonspor further emphasises the support of football in different countries.

WhiteBIT's partnership with FACEIT, the leading platform for e-sports competitions, marks the active participation and support of the development of the e-sports community. By organising joint events for traders and gamers, WhiteBIT and FACEIT promote the development of e-sports and provide opportunities for cross-industry interaction and cooperation. This partnership reflects WhiteBIT's understanding of the synergistic relationship between e-sports and the crypto sector.

Wrapping up

In the second unit of our module, we have delved into the intricacies of blockchain essentials, emphasising the distinction between bitcoin and the broader concept of blockchain, as well as unravelling the significance of decentralisation within this revolutionary technology. Our exploration extended into the inner workings of blockchain, dissecting the components of ledgers, digital signatures, hash functions, and the diverse landscape of blockchain networks. The discussion then delved into the critical consensus mechanisms, navigating the realms of proof of work and proof of stake. Finally, we contemplated the future landscape of blockchain technology, examining its versatile applications and various use cases that extend far beyond cryptocurrency. As we wrap up this module, we have laid a solid foundation for understanding the fundamental concepts and mechanisms that drive the innovative force of blockchain, setting the stage for further exploration and application in the dynamic world of emerging technologies.

CONTINUE

References

Chaum, D. (1983). *Blind Signatures for Untraceable Payments.* Department of Computer Science. University of California.

Nakamoto, S. (2008a). R*e: Bitcoin P2P e-cash paper.* The Mail Archive. https://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html.

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

[Untitled image of bitcoin mining]. (n. d.). https://xcoins.com/es/blog/como-funciona-el-minado-de-bitcoin/.

WhiteBIT. (2023a). *Step-by-step KYC verification on WhiteBIT Web Version* [video file]. YouTube. https://www.youtube.com/watch?v=jyQkn0RpMJg.

WhiteBIT. (2 February 2023). *What is KYC: Meaning, Process, and Advantages*. WB Blog. https://blog.whitebit.com/en/chto-takoe-kyc/.

CONTINUE