Web3 and Decentralization Technology

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.

Blockchain – the essence of it all

Home

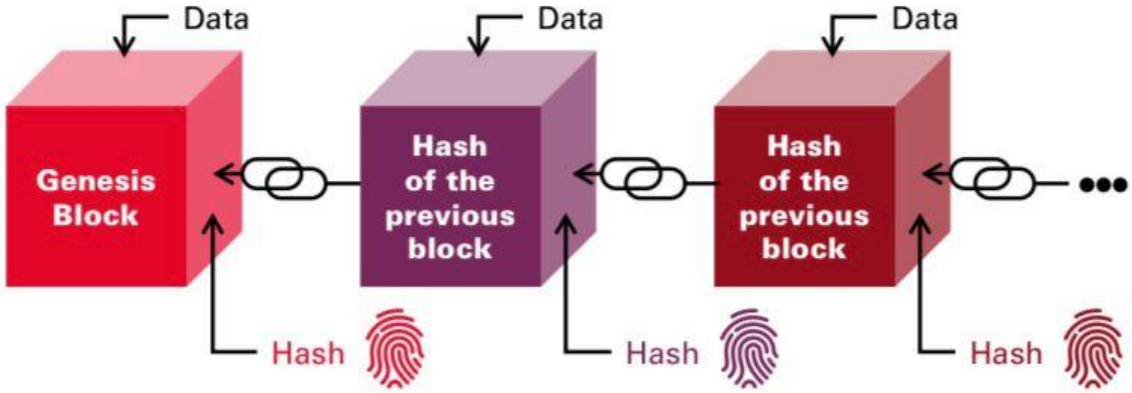
In essence, a blockchain is a collection of data, typically organized as a series of blocks. Each block in the blockchain contains a bunch of data, which can represent various types of information. This data can range from transactions and account status in the case of cryptocurrencies1 like Bitcoin2 and Ethereum3 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 contracts4.

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 mining5. Miners compete with each other to solve complex mathematical problems by finding a special number known as a nonce6. The solution to these problems serves as a so called proof of work7, demonstrating that the miner has invested computational resources in mining the block.

A crucial component of the blockchain is the hash function8. 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.

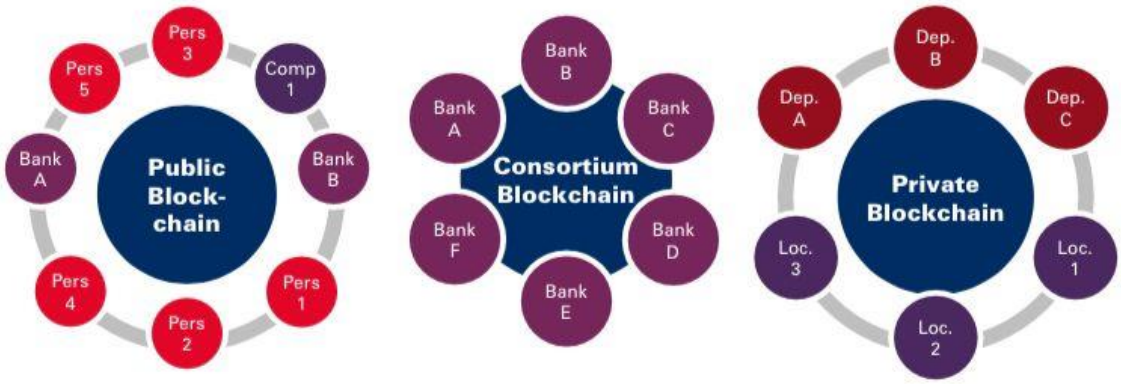
Computers worldwide, along with specialized mining farms, engage in the process of mining to find the correct nonce that satisfies the requirements of the hashing function. This computational effort is distributed across the network, with multiple participants vying to solve the mathematical problem.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



→ 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

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.

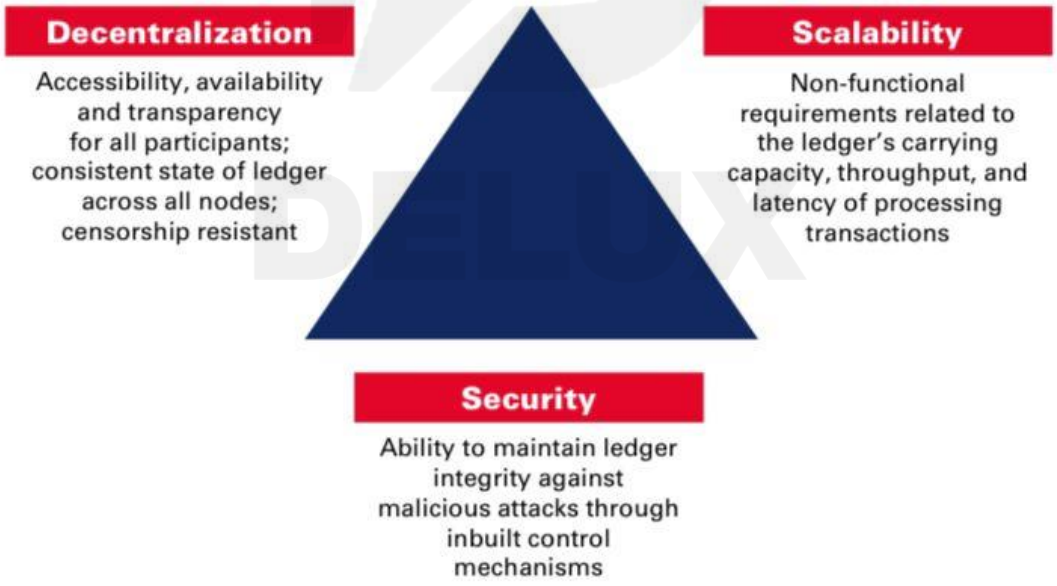
Collision Resistance: A well-designed hashing function makes it extremely unlikely to find two different inputs that generate the same output hash. For example, in the case of SHA-256, currently, no known two inputs exist that produce the same hash, which is important in order to

prevent the possibility of creating different inputs with identical hashes, adding to the robustness of the blockchain.

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.

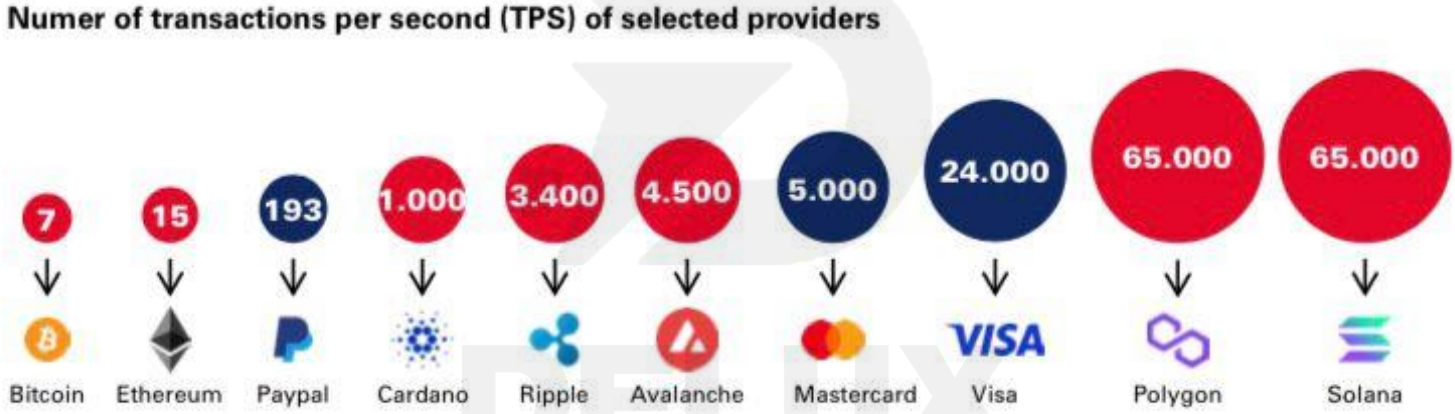


once. High decentralization requires a large number of network participants that verify transactions, and building consensus among more participants typically requires more time. Achieving high security usually requires more computational resources, which can limit the speed of the blockchain or the 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



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 216 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 117 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-Knowledge18**: 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.

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 chains19, 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 up20 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 code21.

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

Crypto Bridge

A blockchain bridge is a connection that enables the transfer of tokens23 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 blockchain24.

One example is having an Ethereum token on the Binance Smart Chain25. 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 Aave26. By moving Ethereum from the Ethereum network to the Polygon27 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.

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.

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.

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.

he
l
e

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-flow29 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.