Web3 Fundamentals

Authored by Martin El-Khouri & Celine Schröder

Table of Contents

Introduction

On March 8th 2023, Bertelsmann Investments published its first Web3 Whitepaper: "Hedging Against Disruption – Using Venture Capital to understand Web3". This initial publication defined Web3 as a backend revolution to the existing internet architecture. As such, Web3, as we lay it out, in no way should be perceived as an industry of its own. Much more, and just like the internet itself, it should be perceived as a new digital infrastructure layer, affecting the way business is done in the digital world and introducing new paradigms and logics to how business is conducted.

While this initial publication focused on assessing the current state of Web3 adoption and presenting our strategy to enter Web3 as Bertelsmann Investments, the Web3 Fundamentals – as the name indicates – dive deeper. With Web3 fundamentals, we intend to explain the underlying technological novelties in Web3 that provide the cornerstones for new, emerging business logics. Understanding the technological implications laid out below is crucial for comprehending the technology's potential impact on business and emerging business paradigms.

This publication starts by providing an overview of the most fundamental terms in the blockchain space to get the reader acquainted with the topic. As we believe that the necessary understanding on Web3 and its business implications requires a level of technical understanding, we delve into some technological concepts that are relevant in the Web3 space. Based on this foundational knowledge, the paper elaborates on different types of blockchain ecosystems, explains the value proposition of cryptocurrencies and the differing kinds and use-cases of these digital assets. By doing so, this publication aims to emphasize the value cryptocurrency and their protocols deliver as networks for innovation. We dive deeper into why the differences between the various blockchains are relevant. We also put spotlight into new concepts of engaging with digital assets, and the technical novelty of programmable, digital assets. We do not assess the potential evaluation or devaluation of cryptocurrencies as a speculative asset class, although we touch on the value creation and capture of cryptocurrencies.

"Web3 Fundamentals" can be read as a compendium or used as a dictionary to look up and understand specific terms and concepts. In Web3, everything is interconnected in some shape or form. By including sections that elaborate on implications for doing business, providing examples and additional information, we aim at providing a framework that translates what is possible from a technology perspective into profound business insight.

Throughout this paper, startups, protocols, scaling solutions and protocols are mentioned. They have been selected based on how they match the explanatory ambition of this work. If you encounter non-Bertelsmann Investments third parties stated, it does not imply any connection between the authors, Bertelsmann Investments or Bertelsmann with the mentioned providers.

The Backbone

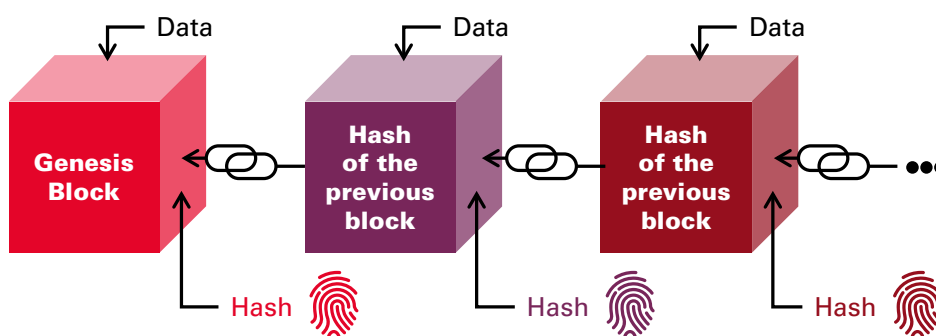## Blockchain – the essence of it all

In essence, a blockchain is a collection of data, typically organized as a series of blocks. Each block in the blockchain contains a bunch of data, which can represent various types of information. This data can range from transactions and account status in the case of cryptocurrencies[1] like Bitcoin[2] and Ethereum[3] to other forms of data such as the usage of Wi-Fi, files, documents, and more.

One of the primary purposes of a blockchain is to maintain a record of transactions, which is often referred to as a ledger. For example, in the case of Bitcoin, the blockchain consists of a list of transactions where the ownership and transfer of bitcoins is recorded. Similarly, in Ethereum, the blockchain not only includes transactions but also stores and executes self-executing contracts, so called smart contracts[4].

Blocks in a blockchain are limited, meaning that there is a maximum amount of data that can be included in each block. Once a block reaches its maximum capacity, a new block needs to be added to the blockchain. In Bitcoin, for instance, the average limit for a block is approximately 2000 transactions.

To ensure the integrity and security of the blockchain, the process of adding new blocks is typically achieved through a process called mining[5]. Miners compete with each other to solve complex mathematical problems by finding a special number known as a nonce[6]. The solution to these problems serves as a so called proof of work[7], demonstrating that the miner has invested computational resources in mining the block.

A crucial component of the blockchain is the hash function[8]. A hashing function is a system where input data is transformed into an output hash. In the context of blockchain technology, hashing functions play a role in verifying the work performed by miners and securing the network. Hashing functions possess several important properties that contribute to the security of the blockchain. For example, it is computationally infeasible to reverse-engineer the input data from the hash. Therefore, one must resort to a trial-and-error approach when trying to find a specific input that generates a desired output hash.

Furthermore, even a slight change in the input data will result in a significantly different output hash, ensuring that even minor alterations to the data being hashed will produce vastly distinct hash values. As a result, tampering with the contents of a block becomes highly detectable since any modification will lead to an entirely different hash.

Computers worldwide, along with specialized mining farms, engage in the process of mining to find the correct nonce that satisfies the requirements of the hashing function. This computational effort is distributed across the network, with multiple participants vying to solve the mathematical problem. Once a miner

---

[1] See chapter 2
[2] See chapter 2
[3] See chapter 2
[4] See chapter 5
[5] See chapter 3
[6] A random value used in blockchain mining to find a hash meeting specific conditions.
[7] See chapter 3
[8] Cryptographic code to ensure transactions.

successfully finds the correct nonce and solves the problem, the block is considered solved and verified by the network. Only once a block has been verified, it is added to the chain.

To ensure that the blocks are added chronologically to the data stored on a blockchain, a specific timestamp is assigned to each block the moment it is added to the chain. By incorporating timestamps, the blockchain creates an immutable and verifiable record of when specific events or transactions occurred. Timestamping plays a crucial role in ensuring the integrity and transparency of the blockchain, as it allows participants to verify the order of events and establish a consistent timeline of activities within the decentralized network.

Public vs. Private vs. Consortium Blockchains

Given the decentralized nature of Web3, this paper focuses on decentralized, public blockchains in this paper. Nevertheless, we recognize the various types of blockchains out there in the following. These include public, private, and consortium blockchains, each of them coming with their very own, distinct characteristics.

BUSINESS IMPLICATIONS

Understanding the distinctions between public, private, and consortium blockchains is crucial for determining the appropriate use cases and designing the architecture of blockchain solutions. Each type has its own strengths and weaknesses, making them suitable for different scenarios based on factors such as trust requirements, data privacy, scalability needs, and the level of decentralization desired.

Public

Public blockchains, such as the Bitcoin, Ethereum, Cardano[9], and Solana[10] blockchain, are open and permissionless networks that anyone can join and participate in. They operate on a decentralized model, where multiple nodes contribute to the validation and consensus[11] of transactions. Public blockchains offer transparency, immutability, and security by enabling anyone to read, write, and verify transactions on the network. The openness of public blockchains allows for greater inclusivity, but it can also present scalability challenges due to the extensive computational resources required for consensus. When we talk about Web3, it is exactly this type of blockchain infrastructure that we are referring to as the new architecture of the internet.

The decentralized architecture of Web3 is enabled by public blockchains due to their transparency, security, decentralized consensus, trustless interactions, tokenization capabilities, support for decentralized applications, so called dApps[12], incentive mechanisms, and enhanced data privacy. These features collectively disrupt the centralized internet, empowering individuals with ownership, control, and new economic opportunities. Private blockchains, on the other hand, are typically more centralized and restricted, limiting their ability to deliver the same level of decentralization and openness.

Private

As restricted, permissioned networks that limit participation to a specific group of known entities, private blockchains are typically used within organizations or consortia, where the participants trust each other and require a higher degree of privacy and control over their data. Private blockchains offer faster transaction speeds and increased scalability compared to public blockchains, because they do not rely on a complex consensus mechanism involving a vast number of decentralized entities. However, the trade-off is that they sacrifice some decentralization and transparency since the consensus mechanism relies on a predefined set of trusted nodes.

---

[9] Blockchain platform founded by Charles Hoskinson, one of the co-founders of Ethereum aiming for a more secure and scalable infrastructure for the development of dApps and smart contracts
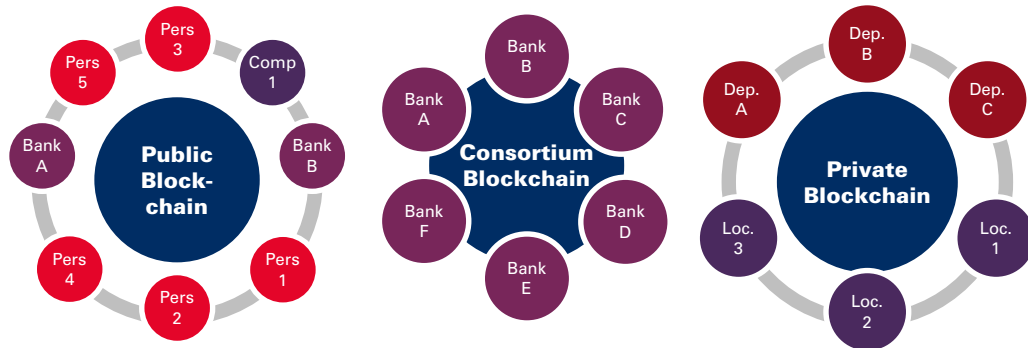
[10] A high-performance blockchain known for its fast transaction speeds and low fees, designed for building decentralized applications and crypto-currencies

[11] The method used to achieve agreement on the blockchain network regarding the state of the distributed ledger.

[12] Decentralized Applications

Consortium

Consortium blockchains represent a middle ground between public and private blockchains. They involve multiple organizations or entities that form a consortium to collectively operate and maintain the blockchain network. Consortium blockchains offer a balance between decentralization and control. They allow multiple organizations to collaborate, share resources, and participate in the consensus process, while still maintaining a certain level of restricted access and governance.

→ Anyone can read, send transactions and expect to see them validated. They are public but anonymous/pseudonymous

→ Consensus process is controlled by a pre-selected set of nodes; e.g. consortium of banks

→ Writing permissions centralized to one organization/entity

INFO

For instance, in a centralized system like a school, only one teacher has the authority to assign and change grades. In contrast, in a decentralized blockchain, multiple participants can have access to view and modify the data, allowing for a more inclusive and transparent system. In a decentralized blockchain, peers within the network can collectively contribute to the validation and verification process. For example, classmates can review each other's test answers and collectively determine the grades based on their assessments. Similarly, in a blockchain, anyone can access and examine the transaction records, ensuring transparency and eliminating the need for a centralized authority.

Furthermore, in many blockchains, participants can actively participate by mining and voting on the validity of transactions. This decentralized consensus mechanism allows individuals to contribute to the blockchain's security and integrity. To prevent fraudulent transactions, asymmetric encryption[13] techniques are employed, where participants use cryptocurrency wallets[14] to secure their transactions and prevent unauthorized alterations. Participating in a blockchain network often comes with incentives. For instance, in Bitcoin, miners are rewarded with newly created bitcoins for successfully mining and adding blocks to the blockchain. This reward system encourages participation and ensures the continued operation and security of the blockchain network.

The term „blockchain" itself reflects the underlying structure and functionality of this technology. Each block within the chain contains data, typically a list of transactions in the case of cryptocurrencies. When a block is solved, meaning the correct hash is found, it is linked to the previous block by including the hash of the previous block in its own data. This linkage creates a chain of blocks, with each block referring to the previous one. Any attempt to modify an old block would disrupt the consistency of subsequent blocks, safeguarding the immutability and integrity of the blockchain.

[13] A cryptographic method using two keys – a public key for encrypting data and a private key for decrypting it. Also known as public-key cryptography.
[14] A digital tool to store, send, and receive cryptocurrency.

Cryptographic Hash Function

Cryptographic hash functions are designed to take an input and generate a unique output, called a hash. One commonly used hashing algorithm is the Secure Hashing Algorithm (SHA), with SHA-256 being a widely used variant. The „256" refers to the amount of 0s and 1s in the output, which computers convert into a string of 64 characters (figures and letters).

There are five main characteristics of a hashing function that contribute to its usefulness in the context of blockchain:

Deterministic Output: A hashing function always produces the same output (hash) for a given input. This property ensures consistency and allows for verification and comparison of data.

Fixed Output Size: Regardless of the amount of data provided as input, a hashing function produces a hash of a fixed size. This is crucial for maintaining efficiency and compatibility within the blockchain network.

Computational Efficiency: Hashing functions are designed to be computationally efficient, allowing for quick calculation and processing of hashes. This efficiency is essential for maintaining the speed and responsiveness of blockchain networks.

One-Way Function: Hashes are generated in such a way that it is computationally infeasible to reverse-engineer or predict the input from the hash. Even a minor change in the input data will result in a significantly different output hash, ensuring the integrity and security of the blockchain, as tampering with the input will lead to a completely different hash.

Collision Resistance: A well-designed hashing function makes it extremely unlikely to find two different inputs that generate the same output hash. For example, in the case of SHA-256, currently, no known two inputs exist that produce the same hash, which is important in order to prevent the possibility of creating different inputs with identical hashes, adding to the robustness of the blockchain.
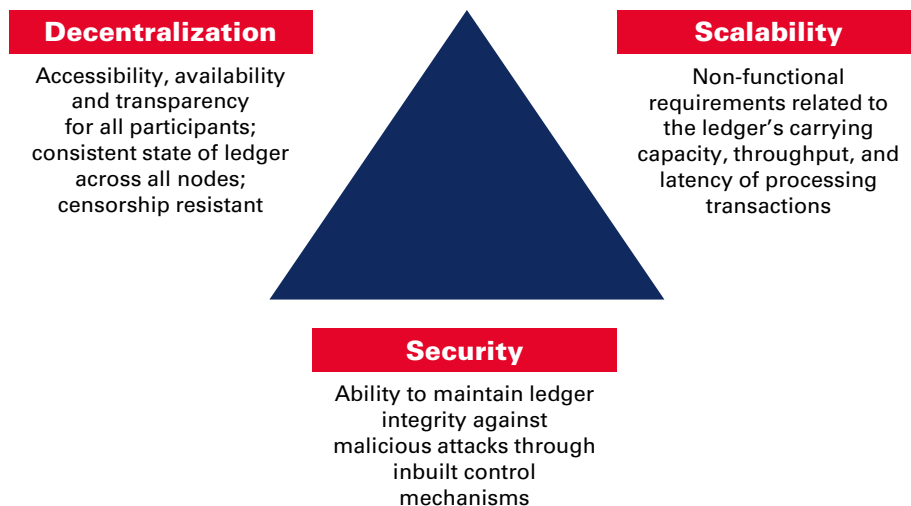
BUSINESS IMPLICATIONS

In the context of a blockchain, when a list of transactions or any other data is hashed, a random set of figures and letters is appended to the data before the SHA-256 calculation. This additional input, known as a nonce, adds an extra layer of randomness and uniqueness to the resulting hash, further enhancing the security and uniqueness of the blockchain. In the Proof of Work (PoW) system utilized by Bitcoin, miners must find a ‚nonce' that, when used in a SHA-256 hash calculation along with the block data, results in a hash value lower than a target set by the network. This nonce, crucial in the mining process, is recorded in the block header, not in the Unspent Transaction Output (UTXO) set. In contrast, Ethereum uses the term ‚nonce' to refer to the sequential number assigned to every transaction sent from a particular address, ensuring all transactions are uniquely identified and processed in order. This Ethereum nonce is an integral part of the transaction data within its own blockchain network.

By employing cryptographic hashing functions, blockchains can ensure data integrity, verify transactions, and provide an efficient mechanism for validating and securing the information stored within the blockchain. These functions serve as the building blocks for the immutability, transparency, and trustworthiness that characterize blockchain technology. These characteristics of a blockchain have implications on business models, as they provide a decentralized and trustless infrastructure capable of reducing the needs for intermediaries, especially in the financial industries. A blockchain solves the digital double-spend without the need for an intermediary, as laid out in Chapter 3.

Scalability – The key to mass adoption

The Blockchain Trilemma

As blockchain technology sets out to provide a decentralized infrastructure that serves as a new architecture of the internet, it needs to meet a number of characteristics in order to be capable of handling massive amounts of transactional data. It needs to be (i) decentral, i.e., no central authority controls or manages the system, (ii) secure, i.e., system is protected from attacks and fraud and challenging for bad actors to alter the chain or commit fraud, and (iii) scalable, i.e., system can handle a large number of transactions quickly and efficiently.

Decentralization

Accessibility, availability and transparency for all participants; consistent state of ledger across all nodes; censorship resistant

Scalability

Non-functional requirements related to the ledger's carrying capacity, throughput, and latency of processing transactions

Security

Ability to maintain ledger integrity against malicious attacks through inbuilt control mechanisms
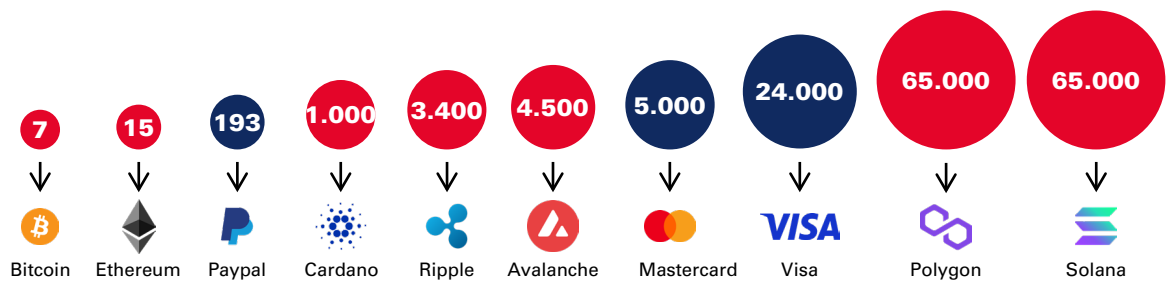
These three characteristics combined represent a concept known as the blockchain trilemma, pointing at the inherent trade-offs that come with designing a blockchain system. According to this trilemma, it is very challenging, if not impossible to achieve all three of these key features at once. High decentralization requires a large number of network participants that verify transactions, and building consensus among more participants typically requires more time. Achieving high security usually requires more computational resources, which can limit the speed of the blockchain or the level of decentralization. A highly scalable blockchain can process a lot of transactions quickly, but this can come at the cost of decentralization or security.

The Blockchain Trilemma suggests that it is tough to have a blockchain that's highly decentralized, very secure, and super scalable at the same time. In order to enhance two out of these three aspects, you would have to compromise on one of the others. This is one of the fundamental problems that many blockchain developers and projects are trying to solve.

Scaling solutions

As a new infrastructure layer for the internet, Web3 has tremendous, transactional relevance. For Web3 to reach mass adoption on a global and sector agnostic scale, blockchains need to be capable of processing transactions at a very large scale. Scaling solutions play a crucial role in addressing the scalability limitations of major blockchains. While blockchains like Bitcoin and Ethereum can typically handle only 7-15 transactions per second (TPS), compared to Visa's capability of processing 24,000 transactions per second, scaling is necessary to compete with centralized systems. New blockchains focus on scalability and achieve much higher TPS, often at the cost of security or decentralization.

Numer of transactions per second (TPS) of selected providers

| 7 | 15 | 193 | 1.000 | 3.400 | 4.500 | 5.000 | 24.000 | 65.000 | 65.000 |
| Bitcoin | Ethereum | Paypal | Cardano | Ripple | Avalanche | Mastercard | Visa | Polygon | Solana |

To achieve scalability, there are two primary approaches: Scaling at the base layer or outsourcing work to a new layer. However, scaling the base layer is challenging due to the above mentioned blockchain trilemma. Therefore, layer 2[16] solutions provide an alternative by introducing external tools and mechanisms to enable scaling without directly affecting the underlying blockchain.
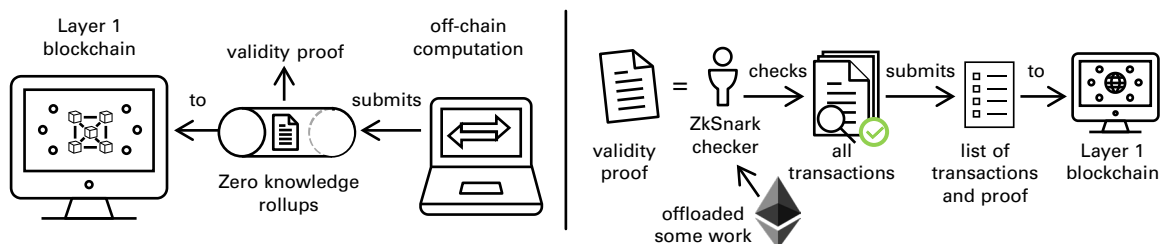
Roll-Ups

Roll-ups perform the execution of a transaction off-chain but submit the final transaction data to the main blockchain at a later point. In the case of Ethereum, rollups leverage the block's capacity to hold not only transactions but also data. By combining multiple transactions into one piece of data, rollups can significantly increase the number of transactions that can be processed within a block. For example, a block on the Ethereum blockchain can only hold 100 transactions. However, if it holds 100 data entries with 10 transactions each, the block can be scaled to hold 1000 transactions.

There are different types of rollups, such as Zksnarks Rollups and Optimistic Rollups.

Zk-SNARKs employ a computation performed off-chain, which is then submitted as a validity proof to the layer 1[17] blockchain. This proof verifies the transactions' authenticity without revealing the specific transaction details, thus achieving zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARK). Let us break down what that means:

// **Zero-Knowledge[18]:** In the scalability context (zk Svnc. Starknet,etc.), ZK is used for the compression of transactions and privacy is not enforced natively. The zero-knowledge property here is natively supported in privacy-preserving protocols like Aztec.Verifier learns nothing about the information the prover has, except that they do indeed have it. No actual information is revealed during this proof, preserving privacy.

// **Succinct:** The proof can be verified quickly, making the process efficient. The proof is small in size and requires a short amount of time to verify.

// **Non-Interactive:** The proof does not require back-and-forth communication between the prover and the verifier. The prover can provide a single proof that the verifier can check without further interaction.

// **Argument of Knowledge:** The proof demonstrates that the prover knows a specific piece of information. It's called an „argument" because it's computationally sound (i.e., a computationally bounded prover cannot convince the verifier of a false statement), but it's not entirely „proof" in a strictly mathematical sense.

Using these types of roll-ups, Ethereum offloads some of its computational work to the zksnarks provers, improving scalability.

---

[15] Sources: Blockchain Council; thecryptobasic; coindcx; bitdegree
[16] A set of solutions built on top of a blockchain (Layer 1) to improve scalability and performance by handling transactions off the main chain
[17] The base layer of a blockchain network where the main protocol and fundamental components reside
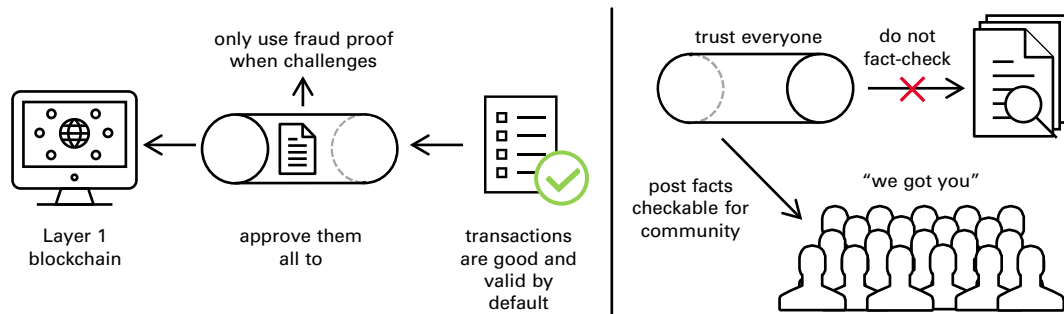[18] A cryptographic method that proves a statement's validity without revealing additional information

EXAMPLE

In a blockchain context, zk-SNARKs are primarily used to ensure privacy and efficiency. For example, in Zcash (a privacy-focused cryptocurrency), zk-SNARKs allow transactions to be verified without revealing the sender, recipient, or transaction amount. This combines the transparency and security of blockchain with the ability to maintain user privacy.

Optimistic Rollups assume that transactions are valid by default and approve them to the main Ethereum chain. They employ a fraud-proof mechanism that is triggered only when challenged. Optimistic Rollups assume truthfulness initially and rely on other participants to fact-check transactions. If fraudulent activity is detected, the transaction is reverted, and the validator responsible is penalized. This approach allows for faster

transaction processing while still ensuring security.

Sidechains

These secondary blockchains run parallel to a main chain. Sidechains can borrow information from the main blockchain, utilize their own resources to execute smart contracts or validate transactions, and then send the data back to the main chain for security purposes. Sidechains rely on the main chain for their operation, while the main chain can function independently without sidechains.

Plasma is a layer 2 solution that utilizes so called child chains[19], also known as plasma chains. These child chains can broadcast significant operations to the main chain while maintaining their own separate operations and transactions. The term „child chain" is used because this blockchain relies on the parent chain for security and network maintenance, much like a child is dependent on a parent in many ways. They are designed to operate independently of the parent chain, and they can handle their own transactions and operate their own applications. The purpose of creating child chains is to increase the scalability of the blockchain network, as each child chain can process its own transactions, thereby reducing the load on the parent chain.

Channels are not really side chains, as a side chain typically maintains a separate consensus mechanism from the L1. Channels rely on the mainnet, and provide another layer 2 solution, allowing users to lock up[20] funds and trade virtual versions of those funds on a faster network. This is similar to how credit card transactions work, where virtual representations of funds are sent between parties. The use of code ensures that users can only send the funds they have locked up. However, channels are limited to transactions and cannot support smart contracts or Virtual Machine code[21].

These layer 2 scaling solutions offer various approaches to enhance the scalability of blockchains while maintaining the required security and decentralization. By introducing off-chain processing, utilizing sidechains, or implementing virtual representations, these solutions provide viable ways to increase transaction throughput and improve the overall performance of blockchain networks.

---

[19] Secondary blockchain operating alongside the main chain to enhance scalability and transaction speed.
[20] Temporarily securing or restricting access to funds or assets.
[21] Instructions for a virtual machine to execute software across different platforms.

BUSINESS IMPLICATIONS

Given the magnitude of the challenge, Layer 2 scaling solutions aim to solve, there is tremendous economic potential involved in them. Business models for layer 2 scaling solutions can vary, but they generally revolve around providing infrastructure, services, or tools that enable users and developers to leverage the benefits of layer 2 scaling.

Infrastructure providers focus on building and maintaining the underlying infrastructure required for layer 2 solutions. This includes developing the layer 2 protocols, consensus mechanisms, and other components necessary for the scaling solution to function effectively. These providers may charge fees for accessing and utilizing their infrastructure in order to monetize. L2s often rely on validators or transaction processors who are responsible for verifying and processing transactions within a respective network. These entities typically earn rewards or fees for their work, similar to how miners are compensated in traditional proof-of-work blockchains. As the solutions themselves also serve as infrastructure layers, there are businesses that offer various services on top of them, typically wallet integrations, developer tools, analytics, user interfaces, or APIs that simplify the adoption and usage of these L2s. Service providers can generate revenue by charging subscription fees, transaction fees, or licensing fees for their services. Some layer 2 scaling solutions have their own native tokens associated with their networks. These tokens may serve multiple purposes, such as staking to secure the network, participating in governance, or paying for transaction fees. The tokens can be distributed through initial coin offerings[22], token sales, or other means, providing a funding mechanism for the development and ongoing operations of the layer 2 solution. Businesses can also generate revenue by forming partnerships and integrations with other projects or platforms. For example, a layer 2 scaling solution provider may collaborate with decentralized applications or blockchain projects, allowing them to leverage the scalability benefits of the layer 2 solution. These partnerships can involve revenue-sharing agreements or other mutually beneficial arrangements.

Crypto Bridge

A blockchain bridge is a connection that enables the transfer of tokens[23] or data from one blockchain or network to another. It allows for interaction with decentralized applications on another chain. In the world of cryptocurrencies, each coin typically has its own blockchain, resulting in multiple independent cryptocurrency networks. Tokens, on the other hand, are virtual representations of assets built on another coin's blockchain[24].

One example is having an Ethereum token on the Binance Smart Chain[25]. These tokens exist as representations on the other coin's network, and mechanisms are employed to ensure that their prices trade similarly. The purpose of a blockchain bridge is to facilitate cross-network transfers and enable users to leverage the functionalities of different networks.

There are several reasons why a blockchain bridge may be desired. For instance, consider the lending and borrowing platform Aave[26]. By moving Ethereum from the Ethereum network to the Polygon[27] network, users can earn higher interest rates on their assets. Blockchain bridges facilitate these transfers, allowing users to take advantage of different networks' features.

Currently, bridges are needed for several reasons. Transaction fees on the Ethereum network can be high, while other networks like Polygon offer significantly lower fees. Additionally, some networks, like Polygon, aim to scale Ethereum but may have different security characteristics due to their more centralized nature. Bridges allow for easier access to these networks and their advantages.

One challenge with bridges is that they require some level of trust. Unlike decentralized applications that rely solely on code and programming languages, blockchain bridges typically involve an entity, person, or company behind them. Many existing bridges are centralized in nature. Another issue is that bridge transfers can be slow, with some taking minutes, hours, or even multiple days, compared to the relatively quick transactions on major networks.

---

[22] A fundraising method where new cryptocurrency tokens are sold to raise capital for a project.
[23] A digital asset that operates on an existing blockchain, often representing assets or utility.
[24] See Chapter 4
[25] Binance's blockchain platform with fast transactions and EVM compatibility.
[26] DeFi protocol for lending, borrowing, and earning interest on digital assets.
[27] Ethereum scaling solution for faster and cheaper transactions.

There are two main ways in which a cryptocurrency bridge operates:

Centralized: In this approach, a bridge functions as an extension of an exchange or a centralized pool. When users deposit their tokens, the centralized authority adds them to the corresponding pool and provides them with an equivalent amount of tokens on the desired network. A fee is charged for the service. However, users must trust the centralized authority not to mishandle their funds, particularly if the process takes an extended period.

Smart Contracts: This method involves the use of smart contracts to bridge cryptocurrencies. When users initiate a transfer, their assets are frozen in a smart contract. They receive a copy of the token on the new network, and the smart contract mints additional tokens on that network based on the frozen assets. This method is typically employed for coins that lack smart contract capabilities, such as Bitcoin, Bitcoin Cash, and Dogecoin, allowing them to interact with networks that support smart contracts, like Ethereum.

While blockchain bridges offer opportunities for interoperability and accessing different network features, they also come with trust and speed considerations. The development of bridges and the collaboration between different blockchains contribute to the progression and broader adoption of cryptocurrencies as a comprehensive solution to various challenges.

BUSINESS IMPLICATIONS

As businesses begin to adopt blockchain technology, they're likely to interact with different blockchains. Bridges offer the flexibility to work across these different chains, using each for their unique advantages.

High transaction costs can be a significant barrier for businesses, especially those with high volumes of transactions. Crypto bridges offer a way to bypass these costs by transferring assets to chains with lower transaction fees. In an increasingly digital and connected world, businesses may need to interact with various partners, customers, and suppliers, each potentially using different blockchains. Crypto bridges enable seamless communication and transactions across these different chains. Embracing crypto bridges now positions a corporate entity to be ahead of the curve and ready for a multi-chain future.

Bridges play a vital role in the interoperability and hence, also in the mass adoption of cryptocurrencies for several reasons:

Interoperability: Different blockchains have their own unique ecosystems and rules. They operate in isolation, leading to a fractured landscape. With crypto bridges, data and value can be transferred seamlessly between different chains, connecting isolated blockchains.

Economic efficiency: By enabling token transfer across chains, bridges can help users avoid high transaction fees on congested networks. This increases the overall efficiency and user friendliness of the crypto economy.

Liquidity: Bridges increase liquidity in the DeFi (Decentralized Finance) space by enabling assets to move across chains. This allows for more trading pairs and options for investors, boosting the utility and value of tokens.

Increased adoption: By making blockchain technology more accessible and user-friendly, bridges can help to drive mass adoption of cryptocurrencies. Users are not limited by the specific technical constraints of each blockchain and can freely move assets where they see the best potential.

Enabling multi-chain applications: Crypto bridges can facilitate the development of applications that utilize features of multiple chains. For example, an app might use Ethereum for its robust smart contract functionality, but utilize a more efficient chain for faster transactions.
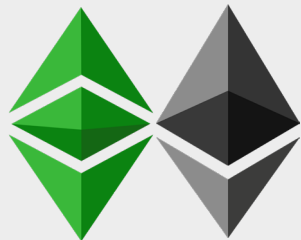
Forks

In the context of programming, a fork refers to an updated or new version of code that is based on existing code with some modifications. In the crypto world, a fork refers to a change in the protocol of a blockchain, which can result in two potential paths for the blockchain to continue.

A soft fork is a type of fork that does not require miners to take any specific actions. Miners can continue to operate and mine blocks using the existing rules and protocols. However, the intended changes and updates to the blockchain are implemented. The new blocks are still compatible with the old blocks, and the network remains backward compatible.

On the other hand, a hard fork requires miners to take certain actions to continue contributing to the network. This could involve updating their software, making changes to certain parameters or rules, or adopting a new consensus mechanism. The changes in a hard fork are significant enough that the new blocks created are incompatible with the old blocks. Miners who want to participate in the new blockchain must upgrade their software to adhere to the new rules. If they continue mining with the old protocol, they will end up on a different chain than the majority of participants who have transitioned to the new protocol.

EXAMPLE

In the early days of Ethereum, there was an organization called The DAO (Decentralized Autonomous Organization) that held a venture capital fund of $150 million. Unfortunately, hackers managed to steal a significant portion of the funds. In response, the Ethereum community, led by Vitalik Buterin, the creator of Ethereum, decided to perform a hard fork to recover the stolen funds. The new blockchain that emerged from this hard fork became the Ethereum network as we know it today. However, there were dissenting voices who believed in the immutability of the blockchain and decided to continue mining the old chain. This original blockchain is now referred to as Ethereum Classic, running on the old rules and protocols of Ethereum.

Forks in cryptocurrencies can result in the creation of separate chains with different rules and characteristics. They can be a way to resolve contentious issues, recover lost funds, or introduce significant upgrades to the network. However, forks can also lead to community fragmentation and differing ideologies regarding the direction of the blockchain.

BUSINESS IMPLICATIONS

Despite being a very technical topic, forks in cryptocurrencies can come along with significant opportunities and challenges for doing business, which anyone building on a blockchain infrastructure should be aware of.

Change in Rules: Businesses need to stay up-to-date with the changes brought by a fork. This can mean updating their systems, changing their operations, or even deciding which version of the blockchain they should follow. This can involve cost and time.

Double Assets: In the case of a hard fork, if a business holds cryptocurrency, it will receive an equivalent amount of the new token on the new chain. This can be an opportunity, but it also presents challenges in terms of accounting, taxation, and management.

Market Uncertainty: Forks often cause uncertainty in the market. This can lead to price volatility of the cryptocurrency, which can affect businesses that hold, use or trade that cryptocurrency.

Community Split: Forks can lead to a split in the community, which can in turn lead to a decrease in network security and value if a significant number of participants decide to leave for the new fork.

Technical Challenges: Depending on the changes brought by the fork, businesses might need to overcome technical challenges to adopt the changes. This can mean adapting their systems to work with the new protocol or even developing entirely new systems.

Regulatory Implications: Forks can also have regulatory implications. Depending on the jurisdiction, businesses might need to follow specific rules when dealing with the new tokens created by the fork.

Reputational Risk: If a business decides to support a fork that is controversial or ends up failing, this could harm their reputation. They need to carefully consider which forks to support and be transparent about their decisions with their customers.

The Paradigm Shift

Cryptocurrencies

Among the numerous use cases associated with Web3 technologies, cryptocurrencies are among the most popular ones. The term "currency", however, can be misleading in many ways.

The term suggests a digital or virtual „currency," which implies it can be used as a medium of exchange, a store of value, and a unit of account, similar to traditional currencies like dollars or euros. Many „cryptocurrencies," particularly those built on platforms like Ethereum, are actually more like digital assets or utility tokens. They represent access to a particular network, service, or resource, rather than acting as a form of money. This is why terms like „crypto asset" or „digital asset" are being used alongside or instead of „cryptocurrency."

> **INFO**
>
> The regulatory definition around digital assets is still discussed with high controversy among law makers and regulators globally. The main challenge is to determine, whether crypto-currencies are securities or not.

When you own a „cryptocurrency" it is somewhat similar to owning shares in a company or a platform. Just as owning a share gives you a claim on a portion of that company's assets and earnings, owning a crypto token can give you a claim on a portion of a network's resources or capabilities. For example, owning Ethereum's Ether tokens allows you to execute smart contracts and create decentralized applications on the Ethereum network. In addition, the native "currency" within such an ecosystem can be a means of payment and an incentive at the same time. It is essential to perform any action on the respective blockchain. Hence, cryptocurrency is not really a currency, as much as there are some crucial differences between crypto assets and company shares. Owning shares in a company often comes along with the right to receive a portion of the company's profits as dividends, and to vote on certain company decisions. With cryptocurrency networks, governance and economic participation in the network is structured differently. Moreover, Ether for instance could de-facto be too useful to be considered as a security, as again, it is needed to use the blockchain, just as gas is needed to drive a car. Separate and apart from any investment contract that may or may not have existed at the birth of the token, Ether might also be too decentralized to fit the relevant test for treatment as a security, which would be favored by most crypto-currency owners. Shares in a company are heavily regulated, with the company required to disclose certain information to shareholders and the public. Cryptocurrencies, on the other hand, are currently much less regulated, and the information available to token holders can vary widely. In addition, the value of a company's shares is linked to the profitability and prospects of the company. In contrast, the value of cryptocurrencies

Top 10 Cryptocurrencies by market capitalisation in US$ bn	
Bitcoin	537,41
Ethereum	198,06
Tether	83,36
BnB	32,72
XRP	28,28
USD Coin	25,32
Solana	9,76
Cardano	9,05
Dodgecoin	8,64
TRON	7,94

As of October 4th 2023

can be influenced by a wide range of factors, including speculation, technology, adoption, specifics related to the tokenomics[28] and market sentiment.

BUSINESS IMPLICATIONS

Cryptocurrencies are among the major fields of application currently resulting out of the application of blockchain technology. Since cryptocurrencies are not controlled by any central authority, they offer alternative monetary ecosystems, as they are not centrally controlled by governments or central banks, but are built on pre-defined mechanisms, which require consensus to be adapted. The cryptographic security measures taken by blockchain networks make it extremely difficult for transactions to be altered or tampered with and all transactions are visible on the blockchain, which can increase trust among users. Cryptocurrencies can be accessed and used by anyone with an internet connection, making them potentially useful in regions with underdeveloped financial infrastructure. Transferring cryptocurrencies can be faster and more efficient than traditional banking and money transfer systems, especially for cross-border transactions. Applying smart contracts to cryptocurrencies, complex transaction-logics can be displayed without the need for an intermediary, giving cryptocurrencies and edge towards traditional, financial processes. Any business model performing on-chain transactions in fact needs the native token to pay transaction and gas fees. Hence, cryptocurrencies can also be perceived as "inventory" for validating and running transactions and processes on a blockchain infrastructure. For any business operating on-chain, this is the biggest value proposition of a coin or token.

Bitcoin

A brief history of Bitcoin

Bitcoin, the world's first decentralized cryptocurrency, was created in 2009 by an anonymous person or group of people using the pseudonym Satoshi Nakamoto. The whitepaper titled „Bitcoin: A Peer-to-Peer Electronic Cash System" was released by Nakamoto in October 2008, outlining the vision and technical details of the cryptocurrency.

The motivation behind Bitcoin was to create a digital currency that operates on a decentralized network, without the need for intermediaries such as banks or governments. It aimed to provide a secure and transparent method of conducting peer-to-peer transactions online, without relying on a central authority. Bitcoin is built on the concept of a blockchain, a distributed ledger that records all transactions and ensures their integrity, and made this concept popular.

Bitcoin gained early adoption among cryptography enthusiasts and individuals interested in exploring alternative financial systems. Over time, its popularity grew, and Bitcoin started to receive wider recognition as a legitimate form of digital currency. It became known for its potential to revolutionize the financial industry by offering financial inclusivity, censorship resistance, and a decentralized store of value.

Bitcoin's Incentivation Mechanisms

Bitcoin operates on a peer-to-peer network, with participants called miners who validate and record transactions on the blockchain. Miners use powerful computers to solve complex mathematical problems that secure the network and add new blocks to the blockchain. In return for their computational efforts, miners are rewarded with newly minted bitcoins and transaction fees paid by users. The primary revenue source for Bitcoin miners who successfully solve a block, is the block reward, which are newly created bitcoins. Initially, the block reward was set at 50 bitcoins per block, but it undergoes a halving event approximately every four years. As of the most recent halving in May 2020, the block reward is 6.25 bitcoins.

In addition to the block reward, miners also earn transaction fees for including transactions in the blocks they mine. These fees are paid by users who want their transactions to be prioritized and confirmed quickly. The transaction fee is determined by the sender and is typically based on the size of the transaction in bytes. Bitcoin's revenue model is primarily based on the issuance of new bitcoins and transaction fees. As the network's security relies on miners' computational power, the block reward incentivizes miners to participate in securing the network and validating transactions.

Bitcoin's Value Proposition

Bitcoin's value proposition lies in its decentralized nature, limited supply, and potential as a storage of value. Unlike traditional fiat currencies, which can be controlled or manipulated by central authorities, Bitcoin's decentralized network ensures that no single entity has control over the currency. This characteristic provides security against censorship, confiscation, and inflation.

Bitcoin's limited supply is another factor contributing to its value. The total supply of bitcoins is capped at 21 million coins, with a finite issuance rate determined by the halving events. This scarcity creates the potential for Bitcoin to serve as a store of value, similar to gold or other precious commodities.

The Bitcoin Standard by Sayfedeen Ammous

„The Bitcoin Standard" provides an in-depth analysis of the stock-to-flow ratio of Bitcoin compared to gold, examining its quantitative aspects and implications for their respective scarcity and value. The stock-to-flow ratio is calculated by dividing the total existing supply of an asset (stock) by the annual production or new supply (flow). Higher stock-to-flow[29] ratios indicate greater scarcity and are typically associated with higher value.

Ammous highlights the historical stock-to-flow ratio of gold, which has been one of the key factors contributing to its value throughout centuries. The annual gold production is relatively small compared to the existing supply, resulting in a high stock-to-flow ratio. This means that it would take a long time to significantly increase the overall gold supply even with increased production.

Flow of Gold
End of 2013 (4,477 tonnes)

176,000 tonnes

Above Ground
Gold Stock

Stock to Flow Ratio IF Stock is   176,000:   58/1
Stock to Flow Ratio IF Stock is   1,200,000:   397/1

Old Scrap
(mostly Jewellery)
1,280 tonnes

3,022 tonnes

GOLD MARKET
Total Flow

Gold Mine
Production

Official Sector
457 tonnes

Mine Flow

4,302 tonnes

Transformed
Gold Stock

Private Investment, Jewellery &
Other Fabrications
3,845 tonnes

---

[29] Ratio assessing asset scarcity by comparing existing supply to new supply.

Bitcoin's stock-to-flow ratio is even more pronounced. Bitcoin's supply is strictly limited to 21 million coins, and the production rate decreases over time through a process called halving. In the first four years since Bitcoin's launch in 2009, the block reward was 50 Bitcoins (BTC) per block. After the first halving event in 2012, it reduced to 25 BTC, and after the second halving in 2016, it became 12.5 BTC. The most recent halving occurred in May 2020, reducing the block reward to 6.25 BTC. This reduction in the production rate every four years results in a diminishing flow compared to the existing supply, significantly increasing Bitcoin's stock-to-flow ratio.

Quantitatively, Bitcoin's stock-to-flow ratio has been estimated by various analysts. PlanB[30], a well-known cryptocurrency researcher, popularized the stock-to-flow model and its application to Bitcoin. Moreover, PlanB extended the stock-to-flow model to predict Bitcoin's future price based on its scarcity. He observed a historical correlation between Bitcoin's stock-to-flow ratio and its market value, suggesting that scarcity plays a significant role in determining its price dynamics. According to this model, Bitcoin's stock-to-flow ratio will continue to increase over time, making it even scarcer than gold, and potentially driving its value upward.

Critics of the stock-to-flow model argue that it oversimplifies Bitcoin's value drivers and ignores other influential factors such as market sentiment, technological developments, regulatory changes, and competition. While the model provides an interesting perspective, it should be considered as one among several approaches to understanding Bitcoin's value proposition.

Altcoins

A brief history of Altcoins

The term „Altcoin[31]" refers to all cryptocurrencies other than Bitcoin. The first altcoins began to emerge in 2011, a few years after the creation of Bitcoin. The first was Namecoin, which aimed to use blockchain technology for decentralized domain name registration. Since then, thousands of altcoins have been created, each aiming to carve out its unique niche or improve upon aspects where Bitcoin may fall short.

Altcoins can differ from Bitcoin in a variety of ways. Some have different underlying algorithms, such as Ethereum's Ethash or Litecoin's Scrypt, while others offer more advanced features or capabilities, such as smart contracts in Ethereum or privacy features in Monero. A significant portion of altcoins are also tokens created on top of other blockchain platforms, such as Ethereum's ERC-20 tokens or Binance Chain's BEP-20[32] tokens.

The role of altcoins in the broader cryptocurrency market has grown dramatically since their inception. Many projects have developed large, active communities and have begun to see mainstream adoption. Moreover, Initial Coin Offerings (ICOs), a fundraising method for blockchain projects where new tokens are sold to investors, have further boosted the creation and popularity of altcoins.

Altcoin business models

The business model of an altcoin can vary greatly based on the underlying technology and the goal of the project. In a generalized sense, altcoins operate in a similar way to Ethereum, which is the most popular Altcoin. They can be considered a form of digital platform or infrastructure that provides various services to users. These services can include enabling transactions, supporting decentralized applications, facilitating smart contracts, or providing a means of value storage, among others.

In the case of altcoins like Litecoin, the business model is straightforward. Litecoin acts as a digital currency, allowing users to send, receive and store value. Users pay transaction fees to incentivize miners to secure the network and verify transactions.

Altcoins like Ethereum or Binance Smart Chain go a step further, providing a platform for decentralized applications. They operate in a similar way to an operating system in traditional computing, allowing developers to build and run applications on their blockchain. The altcoin in this case is used to pay for transactions, deploy smart contracts, or interact with dApps on the network.

---

[29] Ratio assessing asset scarcity by comparing existing supply to new supply.
[30] Twitter account proposing the Stock-to-Flow (S2F) model for Bitcoin price prediction.
[31] Any cryptocurrency other than Bitcoin.
[32] Token standard for fungible tokens on Binance Smart Chain.
[33] Incentives given to miners or validators for adding blocks to the blockchain.

In return for securing the network and processing transactions, miners or validators in these networks are rewarded with new coins, a process known as block rewards[33], and transaction fees. This is similar to the way Bitcoin operates.

Transaction cost and network fees

As with Ethereum, the cost of transactions on most altcoin networks depends on the resources needed to execute the transaction and the current demand for those resources. For example, Ethereum's „gas[34]" model (prior to its merge to a proof of stake consensus mechanism) is also used in many altcoin networks, such as Binance Smart Chain, where it's called „gas" as well.

However, the specific models and costs can vary. For example, in Cardano, transaction fees are determined by a formula that takes into account the size of the transaction in bytes and the amount of computation required to process it. Fees are then paid out to stakers[35] rather than miners.

The primary currency for transactions

Like Ethereum, the primary currency for transactions on most altcoin networks is the altcoin itself. For example, on the Cardano network, ADA is used to pay for transactions and to stake in the network's consensus mechanism. Similarly, on the Binance Smart Chain, BNB is used to pay for transactions.

Supplying the altcoin typically involves participating in the network's consensus mechanism. For Proof of Work (PoW) networks like Litecoin, this involves mining, where miners solve complex mathematical problems to add new blocks to the blockchain. For PoS networks like Cardano, supplying the network involves staking, where participants lock up a certain amount of their cryptocurrency to support the network's operations, validate transactions, and help secure the blockchain, often in exchange for earning additional cryptocurrency as rewards.

Ethereum – A case study[36]

A brief history of Ethereum

Ethereum is a decentralized, open-source blockchain platform that was proposed in late 2013 and officially launched in July 2015. It was founded by Vitalik Buterin, a Canadian-Russian programmer and cryptocurrency researcher, along with several co-founders including Gavin Wood, Joseph Lubin, Anthony Di Iorio, and Charles Hoskinson.

Vitalik Buterin initially conceptualized Ethereum as an extension of the Bitcoin blockchain, aiming to create a platform that would support more complex applications beyond simple financial transactions. He published the Ethereum whitepaper in late 2013, outlining his vision for a programmable blockchain platform that could execute smart contracts.

The motivation behind Ethereum was to provide developers with a platform to build decentralized applications and smart contracts. Ethereum's creators aimed to enable the development of a wide range of decentralized applications, from financial services to decentralized exchanges, decentralized social networks, and more.

Since its launch, Ethereum has gained significant traction and has become one of the most prominent and widely used blockchain platforms. It has attracted a large developer community and numerous projects built on its blockchain. The introduction of Initial Coin Offerings in 2017 further boosted Ethereum's popularity as many projects raised funds by issuing tokens on the Ethereum platform.

---

[34] Unit of measurement for computational effort and fees in blockchain transactions.
[35] Participant in proof-of-stake blockchain who holds and locks up cryptocurrency for validating transactions and earning rewards.
[36] Ethereum Price Target: $11.8k by 2030 | VanEck

Ethereum's business model

Protocols are economic ecosystems that can create and capture value depending on their technological sophistication. Ethereum can be envisioned as a self-contained macroeconomic ecosystem, analogous to a country, where economic activities take place within a secure and regulated environment. It functions as an online marketplace, comparable to an expansive shopping center, catering to a wide range of e-commerce activities.

Within this virtual marketplace, users of Ethereum interact through digital wallets, much like individuals shopping in various stores within a physical shopping center. In Ethereum, businesses are represented by smart contract codes, serving as the foundation for economic transactions. These smart contracts define the structure and regulations of the e-commerce platform, ensuring a fair and transparent environment. Validators play a vital role in this ecosystem, verifying transactions and upholding the rules defined by Ethereum's software. Their efforts secure the platform and maintain a comprehensive record of all transactions occurring within it.

Similar to physical shopping centers, Ethereum has limited space available for conducting transactions and exchanging value. Ethereum allocates this space and charges users for their transactions, akin to rental fees or service charges incurred in traditional commercial spaces. As an open-source software hosted on a global network of computers, Ethereum operates on a set of logical rules known as a protocol. This protocol establishes a common understanding of ownership, commerce, and business principles, allowing participants to engage in economic activities without the need to trust one another explicitly. The code of Ethereum provides clear and unambiguous rules, ensuring strong property rights and fostering an environment conducive to unrestricted business formation and free exchange. Validators, the computers operating Ethereum, as mentioned earlier, are incentivized for their services. They receive rewards through inflationary mechanisms and a portion of the fees paid by users conducting transactions on the Ethereum network. This incentive structure encourages validators to contribute to the network's security and integrity. Businesses within Ethereum are established by deploying a series of smart contracts, representing diverse sectors such as banking, auctions, social networks, gaming, cloud services, and commodities exchanges. Smart contracts serve as code libraries that execute functions automatically when invoked by users, eliminating the need for intermediaries. This feature empowers developers to replicate the operations of real-world businesses within Ethereum, leveraging the benefits of automation and decentralized execution.

By utilizing Ethereum, businesses can maintain their financial operations entirely within the Ethereum ecosystem. They can store their treasury in Ethereum, enabling smart contract payments to employees, vendors, contractors, and suppliers who also possess Ethereum wallets.

Ethereum can be viewed as a macroeconomic ecosystem, akin to a country, where economic activities thrive within a secure and regulated environment. Users interact through digital wallets, businesses are represented by smart contracts, and validators ensure adherence to the platform's rules. Ethereum's open-source nature, along with its logical protocol, fosters trustless commerce, strong property rights, and unrestricted business formation. By leveraging smart contracts, businesses can automate processes, and Ethereum's native incentives reward validators for maintaining the network's integrity.

INFO

Ethereum is often referred to as programmable money because it enables users to execute various actions and calculations on its network. These actions require a certain number of computational resources, and that's where gas comes in. Gas is the fuel that powers the code and computations on the Ethereum network.

The term „gas" is used because it is similar to the gasoline used to fuel a car. It ensures that the cost of executing actions on the network remains consistent, regardless of the price of Ethereum itself. The cost of a transaction is determined by multiplying the gas cost by the gas price.

The gas cost for a transaction remains constant, such as 21,000 gas. However, the gas price can vary. To understand the total cost of a transaction, you multiply the gas cost by the gas price. Gas prices are denominated in Wei, which is a fraction of an Ethereum. For example, 1 Giga Wei (gwei[37]) is equal to 0.000000001 Ethereum.

[37] Smallest denomination of Ethereum, used to measure gas prices.

Let's consider an example of sending money to a friend. Suppose the gas cost for the transaction is 21,000 gas, and the gas price is 100 gwei. If the price of Ethereum is $2,000, the calculation would be: 21,000 gas x 100 gwei = 0.0021 Ethereum. Multiplying this by the current price of Ethereum gives you the cost of the transaction in cash, which in this case would be $4.20. In situations where the network is congested, the gas price may increase. This means the cost of the transaction will be higher. Miners on the Ethereum network prioritize transactions based on the gas price, as they can only include a limited number of transactions in each block. The higher the gas price, the faster the transaction will be processed.

Gas and gwei were introduced into the Ethereum network to ensure that users pay for the computational resources they consume. Without gas limits and gwei prices, malicious actors could exploit the network by running code that never stops, potentially causing significant disruptions. The implementation of gas fees prevents such scenarios and ensures the sustainability and security of the Ethereum blockchain.

One significant improvement to the Ethereum network is EIP-1559[38]. This upgrade, which went live in August 2021, changes the way transaction fees are handled. It introduces a mechanism to burn a portion of the transaction fee, effectively reducing the overall supply of Ethereum. Previously, miners received the full transaction fee as a reward, but with EIP-1559, a portion of that fee is burned, making mining less profitable and reducing the overall supply of Ethereum over time.

These fees depend on the computational intensity and the current demand for computation on the Ethereum network. Interestingly, unlike traditional businesses where the business covers the overhead costs like rent and electricity, users directly pay these overhead costs to Ethereum, the host and main vendor for on-chain businesses. Therefore, users cover both the hosting costs and the computational costs of Ethereum through their transactions.

The primary currency for exchange on the Ethereum network is the ETH token. Users must use ETH to cover the costs of their actions, akin to purchasing game points at an arcade to play games. For any activity on Ethereum, ETH tokens are necessary. Additionally, validators must provide ETH as collateral to vouch for their integrity.

If a validator behaves dishonestly, their ETH is confiscated. Given that ETH tokens are used to pay validators (who sell ETH to cover expenses), this merges the supply and demand- Ethereum users purchase tokens to use Ethereum, and validators sell tokens to „supply" Ethereum.

"Ethereum's core business – the provision of immutable, decentralized computing through the sale of block space."

Matthew Sigel, Head of Digital Asset Research Van Eck

What exactly is supplying Ethereum? Essentially, it involves participating in Ethereum's consensus mechanism, which verifies value transfers, deploys smart contract codes, or enables calls to Ethereum's software. All business operations and asset transfers are recorded as ledger entries on blocks. Blocks are essentially the task list for the Ethereum computer, and every twelve seconds, these tasks are executed. The list instructs Ethereum to execute an action or a series of actions on behalf of the users. These instructions could be as straightforward as transferring value or as intricate as simultaneous buying and selling of several tokens across various Ethereum-based token exchanges. Users secure their inclusion on the block for their actions by paying a base fee and an inclusion fee. If Ethereum's task list is in high demand, users can increase their inclusion fee or „tip" to ensure their request is carried out. Moreover, Ethereum has designed a marketplace to auction off the privilege of ordering the task list on each block due to the significant value in transaction sequencing. These two activities currently constitute Ethereum's core business-selling block space and allowing others to order it. Essentially, Ethereum is selling secure, immutable block space that facilitates e-commerce.

[38] Proposed upgrade to Ethereum's fee structure for improved user experience and fee efficiency.

Revenue Recognition on Ethereum according to VanEck

BUSINESS IMPLICATIONS

VanEck's research identifies revenue in Ethereum's core business as the provision of immutable, decentralized computing through the sale of block space, rather than considering Ethereum as a traditional business. Transaction fees, including both the base fee and tip fee, are counted as a revenue line. While some analysts only consider the base fee, VanEck includes both base and tip fees, as they reflect economic activity related to the sale of block space. This approach acknowledges the economic value generated by these actions and their impact on Ethereum as a business.

Furthermore, VanEck subtracts the ETH burned[39] from the base fee from the total supply of ETH to calculate token value based on the reduced supply total at the end of the year. This reduction in token supply due to ETH usage significantly influences the current token valuation. Inflationary security issuance is not considered a revenue item as it does not directly relate to the purchase of block space by external entities.

VanEck also recognizes Miner Extractable Value (MEV[40]) as a revenue item for ETH. With entities like Flashbots auctioning off blockspace, a portion of the MEV accrues to ETH stakers through validators. Similar to tip fees, block-building fees are also included in Ethereum's revenue calculations as they represent economic activity associated with the sale of blockspace[41].

Additionally, VanEck believes that ETH is evolving beyond a transactional currency or a consumable commodity. While not a complete store of value like Bitcoin, ETH has the potential to become a store-of-value asset for state actors seeking to maximize human capital. They introduce the concept of „Security as a Service, where ETH's value can be utilized both within and outside of Ethereum to secure applications, protocols, and ecosystems. ETH can be locked behind guarantees to ensure honesty, with its value potentially seized as collateral in case of violations or compensations.

In conclusion, VanEck's analysis considers the value of ETH as a token, the safety of Ethereum's software, and the potential for ETH holders participating in Security as a Service to be rewarded based on the value generated by priority fees, tips, block-building fees, and ETH inflationary issuance. The multiple applied reflects the average security risks and investment risks associated with using ETH as a security provision asset.

MEV Revenue: Transaction Ordering, On-Chain Activity & Long-term Projections

According to VanEck's research, Miner Extractable Value (MEV) is a significant aspect of blockchain that cannot be eradicated but can be limited. MEV refers to the profits obtained by ordering transactions within each block. VanEck believes that MEV will continue to play a vital role in securing blockchains over the long term due to its substantial value. They compare its persistence to valuable shelf space in a supermarket, where entities are willing to pay to occupy prime space at the expense of others. Similarly, ordering transactions holds inherent value, and monetizing that ordering can lead to immense gains.

Due to the strong correlation between MEV and on-chain activity, accurately predicting MEV is challenging. VanEck's estimate assumes a direct relationship between MEV and the value of assets hosted on Ethereum. They view this as a „management fee" for keeping value on the Ethereum network. VanEck's current estimate suggests that MEV value approximates around 2.0% of on-chain Total Value Locked (TVL[42]) on Ethereum over the past year. However, they anticipate that MEV as a percentage of assets will decline in the long term as protocols and applications take measures to reduce its impact and remit some value back to users. Consequently, VanEck expects the MEV take rate to dwindle to 0.15%. They consider the total value of on-chain assets in relation to the overall value of assets hosted on the blockchain, which is influenced by the share of the Fee-Based Production[43] (FBP) that blockchains retain and Ethereum's market share.

---

[39] Permanent removal of tokens from circulation to reduce supply and potentially increase value.
[40] Miner Extractable Value, potential profits from transaction manipulation by miners in a blockchain network.
[41] Limited capacity for transactions within a block or blockchain.
[42] Total Value Locked, measures the total value of assets deposited in a DeFi protocol.
[43] Fee-Based Production model charges fees for services or activities on a blockchain network or platform.

L2 Settlement Dynamics:
Scaling Solutions, Revenue Distribution & Future Margin Projections

VanEck emphasizes that Layer 2 settlement represents the primary long-term scaling solution for executing transactions on Ethereum and is thus considered the most crucial business line for Ethereum's future. L2 settlement entails posting transaction batches to Ethereum. VanEck's projections estimate settlement revenue based on L2 revenue and the margin relationship between „profits" and the cost of security for sending batches to Ethereum. They assume L2 revenue is composed of MEV and transaction revenues, both estimated using the Ethereum framework. Furthermore, VanEck assumes that L2s pay a portion of these revenues as security fees to Ethereum. They have observed L2 „margins" fluctuating between 15% and 40% depending on Ethereum's gas costs. In the long run, VanEck asserts that most L2 revenue, including L2 MEV, will still accrue to Ethereum. They anticipate intense competition among thousands of L2s for block space and margins, leading to a projected long-term margin rate of 10% for L2s, compared to the current range of 15% to 40%. They acknowledge that this estimate is somewhat arbitrary but expect shrinking margins for L2s as numerous chains emerge to compete for Ethereum's block space. VanEck assumes that 98% of all transactions will be executed on L2s, while 50% of the total asset value will rest on L2s. Despite this, Ethereum is expected to host half of the ecosystem's value due to the need for extreme security, composability[44], and atomicity[45] levels in some assets and transactions.

Ethereum's Emerging Security as a Service Model

VanEck defines Ethereum's Security as a Service business as revenue generated by exporting ETH token value to support external ecosystems, applications, and protocols. This use case for ETH is still evolving and challenging to predict.

This is rooted in the idea that the Ethereum network exports security in the form of its native cryptocurrency to external ecosystems, applications, and protocols. This essentially means that other projects or blockchains can „borrow" the security properties of Ethereum by anchoring or bridging their assets to Ethereum.

One of Ethereum's primary value propositions is its decentralized and secure network, upheld by a large number of nodes and the value staked or held in ETH. This security can be beneficial to other projects or blockchains that might not have as robust or decentralized a network as Ethereum.

When assets are „bridged" from one blockchain to another, it often means they're represented as a tokenized version on the other chain. For instance, wrapped Bitcoin (WBTC) on Ethereum is a tokenized representation of Bitcoin. This requires locking up the original asset (e.g., BTC) and minting an equivalent amount of the tokenized version on the other chain. In doing so, the security of Ethereum protects the value of these wrapped or tokenized assets.

If Ethereum solidifies its position as a primary security provider for other chains and protocols, this could drive demand for ETH, both as a staking asset and as a bridged asset. This would also enhance the value proposition of Ethereum and ETH as foundational components in the broader crypto ecosystem.

To estimate the percentage of ETH exported for security provision fees, VanEck looks at current and past examples of bridged assets. Currently, around 0.47% of ETH is bridged off Ethereum, similar to the percentage of ATOM[46] off-chain. In the past, BTC wrapped[47] and exported to other chains reached as high as 1.7%, and during Ethereum's peak bridging activity, over 15% of Ethereum's USDC supply was bridged off-chain. As a starting point, VanEck assumes that 10% of ETH is used for off-chain security provision and should command a 2x premium to on-chain ETH due to risk considerations.

The idea that off-chain ETH should command a 2x premium over on-chain ETH is rooted in the additional risks associated with bridging assets between chains. Bridging can introduce various risks, including smart contract vulnerabilities or potential centralization points in the bridging process.

---

[44] The ability of different software components to seamlessly interact and combine in a modular manner.
[45] Property of transactions ensuring they are either fully completed or fully rolled back in case of failure.
[46] Native cryptocurrency of the Cosmos network, used for staking, governance, and participating in block validation.
[47] Process of representing an asset from one blockchain with a token on another blockchain to enable cross-chain functionality.

Crypto Wallet

Crypto wallets, just like regular wallets, allow users to store and manage their digital assets, but with enhanced security and permanence compared to regular wallets. With the increasing number of projects, tokens, and coins in the crypto space, users may need to utilize separate wallets to store their assets effectively.

Crypto wallets are software programs or systems that enable the storage of public and private keys. These keys allow users to send, receive, and monitor their assets securely. When you have a wallet, you have two keys: a public key and a private key. The public key acts as your address, similar to a PayPal email, which you can share with others to receive payments. However, it is crucial to keep your private key confidential, as it serves as the password to your wallet and grants complete access to your funds. While the public key is used to receive transactions, the private key enables you to send them. The following sub-chapter includes a detailed definition of public and private keys.

Different cryptocurrencies may have varying address structures, but generally, the keys consist of a random mix of letters and numbers.

There are various types of crypto wallets available, including software wallets, hardware wallets, and paper wallets[48]. Software wallets are usually online-based and can be accessed through centralized platforms like Coinbase or Binance or decentralized like Metamask. The public and private keys are stored on their servers, and users can access them through their account. It is important to note that with software wallets, the control of your private keys lies with the service provider, which introduces some level of risk, especially when the software wallet is controlled, as the case with Coinbase, Binance, and famously, FTX, by a centralized entity.

Hardware wallets offer a higher level of security by storing your keys on physical devices similar to USB sticks. These wallets allow you to unplug the device and ensure that no one else has access to your keys. Hardware wallets often have robust security measures, such as using a 24-key phrase system to access the wallet. However, it is crucial to remember the key phrases, as there may be no recovery process if they are forgotten.

Paper wallets involve writing down your private and public keys, and sometimes QR codes, on a physical piece of paper. While paper wallets offer a high level of security, they are less practical for frequent transactions. The main drawback is the risk of losing or damaging the piece of paper, which would result in the loss of access to your funds.

Crypto wallets can be classified into two categories: hot wallets[49] and cold wallets[50]. Hot wallets are connected to the internet, either through a company or your own computer, and can be accessed online or through applications. They are susceptible to online attacks, and the exposure of your private key could result in the loss of your funds. On the other hand, cold wallets are offline wallets that are typically connected to a computer through USB or written down on paper. They offer a higher level of security since they are not connected to the internet. However, the main vulnerabilities with cold wallets are the risk of losing the physical device or forgetting the passphrases required to access the wallet.

The choice of wallet depends on the specific use case and the level of security required. For example, if you are actively mining crypto and need immediate access to send the funds, a hot wallet like Coinbase may be suitable. However, for larger investments, a cold wallet like Ledger Live provides enhanced security by allowing you to disconnect the device from the internet and protect your private keys from potential hackers.

[48] Physical printout containing the public and private keys of a cryptocurrency wallet, used for offline storage.
[49] Internet-connected cryptocurrency wallet for active transactions, offering convenience but higher security risks.
[50] Offline cryptocurrency storage for enhanced security.

Public & Private Keys

In the context of crypto wallets, public and private keys play a crucial role in securing transactions. To understand how they work, it's helpful to distinguish between symmetric encryption and asymmetric encryption.

Symmetric encryption involves using a single password or key to both encrypt and decrypt a message. However, sharing this password poses a problem because anyone with access to it can encrypt messages as well, and there is no way to trace who used it.

Asymmetric encryption, on the other hand, utilizes two distinct keys: a private key and a public key. With this approach, you encrypt a message using your private key but provide the receiver with your public key to decrypt it. This ensures that only you can create messages with your private key, and only individuals possessing the corresponding public key can decrypt them. If the receiver wants to respond, they would use their own private key to encrypt the message and provide you with their public key to read it.

In the context of crypto wallets, you share your public key (which is also your wallet address) with others to receive payments. It's important to safeguard your private key, as it grants access to your funds. Your public key serves multiple purposes: it acts as an address for others to send you money, and it is used to verify that messages or transactions were actually created by you.

When you send money on the blockchain, you use your private key to sign the transaction, indicating your intent to send the funds. This prevents others from falsely claiming that you paid them a certain amount, as the public key can be used to verify the authenticity of the transaction. The private key effectively stamps the transaction, while the public key ensures that it was indeed stamped by you.

For example, let's consider a transaction: „01 - Bill pays Bob $50 – 3xk1k48." "01" is the unique number and "Bill pays Bob $50" are the transaction details. The private key is used to encrypt the unique number and the transaction details, resulting in the stamp "3xk1k48". Other participants can check if the stamp is genuine by using your public key. The combination of your public key, the transaction, and the correct stamp indicates that the transaction is valid and originated from you. Changing the unique number in the transaction would lead to a completely different stamp, ensuring that e.g. Bob cannot duplicate the transaction.

Since your public key is publicly accessible, anyone can view all of your transactions on the blockchain. However, the private key remains confidential, allowing only you to generate the necessary stamps for your transactions.

Mechanics

Consensus Mechanisms

Consensus[51] refers to a group of participants reaching an agreement on the state of a distributed ledger. In a blockchain network, participants, also known as nodes, contribute to the maintenance and validation of the distributed ledger. These nodes can be individuals, organizations, or computers that actively participate in the consensus process. Unlike traditional centralized systems, where decisions are made by a single authority, blockchain consensus mechanisms ensure that contributions come from all users participating in the network, as indicated in Chapter 1. This decentralized approach ensures that information recorded on the ledger cannot be fraudulently controlled or manipulated by any single entity.

Consensus models are the means by which blockchain networks achieve agreement among participants. Cryptocurrencies, for instance, require consensus on the state of the blockchain, including transactions, data, and smart contracts. Consensus mechanisms are among the most important aspects of blockchain technology, both from a technological point of view, but also with regards to their implications. Two widely recognized and successful consensus models are Proof of Work (PoW)[52] and Proof of Stake (PoS)[53].

It is important to note that consensus mechanisms play a significant role in ensuring the security, efficiency, and overall functioning of blockchain networks. They allow participants to agree on the validity of transactions and the state of the distributed ledger, creating a trustless and reliable system. By achieving consensus, blockchain technology enables the transparent and decentralized nature of cryptocurrencies and other blockchain-based applications.

EXAMPLE

In a normal database system that holds information, for example medical report cards, a single person or a computer is given the responsibility to manage the entire database. This person or computer is the only one tasked with the job to update, maintain, delete, and add new patient information to the database. Nobody except for that person has access to the database, and technically, if the person or computer would decide to, it could delete your account, or they could claim that you own it a substantial amount of money, at their will. They can alter and manipulate the data as they please. With blockchain technology, this is completely different. Being a distributed ledger, this technology is self-governing. That means that, as indicated above, there is no one person or entity that can control or change it. Instead, contributions come from all users who participate in the network. Taking this concrete example, if somebody would come out claiming you own them a substantial amount of money, they would quickly be outed as a fraud by the rest of the people in the network (validators) that are checking them. This is the first benefit of a consensus model: In an ever changing system like the blockchain, you need a reliable, fair, real time, efficient and transparent that guarantees that transactions are executed and genuine in their nature, and the consensus ensures that every network participant is on the same page with the transactions happening on the network.

---

[51] Agreement and validation process in a blockchain network to maintain a shared ledger.
[52] Explained in the next chapter
[53] Explained in the next chapter

Proof-of-Work (PoW)

Proof of Work (PoW) is a fundamental consensus mechanism that provides security and prevents double spending in blockchain networks. It is an algorithm designed to require a significant amount of computational effort in order to deter or eliminate fraudulent use of computing power. It was first introduced on the Bitcoin network in 2009 as a solution to the double spending problem.

The double spending problem is an inherent challenge in the digital world, where the concept of digital scarcity is does not exist. The problem occurs every time someone tries to make a transaction, like sending a PDF-file from A to B. The sender and the receiver will end up having a copy of the document. There is no such thing as an element of provenance, or an original file. The double spending problem also occurs every time people transact currency they do not possess. This creates duplicate coins, reduces the value of the currency, and makes it unpredictable and unreliable. To date, this double spending problem is solved by intermediaries, who's business model it is to validate transactions and make sure that digital transactions that are deducted somewhere, are added where they are supposed to be added. Blockchain solves this digital double spending problem without the need for an intermediary. Precisely, it is the consensus mechanism that does that.

PoW addresses this issue by utilizing computers to prove that a significant amount of work and time have been invested in finding the solution to a computational puzzle. By putting in computational work, miners ensure that any transactions added to the blockchain are valid. The more work a miner puts in, the higher their chances of winning a block reward. Block rewards are incentives given by the blockchain network to miners for successfully mining and adding new blocks to the blockchain.

INFO

The problem of the digital double-spend has been a challenge, content companies have been dealing with since the emergence of the internet. The multiplication of content has led to multiple challenges when it comes to the enforcement of intellectual property rights. This challenge is magnified by the emergence of generative AI and the impact of this technological breakthrough on the content industry. Enforcement of authenticity is difficult, as assets in the digital world do not exist without intermediaries verifying them as such. Consensus mechanisms are foundational for a new, digital infrastructure, based on which data obtain provenance and intrinsic value. When content can easily and automatically be altered, which is what generative AI is capable of, the relevance for enforcement of intellectual property goes beyond content business models, it will be foundational for the integrity of anyone's personal, digital identity.

One of the key aspects of PoW is that anyone can participate in the network with any computer. However, the more computers a miner has, and the more powerful these are, the higher their likelihood of winning blocks. When a miner successfully mines a block, the transactions within that block are validated, and the records of all participants in the network are updated to include the new blocks. The PoW consensus mechanism ensures a reliable, safe, permanent, fair, and transparent system by forming agreement based on the contributions of network participants. To attack the blockchain, and ultimately alter it, an attacker would need to control 51%[54] of the total computing power in the network. Given the enormous scale of networks like Bitcoin, this would require a significant amount of computational power and would cost billions of dollars, making it economically infeasible.

The ability to mine a block is determined by the computational power of each miner.	A reward is given to the miner who solves each block.	In PoW hackers need 51% of the network computing power to add a block and execute a 51% attack, which is highly unlikely but not impossible.

[54] Security threat where an entity controls over 50% of a blockchain network's mining power, potentially enabling manipulation or disruption.

In the PoW-consensus mechanism, miners broadcast the details of a transaction when they add new blocks to the network. Upon receiving the broadcast, nodes interrupt their current activities to double-check the transaction, ensuring that the asset being transferred has not been double spent. This synchronization ensures that all nodes maintain a consistent copy of the blockchain. Miners compete with thousands of others to earn rewards in the form of the cryptocurrency being mined. Once a miner solves the puzzle of a block, they are rewarded and share their solution with others, allowing them to update their ledger and begin working on the next solution. The difficulty of the puzzle is adjusted dynamically to ensure that blocks are not solved too quickly or too slowly.

INFO

Challenges of PoW:

Despite being the trusted consensus mechanism of the most popular blockchain, Bitcoin, PoW has its challenges and limitations. One concern is its impact on the environment, as the computational work requires significant energy consumption. Additionally, PoW struggles with scalability since only one block is solved approximately every 10 minutes, and blocks have transaction limits. During peak times, fees to send transactions over a PoW blockchain can become prohibitively high. Accurate comparisons between the energy usage of Bitcoin and the traditional financial system can be complex, due to the differing nature of these systems and the lack of precise data. Bitcoin's energy consumption primarily comes from the above mentioned mining process. The Cambridge Centre for Alternative Finance estimated that the Bitcoin network consumed around 121.36 terawatt-hours per year in 2021[57], which would place it among the top 30 energy consumers if it were a country. This figure can fluctuate based on Bitcoin's price, as higher prices make mining more profitable and incentivize more miners to participate, consuming more energy. The traditional banking system's energy consumption, on the other hand, is dispersed across numerous activities: maintaining and running data centers, branch locations, and ATMs; production and distribution of physical money; the energy footprint of associated industries like credit card companies, payment networks, etc. Estimating this can be difficult due to the vast and diverse nature of these systems. However, some estimates suggest the global banking industry uses over 100 TWh[58] per year, while others suggest it could be several times higher.

In terms of efficiency, Bitcoin's PoW is often criticized as it secures the network by intentionally making calculations energy-intensive and difficult, whereas the energy usage in the traditional financial sector can be seen as a byproduct of providing a broad suite of financial services, not merely securing a payment network.

Another challenge is the absence of severe penalties for miners with malicious intent. Despite increasing the cost of attempting to add blocks or preventing them from doing so, miners engaging in misconduct are not adequately punished, leaving room for further exploitation.

From an economic perspective, participating in PoW requires significant investments in computer hardware and electricity. Miners are incentivized to find ways to access cheaper and, ideally, cleaner energy. However, in reality, miners have no inherent motivation to prioritize clean energy unless it becomes more affordable. Furthermore, the demand for mining equipment has led to higher prices for used graphic cards, incentivizing the growth of faster computing and increasing production for equipment manufacturers.

| Impact on the environment | Scalability | High transaction fees in peak times | Absence of severe penalties for miners with malicious intent | Significant investments in computer hardware and electricity |

Despite these challenges, Proof of Work remains a widely used and foundational consensus mechanism in many blockchain networks. It provides security, ensures immutability, and enables trustless transactions by requiring participants to invest computational resources and compete for the opportunity to validate blocks and earn rewards.

[57] Source: Harvard Business Review, 2021
[58] Source: Harvard Business Review, 2021

Mining Pool

Mining cryptocurrencies independently with a general personal computer may take a significant amount of time, 3.500 days on average for Bitcoin, to successfully solve a block on your own[59].

To address this issue and to increase the chances of earning rewards in a more timely manner, miners can join a mining pool. In a mining pool, a group of miners with a common goal of mining a specific cryptocurrency, such as Bitcoin, collaborate and combine their computing power. By working collectively, the pool significantly reduces the time it takes to solve a block. What would have taken an individual miner months or years can now be achieved by the pool in an average of a couple of hours.

When the mining pool successfully solves a block and earns the associated block reward, the reward is divided among the participants based on their contribution. Although not every miner in the pool directly finds the solution, their collective effort is recognized, and the reward is distributed fairly. Miners who contribute more computational power or work harder typically receive a larger share of the reward, ensuring fairness and incentivizing active participation.

One challenge in mining pools is ensuring that participants report their mining activity accurately, as there is a temptation to inflate the reported mining power to claim a larger share of the reward. To address this, mining pools use a concept called „shares[60]." Instead of requiring miners to find the exact solution to the current block, the pool accepts any solution that meets a certain level of difficulty, typically with a lower number of required zeros in the hash. These valid solutions, known as shares, serve as proof of the miner's contribution and are submitted to the pool.

The purpose of a mining pool is to provide miners with more frequent and reliable payouts. Instead of waiting for a year or more to potentially receive a block reward, being part of a pool allows miners to earn smaller but more consistent payouts, often on an hourly or daily basis. This stability in rewards is particularly beneficial for miners who rely on mining as a source of income.

Mining pools typically charge a small fee, usually around 1% of the earned rewards, to cover their operational costs, support ongoing development, and maintain the pool infrastructure, such as web hosting and technical support. These fees contribute to the sustainability and smooth functioning of the pool.

Proof-of-Stake (PoS)

Proof of Stake is a consensus mechanism that provides an alternative to PoW by selecting a single validator to validate a block and receive a reward. In PoS, participants must put up a stake, a certain amount of the native coin, to have the opportunity to be chosen as a validator.

To ensure the integrity of the network, validators are incentivized to act honestly. If a validator fails to validate a block, whether due to intentional negligence, technical issues, or other reasons, their stake can be taken away as a form of punishment. This process is known as slashing, where a portion of the initially locked-up coins is forfeited.

The selection of validators in PoS models involves several factors. These factors may include the total number of coins staked, as individuals with more staked coins are considered more trustworthy, and the duration of the staking period, as longer-term stakers demonstrate reliability and trustworthiness. Additionally, randomness is often incorporated into the selection process to ensure a fair opportunity for all participants.

Validation computations in PoS are designed to be computationally efficient, allowing a single computer to solve them quickly. This streamlined approach enables faster block validation and reduces the environmental impact compared to PoW significantly, as it requires significantly less energy consumption. PoS also

---

[59] Source: BTC Mining Calculator
[60] Units of work contributed by miners in a mining pool, used to distribute rewards proportionally based on contribution.

addresses the issue of cheating or fraudulent behavior. If a validator attempts to create fake transactions or gives themselves free coins, their actions can be fact-checked. Validators are subject to scrutiny by other participants, who can report issues and verify the validity of their blocks. If misconduct is detected, the validator stands to lose a portion or all of their stake.

The ability to mine is determined by how many tokens of this currency the user owns.	In PoS, the miner does not earn rewards but is paid with network fees.	In PoS a hacker would need to own 51% of all the cryptocurrencies on the network to execute an attack, which is practically impossible.

INFO

Why doesn't Bitcoin switch to PoS?

A critical aspect of PoS is its potential for network security and prevention of attacks. However, a premature switch from PoW to PoS can expose the blockchain to a higher risk of a 51% attack. On the other hand, a delayed switch may result in the wasteful consumption of massive amounts of electricity. In the case of Bitcoin, a transition to PoS is unlikely since the consensus mechanism is hard-coded and cannot be changed due to the unknown identity of its creator, Satoshi Nakamoto. A switch to PoS for Bitcoin would require a fork[61], a change in the code that would necessitate the agreement of 51% of the Bitcoin network's participants.

BUSINESS IMPLICATIONS

Becoming a validator in PoS does not require expensive hardware. Instead, participants invest in the native coin itself, as owning a larger stake increases their chances of being selected as a validator. This investment in the native coin stimulates demand, as it can produce income through staking rewards[62]. Consequently, the value of the coin may increase as more individuals seek to acquire it to participate in staking.

Delegated Proof of Stake DPoS is a variation of PoS that allows individuals to delegate their voting power to validators who have the necessary infrastructure. This enables participants to stake their coins and use their voting power to delegate the task of block validation to reliable validator nodes. DPoS eliminates the need for specialized equipment or extensive technical knowledge, making it more accessible for individuals to participate and secure the blockchain.

Today, PoS business models are capable of handling a significantly larger amount of transactions in a much quicker way than PoW blockchains. This, and the fact that they can do that more efficiently, makes the PoS consensus mechanism significantly more attractive for the deployment of smart contracts and large scale business processes. As the native tokens in a PoS ecosystem are not only an asset that fluctuates in its intrinsic value, but can also be used to govern the ecosystem and pay transaction fees, business models that plug into a PoS infrastructure can incentivize user participation and enhance engagement by offering staking rewards. Opening and distributing the network creates ownership at the customer level, which might result in a stronger, and more dedicated user base for any given decentralized application. PoS also allows for the democratization of business processes. Businesses can leverage PoS models to create decentralized platforms where stakeholders have a say in the direction of the platform, based on the stake they hold. Businesses operating on PoS systems can increase trust among their users by showing that decisions are made by those who have a stake in the business. This could lead to improved brand reputation and customer loyalty, and can play a pivotal rule in enforcing global standards across highly heterogenous jurisdictions.

---

[61] Split or divergence in a blockchain, resulting in separate chains with different rules.
[62] Incentives earned by participants who lock up their cryptocurrency to support a blockchain network.

Staking

The term "Staking" has already been mentioned a number of times. It describes a process in which individuals lock up their coins as collateral to participate in PoS consensus mechanisms of protocols, which were described above. By staking coins, participants contribute to the security and operation of the blockchain network and commit a certain amount of their native coins as collateral. This locked-up stake demonstrates their commitment and involvement in the network. In return for their participation, stakers have the opportunity to earn rewards if they successfully validate blocks and contribute to the network's consensus. When staking, there are certain things that should be considered.

Staked coins enter a locked state for a specific period. During this time, participants cannot move or transfer their coins. The lock-up period can vary, ranging from a minimum of a month up to a year, depending on the network's design and rules.

Participants need to have coding skills and the ability to set up their computer to participate in the validation process. They are responsible for configuring their systems correctly and resolving any technical issues that may arise. It's important to have a good understanding of the technical aspects to ensure a smooth staking experience. On a corporate level, these capacities are usually missing.

While participants can stake their coins themselves, there are platforms that offer staking services. These platforms allow participants to delegate their stake to a trusted validator who handles the validation process on their behalf. However, it's essential to be cautious when choosing a platform, as some may charge a commission fee for their services. Participants should consider the reliability and reputation of the platform to mitigate the risk of the commission provider running away with the deposited coins.

The time it takes to receive staking rewards varies depending on the chosen blockchain network. Some networks distribute rewards within minutes, while others may have longer payout durations, ranging from days to weeks. Understanding the reward payout time of the network is crucial for managing expectations and planning.

Although validators strive to make accurate and valid decisions, there is a small chance of disagreement or false accusations by the network. In such cases, even if a validator's actions align with the correct validation, they may still face penalties. Validators need to consider the potential risks associated with validation decisions and the possibility of losing a portion of their staked coins due to network disagreement.

The Tools

Crypto Coin vs. Token

"Coins" and "tokens" are frequently used quite randomly. However, there are distinct differences between the two terms in the world of cryptocurrencies. Coins operate on their own native blockchain, while tokens rely on the infrastructure of another blockchain.

Coins are cryptocurrencies that have their own blockchain, serving as a self-contained system to track all data and transactions. They operate independently and are responsible for validating transactions within their network. For example, Bitcoin and Ethereum are prominent examples of coins, each with its own blockchain infrastructure.

On the other hand, tokens utilize the blockchain of another cryptocurrency as their infrastructure. A token does not require creating a blockchain from scratch or writing code for validation. Instead, it is created and operates on an existing blockchain. Ethereum's team has continuously worked on enhancing the system, ensuring security, and patching vulnerabilities. Different types of token standards can be minted, using the Ethereum ecosystem.

Tokens built on the Ethereum network, such as ERC20[63] tokens, leverage the capabilities of Ethereum's blockchain as their backbone and infrastructure. For instance, the Basic Attention Token is an ERC20 token created by the Brave team. Instead of building their own blockchain, the team focused on developing the Brave browser[64] and using Ethereum's network to facilitate a system where users can reward content creators.

It's important to note that teams working on tokens can migrate to becoming coins if their project gains significant traction. An example is the exchange Crypto.com, which transitioned from having a token to launching its own mainnet (the status, on which a protocol has passed the design phase and has gone live) and introducing its native coin. To facilitate this transition, a bridge[65] can be created to allow users to exchange their previous tokens for the new coins.

Additionally, there are tokens that exist on multiple networks. These tokens maintain representations on different networks, allowing users to interact with them according to the specific network's functionalities. For example, a Binance-peg Ethereum token on the Binance Smart Chain represents Ethereum's value within the Binance ecosystem, providing more affordable transactions.

Tokens serve various purposes and fall into different categories, even though there is no clear consensus on how to categorize tokens, with many of them usually falling into multiple categories:

Platform Tokens: These tokens support decentralized apps on the blockchain. Uniswap, for instance, is a decentralized exchange protocol that has its own token, allowing investors to participate in the platform and potentially influence future changes or earn profits from trades.

Security Tokens: These tokens represent ownership of real-world assets. For example, a token may be minted to track the price of gold. By holding the token, individuals gain exposure to the asset's value without physically possessing it. Security tokens enhance security as it is more difficult to hack a token than to break into a physical storage facility.

---

[63] Standard for creating and implementing fungible tokens on the Ethereum blockchain.
[64] Privacy-focused web browser with built-in ad-blocking and rewards for users and content creators.
[65] Technology or protocol enabling transfer of assets or data between different blockchain networks for cross-chain interoperability.

Transactional Tokens: These tokens provide a fast and convenient method for transferring value. For example, USDC is a token pegged to the US Dollar, enabling easy and low-cost transactions, making it suitable for everyday payments.

Utility Tokens: Utility tokens have value tied to their ownership and can be used for specific purposes within a platform or ecosystem. The Basic Attention Token mentioned earlier serves as a utility token within the Brave browser, allowing users to advertise and reward content creators. The Brave browser anonymously tracks users' attention by monitoring their engagement with websites and ads, measuring metrics such as time spent on a page, active tab, and mouse movements. Users who opt for Brave's privacy-preserving advertising model can choose to view privacy-respecting ads and receive BAT tokens as rewards. These tokens are directly distributed to users' Brave browser wallets. BAT enables users to tip their favorite content creators with tokens, providing an alternative revenue source and incentivizing high-quality content. Advertisers can use BAT tokens to purchase ad space within Brave, reaching users who prioritize privacy. Publishers receive a share of ad revenue in BAT tokens based on their content's engagement. BAT is seamlessly integrated into Brave's built-in cryptocurrency wallet, ensuring secure and user-friendly management of the tokens.

Governance Tokens: These tokens enable holders to participate in decision-making processes within a platform or protocol. Token holders can vote on proposals or changes. In the case of Uniswap, future governance tokens could be used to vote on fee adjustments, giving holders more influence over the platform. Token holders wield governance power, proposing and voting on platform changes. UNI can be earned through liquidity mining, incentivizing liquidity provision. Staking UNI allows holders to earn protocol fees. The token fosters community engagement, enabling active participation in discussions and decision-making.

Tokenomics

BUSINESS IMPLICATIONS

Every institution exploring investment opportunities in the cryptocurrency landscape invariably poses the same query: What is the source of value for cryptocurrencies? The most concise answer is that they represent the only asset class independent from the conventional financial framework. These digital assets don't necessitate intermediaries for transactions, are largely immune to censorship and closure, and certain types offer unmatched privacy to their users. Some of these assets are fueling decentralized ecosystems on the basis of which applications are built, and the assets are necessary in order to use these platforms.

However, when it comes to understanding the value discrepancy between different cryptocurrencies, the issue becomes more intricate. For instance, Bitcoin and Dogecoin might seem similar at a surface level, both featuring regularly in media and sharing some foundational code. But, despite these commonalities, the value of one Bitcoin currently stands at 25,000 $, while a single Dogecoin fetches merely a few cents. This discrepancy stems primarily from the principle of tokenomics, a critical aspect for crypto investors. Tokenomics, as the name implies, stands for token economics, encapsulating a plethora of Key Performance Indicators tied to a cryptocurrency, token or coin. These include supply, allocation, distribution, emission, and utility.

Supply: Several cryptocurrencies like Dogecoin or Shiba Inu[66] boast vast supplies, driving their ranking among the largest projects by market capitalization despite the relatively low value of each individual coin. Others maintain a more restricted supply, potentially leading to per-coin values that surpass Bitcoin, even if their overall market capitalization is just a fraction of that of Dogecoin. The lower the market capitalization, the more straightforward it becomes for a project's value to double. When evaluating a coin or project's market capitalization, it's crucial to focus on the amount of circulating coins. Nearly every cryptocurrency has coins or tokens that aren't currently in circulation, either due to being locked or pending mining. The fully diluted valuation of a cryptocurrency gives an estimated market capitalization if all coins or tokens were to circulate. This measure is critical for assessing a project's entire network value.

[66] Cryptocurrency known for its lighthearted nature, featuring a Shiba Inu dog logo and active online community.

Allocation and Distribution: Cryptocurrencies are typically generated in one of two ways:

1. **Fair Launch:**
   A tight-knit community begins the collective mining of a coin or token. Bitcoin, Litecoin, and Dogecoin exemplify this model, featuring no allocated coins or tokens at inception.

2. **Pre-mine:**
   In this model, the project team mints some or all of the coins or tokens before making the network public. A fraction of these pre-minted coins or tokens is often sold to garner funds for network development. Frequently, pre-mined tokens are allocated to the team and private investors like venture capital firms, with only a minor share sold to retail investors, such as through an Initial Coin Offering (ICO). This dynamic leads to the limited circulating supply observed for many cryptocurrencies. This becomes an issue if a large proportion of coins or tokens is allocated to the team and private investors, as it could impede the growth of that cryptocurrency if these holders decide to sell their shares during a bull market.

A project's distribution involves determining the scale and ownership of a token. It's crucial to ensure that a project isn't overly centralized, which could give undue control to the dominant party. Additionally, a large amount of tokens concentrated in a few wallets can pose a risk to the asset's price, as these principal holders could suddenly offload their crypto, causing a drastic price drop.

Vesting: For pre-mined cryptocurrencies, vesting refers to the anticipated allocation of coins or tokens over a given period. It's common for projects with a pre-mine to lock a certain percentage of their tokens and release them gradually. This method enhances the confidence of regular token holders by preventing a sudden influx of tokens allocated to the team and private investors. These vesting schedules are typically well-thought-out and extend over several years. A rapid release of a large number of tokens can negatively affect the token's price.

Inflation: By design, a cryptocurrency is either inflationary or deflationary. If a cryptocurrency has high inflation, it can depreciate the value of circulating coins or tokens over time. Unless the inflation is extreme, it has minimal to no effect on a cryptocurrency's short-term price potential. PoS cryptocurrencies often incorporate some inflation to incentivize validators and delegators in their networks. This usually ranges between five to fifteen percent, with some cryptocurrencies adjusting their inflation based on staking participation to maintain network security. Numerous DeFi tokens also use inflation to reward liquidity providers and yield farmers on their protocols. If a cryptocurrency is deflationary, a reduction in supply boosts the value of the cryptocurrency over time. This deflation is part of the reason why cryptocurrencies like Bitcoin are highly valuable. Even though new Bitcoin are minted every 10 minutes, it has a maximum supply of 21 million, and the amount of new Bitcoin produced per block halve approximately every four years. Human errors like losing hard drives containing Bitcoin or forgetting wallet passwords contribute to the deflation by reducing the total supply of Bitcoin in circulation, making Bitcoin and similar cryptocurrency projects effectively deflationary.

Staking: When staking cryptocurrency as a validator or a delegator, those coins or tokens are typically locked up for a certain period. This mechanism indirectly limits the circulating supply of the respective token, possibly inducing positive price action. The greater the amount staked and the longer the unlock period, the easier it is to capitalize on positive price movements. Some projects, like Cardano, do not incorporate such lock-ups, meaning staked coins can be transferred to exchanges and liquidated at any point.

Utility: Also known as a use case, utility represents anything that drives demand for a currency or coin. Bitcoin's main utility is as a store of value, akin to gold. The key difference is that Bitcoin is accessible to virtually anyone with an internet connection. Considering the depreciating value of fiat currencies, there's significant demand for an easily accessible store of value like Bitcoin. Ethereum's primary use case is for paying fees to use the decentralized apps built on it and to transfer ERC20 tokens. The hundreds of dApps and thousands of ERC20 tokens represent substantial demand for Ethereum to cover gas fees, making it the second most valuable cryptocurrency on the market. Many DeFi tokens function as voting tools in the governance systems of their respective protocols. As the total value locked in a protocol rises, so does the demand for its governance token. It's interesting to note that the market caps of many DeFi tokens, like Aave, closely match the total value locked in their protocols, providing an indicator of whether a protocol is undervalued or overvalued.

NFTs

A non-fungible token (NFT) is a type of digital token or asset that represents ownership of a unique item or piece of data. It can be compared to digital trading cards or digital paintings, where each NFT is distinct and cannot be divided or interchanged like a fungible asset such as Bitcoin.

When you buy an NFT, you are essentially acquiring the rights to that specific asset. Unlike fungible tokens, which are identical to one another, NFTs are always different and unique. They are represented by a small piece of data owned by an address. Ownership of this data can be bought and sold to different addresses, and the transaction history of NFTs is verifiable on a blockchain.

It is important to understand that you are acquiring a piece of data that represents something larger when you purchase an NFT. For example, buying an NFT may give you ownership of a digital image or GIF hosted on a server. The specific piece of data that you own is stored on the blockchain, and it is not the access to the server or the image itself. It is crucial to be aware that the server or the image could potentially change, but the ownership of the data represented by the NFT remains intact. Often, NFTs are confused with digital collectibles. In fact, however, an NFT can represent any piece of data that is supposed to entail the concept of provenance. In a revised internet architecture, any piece of data could become an NFT. This would represent the most significant paradigm shift to the enforcement of intellectual property in the digital world. Any piece of digital content can be an NFT. A book, a song, a dataset of medical analyses.

The concept of an NFT introduces the concept of digital scarcity, and with it, it allows for the existence of digital assets.

The concept of an NFT introduces the concept of digital scarcity, and with it, it allows for the existence of digital assets. Data now become ownable, valuable, investable and programmable. NFTs can also be fractionalized, adding potential liquidity to previously illiquid asset classes.

NFTs derive their value from several factors. First, NFTs associated with the first creations of specific artists or businesses often hold value, just as early editions of collectibles gain popularity. Additionally, NFTs that offer real-world benefits or utilities can be highly sought after. For example, an NFT associated with Elvis Presley offering lifetime access to his shows would have significant value. Rarity or uniqueness also contributes to an NFT's value. Just like the original Mona Lisa painting, owning the original or limited edition of an NFT can make it more valuable. Furthermore, the ownership history of an NFT can impact its value. If a notable individual like Robert Downey Jr. previously owned an NFT, it may command a higher price due to its connection to a famous owner.

When evaluating the value of an NFT, it's essential to consider these factors and ask pertinent questions. For instance, in the case of purchasing Jack Dorsey's first tweet for $2.5 million, it fulfills the criteria of being the first NFT in that category and being unique. However, it lacks utility and ownership history, as no famous individual has owned that specific NFT yet. Therefore, buying such an NFT primarily relies on the belief that its value will increase over time.

While it is technically possible to copy an NFT, the original NFT's address can be traced back to the original creator through the transaction history recorded on the blockchain. Additionally, it's worth noting that someone could create a new NFT pointing to the same hosting address or a different address with the same image or GIF.

To purchase an NFT, you typically need to use marketplaces specialized in NFTs. Most NFTs are bought and sold using Ethereum, so owning Ethereum is usually necessary. The process involves creating an account on an NFT exchange, buying cryptocurrency on another exchange, transferring it to your NFT wallet, and bidding on or purchasing the desired NFT. NFT wallets are similar to other cryptocurrency wallets, typically comprising a public and private key. After your purchase, it's advisable to store your NFT securely, such as on a hardware wallet, to protect it and showcase it to others.

Airdrop

Airdrops are akin to delightful surprise bonuses in the crypto realm, whereby developers or platforms dispense free tokens or coins to users such as yourself. The underlying objective is to promote their digital assets and incentivize their wider adoption and usage.

To illustrate, imagine that you're an active user on a decentralized exchange known as Uniswap. Recently, Uniswap unveiled a fresh governance token named UNI. In a bid to reward their early users, Uniswap staged a retroactive airdrop. Essentially, they retrospectively allocated around 400 UNI tokens to each wallet address that had previously interacted with their platform. Merely by your past engagement with Uniswap, you are now in possession of valuable tokens, which you obtained gratis.

Airdrops also serve as an effective strategy when companies seek to augment their user base. They might distribute a modest amount of their token as an airdrop in exchange for your email address. This method allows them to maintain direct contact with you, providing updates or exclusive promotions. It's akin to receiving a small token of appreciation for becoming part of their community.
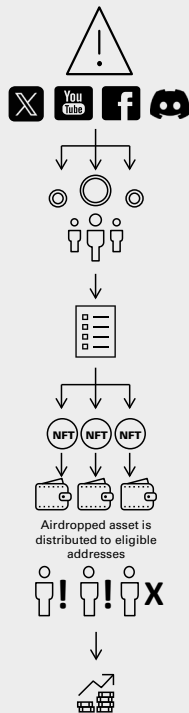
To stay abreast of captivating airdrops, you could frequent websites such as airdrops.io. Such platforms feature calendars outlining upcoming airdrops related to an array of tokens. You may stumble upon projects offering tokens in return for straightforward actions like signing up or accomplishing specific tasks. This presents an opportunity for you to participate in novel projects and potentially accrue valuable tokens in the process.

Airdrops can also cater exclusively to certain communities. For instance, if you're the proud owner of a unique digital artwork, or NFT, certain projects may reward NFT owners with exclusive airdrops. These could entail a special edition token, privileged access to limited edition NFTs, or even tangible goods affiliated with the artwork.

Therefore, for you as a participant in the cryptocurrency ecosystem, airdrops can manifest as unanticipated gifts that let you explore new tokens, get recognition for your early patronage, or even secure exclusive perks based on your membership in specific communities. It's a thrilling avenue to engage with diverse projects and potentially profit from the tokens you acquire at no cost.

EXAMPLE

Airdrops in the context of the Board Ape Yacht Club (BAYC) or any other NFT project usually involve the free distribution of new tokens, digital assets, or other forms of value to existing holders of a particular token or NFT. As of my knowledge cutoff in September 2021, BAYC hasn't yet initiated an airdrop, but I'll explain the general process:

Announcement: Airdrops usually begin with an announcement from the project developers. This might be done through a project's official website, social media channels, or other communication platforms like Discord.

The announcement typically outlines the eligibility criteria for the airdrop (usually owning a certain NFT or token by a specific snapshot date), the date of the airdrop, and instructions on how to claim the airdropped items.

Snapshot: The project team will take a „snapshot" of the blockchain at a certain point in time. This snapshot will record the addresses that hold the qualifying NFTs or tokens. Only the owners of the NFTs at the time of the snapshot will be eligible for the airdrop.

Distribution: After the snapshot, the airdropped tokens or assets are distributed to the eligible addresses. The distribution might happen automatically, or owners might need to claim their airdropped assets manually by interacting with a smart contract.

Claiming: Depending on the project, owners might have to take some action to receive their airdropped assets. This could involve connecting their wallet to a specific website or platform and confirming the transaction.

Trading: Once claimed, these new tokens or assets can typically be traded on various platforms. The value of these airdrops can vary significantly, depending on market demand and the perceived value of the airdropped asset.

Airdropped asset is distributed to eligible addresses

Decentralized Autonomous Organization

A decentralized autonomous organization (DAO) is an organization that operates through code agreed upon by its participants. It relies on smart contracts to automate various tasks, making it self-sustainable and autonomous. A DAO can be thought of as an organization run by code rather than human decision-makers. It eliminates the need for traditional decision-making processes and replaces them with automated processes.

To better understand how a DAO functions, consider the analogy of a vending machine. In a DAO-like scenario, every aspect that requires human involvement would be replaced with code or code-based counterparts, such as robots. For instance, the vending machine would automatically monitor its stock and send restocking information to a server when necessary. A robot would then be responsible for restocking the machine and handling cash deposits.

While this level of automation may seem far-fetched, it represents the essence of how a DAO operates. Unlike traditional organizations like Apple, Netflix, or Walmart, which have boards of directors making decisions that are then implemented through a chain of command, DAOs operate differently. In a DAO, decisions made by stakeholders are directly implemented through changes in the organization's underlying code. This allows for more efficient and streamlined operations.

DAOs have the potential for continuous improvement and growth because shareholders can propose and vote on changes. In the world of cryptocurrencies, a DAO often launches with a set number of tokens, and each token represents a vote. Token holders with a significant number of tokens have more voting power. This system gives the tokens value and provides a means for the DAO to evolve and make improvements. It can even hire and pay developers within the organization using cryptocurrency.

[67] See next Chapter

One of the benefits of a DAO is that it is trustless. You don't have to rely on a CEO or manager for decision-making, as the organization is driven by code. A DAO is also resistant to shut down, as it cannot be easily dismantled by government intervention. Unlike centralized organizations, DAOs are open source, allowing anyone to review and improve upon the code, making them more reliable.

However, DAOs also have their downsides. They can be vulnerable to attacks since the code is open for scrutiny. Attackers who understand the code's intricacies can reverse-engineer it, test their attacks, and potentially exploit vulnerabilities. Additionally, business secrets are challenging to maintain in a DAO since the code is open source, making it difficult to keep proprietary information confidential.
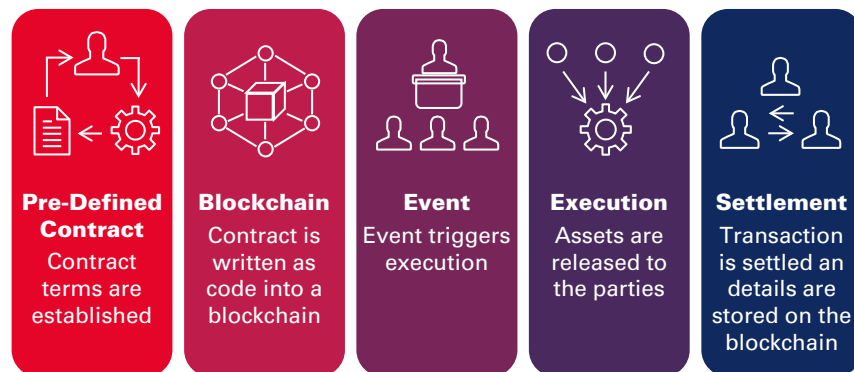
The most famous DAO is „The DAO," a venture capitalist fund created in 2016. It gained attention for its failure when hackers exploited a vulnerability, resulting in the loss of around $50 million worth of Ethereum. To address the issue, the main developers of Ethereum performed a hard fork[67] from Ethereum Classic to Ethereum.

DAOs represent a vision of the future where organizations rely on smart contracts and code instead of people. While they offer benefits such as automation and transparency, they also present challenges in terms of security and the protection of proprietary information. As technology progresses, the role of DAOs in various industries may continue to evolve.

Smart Contracts

Among all the terms mentioned in this paper, smart contracts are probably the most relevant of them all when it comes to their impact on how business is conducted on a decentralized, blockchain-based infrastructure.

Essentially, smart contracts are pieces of code that execute specific actions based on predefined conditions, following the principle of „if this, then that." The most common platform for writing smart contracts is the Ethereum network, utilizing a programming language called Solidity and the so called Ethereum Virtual Machine (EVM)[68]. Many other platforms are smart contract compatible and most of them are because they use Ethereum's EVM as a foundation for that.

Pre-Defined Contract Contract terms are established

Blockchain Contract is written as code into a blockchain

Event Event triggers execution

Execution Assets are released to the parties

Settlement Transaction is settled an details are stored on the blockchain

These contracts enable a wide range of functionalities, with various examples showcasing their versatility:

Financial Agreements: A smart contract can facilitate the exchange of assets based on specific conditions. For instance, if you give me five Ethereum, I will provide you with 20 Basic Attention Tokens in return. This type of contract automates transactions and ensures transparency.

Milestone-based Rewards: Smart contracts can be programmed to trigger rewards based on predetermined milestones. For example, if you achieve at least 100,000 subscribers by the end of the year, 20 Ethereum will be added to your account. Such contracts automate the distribution of rewards, removing the need for manual intervention.

[68] Ethereum Virtual Machine, runtime environment for executing smart contracts on the Ethereum blockchain.

Insurance Contracts: Smart contracts find applications in the insurance industry. Consider a scenario where Farmer John's account receives $100,000 as crop insurance if the temperature exceeds 95 degrees for more than four consecutive days. The smart contract monitors the temperature data and automatically initiates the insurance payout, removing the need for lengthy claims processes.

Crowdfunding and Incentives: Smart contracts can be employed for crowdfunding purposes. By creating a contract where people can donate Ethereum to a specific address, it becomes possible to provide incentives once a certain threshold, such as 500 Ethereum, is reached. For instance, each donor could receive a portion of an online artwork, an NFT, or access to a community. The possibilities for utilizing smart contracts in this manner are extensive.

Smart contracts are immutable, meaning they cannot be changed once deployed on the blockchain. They operate as code on the blockchain that executes specific actions when triggered. This characteristic ensures the reliability and transparency of the contracts. However, it also implies that any bugs or inefficiencies in the code persist unless a new smart contract is created and users are instructed not to use the old one.

Smart contracts are distributed agreements, which eliminate discrepancies by removing the need for intermediaries. They function as agreements between multiple parties online, executing automatically when predefined conditions are met. By reducing the need to rely on human involvement, smart contracts minimize errors and streamline processes, and doing so while the distributed nature of smart contracts ensures transparency and accessibility. The code resides on numerous computers worldwide, enabling anyone to inspect the contract's functionality and how individuals have interacted with it. Consequently, financial agreements become indisputable as they are governed by immutable code accessible to all participants.

Examples of smart contracts in action include:

Flash Loans : Smart contracts can execute complex financial operations such as flash loans. These loans are granted and repaid within a single transaction. The contract self-checks if the borrower can repay the loan and, if feasible, executes the code. Flash loans provide borrowers with immediate access to funds for various purposes.

Insurance: Smart contracts enable the creation and execution of decentralized insurance policies. The contract automatically verifies predefined conditions and initiates claims or payouts accordingly, eliminating the need for traditional insurance intermediaries.

Token Switching: Smart contracts can facilitate token swapping in decentralized exchanges. By creating a pool of two different tokens and employing smart contracts, traders can switch one token for another. As one token's volume increases, the price of the other token in the pool adjusts accordingly, ensuring stability and liquidity.

Real Estate Transactions: Smart contracts have the potential to revolutionize real estate transactions. For instance, a smart contract can hold the deed of a house on the blockchain, transferring ownership to the party possessing the contract. This streamlined process eliminates intermediaries, reduces transaction times, and enhances accessibility to the real estate market.

In summary, smart contracts provide automation, transparency, and security in various domains, ranging from finance and insurance to crowdfunding and real estate. By leveraging the power of blockchain technology, smart contracts enable the execution of predefined actions based on specified conditions, revolutionizing traditional agreements and processes.

---

[69] Temporary, collateral-free cryptocurrency loans that must be repaid within the same transaction, commonly used for time-sensitive financial operations in DeFi.

The Economy

Decentralized Finance

Decentralized Finance (DeFi) represents a paradigm shift away from centralized finance, which is controlled by governments and banks, to a system governed by smart contracts, cryptography, and blockchain technology. Unlike traditional finance, DeFi eliminates the need to trust intermediaries and instead relies on transparent and secure code. Let's explore the key pillars of DeFi and their use cases:

Stablecoins: Stablecoins are cryptocurrencies that maintain a value pegged to a real-world asset, such as the US Dollar. They provide a reliable way to trade and transact without the volatility associated with other cryptocurrencies. By using stablecoins, users can avoid high fees and lengthy waiting times typically associated with centralized exchanges and traditional banking systems. Stablecoins enable quick transactions within minutes and lower fees, making them an attractive alternative for individuals seeking financial freedom outside government-controlled banks.

BUSINESS IMPLICATIONS

Stablecoins have emerged as intriguing instruments with the potential to provide value for businesses in various ways. One area where they showcase their potential is in payment efficiency. With their ability to facilitate cross-border transactions at a lower cost and faster speed than traditional banking systems, stablecoins offer an avenue for corporates to streamline their international payments. This can result in improved cash flow and reduced transaction costs, which are important considerations for businesses aiming to optimize their financial operations.

Supply chain optimization is another area where stablecoins can play a role. By enabling transparent and efficient transactions, stablecoins can contribute to smoother operations and enhanced relationships with suppliers. The potential value lies in reduced holding costs, improved liquidity, and increased operational efficiency. However, it's important for corporates to assess the specific dynamics of their supply chain and evaluate whether stablecoins align with their unique requirements.

In DeFi, stablecoins can be leveraged by corporates for additional liquidity, treasury management, and yield-earning possibilities. While these avenues may offer potential value, it's crucial for corporates to approach DeFi with caution, considering factors such as regulatory frameworks, market volatility, and counterparty risks.

Generally, stablecoins can be a powerful tool to foster financial inclusion. By utilizing stablecoin-based payment solutions, businesses can extend their reach to unbanked or underbanked populations, creating opportunities for new market segments. The value lies in increased market penetration and the potential for expanded customer bases.

Another aspect for stable coins to create value is risk management. As stablecoins offer relative stability compared to other cryptocurrencies, they can serve as potential hedging instruments against market volatility.

Ultimately, the value captured through stablecoin adoption will vary depending on each corporate's unique circumstances and objectives. Quantitative analysis, careful consideration of risks, and a balanced approach to implementation are essential for corporate innovators seeking to harness the potential benefits of stablecoins while mitigating potential drawbacks. By adopting a measured and strategic approach, corporates can effectively evaluate and leverage stablecoins to drive innovation and optimize their financial operations.

Lending and Borrowing: With the use of smart contracts, DeFi allows for lending and borrowing without the need for traditional banks. Individuals can lend their funds and earn interest while retaining custody of their assets. Borrowers can collateralize their loans by depositing assets into smart contracts, providing security for lenders. For instance, Person A can deposit their coins into a smart contract and receive tokens representing the original deposit plus interest. Meanwhile, Person B can borrow coins by overcollateralizing their loan. Smart contracts automate interest calculations and loan repayments, reducing the need for human intervention.

A special example in this context is the emergence of flash loans. These are ultra-short-term loans that are executed and settled within seconds, typically lasting no more than a few blocks on the blockchain. Flash loans enable individuals to access significant capital without the need for upfront collateral or credit checks. For example, if there's a temporary price discrepancy in the cryptocurrency market where Ethereum can be bought for $10 on one exchange and sold for $11 on another, a flash loan can be utilized. With a flash loan, you can borrow millions of dollars within seconds, without putting any money down. By executing a small smart contract, you can buy Ethereum for $10 and immediately sell it for $11, using the proceeds to repay the loan. The entire process is automated and completed within the short duration of the flash loan.

Decentralized Exchanges: Decentralized exchanges (DEXes) enable the exchange of cryptocurrencies without relying on intermediaries. These exchanges operate on the blockchain, utilizing smart contracts to facilitate trades. DEXes typically operate through liquidity pools[70] where investors pool their funds, and traders can execute trades. Fees collected from trades are distributed back to the investors, following predefined rules embedded in the smart contracts. Decentralized exchanges offer lower fees, enhanced liquidity, and a wider range of available tokens compared to centralized exchanges. They empower individuals to trade and invest in various tokens and coins without the need for regulatory oversight.

Insurance: DeFi allows for the creation of decentralized insurance platforms through smart contracts. For example, a farmer may purchase crop insurance using a smart contract. The contract could specify that if there are any days in the summer with temperatures exceeding 90 degrees Fahrenheit for four consecutive days, a payout of $100,000 will be made to the farmer. Smart contracts can utilize oracles[71] as trusted sources to gather real-world data, such as temperature readings, to determine if the insurance requirements are met. Investors who provide liquidity to decentralized insurance platforms may earn interest on their deposits, making it an attractive investment opportunity.

Margin Trading: In DeFi, margin trading offers opportunities for users to amplify their trading potential. Traditional finance requires identity verification and substantial capital for margin trading, along with high fees. In contrast, DeFi allows anyone with funds to engage in margin trading in a quick and secure manner. Users can leverage borrowed funds to magnify their trading positions. Smart contracts automatically liquidate positions if the value of the collateral falls below a certain threshold, ensuring the lender is repaid. Decentralized margin trading opens up new possibilities for individuals worldwide to engage in speculative trading without onerous requirements or excessive fees.

Decentralized Finance revolutionizes the financial landscape by leveraging the power of smart contracts, cryptography, and blockchain technology. It offers greater accessibility, lower costs, increased transparency, and enhanced financial autonomy. With DeFi, individuals can participate in various financial activities, such as trading, lending, borrowing, insurance, and margin trading, in a decentralized, secure, and efficient manner.

Liquidity Pool

A liquidity pool is a pool of funds created by a smart contract that enables traders to trade tokens and coins even when there are no immediate buyers or sellers available. Unlike traditional stock markets that rely on order books, liquidity pools utilize an algorithmic model to ensure continuous trading regardless of the market conditions.

---

[70] Pool of funds in a smart contract used for trading and liquidity in decentralized exchanges and DeFi platforms.
[71] External data sources that provide real-world information to blockchain smart contracts.

In a traditional stock market, buyers and sellers submit their orders stating the quantity of stock they wish to buy or sell and the desired price. Trades occur when a buyer and seller match at the same price, and the buyer receives the stock while the seller receives the cash. However, this model can be inefficient as traders have to set prices that align with others' expectations, leading to delays or suboptimal trades.

A liquidity pool operates differently. It is a smart contract that holds a combination of assets, such as Ethereum (ETH) and Basic Attention Token (BAT), in a predetermined ratio, often 50/50. For instance, if you want to provide liquidity to the liquidity pool, you may need to contribute $250 worth of ETH and $250 worth of BAT. Most liquidity pools employ a constant product automated market maker algorithm.

As more BAT is bought using ETH, the price of BAT gradually increases. For example, the first BAT may be priced at $1.20, the second BAT at $1.20 1/10, and the hundredth BAT at $1.50. The algorithm adjusts the price to maintain the 50/50 ratio between ETH and BAT in the pool. If the pool observes more BAT being bought and perceives a drop in the price of ETH due to increased supply, it raises the price of BAT.

Every transaction in a liquidity pool incurs a small fee. Platforms like Uniswap allow users to trade various Ethereum tokens with minimal fees. In cases where direct trading pairs are not available, decentralized exchanges can route trades through multiple liquidity pools to enable token swaps.

When individuals invest in a liquidity pool, they become liquidity providers. The fees collected from transactions are distributed among the providers, offering an incentive to participate. While some decentralized exchanges provide high annual percentage rates (APR) for liquidity providers, the rewards may decrease as more participants join. However, the increased liquidity leads to a more stable price for the assets in the pool.

One essential characteristic of liquidity pools is that as the liquidity grows, it becomes harder to impact the price of the assets with a relatively small transaction. For example, a $500 ETH deposit in a $2,000 liquidity pool could significantly affect the price of BAT since it represents a significant portion of the pool. However, the same deposit in a $5,000,000 pool would have a minimal impact due to the size of the pool.

Arbitrage traders play a vital role in liquidity pools. When someone buys a substantial amount of BAT from a pool, it can cause the price of ETH in that pool to drop to e.g. $450 for each ETH. Arbitrage traders can exploit this price discrepancy by buying ETH at a lower price from the pool and selling it at a higher price e.g. $500 on another exchange, making a profit. These traders help maintain price consistency across different platforms and contribute to the stability of the token.

Liquidity pools can become complex, with platforms like Balancer allowing up to eight assets in a single pool, showcasing the limitless possibilities of decentralized finance. However, investing in liquidity pools comes with risks. Impermanent loss occurs when the value of assets held in the pool changes relative to holding them individually. Rug pulls are instances where liquidity is drained from a pool by malicious actors. It is important for investors to understand and manage these risks before participating in liquidity pools.

Oracles

An oracle acts as an intermediary between the blockchain and the real world, enabling the smart contract to access information that it cannot gather on its own. However, it is important to note that oracles are not physical entities; they are typically code programmed by individuals or organizations and trusted by the community. Just like the internet, oracles are a collective concept that allows us to utilize external data.

Oracles play a crucial role in bridging the gap between blockchain networks and the real world by providing trusted and reliable external data. While blockchains are self-contained and unable to access information beyond their code and transactions, smart contracts can be designed to rely on third-party data through the use of oracles.

One example of the use of oracles is in tracking stock prices. By creating a token that mirrors the price of a specific stock, investors outside of the United States, for instance, can invest in stocks without needing to comply with local regulations. An oracle can provide the real-world stock price data, allowing the blockchain to create synthetic tokens that track the stock price accurately. The Mirror Protocol, utilizing Chainlink, has implemented this concept, offering tokens such as mgoog that mimic the price movements of real-world stocks like Google.

Any input   **Any Blockchain**   **Any output**

Another use case for oracles is in farming insurance. For instance, an oracle can be utilized to inform the blockchain about adverse weather conditions such as drought. By feeding the oracle with temperature data specific to a location, the blockchain can trigger automated actions related to farming insurance, such as initiating payouts when certain conditions are met.

One significant advantage of decentralized oracles is that they do not rely on a single data source. Similar to blockchains, oracles should be decentralized to avoid a single point of failure and ensure the reliability and integrity of the data. Chainlink, for example, operates an entire blockchain dedicated to providing reliable real-world data, ranging from temperatures to prices.

Oracles can be categorized into three main types: hardware oracles, software oracles, and human oracles. Hardware oracles retrieve data from real-world sensors, such as thermometers, weighing scales, or NFC tags. Software oracles, on the other hand, retrieve information from the web, including stock market data or the number of users on a website.

By leveraging oracles, blockchain applications can extend their functionality and interact with real-world data, enhancing transparency and trust in decentralized systems. The continuous development of decentralized oracles contributes to the growth and adoption of various blockchain use cases across industries.

Implications for Business

In this chapter, we delve into the transformative impact of Web3 on businesses, building upon the technological elaborations discussed earlier. Central to our discussion is the advent of digital scarcity, made possible through blockchain technology, and its potential to obviate the need for intermediaries. We will elaborate how this innovation enables to solve the digital double-spend problem and the plethora of efficiencies it brings along. Moreover, we will cast a spotlight on the transformative role of smart contracts in automating the enforcement of intellectual property rights and streamlining value chains. We will also navigate through the groundbreaking developments in frictionless payments and cross-border transactions facilitated by decentralized networks. In addition to the promising avenues, we will temper our discussion with an insight into the challenges that these technologies face, and the complexities inherent in their integration and adoption across industries.

Digital scarcity, immutable and unalterable data change the way business is conducted

One of the most significant impacts on businesses will likely come from the fact that Web3 is introducing a novel concept of digital scarcity. The single most important value proposition of blockchain technology is solving the digital double-spending problem without the need for an intermediary. Not only is it likely that this will make transactional and verifiable processes much more efficient, it is also likely that many of the traditional intermediary functions that businesses have occupied will become redundant or have to adapt in the future. Smart contracts and NFTs are disruptive forces as they capture a significant amount of the current value chain.

This is not specific to one industry. Any business operating in the wider sphere of digital content – from medical documents to music, movies, books and advertisement, anything involving intellectual property rights and catering to or monetizing on powerful communities should put an emphasis on understanding the business implications of Web3.

The enforcement of IP in the digital space has always been one of the most significant challenges content companies encounter. In the past, the solution to this has been provided by traditional rights management companies, labels, and, in many cases, publishers. It will be important to further explore which value propositions brought by these intermediaries will be disrupted by the application of smart contracts and oracles, and to what extent.

In a fully unfolded Web3 internet infrastructure, every piece of data could develop a provenance, for instance by being represented as an NFT, or a soul-bound token. In this scenario, the traceability of data would be an integral part of the internet-architecture we are using. In theory, no middlemen would be needed to enforce property rights anymore. The enforcement would be built into the ecosystem, executed by smart contracts based on the use of oracles, representing significant, disruptive potential and leading to many intermediary services becoming potentially redundant. While this is, as indicated, a disruptive risk to many of the existing, digital business models, which capture value by essentially verifying transactions and solving various interpretations of the digital double spend, this also is a big opportunity that has exponentially increased in relevance in recent months.

> **The concept of digital scarcity embedded in the internet backend is among the top business implications that come along with Web3 technologies.**

With the rise of Generative AI, content can randomly be altered, faked and distributed and can hardly be differentiated from the original anymore. The current internet infrastructure does not include a framework for enforcing intellectual property automatically, and centralized institutions will not be capable of handling and accessing transactions holistically. Currently, only Web3 technologies can offer a solution and install the necessary backend to cover this important task. The concept of digital scarcity embedded in the internet backend would help control the inflation of content and lack of provenance. This is among the current top business opportunities coming along with Web3 technologies as the rise of Generative AI requires such IP enforcement capacities.

Allowing for the transition from virtual worlds to virtual and immersive realities

The above-mentioned value propositions and business implications of Web3 technologies, with regards to digital scarcity, immutable and unalterable data, compared with the rise of generative AI, become even more important against the background of an emerging concept of parallel/virtual realities, also known as the Metaverse. The Metaverse itself is a concept that, depending on how we define it, cannot be realized without digital assets. If people cannot own digital products, experiences, or any other shape or form of data in the digital space without the need for an intermediary, then one might argue that the Metaverse will always stay a virtual/mixed reality. If the ownership of data is organized decentrally on a Web3 infrastructure a virtual experience will become more immersive. Being able to track and trace the provenance of digital assets is already important in the world we are living in, but its importance is magnified in a space where everything is digital.

The above-explained impact of artificial intelligence, specifically generative AI, on the manipulation of data and editing of existing content becomes even more threatening if not managed properly in the digital space. This is especially true for digital avatars. In the digital world, it must be ensured that a personal digital twin is owned and controlled by those who are represented by it. Any copies, manipulations, and alterations to digital twins and avatars must be immediately identifiable in order to prevent the misuse of personal data and any reputational risk, not only to corporate entities or groups but also to the individual.

In a fully realized Web3 vision, ownership of data remains with the content creator and will only be given away based on the consensus of the parties involved. Consequently, businesses will likely focus on the true value of any data in terms of evaluating whether any business endeavor is worth pursuing.

> **Any copies, manipulations, and alterations to digital twins must be immediately identifiable in order to prevent the misuse of individual data.**

Value in Web3 is not primarily captured by facilitating processes anymore, as many processes that currently require intermediaries to foster in transactions, conduct settlements, or verify processes will likely be automated by smart contracts.

The seamless "Fintechization" of everything

As indicated above, disintermediation is likely one of the most relevant business implications of Web3 technologies. In Web3, transactions are usually processed through decentralized networks, which means that there is no need for any central authority to validate transactions. This can lead to faster and cheaper transactions as settlement automatically occurs on the underlying infrastructure. Self-executing contracts with terms directly written into code can automate and streamline processes that would otherwise require manual intervention. Today, smart contracts and blockchain-related payments via cryptocurrency and stable coins are showing the tremendous value proposition and value capture that this technology can entail. Applying the concept of tokenization, as many stock exchanges are currently evaluating, allows for physical or digital assets to be represented as tokens on the blockchain. This tokenization captures additional value through increased efficiency.

The immutable nature of the technology ensures that once a transaction is recorded, it cannot be altered. This provides a level of transparency and security that can be more efficient and trustworthy than traditional Web 2 systems. Market makers, for instance, play a crucial role in financial markets by providing liquidity. They continuously buy and sell financial instruments to ensure that there is enough volume for traders to transact without large price movements. In the Web3 context, there are already significant changes in how market makers operate. While traditional market making involves multiple intermediaries like brokers and clearinghouses, which can add costs and delays, in Web3, the process is streamlined through smart contracts and decentralized exchanges, so called automated market makers.

Traditional market making involves multiple intermediaries like brokers and clearinghouses, which can add costs and delays.

These are usually significantly more cost efficient than traditional market makers. In addition, market makers in Web3 can tap into global markets more easily as the technology streamlines certain processes across jurisdictions. Decentralization and tokenization features of Web3 make it easier for market makers to offer their services in different regions without the need for extensive local infrastructure.

Tokenization can open up new asset classes like tokenized real estate, art, or intellectual property. Market makers can diversify and create new revenue streams by providing liquidity to these emerging markets, which is currently missing as these are still niche markets.

Having liquidity in niche markets is important for price stability, market efficiency, investor confidence, and many other aspects in terms of a value proposition. It is likely to see increasing value being captured on the payments and transaction side of things. However, it is important to mention that operating as an automated market maker or as a payment facilitator or any other type of financial transaction offering in Web3 also entails a number of challenges within this ecosystem.

Market makers, for instance in the Web3 space, need to consider factors like smart contract vulnerabilities. Since smart contracts are self-executing codes, they need to be carefully written and implemented, as any negative consequences can be devastating. Additionally, there is high regulatory uncertainty at the moment making the mass adoption of these types of projects complex and difficult. Moreover, the volatility of cryptocurrencies is a challenge when it comes to using them as, for instance, cross-border payment assets. The solution to that is usually stable coins, but even regarding stable coins, there have been a number of issues that have not contributed to fostering trust. However, the more mainstream adoption the technology receives, the more likely it is that these risks will be mitigated.

Introducing the economics of community

The business implications for communities can be derived from two of the technological advancements explained above: NFTs and Tokenization[72].

Given their economic potential, tokenized communities have much in common with more traditional organizations, however, the economic models they promote are completely different. Traditional companies are based on assets and the cash flows they generate. The higher the expectation for a company to absorb more capital in the future, the higher their valuation becomes. Platform capitalism is essentially built on permissioned, access-gated, high friction exchange at the cost of participants and to the benefit of intermediaries. The user of a platform is the product, the data is monetized by delivering targeted advertisement. Web3 however offers the exact opposite, which essentially can be described as a democratization of ownership, and hence a democratization of the lifetime value of intellectual property. Protocols, which we have defined as the fundamental layer of Web3, open up a radically expansive new model to create public infrastructure. These protocols are valuable not because of the cash flows they generate through fees or the valuation of the coins and tokens, much more, their value accrues from different parties mutually owning the protocol, and those parties either build or use these protocols to create and capture value. Considering humans as mostly rational actors, they are not incentivized to do anything that devaluates the protocol and equally, they are not incentivized to extract value from it. This is a fundamentally different

---

[72] This entire section is inspired by Jehad Ismail and Jacob Thorne; All elements of this section are derived from Tokenized Communities — Forefront (mirror.xyz)

approach to a traditional company, which constantly extracts value for shareholders, while protocols are valuable when they continuously create value for the public.

The key to this new type of community lies in tokenization. Communities in Web3 often start without a clear goal, just like offline communities, without a clear destination. They develop their narratives through decentralized means. While the mission may not be clear initially, the consensus mechanism always must be embraced by all stakeholders involved, as the way

Protocols are valuable when they continuously create value for the public. Companies are valuable when they extract value for shareholders.

these communities function is based on the tokenomics of a project. The token is used as a primary means of coordination. The token also is a proxy for a larger set of values. Tokens can be the key to access gated experiences, which is one aspect of their value creation. Given that tokens revolve around a specific community, they can be considered "platformless social ecosystems".

Tokens revolving around a community are 'platformless' social ecosystems.

The token is the primary means of communication, and these communities are not tied to any communication tool or social media platform. They are independent of centralized infrastructure. A good way to test this for most tokenized communities today is to ask:

If their primary communications tool disappeared, would this community still exist? The fact that these communities do not require a centralized platform makes them truly global and borderless.

Instead of one leader in a community, there are many leaders in new, self-managing communities. Hierarchy is dynamic based on the specific function being carried out, the scope of the decision, or the context of the work. Tokenized communities enable us to unlock new forms of work and coordination across previously unrelated groups of people, and these use the tokens to collectively govern the community. This does not mean that token-holders vote on every decision in the community. Instead it means that power in the organization ultimately lies in the hands of those involved. Tokenized communities ensure some means of voting out core contributors and creating, editing, and ratifying community-wide proposals. This is most commonly manifested in treasury governance where members of tokenized communities have a say in how the group's treasury is allocated. While leaders might be pushing the community forward, tokenized communities make sure that the puck stops with the collective. Tokenized communities are working toward a collective goal or upholding a shared set of values. In other words, tokenized communities use tokens to coordinate around the proliferation of a shared element of culture that evolves as it spreads throughout a network. What differentiates communities and traditional organizations the most is that they are positive sum, as value creation happens by building expansive value on top of existing protocols and information in line with the shared idea or set of values of the respective community. A tokenized community creates value for the entire network, giving supply and demand side access to all tokenholders.

Using a token does not inherently make a community self-managing or decentralized, the benefits of (and value accrual to) the token are not maximized unless those criteria are upheld.

A tokenized community creates value for the entire network, giving supply and demand side access to all tokenholders.

However, no organization will fulfill the first 6 criteria (tokenized, platformless, self-managing, collectively governed, meme-driven and positive-sum, purely on day one. Tokenized communities are progressively working to fulfill the above criteria, making an underlying and defining north star of every tokenized community to build a better tokenized community. This is best articulated in the thesis around „progressive decentralization."

A new incentive model for advertisers

Tokenized communities sustain themselves by ensuring that individual members and contributors get paid, so that they are not forced to allocate time elsewhere. Unlike protocols, people need to be paid. And the answer to that might lie in a fundamental shift from an internet of advertisement to a digital world of brand-attachment. Economic models for tokenized communities should be viewed through the lens creating value for the community rather than capturing value from the customer. This value can be derived from brands attaching themselves to cultural movements early on and can be realized via the application of NFTs.

Provenance gives power to communities, and communities all revolve around content. NFTs will play a crucial role in redefining value in the digital space. And this kind of value is created through the merger of creator, content and community. That is the concept of provenance. This concept alone has the potential to disrupt many of the media industry's current logics. Introducing the concept of exclusivity and scarcity to the industry, for the first time in history, there is an incentive to challenge the current logic of measuring value in the digital space.

The creator, the content, and the willingness to pay by a significant number of consumers to become part of an exclusive community determines a price. The price is the amount people are willing to pay to join a community. While initially this price might be denominated in the respective community token only, it can be opened up the moment the community's set of values is attracting brands willing to attach to it.

As every piece of content must be worth paying for in order to own it, and every community worth joining requires a tangible buy-in, the focus in the content industry can shift from selling as much as possible to providing content that is as valuable as possible. In such a world, those who add value are rewarded. And as the community defines the true value of an asset, they will also be rewarded – by exclusive experiences, shares of generated revenue, the appreciation of the NFT they hold. Brands will tap on these communities to capture their identity, or they will create their own. The value of a media asset will equal the value of its community. And the value of a community can be evaluated by measuring the virality of the stories told around it. That is why, in contrast to Web2, in such a world, brands and communities merge. The narratives chosen by the community define the brand. And the community defines the brand's value.

As mentioned above, platforms such as Google and Facebook are centralized and have full control over the infrastructure and user data. Advertisers have to adhere to the terms and conditions set by these platforms, and the platforms decide on the algorithms for ad distribution, whereas in Web3, decentralized applications built on blockchain networks enable peer-to-peer transactions. Advertisers can use these decentralized apps to directly engage with the audience without intermediaries, resulting in more transparent transactions.

Platforms collect enormous amounts of user data and use it to create targeted ads. However, this has raised concerns about privacy and data misuse. The implementation of GDPR and other privacy regulations is an effort to curb these issues, specifically given the fact that users are in no way paid for providing these data.

To conclude, Web3 leverages decentralized identity solutions, allowing users to own and control access to their own data. Users can choose to share certain data in exchange for incentives or a more personalized ad experience, promoting a more ethical data-sharing model, and implementing a value for data, which is digital content, in the underlying internet infrastructure. This breaks-up the current revenue models in platform capitalism. Revenue sharing in Web2 is skewed in favor of the platform. For example, YouTube typically takes a 45% cut of ad revenue generated by creators. The payment terms are also controlled by the platform. For Instagram, Facebook and Twitter, the take rates are almost 100%, and even the Appstore takes a cut of 30%. In Web3, smart contracts allow for automated and transparent revenue sharing.

As we transition from Web2 to Web3, it is expected that user-centric models will continue to evolve, offering more control and ownership to users and content creators. Web3's inherent transparency and decentralization can potentially lead to more equitable revenue distribution and a fairer advertising model.

Closing Remarks

This paper has outlined the multiple opportunities and implications of Web3 for businesses. The advent of blockchain technology and digital scarcity has demonstrated unparalleled possibilities in solving issues like the double-spending problem, automating enforcement of intellectual property rights, and facilitating frictionless payments, while also heralding challenges and complexities.

The innovative role of smart contracts in streamlining value chains and facilitating cross-border transactions, coupled with decentralized networks, fundamentally changes the business landscape. Furthermore, the potential of NFTs, traceability of digital assets, and the consequent creation of parallel/virtual realities are transformative aspects, whose full magnitude is yet to be completely understood. Additionally, tokenized communities represent a seismic shift in how value is generated and shared. They stand in strong contrast to traditional business models, as they prioritize a positive-sum, value-creating approach that democratizes ownership and fosters shared cultural values. This is further augmented by the potential new incentives model for advertisers, where decentralized applications on blockchain networks could fundamentally reshape advertising, marketing, and data sharing ethics.

In summary, Web3 is not just a technological evolution; it is a paradigm shift in how businesses will operate, thrive, and engage with stakeholders. The myriad of possibilities are bound only by imagination and innovation. However, the journey ahead is not without challenges, particularly in terms of adoption, integration, regulatory compliance, and security.

As we stand at the verge of this revolution, it is crucial for business leaders and decision-makers to adopt a long-term strategic approach. The multifaceted nature of Web3 demands a comprehensive understanding, as the decisions made today will chart the course for the business landscapes of tomorrow. It is important to delve deeper into corporate-level considerations, explore new business models and evaluate where and how Web3 technologies can be applied most effectively. In an age where change is the only constant, proactive engagement and astute strategizing are not merely advantageous – they are essential for future success and sustainability in the Web3 era.

Appendix

Glossary

Aave	A decentralized lending platform within the Aave protocol, allowing users to earn interest on deposits and borrow assets.
Airdrop	The distribution of free cryptocurrency tokens to a group of users, often used for marketing or promotional purposes.
Altcoin	Any cryptocurrency other than Bitcoin. Altcoins aim to offer alternative features, functionalities, or improvements over Bitcoin.
Asymmetric Encryption	A cryptographic technique that uses a pair of keys, a public key for encryption and a private key for decryption, ensuring secure communication and data protection.
Atomicity	Property of transactions ensuring they are either fully completed or fully rolled back in case of failure.
BEP-20	A token standard on the Binance Smart Chain (BSC) that defines the rules and interface for creating fungible tokens.
Bitcoin	The first and most well-known cryptocurrency, created in 2009 by an anonymous person or group known as Satoshi Nakamoto.
Blockchain	A decentralized and immutable digital ledger that records transactions across multiple computers or nodes.
Binance Smart Chain	A blockchain platform developed by Binance, offering fast and low-cost transactions, smart contracts, and compatibility with the Ethereum Virtual Machine (EVM).
Brave	A privacy-focused web browser with built-in ad-blocking and rewards for users and content creators.
Bridge	Technology or protocol enabling transfer of assets or data between different blockchain networks for cross-chain interoperability.
Burn	The intentional and permanent removal of cryptocurrency tokens from circulation, typically done to reduce the token supply or increase scarcity.
Cardano	A blockchain platform known for its focus on security, scalability, and sustainability, utilizing a proof-of-stake (PoS) consensus mechanism.
Channels	Off-chain payment channels that allow for faster and cheaper transactions between participants.
Child Chain	A blockchain that operates alongside a main blockchain, handling specific transactions or functions to improve scalability.
Coin	A general term used to refer to a specific cryptocurrency or digital currency.
Cold Wallet	A cryptocurrency wallet that is offline and not connected to the internet, offering enhanced security but limited accessibility.
Composability	The ability of different software components to seamlessly interact and combine in a modular manner.
Consensus	Agreement and validation process in a blockchain network to maintain a shared ledger.
Consortium Blockchain	A blockchain network governed by a consortium or group of organizations working together.
Crypto Bridge	A platform or protocol that enables the transfer of digital assets between

	different blockchain networks.
Crypto Wallet	Software or hardware used to securely store, manage, and interact with cryptocurrencies.
Cryptocurrency	Digital or virtual currency that uses cryptography for security and operates independently of central banks.
DAO	Decentralized Autonomous Organization, an organization governed by smart contracts and operated by a community of participants.
DeFi	Decentralized Finance refers to a set of financial applications and protocols built on blockchain technology, offering traditional financial services in a decentralized and permissionless manner.
Decentralized Exchanges	Exchanges that operate on blockchain networks, allowing users to trade cryptocurrencies directly without intermediaries.
Decentralized Finance (DeFi)	See DeFi.
Distributed Ledger	A type of ledger that is replicated and shared across multiple nodes or computers.
Dogecoin	Cryptocurrency known for its lighthearted nature, featuring a Shiba Inu dog logo and active online community.
Double Spending (Problem)	The risk of spending the same cryptocurrency or digital asset more than once, which blockchain technology aims to prevent.
EIP	Ethereum Improvement Proposal, a formal document outlining proposed improvements or changes to the Ethereum network.
ERC-20	Ethereum Request for Comments 20, a widely adopted technical standard for creating and implementing fungible tokens on the Ethereum blockchain.
Ethereum	A decentralized blockchain platform that supports the creation of smart contracts and the development of decentralized applications (dApps).
Ethereum Virtual Machine (EVM)	The runtime environment on Ethereum that allows the execution of smart contracts and decentralized applications.
FBP	Fee-Based Production, a concept in blockchain networks where users pay fees for resource consumption and computational processing.
Fee-Based Production	See FBP.
Flash Loans	Temporary, collateral-free cryptocurrency loans that must be repaid within the same transaction, commonly used for time-sensitive financial operations in DeFi.
Fork	A split or divergence in the blockchain's protocol resulting in two separate and distinct chains.
Gas	Unit of measurement for computational effort and fees in blockchain transactions.
Gas Cost	The total fee in cryptocurrency required to execute a transaction or smart contract on the blockchain.
Gas Price	The price or amount of cryptocurrency paid per unit of gas in a transaction on the blockchain.
Governance Tokens	Tokens that grant holders the right to participate in the decision-making processes and governance of a blockchain network.
Gwei	Smallest denomination of Ethereum, used to measure gas prices.
Hard Fork	A non-backward-compatible upgrade to the blockchain protocol, introducing new rules that are incompatible with the previous rules.
Hardware Oracles	Physical devices or systems that collect and deliver real-world data to blockchain networks.
Hardware Wallet	A physical device used to store private keys offline for enhanced security.
Hot Wallet	A cryptocurrency wallet that is connected to the internet and allows for immediate access to funds for transactions.
Human Oracles	Individuals who manually input or verify real-world data on behalf of smart contracts.

ICO	Initial Coin Offering, a fundraising method in which a project or company sells a new cryptocurrency token to investors in exchange for funding.
Impermanent Loss	A temporary loss experienced by liquidity providers in an automated market maker (AMM) due to price volatility.
Initial Coin Offering	See ICO.
Liquidity Pool	Pool of funds in a smart contract used for trading and liquidity in decentralized exchanges and DeFi platforms.
Liquidity Providers	Individuals or entities that contribute funds to a liquidity pool, enabling trading and liquidity in decentralized platforms.
Locking Period	The duration for which cryptocurrency is held and locked in a staking or smart contract.
MEV	Miner Extractable Value, the potential profit or advantage that miners can gain by manipulating transaction ordering or block inclusion.
Mining	The process of validating and adding new transactions to the blockchain by solving computational puzzles.
Mining Pool	A collective group of miners who pool their resources to increase their chances of mining a block and earning rewards.
NFT	Non-Fungible Token, a unique digital asset representing ownership or proof of authenticity for a specific item or piece of content.
Nodes	Computers or devices that participate in maintaining the blockchain network by validating and storing data.
Nonce	A number used in blockchain mining that, when combined with other data, produces a hash with specific properties.
Optimistic Rollups	Rollup solutions that rely on optimistic assumptions to execute and validate transactions off-chain.
Oracles	External data sources that provide real-world information to blockchain smart contracts.
Paper Wallet	A physical printout or document containing the public and private keys of a cryptocurrency wallet.
Platform Tokens	Tokens specific to a blockchain platform that are used for accessing or utilizing its services.
Plasma	A framework for creating scalable blockchain networks through the use of child chains.
Polkadot	Multi-chain platform that enables interoperability between different blockchains, allowing them to share information and assets.
Private Blockchain	A blockchain network that restricts access and participation to selected entities or individuals.
Private Key	A secret cryptographic key that provides access to the funds or assets stored in a cryptocurrency wallet.
Proof of Stake (PoS)	Consensus mechanism where validators are chosen to create new blocks based on the amount of cryptocurrency they hold and „stake."
Proof of Work (PoW)	Consensus mechanism where miners solve complex mathematical puzzles to validate transactions and secure the blockchain.
Public Blockchain	A blockchain network that is open and accessible to anyone who wants to participate.
Public Key	A cryptographic key used for encryption and verifying digital signatures in blockchain transactions.
Retroactive Airdrop	An airdrop that distributes tokens retrospectively to existing users based on past participation or activity.
Rollups	Layer 2 scaling solutions that aggregate multiple transactions into a single batch to reduce on-chain congestion.
Rug Pull	A fraudulent practice where the creators or developers of a project abruptly withdraw liquidity or funds, leaving investors with worthless tokens.

Security Tokens	Tokens that represent ownership or investment in an underlying asset, such as shares in a company or real estate.
Shares	Units of work contributed by miners in a mining pool, used to distribute rewards proportionally based on contribution.
Sidechains	Separate blockchain networks connected to the main blockchain, allowing for more scalability and specialized functionalities.
Slashing	The penalty imposed on validators for malicious behavior or violating consensus rules in a proof-of-stake network.
Soft Fork	A backward-compatible upgrade to the blockchain protocol, introducing new rules that are more restrictive than the previous rules.
Solana	High-performance blockchain platform designed for decentralized applications and crypto projects.
Staker	A participant who holds and actively participates in staking cryptocurrency within a blockchain network.
Staking	The act of holding and locking up cryptocurrency to support network operations and earn rewards.
Stamp	A timestamp or proof of existence for a particular document or file on the blockchain.
Stellar	Open-source blockchain platform that facilitates fast and low-cost cross-border transactions and token issuance.
Symmetric Encryption	Encryption where the same key is used for both encrypting and decrypting the data.
Token	A digital asset that represents a particular value or utility on a blockchain network.
Token Sales	The process of selling or distributing tokens to the public, often used for fundraising or project development.
Tokenomics	The study of the design, distribution, and economics of tokens within a cryptocurrency ecosystem.
TPS (Transactions per Second)	The number of transactions a blockchain network can process in one second.
Transactional Tokens	Tokens used primarily for facilitating transactions within a specific ecosystem or network.
Tron	Blockchain platform focused on decentralized content sharing and entertainment applications.
TVL (Total Value Locked)	The total amount of cryptocurrency assets locked or invested in a specific DeFi protocol or platform.
Uniswap	Decentralized exchange (DEX) protocol that allows for seamless token swaps and liquidity provision.
Utility Tokens	Tokens that provide access to a product or service within a particular platform or ecosystem.
Validation	The process of verifying and confirming the accuracy and legitimacy of transactions or data on the blockchain.
VeChain	Blockchain platform designed for supply chain management and tracking, enhancing transparency and efficiency.
Virtual Machine code	Low-level code that runs on a virtual machine, such as the Ethereum Virtual Machine (EVM), executing smart contracts and dApps.
Wrapped	Refers to a tokenized representation of an underlying asset on a blockchain, allowing it to be traded or used within the ecosystem.
XRP Ledger	Decentralized blockchain and cryptocurrency platform powering the Ripple network.

This publication is authored by Martin El-Khouri, Bertelsmann Investments

Bertelsmann Investments (BI) comprises Bertelsmann's global venture capital activities as well as the Bertelsmann Next growth unit. The venture capital arm includes the Bertelsmann Asia Investments (BAI), Bertelsmann India Investments (BII) and Bertelsmann Digital Media Investments (BDMI) funds, as well as selected fund and direct holdings in markets including Europe, the United States, Brazil, Southeast Asia and Africa. The Bertelsmann Next unit advances the entrepreneurial development of new growth sectors and business areas, including digital health, mobile gaming and HR Tech. To date, around €1.7 billion has been invested in more than 400 innovative companies and funds through Bertelsmann Investments. Bertelsmann Investments currently holds over 300 active investments worldwide through its network of start-ups and funds.

B3-THE HUB was founded in 2023 and serves as the central point of contact for Web3 activities at Bertelsmann Investments (BI) and beyond. Acting as a bridge between the startup world and the various corporate divisions of Bertelsmann, THE HUB aims to drive the structural transformation of digital business models towards Web3. BI has already invested over 40 million euros in Web3-related business models and has collaborated on numerous projects within the Bertelsmann Group. Through its initiatives, THE HUB is expected to create significant strategic value for the corporation.