

June 5, 2020

# About Author - Shermin Voshmgir

[ [Twitter](#) ] [ [LinkedIn](#) ] [ [Medium](#) ]

Shermin Voshmgir is the director of the [Research Institute for Cryptoeconomics](#) at the Vienna University of Economics, and the founder of BlockchainHub in Berlin. She is also a well known public speaker & writer on the topic of tokens, blockchain, and the Web3. In the past, she was a curator of “The DAO”, and advisor to various startups like Jolocom, Wunder and the Estonian E-residency program. In addition to her studies at the Vienna University of Economics she studied filmmaking in Madrid. Her past work experience ranges from Internet startups, research & art. She is Austrian, with Iranian roots, and lives between Vienna and Berlin.

## Key Concepts

### Stages Of The Web

	Web 1.0	Web 2.0	Web 3.0
			The Bitcoin network and other distributed ledgers all represent a collectively maintained public infrastructure and are the backbone of the next generation Internet, what the crypto community refers to as the Web3.
Business model		Users pay with data	Pay with time

## Key Terms

### General

Keywords	Definition(s)	Examples
Distributed Ledger	The Bitcoin network introduced a mechanism for each node in a network to send and receive tokens, and record the state of tokens, in a digitally native format. The consensus protocol of the Bitcoin network is designed in a way that the network can collectively remember preceding events or user interactions, resolving the “double-spending” problem by providing a single source of reference for who received what and when. The Bitcoin protocol can, therefore, be seen as a game changer, paving the way to a more decentralized Web. The Bitcoin white paper of 2008 initiated a new form of public infrastructure where the state of all Bitcoin tokens are collectively maintained.	

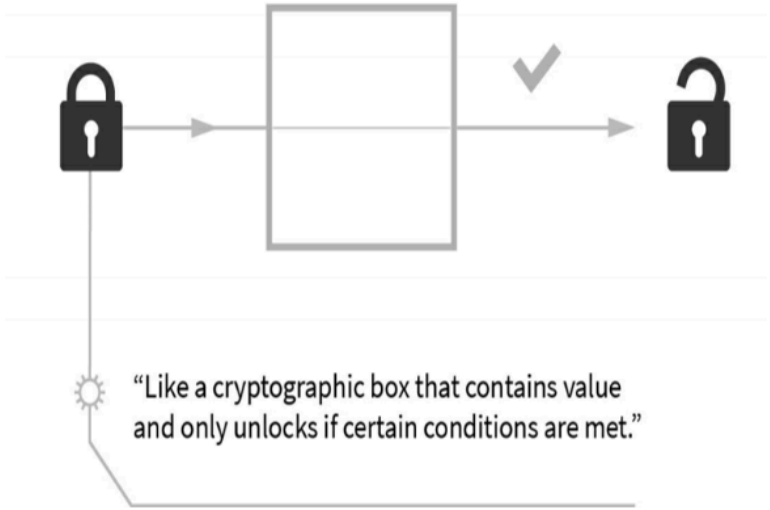
Layers		<ul style="list-style-type: none"><li>Application</li></ul>
	<ul style="list-style-type: none"><li></li></ul>	

<p>Fungibility</p>	<p>From an asset perspective, fungibility refers to the interchangeability of a unit of an asset with other units of the same asset.</p> <p>Two key qualities:</p> <ol style="list-style-type: none"><li>1. Only quantity matters, which means that units of fungible assets of the same kind are indistinguishable.</li><li>2. Any amount can be <b>merged or divided</b> into a larger or smaller amount of it, making it indistinguishable from the rest.</li></ol> <p>These qualities are important in order use something as a:</p> <ul style="list-style-type: none"><li>• Store of value</li><li>• Medium of exchange</li><li>• Unit of account.</li></ul> <p>Some examples...</p> <ul style="list-style-type: none"><li>• <b>Currency.</b> If you were to lend 10 EUR to someone, for example, it would not matter if that person returns the exact same 10 EUR bill or another one, or various bills and coins that amount to the value of 10 EUR.</li><li>• <b>Commodities.</b> The same applies to one barrel of crude oil. Flour is another example of a fungible asset, and is also one of the reasons why it was used as a commodity currency in the past.</li></ul> <p><b>NFT can become fungible via fractionalization</b></p> <p>“The tokenized representation of property rights of a an apartment is unique in nature, because that apartment has different properties than any other apartment. But when you issues fractions of that NFT representing your apartment, these fractions can be fungible within your NFT token set. On the other hand, non-fungible assets such as securities could become fungible if you attach more complex properties (such as special voting rights, not transferability clauses etc.) to them which might not have been as feasible before.”</p>	<p><b>EXAMPLES</b></p> <p><b>General</b></p> <ul style="list-style-type: none"><li>• Currency</li><li>• Commodity</li><li>• Precious metals</li></ul> <p><b>Token</b></p> <ul style="list-style-type: none"><li>• Bitcoin</li><li>• Ethereum</li><li>• Etc</li></ul> <p><b>USE CASES</b></p> <ul style="list-style-type: none"><li>• <b>Digital assets that are unique in nature</b> can be tokenized<ul style="list-style-type: none"><li>○ crypto-collectibles (art and other collectibles),</li><li>○ crypto-games, but also written content, music, movies (example <a href="#">Pictosis</a>), — or <a href="#">scientific papers</a>.</li><li>○ Examples for NFT Marketplaces for cryptoart are: Foundation, MakersPlace, Nifty Gateway, SuperRare, Opensea, Rarible, KnownOrigin, or Zora.</li><li>○ Other types of tokenized digital content have other markets that are slowly emerging.</li></ul></li><li>• <b>Real assets that are unique in nature:</b> NFTs allow the tokenization of unique investments tied to a physical assets, like...<ul style="list-style-type: none"><li>○ Artwork</li><li>○ Real estate</li><li>○ Investment in a SME (Small and medium sized company)</li><li>○ Building. ownership titles of a fraction of the real estate, while other tokens could grant special privileges like access rights.</li><li>○ NFTs can grant token holders different rights and levels of control over their assets. The management of the fractionalized investment rights in these assets is much cheaper and could create new market dynamics by making certain markets more liquid than they are today.</li></ul></li><li>• <b>Identity Tokens, Certificates, &amp; Reputation:</b> Anything that uniquely represents a person could be represented as a non-fungible token: any type of ID or certificate like school transcripts, university degrees, or software licenses that are tied to the existence of one single person. A diploma could be issued and collectively managed by a distributed ledger with no need to be translated, manually notarized, or verified. Wallet-like software could manage all personal data without the need for centralized institutions storing our data. The token would represent a container for identity information related to a specific person without giving information about what is identified. Certification claims can be associated with the token, which would be issued by the trusted entities that issue these certifications. If properly designed, reputation tokens could be attached to identities and resolve challenges like “fake news.”</li><li>• <b>Access Tokens:</b> NFT could be used to manage any type of access right that is tied to a special person, a special property, or a special event. By using public key cryptography, distributed ledgers can offer more secure</li></ul>
--------------------	--	--

		<p>and decentrally verified access-rights management than centrally managed digital access-rights management solutions.NFTs in combination with other Web3 protocols can be used to replace physical keys, state of the art digital keys, and passwords.</p> <ul style="list-style-type: none"><li>● <b>Asset Transfer Tokens:</b> When someone passes away today, the assets of that person often needs to be split between multiple heirs, which can produce considerable bureaucratic overhead and coordination costs to split the value of these assets specified in a notarized will. While fractional ownership is possible today, NFT based asset transfer tokens managed by a distributed ledger would make the transfer of assets in the case of wills much more frictionless.</li></ul>
Non-fungible (unique) token		
Token		<p><b>Fungible</b></p> <ul style="list-style-type: none"><li>● Bitcoin</li><li>● Ethereum</li><li>● Etc</li></ul> <p><b>Non-Fungible</b></p> <ul style="list-style-type: none"><li>● Art</li><li>● Media</li><li>● ID cards</li><li>● Ownership of a house</li><li>● Tenant rights</li><li>● Car</li><li>● Gym membership</li></ul> <p><b>Web 3.0 Tokens</b></p> <p>Web3 tokens are programmable rights management tools that can have much more complex properties than fungible currency tokens.</p> <p>They can represent any:</p> <ul style="list-style-type: none"><li>● Asset</li><li>● Access right</li><li>● Voting right or management right.</li></ul> <p>Here is a broad overview of the different range of properties a token can have:</p> <ol style="list-style-type: none"><li>1. Technical perspective</li><li>2. Rights perspective</li><li>3. Fungibility perspective</li><li>4. Transferability perspective</li><li>5. Durability perspective</li><li>6. Regulatory perspective</li><li>7. Incentive perspective</li><li>8. Supply perspective</li><li>9. Token flow perspective</li><li>10.Privacy perspective.</li></ol>
Smart Contract	<p>Contracts defined and enforced by algorithms rather than law.</p> <p>A smart contract is a piece of software that is processed by a distributed ledger. It is a rights</p>	<ul style="list-style-type: none"><li>● <b>ERC-20.</b> Defines a common list of rules for Ethereum tokens, including how the tokens are transferred from one Ethereum address to another and how data within each token is accessed. These token contracts manage the logic and maintain a list of all issued tokens, and</li></ul>

management tool that can formalize and execute agreements between untrusted participants over the Internet, and comes with inbuilt compliance and controlling. Smart contracts can reduce the costs of formalization and enforcement of a simple agreement between two parties, the bylaws of an organization, or to create different types of tokens.

## Smart Contracts



## Aspects of Smart Contracts

Technical Aspects	Legal Aspects	Economic Aspects
Self-verifying (Auditing on the fly.)	Smart contracts can map legal obligations into an automated process. If implemented correctly, they can provide a greater degree of contractual security at lower costs than current legal systems.	Higher transparency
Self-executing (Enforcement on the fly.)		Fewer intermediaries
Tamper resistant (No cheating.)		Lower transaction costs

A smart contract can be invoked from entities within (other smart contracts) and outside (external data sources) a blockchain network. External data feeds, so-called “oracles,” inject data that is relevant to the smart contract from the off-chain world into the smart contract. They can track performance of the agreement in real time and can therefore save costs, as compliance and controlling happen on the fly. Smart contracts reduce the transaction costs of agreements. Specifically, they reduce the costs of (i) reaching an agreement, (ii) formalization, and (iii) enforcement. If implemented correctly, smart contracts could provide transaction security superior to traditional contract law, thereby reducing coordination costs of auditing and enforcement of such agreements. Smart contracts also bypass the principal-agent dilemma<sup>21</sup> of organizations, providing more transparency and accountability, and reducing bureaucracy (read more: Part 2 - Institutional Economics of DAOs).

Voshmgir, Shermin. Token Economy: How the Web3 reinvents the Internet (pp. 115-116). Token Kitchen. Kindle Edition.

can represent any asset that has features of a fungible commodity. A majority of early tokens issued on the Ethereum network were ERC-20 compliant fungible tokens.

- **ERC-721 (introduced 2017).** Introduced a free and open standard that describes how to issue so-called “non-fungible tokens” on the Ethereum network and introduced the era of building more complex features into tokens.

From a tech perspective, the ERC-721 token standard allows for more detailed attributes that make a token special, beyond the attributes that can be found in ERC-20 tokens. It allows the inclusion of metadata about an asset and information about ownership. When validated, such additional information can add value, guaranteeing the provenance of art, collectibles, or along the supply chain of other goods and services.

### Companies Helping Smart Contracts Come Into Existence

- Kleros
- Openlaw
- Jur

### Use Cases

- **Self-managing forest,** as in the case of “Terra0,” where a smart contract on the Ethereum blockchain manages the logging and selling of trees from a forest in Germany. Drones and satellites monitor the growth of the forest and trigger events in the smart contract, like subcontracting agreements to log the forest and sell off the wood.
- **Decentralized autonomous organizations (DAOs)** are such an example and probably represent the most common form of complex smart contracts.
- **Social media.** In the Web3, smart contracts can enable purpose-driven ecosystems, in which users can benefit from their network activities by getting rewarded with network tokens. An example thereof would be “Steemit,” a decentralized social network that is organized as a DAO and incentivizes user contributions with network tokens (read more: Part 4 - Steemit).
- **IOT.** Machine-to-machine settlement in an “Internet of Things.” This, however, requires that all objects in such an Internet of Things have a blockchain identity, and can thus be uniquely addressed. Addressability of each single machine or other physical object needs to be tamper proof. This can be achieved by tagging or chipping objects with a so-called “crypto accelerator,” which is also referred to as a “digital twin.” A crypto accelerator is a small micro-controller optimized to run the most important cryptographic algorithms.
  - It can have the size of a sticker on a piece of fruit and therefore serve as a basis for use cases like supply chain transparency. With a digital twin, any physical object can send unique digital signatures, or send and receive tokens.

### Second Order Effects

		<ul style="list-style-type: none"><li>● <b>Reinvention Of Legal Profession.</b> Many traditional intermediaries, like lawyers, brokers, and bankers, or public administrators, and Internet platforms might no longer be necessary, or at least some of their services might become obsolete: Cars could use smart contracts to pay their own bills upon fueling up at the gas station, or charging up at an electric charging pole. Invoices could be settled upon arrival of a product shipment. Smart share certificates in the form of tokenized securities could be programmed to conduct automated payout of dividends (read more: Part 4 - Asset Tokens &amp; Fractional Ownership).</li><li>● Reduction of transaction costs<ul style="list-style-type: none"><li>○ Micropayments could become more economically feasible</li></ul></li><li>● Projecting the current rate of development of this technology into the future, and taking into account convergence with other emerging technologies like IoT, Big Data, and AI, we can now envision a world where individuals, organizations, and machines can freely interact with one another with little friction and at a fraction of current costs.</li><li>●</li><li>●</li></ul>
Cryptocurrencies		
Blockchain	Bitcoin is a blockchain network	
Distributed Autonomous Organization (DAO)		
Nodes		
State	The Internet we use today is “stateless.” It doesn’t have a native mechanism to transfer what computer science refers to as “state.” State refers to information, or the status of “Who is who?”; “Who owns what?”; and “Who has the right to do what?” in a network. The ability to transfer value easily and P2P is essential for efficient markets, and “state” is a key property for managing and transferring values.	
Blockchain client (wallet)	<p>A decentralized application is a blockchain client - often also referred to as the “wallet.”</p> <p>The wallet also manages the public-private key-pair and the blockchain address, to provide a unique identity for network nodes so they can securely interact with the network</p>	

Tokens

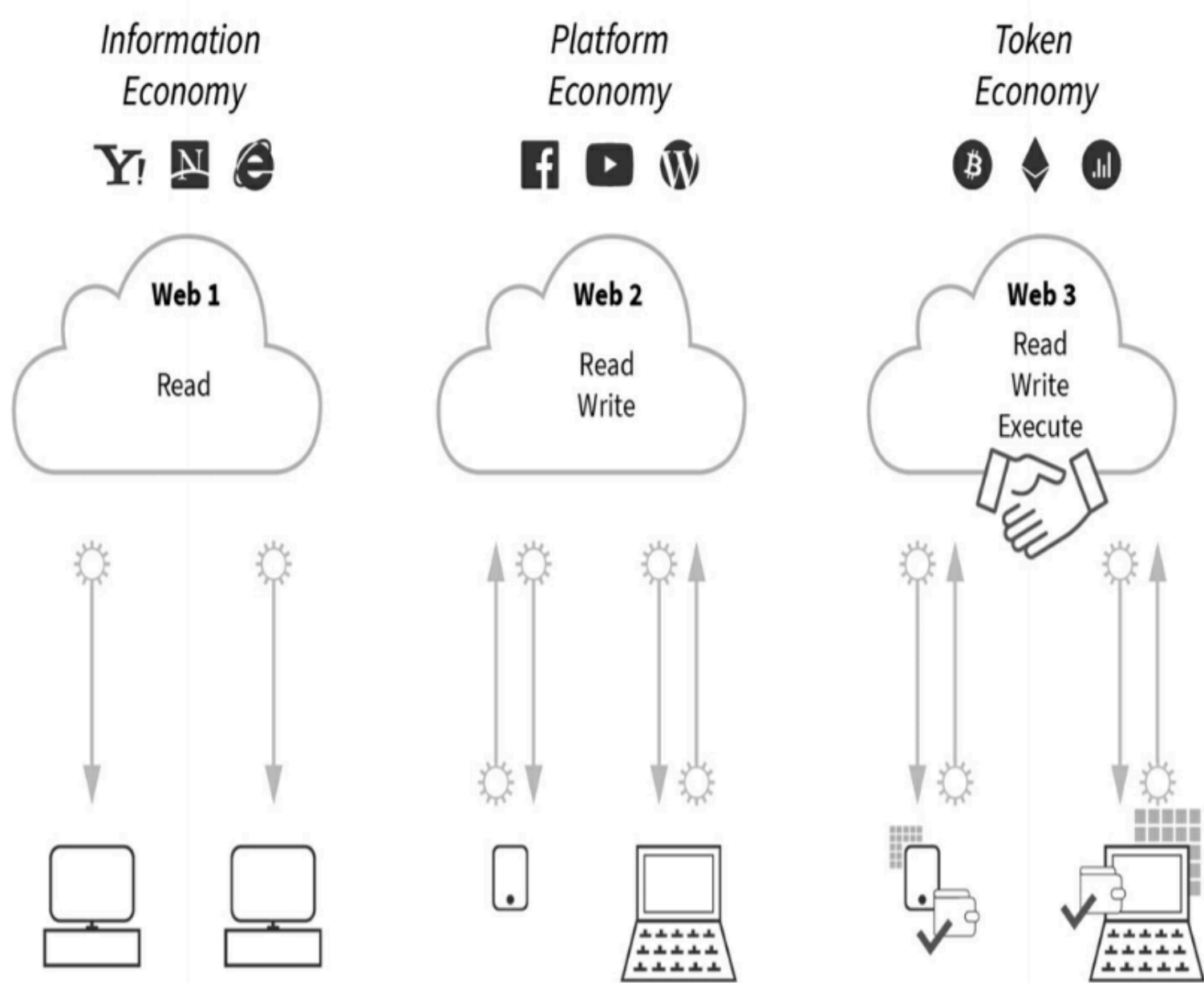
# Token Properties

Technology	Infrastructure token		Application token	
Infrastructure	Tokens are managed by a public infrastructure (Ethereum) where the ledger is collaboratively managed by anonymous actors.		Tokens are managed by a federated network The ledger is operated by a consortium of known actors.^	
Minted upon?	Pre-minted and issued by graphic designer		Minted upon "proof-of" a specific network contribution	
Rights	Property right	Access right	Voting right	Management right
Fungibility	Unique attributes		Identical attributes	
Durability	Expiry date or expiry event		No expiry date or expiry event	
Transferability	transferrable	limited/conditional transferability		non-transferrable
Incentive	Endogenous: token "created out of internal value creation" Which means that the token is minted upon proof-of-network-contribution		Exogenous: token can be bought with money or other assets This means that the token is not minted upon proof-of-network-contribution	
Privacy	More "privacy by design" (depends on type of cryptography used in underlying network infrastructure)		Less "privacy by design" (depends on type of cryptography used in underlying network infrastructure)	
Other Legal Aspects	Token classification & regulation is clear		Token classification & regulation is unclear	

TOKEN KITCHEN  
https://token.kitchen



# History of the Web



## Hello World

Tim Berners Lee introduced a new standard that allowed for creating visually appealing web pages with just a few lines of code, and surfing the Internet following links, instead of using command-line interfaces. The Internet became more usable. Anyone could now use the Internet and was referred to as “Information Data Highway.”

Apps: Web browsers, search engines.

## Frontend Revolution

The Internet became more mature. Apps could be used to read and write simultaneously. This revolutionized social & economic interactions, bringing producers and consumers of information, goods, and services closer together. But always with a middleman: a platform acting as a trusted intermediary between two people who do not know or trust each other.

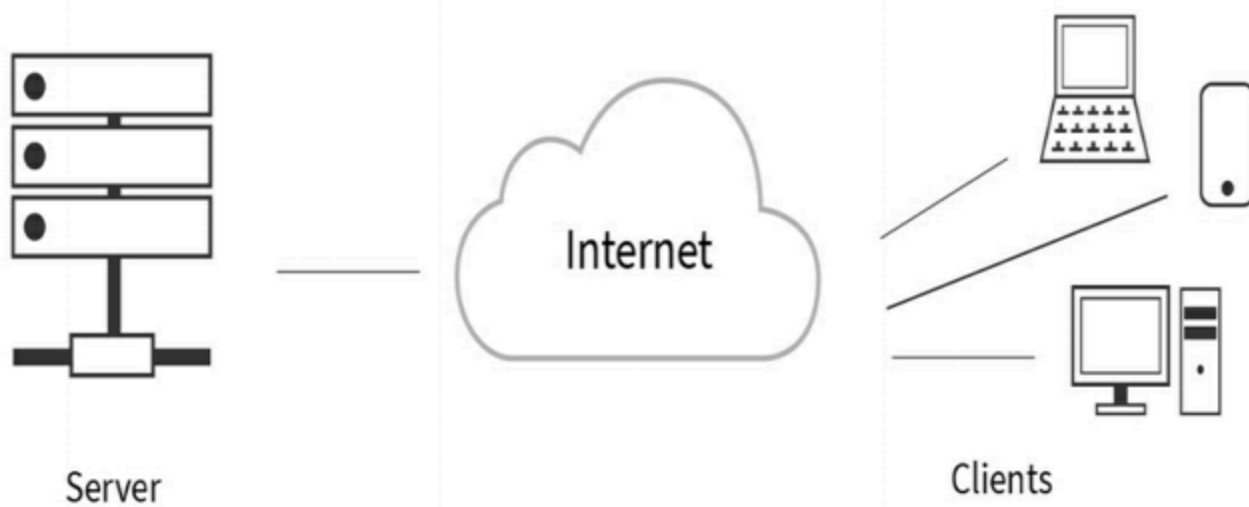
Apps: Wikipedia, social media, and e-commerce.

## Backend Revolution

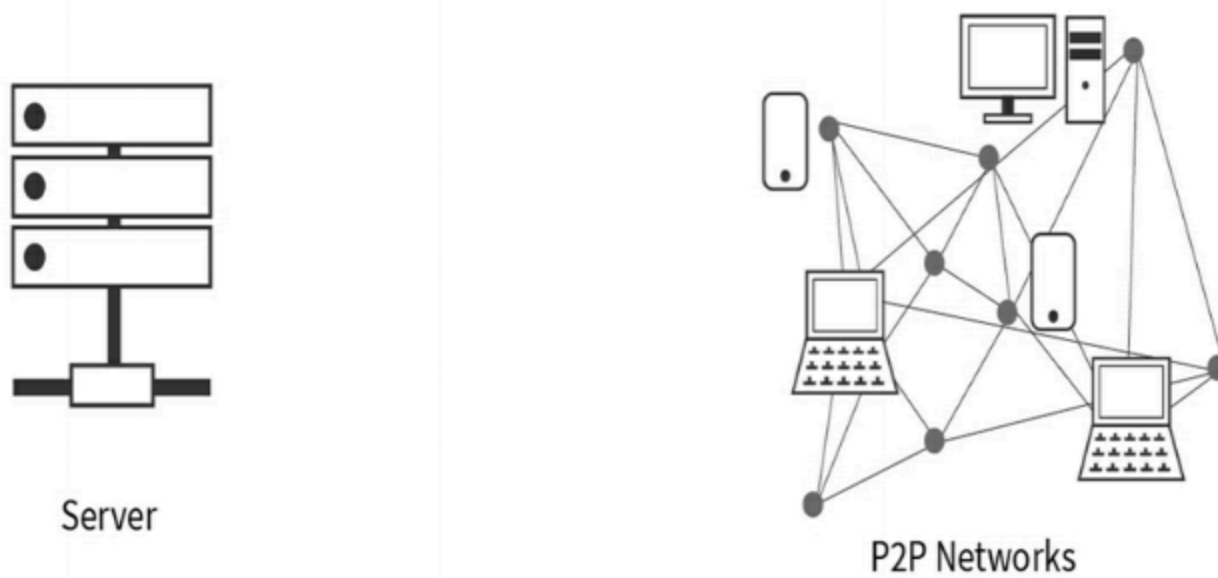
Frontend remains the same, but the data structures in the backend change. Anyone can participate in verifying transactions and be compensated for their contribution with a network token. Agreements are executed on the fly and P2P with smart contracts. Web3 applications need a connection to a distributed ledger, which is managed by a special application called “wallet.”

App: Tokens

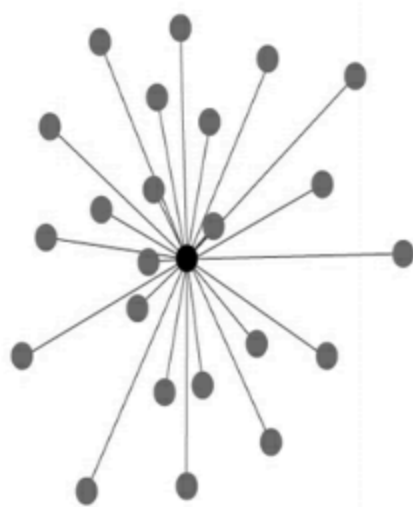
# Client-Server Internet



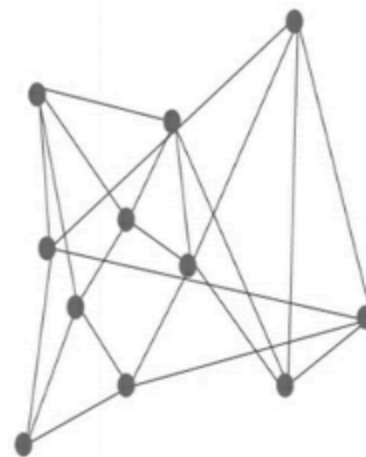
## Data Monopoly vs. Data Sovereignty



## Centralized vs. Distributed



Unique Point  
of Failure



No unique Point of Failure  
⇒ more secure

# Contents

## Part 1a: Web3 Basics

Title	Contents
Tokenized Networks: Web3, the Stateful Web	<p><b>If we assume that the WWW revolutionized information, and that the Web2 revolutionized interactions, the Web3 has the potential to revolutionize agreements and value exchange.</b> The Web3 changes the data structures in the backend of the Internet, introducing a universal state layer, often by incentivizing network actors with a token. The backbone of this Web3 is represented by a series of blockchain networks or similar distributed ledgers.</p> <p><b>While the Web2 was a front-end revolution, the Web3 is a backend revolution.</b> The Web3 reinvents how the Internet is wired in the backend, combining the system functions of the Internet with the system functions of computers. However, nothing much will change on the front-end of the Internet for the average user. <b>The Web3 represents a set of protocols, with distributed ledgers as their backbone.</b> Data is collaboratively managed by a P2P network of computers. The management rules are formalized in the protocol and secured by majority consensus of all network participants, who are incentivized with a network token for their activities. The protocol formalizes the governance rules of the network and ensures that people who do not know or trust each other reach and settle agreements over the Web. While trying to manipulate data on a server resembles breaking into a house, where security is provided by a fence and an alarm system, the Web3 is designed in a way that you would need to break into multiple houses around the globe simultaneously, which each have their own fence and alarm system. This is possible but prohibitively expensive.</p>
Blockchain: A Stateful Purpose	<p>The Internet we use today is “stateless.” It doesn’t have a native mechanism to transfer what computer science refers to as “state.” State refers to information, or the status of “Who is who?”; “Who owns what?”; and “Who has the right to do what?” in a network. The ability to transfer value easily and P2P is essential for efficient markets, and “state” is a key property for managing and transferring values. <b>In the Web3, values are represented by cryptographically secured tokens.</b></p> <p>[...]</p> <p><b>If you can’t hold state in the Internet, you cannot transfer value without centralized institutions acting as clearing entities.</b> While today’s Internet has accelerated information transfer by orders of magnitude of what was possible before, we still need trusted institutions such as Internet platform providers to broker our actions as a workaround for this lack of state. Stateless protocols like the current Web only manage the transfer of information, where the sender or receiver of that information is unaware of the state of the other. This lack of state is based on the simplicity of the protocols that the Web is built on, such TCP/IP, SMTP, or HTTP. This family of protocols regulates the transmission of data, not how data is stored. Data could be stored centrally, or decentrally. For many reasons, centralized data storage became the mainstream form of data storage and management.</p> <p>[...]</p> <p>Web2 platforms have introduced many beneficial services and created considerable social and economic value over the years. However, wealth was mostly accumulated by the companies offering the services, and less by the general public contributing content and value to those services. Instead of decentralizing the world, Web2 platforms contributed to a re-centralization of economic decision making, R&amp;D decision making, and subsequently, to an enormous concentration of power around these platform providers. Furthermore, since the early Internet was created around the idea of free information, customers were often not willing to pay for online content with a recurring subscription fee, and micropayments are still not feasible, in most cases. Therefore, many of these Web2 platforms needed to find alternative ways to profit from the free services they provided, and this alternative was advertising. What followed was targeted advertizing based on user behavior and the commodification of private data. Business models have, therefore, developed around targeted advertising that builds on the data sets collected, which provide “state” for these platforms. <b>As a result of this, users are paying for services with their private data.</b></p>
Web3 Protocols	<ul style="list-style-type: none"><li>● <b>Processor</b> (Blockchain networks (ie - bitcoin)). A blockchain network is simply the processor for decentralized applications that operate on top of the Web3. It serves as a distributed accounting machine recording all token transactions and performing computation.</li></ul>

	<ul style="list-style-type: none"><li>• Computation</li><li>• File storage</li><li>• Messaging</li><li>• Identities</li><li>• External data (oracles)</li><li>• and many other decentralized services.</li></ul>
Decentralized Applications in the Web3	<p>As opposed to centralized applications that run on a single computer, decentralized applications run on a P2P network of computers.</p> <p>Decentralized applications do not look any different from current websites or mobile apps. The front-end represents what you see, and the backend of a decentralized application represents the entire business logic. A decentralized application is a blockchain client - often also referred to as the “wallet.” It uses the same technologies to render a webpage or a mobile app (like HTML, CSS, Javascript) but communicates with a blockchain network instead of a server and, in the case of smart contract networks, also the smart contracts</p>
Chapter Summary	<p>The Internet we have today is broken. We do not control our data, nor do we have a native value settlement layer. Every time we interact over the Internet, copies of our data get sent to the server of a service provider, and every time that happens, we lose control over our data. This raises issues of trust.</p> <p>~</p> <p>The Internet we use today stores and manages data on the servers of trusted institutions. In the Web3 data is stored in multiple copies of a P2P network, and the management rules are formalized in the protocol, and secured by majority consensus of all network participants, often (but not always) incentivized with a network token for their activities.</p> <p>~</p> <p>In the Web3 the state of the network (represented by the ledger) is collectively maintained.</p> <p>~</p> <p>While the Web2 was a front-end revolution, the Web3 is a backend revolution, introducing a universal state layer. It is a set of protocols led by a blockchain network or similar distributed ledger, which intends to reinvent how the Internet is wired in the backend. The Web3 combines the system functions of the Internet with the system functions of computers.</p> <p>~</p> <p>As opposed to centralized applications that run on a single computer, decentralized applications run on a P2P network of computers. They have existed since the advent of P2P networks. Decentralized applications don’t necessarily need to run on top of a blockchain network.</p> <p>~</p> <p>A decentralized application is a blockchain client called “wallet.” It uses the same technologies to render a webpage or a mobile app (like HTML, CSS, Javascript) but communicates with a blockchain network instead of a server and, in the case of smart contract networks, also the smart contracts. The wallet also manages the public-private key-pair and the blockchain address, to provide a unique identity for network nodes and allow them to interact with the network.</p>
Chapter References & Further Reading	<p>Benet, Juan: “IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3),” retrieved, Sept 10, 2018: <a href="https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf">https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf</a></p> <p>Ehrsam, Fred; “The dApp Developer Stack: The Blockchain Industry Barometer”, Apr 30, 2017, retrieved from: <a href="https://medium.com/@FEhrsam/the-dapp-developer-stack-the-blockchain-industry-barometer-8d55ec1c7d4">https://medium.com/@FEhrsam/the-dapp-developer-stack-the-blockchain-industry-barometer-8d55ec1c7d4</a></p> <p>Gáucho Pereira Felipe Gáucho: “The Web3 Video Stack Charting the infrastructure for a decentralized mediaverse!”Aug 16, 2018, retrieved from: <a href="https://tokeneconomy.co/web3videostack-c423481c32a5">https://tokeneconomy.co/web3videostack-c423481c32a5</a></p> <p>Gillies, James; Cailliau, Robert: “How the Web was Born: The Story of the World Wide Web”, Oxford University Press, 2000, retrieved from <a href="https://books.google.de/books?id=pIH-JijUNS0C&amp;lpg=PA25&amp;ots=MKZj0F7pJN&amp;pg=PA25&amp;redir_esc=y#v=onepage&amp;q&amp;f=false">https://books.google.de/books?id=pIH-JijUNS0C&amp;lpg=PA25&amp;ots=MKZj0F7pJN&amp;pg=PA25&amp;redir_esc=y#v=onepage&amp;q&amp;f=false</a></p> <p>Koblitz, N.: „Elliptic curve cryptosystems“. Mathematics of Computation. 48 (177): 203–209, 1987</p> <p>Laplante, Philip A.: “Dictionary of Computer Science, Engineering and Technology”, 2000, CRC Press. p. 466.</p> <p>McConaghy, Trent: “Blockchain Infrastructure Landscape: A First Principles Framing Manifesting Storage, Computation, and Communications”, Jul 15, 2017, retrieved from: <a href="https://medium.com/@trentmc0/blockchain-infrastructure-landscape-a-first-principles-framing-92cc5549bafe">https://medium.com/@trentmc0/blockchain-infrastructure-landscape-a-first-principles-framing-92cc5549bafe</a></p>

Miller, V.; "Use of elliptic curves in cryptography". CRYPTO. Lecture Notes in Computer Science. 85. pp. 417–426, 1985

Misra, Jayadev: "A Discipline of Multiprogramming: Programming Theory for Distributed Applications" Springer, 2001.

Monegro, Joel: "Fat Protocols", Aug 8, 2016, retrieved from: <https://www.usv.com/blog/fat-protocols>

Nakamoto, Satoshi: „Bitcoin: A Peer-to-Peer Electronic Cash System,“ Bitcoin.org, 2008, Archived from the original on 20 March 2014, retrieved from: <https://bitcoin.org/bitcoin.pdf>

N.N.: "Web3 Foundation - Website," retrieved from: <https://web3.foundation/>

N.N.: "Comprehensive wiki of generalised Web3 stack," retrieved, Sept 10, 2018: <https://github.com/w3f/Web3-wiki/wiki>

Pon, Bruce: "Blockchain will usher in the era of decentralised computing", Apr 15, 2016, retrieved from: <https://blog.bigchaindb.com/blockchain-will-usher-in-the-era-of-decentralised-computing-7f35e94af0b6>

Samani, Kyle: "The Web3 Stack", July 10, 2018, retrieved from: <https://multicoin.capital/2018/07/10/the-web3-stack/>

Stallings, W.: "Computer Networking with Internet Protocols and Technology", Pearson Education, 2004.

Tekisalp, Emre: "Understanding Web 3 — A User Controlled Internet. Coinbase breaks down the motivation and technology behind the development of Web 3", Coinbase, Aug 29, 2018, retrieved from : <https://blog.coinbase.com/understanding-web-3-a-user-controlled-internet-a39c21cf83f3>

Thomas, John; Mantri, Pam: "Complex Adaptive Blockchain Governance", MATEC Web of Conferences 223, 01010 (2018) <https://doi.org/10.1051/matecconf/201822301010> ICAD 2018, , retrieved from: [https://www.matec-conferences.org/articles/matecconf/pdf/2018/82/matecconf\\_icad2018\\_01010.pdf](https://www.matec-conferences.org/articles/matecconf/pdf/2018/82/matecconf_icad2018_01010.pdf)

Tual, Stephan: "Web 3.0 Revisited — Part One: "Across Chains and Across Protocols", May 26, 2017: <https://blog.stephantual.com/web-3-0-revisited-part-one-across-chains-and-across-protocols-4282b01054c5>

Vinton G. Cerf; Robert E. Kahn (May 1974). „A Protocol for Packet Network Intercommunication“. IEEE Transactions on Communications. 22 (5): 637–648. doi:10.1109/tcom.1974.

Wolpert, John: "Bring on the Stateful Internet", Aug 2, 2018, retrieved from: <https://media.consensys.net/bring-on-the-stateful-internet-d589adc7bb65>

Wood, Gavin: "ÐApps: What Web 3.0 Looks Like", April 17. 2014, retrieved from: <http://gavwood.com/dappsweb3.html>

Filecoin: <https://filecoin.io/>

Golem: <https://golem.netw>

IPFS: <https://ipfs.io/>

SIA: <https://sia.tech/>

Storj: <https://storj.io>

Swarm: <https://swarm-guide.readthedocs.io/en/latest/>

# Part 1b: Web3 Basics

Title	Contents
Keeping Track of the Tokens: Bitcoin, Blockchain, & Other Distributed Ledgers	Blockchain networks build on the idea of P2P networks, providing a universal data set that every actor can trust, even though they might not know or trust each other. Immutable copies of that data are stored and managed on every node in the network. Economic incentives in the form of native network tokens are applied to make the network fault tolerant, attack resistant, and collusion resistant.
Cryptoeconomics, Consensus & Proof-of-Work	As opposed to centralized applications that run on a single computer, decentralized applications run
Network Nodes	
Network Attacks	
Protocol Forks & Network Splits	
Alternative Distributed Ledger Systems	
Alternative Consensus Mechanisms to Proof Of Work	
With or without a Token?	
Use Cases & Applications	<ul style="list-style-type: none"><li>● <b>Transparency &amp; control:</b> Blockchain networks and other distributed ledgers allow more transparency and control along the supply chain of goods and services, including financial services that have been tokenized, which would resolve many questions around supply chain transparency, reduction of corruption, and more control over what happens to our private data.</li><li>● <b>Reduction of bureaucracy:</b> Smart contracts and similar rights management solutions have the potential to reduce bureaucracy and the coordination costs of business transactions (read more: Part 2 - Smart Contracts).</li><li>● <b>Resolve principal-agent dilemma of organizations:</b> Distributed ledgers also provide a global coordination tool for new types of decentralized and sometimes also autonomous organizations (read more: Part 2 - Institutional Economics &amp; Governance of DAOs).</li><li>● <b>Tokens as the killer-app:</b> Cryptographic tokens as an application of blockchain networks and derived ledgers might be as revolutionary as the emergence of the WWW, which allowed the creation of visually appealing web pages with just a few lines of code, and surfing the Internet by following links instead of using command-line interfaces. <b>It has become just as easy to create a token with a few lines of smart contract code</b> (read more: Part 3 &amp; Part 4).</li></ul> <p>One of the biggest use cases of distributed ledgers is <b>transparency and provenance along the supply chain of goods and services</b>. Supply chains represent a complex network of geographically distant and legally independent entities that exchange goods, payments, and documents across a dynamic network. Their architecture is quite similar to blockchain networks, but as opposed to blockchain networks, all documents are managed in data silos. As a result, document handling systems along these supply-chain networks are often inefficient, have complex interfaces, and are cost intense. Sustainable behavior of companies and individuals alike is hard to track and not well rewarded. Buyers and sellers have little or no information about the provenance of the products they buy, including potential fraud, pollution, or human rights abuses.</p>



	<p>Distributed ledgers allow a disparate group of network actors along a supply chain to exchange data seamlessly. Documents and transactions can be processed in almost real time, since auditing and enforcement can be automated, mitigating challenges such as multiple document copies and data inconsistencies. Tracking the provenance of goods and services along global supply chains can become much more feasible than today. Web3-based solutions can provide (i) more transparency of environmental impacts and (ii) origins, production type, and ingredients of the food we eat, and conditions under which the plants are grown or how animals are treated. Many companies and industry initiatives, such as “Provenance,” “Ambrosus,” “Modum,” “OriginTrail,” “Vechain,” “Wabi,” or “Wantonchain,” have started to implement Web3-based infrastructures to optimize their value chains, improve inefficiencies, free up working capital, and make goods and services more accessible. Such solutions, however, always need a combination of a set of technologies, including machine learning algorithms and data from the physical Web, the Internet of Things (read more: Part 2 - Smart Contract Oracles). Distributed ledger applications can also provide better accountability regarding human rights, such as general working conditions, child labor, or fair wages. Projects working on such solutions: “bext360,” “fairfood,” and “Namahe.” They can further be used to provide more control over our private data (read more: Part 1 - User-Centric Identities - Data Protection) and create P2P data markets (Ocean Protocol). While in theory this level of transparency of what happened to one’s private data could also be provided with current solutions, we would have to trust a centralized institution.</p>
Chapter Summary	<p>Blockchain networks are public infrastructures that collectively maintain a shared and distributed ledger, where immutable and encrypted copies of the information are stored on every computer in the network.</p> <p>The ledger contains all transactions ever made. Transactions are stored in a tamper-proof fashion: alteration in a block will change the subsequent blocks. The ledger, stored on all the computers of the network, guarantees that each token is transferred only once. It acts as a digital notary, and a publicly verifiable timestamp.</p> <p>All network participants have equal access to the same data in real time. Transactions processed by the network are transparent to all actors and can be traced back to their origin.</p> <p>Unlike distributed databases, blockchains allow for distributed control, where different parties that do not trust each other can share information without requiring a central administrator. Algorithmic administration of business logic and governance rules, with consensus protocols and smart contracts provide for the next level of automation of our socio-economic activities.</p> <p>The blockchain concept builds on the idea of P2P networks and provides a universal data set that every actor can trust, even though they might not know or trust each other. People and institutions who do not know or trust each other and reside in different countries, being subject to different jurisdictions, and who have no legally binding agreements with each other can now interact over the Internet without the need for trusted third parties like banks, Internet platforms, or other types of clearing institutions.</p> <p>Ideas around cryptographically secured P2P networks have been discussed in the academic environment in different evolutionary stages since the 1980s. However, before the emergence of Bitcoin, there had never been a practical implementation of a P2P network that managed to avoid the double-spending problem, without the need for trusted intermediaries guaranteeing value exchange.</p> <p>The “double-spending problem” refers to the fact that in the current Internet, digital money, in the form of a file, can be copied, and copies of that same digital file can be sent from one computer to multiple other computers at the same time.</p> <p>Consensus mechanisms, such as Proof-of-Work, allow for distributed control. They are based on the combination of economic incentives and cryptography. Applied game theory is used to reward network actors with a native network token. This reward mechanism is designed in a way that it is economically infeasible to cheat the network. It makes it exceedingly difficult to falsify the blockchain, due to the immense amount of computing power that would be required to do so.</p> <p>As opposed to public and permissionless networks, permissioned networks are invite only, which means that all validators are members of a consortium.</p> <p>“Distributed ledger” has emerged as an umbrella term used to describe technologies which distribute records or information among all those using it, whether permissioned or permissionless, and independent of their consensus mechanisms or data structures.</p>
Chapter References & Further Reading	<p>* Agreda, Victor: “Taxonomy of Blockchain Consensus,” <a href="https://strategiccoin.com/taxonomy-of-blockchains-consensus-2018/">https://strategiccoin.com/taxonomy-of-blockchains-consensus-2018/</a> * Antonopoulos, Andreas; „Bitcoin</p>

security model: trust by computation“. Radar. O'Reilly, 2014, Archived from the original on 31 October 2018: <http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html> \* Antonopoulos, Andreas M.; “Mastering Bitcoin. Unlocking Digital Cryptocurrencies”, Sebastopol, CA: O'Reilly Media, 2014

\* Back, Adam; „A partial hash collision based postage scheme“, October 2014 <http://www.hashcash.org/papers/announce.txt> \* Ballandies, Mark C.; Dapp, Marcus M.; Pournaras, Evangelos: “Decrypting Distributed Ledger Design - Taxonomy, Classification and Blockchain Community Evaluation”, 2018: <https://arxiv.org/pdf/1811.03419.pdf> \* Bitcoin.Wiki contributors: “Softfork”, Bitcoin Wiki: <https://en.bitcoin.it/wiki/Softfork> (accessed Nov 30, 2018). \* Buterin, Vitalik: “The Meaning of Decentralization”, Feb 6, 2017: <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274> \* Buterin, Vitalik: “On Public and Private Blockchains”, Aug 6, 2015: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/> \* Catalini, Christian; Gans, Joshua S.; „Some Simple Economics of the Blockchain“. SSRN Electronic Journal, 2016 \* Ethereum White Paper: <https://github.com/ethereum/wiki/wiki/White-Paper> \* Ethereum Yellow Paper: <https://ethereum.github.io/yellowpaper/paper.pdf> \* Gervais, Arthur; Karame, Ghassan O.; Capkun, Vedran; Capkun, Srdjan. „Is Bitcoin a Decentralized Currency?“, InfoQ & IEEE computer society, Archived from the original on 10 Nov 2018: [https://www.researchgate.net/publication/270802537\\_Is\\_Bitcoin\\_a\\_Decentralized\\_Currency](https://www.researchgate.net/publication/270802537_Is_Bitcoin_a_Decentralized_Currency) \* Golden, Sara; Price, Allison: “Sustainable Supply Chains. Better Global Outcomes with Blockchain.” Jan 2018, retrieved from: [https://www.newamerica.org/documents/2067/BTA\\_Supply\\_Chain\\_Report\\_r2.pdf](https://www.newamerica.org/documents/2067/BTA_Supply_Chain_Report_r2.pdf) \* Jackson, Matthew O.: “Mechanism Theory”, Humanities and Social Sciences 228-77, California Institute of Technology Pasadena, California 91125, U.S.A. October 12, 2000, revised December 8, 2003 \* Kravchenko, Pavel: “Ok, I need a blockchain, but which one?”, Sep 26, 2016: <https://medium.com/@pavelkravchenko/ok-i-need-a-blockchain-but-which-one-ca75c1e2100> \* Nakamoto, Satoshi: “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008: <https://bitcoin.org/bitcoin.pdf> \* N.N. “A Crash Course in Mechanism Design for Cryptoeconomic Applications - Understanding the Basic Fundamentals of “Cryptoeconomics”, BlockChannel, Oct 17, 2017: <https://medium.com/blockchannel/a-crash-course-in-mechanism-design-for-cryptoeconomic-applications-a9f06ab6a976> \* N.N.: "Blockchains: The great chain of being sure about things", The Economist, 31 October 2015: <https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things> \* Poelstra, Andrew: “Mimblewimble”, 2016-10-06 (commit e9f45ec) [diyhpl.us/~bryan/papers2/bitcoin/mimblewimble-andytoshi-draft-2016-10-20.pdf](https://github.com/andrewpoelstra/mimblewimble/blob/master/draft-2016-10-20.pdf) \* Satyawan, Tarar “A Crash Course on Consensus Protocols”, May 9, 2018: <https://medium.com/@satyawan.tarar1985/a-crash-course-on-consensus-protocols-29264c393097> \* Tasca, Paolo; Tessone, Claudio J.: “A Taxonomy of Blockchain Technologies: Principles of Identification and Classification”, Ledger, Vol 4, 2019: <http://ledger.pitt.edu/ojs/index.php/ledger/issue/view/5> \* Stark, Josh: “Making Sense of Cryptoeconomics”, Aug 19, 2017 <https://www.coindesk.com/making-sense-cryptoeconomics> \* Tomaino, Nick, “Cryptoeconomics 10”, Jun 4, 2017, <https://thecontrol.co/cryptoeconomics-101-e5c883e9a8ff> \* Wang, Wenbo; Dinh Thai Hoang, Hu, Peizhao; Xiong, Zehui; Niyato, Dusit; Wang, Ping; Wen, Yonggang; In Kim, Dong: “A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks”: <https://arxiv.org/pdf/1805.02707.pdf> \* Wei, Bai: “Mechanism Design in Cryptoeconomics”, May 31, 2018: <https://medium.com/secbit-media/mechanism-design-in-cryptoeconomics-6630673b79af> \* Voshmgir, Shermin: “Blockchain & Sustainability,” Crypto3conomics blog, Medium, Aug 11, 2018, retrieved from: <https://medium.com/crypto3conomics/blockchain-sustainability-7d1dd90e9db6> \* Wikipedia contributors: "Blockchain," Wikipedia, The Free Encyclopedia, <https://en.wikipedia.org/wiki/Blockchain> (accessed Nov 11, 2018). \* Witherspoon, Zane : "A Hitchhiker’s Guide to Consensus Algorithms," November 28th 2017: <https://hackernoon.com/a-hitchhikers-guide-to-consensus-algorithms-d81aae3eb0e3> \* Bitcoin 51% Attack Calculator: <https://gobitcoin.io/tools/cost-51-attack/> \* 51% Attack Calculator: <https://crypto51.app/> \* Ambrosus: <https://ambrosus.com/> \* Bitcoin Gold: <https://bitcoingold.org/> \* Bitcoin Diamond: <https://www.bitcoindiamond.org/> \* Bitcoin Cash: <https://www.bitcoincash.org/> \* Bitcoin Platinum: <https://bitcoinplatinum.github.io/> \* BitShares: <https://bitshares.org/> \* Block Lattice: <https://docs.nano.org/integration-guides/the-basics/#block-lattice-design> \* BlackCoin: <http://blackcoin.co/> \* Bitcoin Cash: <https://bitcoincash.org/> \* Byteball: <https://byteball.org/> \* Cardano: <https://cardano.org/en/home/> \* Colored Coins: <http://coloredcoins.org/> \* Cosmos: <https://cosmos.com/> \* Decred: <https://dcred.org/> \* Dfinity: <https://dfinity.org/> \* fairfood: <http://fairfood.nl/> \* Ethereum Classic: <https://ethereumclassic.org/> \* EOS: <https://eos.io/> \* Hyperledger Fabric: <https://hyperledger.org/projects/fabric> \* Litecoin: <https://litecoin.org/> \* Lisk: <https://lisk.io/> \* IOTA: <https://iota.org/> \* IoT Chain: <https://iotchain.io/> \* Mastercoin: <https://en.wikipedia.org/wiki/Mastercoin> \* Modum: <https://modum.io/> \* Nano: <https://nano.org/> \* Neo: <https://neo.org/> \* Nxt: <https://nxt.org/> \* NuShares/NuBits: <https://nubits.com/nushares>

\* Ocean: <https://oceanprotocol.com/> \* OriginTrail: <https://origintrail.io/> \* Provenance: <https://provenance.org/> \* Qora: <http://www.qora.org/> \* Ontology: <https://ont.io/> \* Ripple: <https://ripple.com/> \* Stellar: <https://stellar.org/> \* Steemit: <https://steemit.com/> \* Tezos: <https://tezos.com/> \* Vechain: <https://www.vechain.org/> \* Wabi: <https://wacoin.io/> \* Wantonchain: <https://www.waltonchain.org/>





Part 1c: Web3 Basics

Title	Contents
Token Security: Cryptography	
Public-Key Cryptography	
Secure Algorithms	
Hashing	
Wallets & Digital Signatures	
Types of Wallets & Key Management	
Sending Tokens	
Chapter Summary	<p>Cryptography is the practice and study of secure communication in the presence of third parties. The aim is to create information systems that are resilient against eavesdropping, manipulation, and other forms of attack.</p> <p>~</p> <p>Cryptography in blockchain networks allows for transparency of interactions while maintaining the privacy of all network actors.</p> <p>~</p> <p>Public-key cryptography is used to prove one’s identity with a set of cryptographic keys: a private key and a public key, which in combination with a transaction creates our digital signature. This digital signature proves ownership of our tokens and allows us to control them through a piece of software called a “wallet.”</p> <p>~</p> <p>Similar to a handwritten signature, a digital signature is used to verify that you are who you say you are. In Bitcoin and other blockchains, digital signatures are mathematical functions that reference a specific wallet address that manages your tokens on a blockchain.</p> <p>~</p> <p>A hash function is a mathematical algorithm that can take any type of input, such as a string, a text file, or a picture file, and digest it to a fixed-size output string called a hash. It is a one-way function, which means that the only way to recreate the original input data (message) from the hash is to attempt to try all possible variations to see if they produce a match. While this is possible, it is time consuming and therefore expensive.</p>

Part 1d: Web3 Basics

Title	Contents

Chapter Summary	<p>Historically, identity processes, such as passports, driver’s licenses, social security cards, or serial numbers for goods, have been issued by centralized institutions such as local and national governments and other trusted institutions. The emergence of the Internet created the need for digital identification systems.</p> <p>~</p> <p>From a computer science perspective, the term “identity” can be reduced to the data elements related to the identity management process: “identifier,” “authentication,” and “credentials.”</p> <p>~</p> <p>Identifiers are needed to uniquely identify a person, institution, or object. An identifier needs to be unique and persistent over time.</p> <p>~</p> <p>Authentication is the process with which a person, institution, or object can prove that they are who they claim they are. A person can authenticate themselves by proving ownership of an object (ID card, hardware wallet, software wallet), knowledge (password or PIN), or by a personal property (biometric data, signature). Often, a combination of these systems is used.</p> <p>~</p> <p>An identity is useless without linking data related to a person (personal data), institution (institutional data), or object (object-related data) to the identifier.</p> <p>~</p> <p>The current Internet was built around connecting machines, not people. The Internet does not provide a native identity layer for people, institutions, or objects other than the operating nodes in a network of computers. Workaround solutions have been built on the application layer using internal databases (private infrastructure) to manage all the data involved with digital identity management processes. All user-related data is managed by the service provider, on their private server infrastructure, and that all elements related to the identity management process are centralized.</p> <p>~</p> <p>These data silos and proprietary identity solutions have created considerable costs and trade-offs, both for companies and users alike such as (i) password chaos, (ii) protection against bad actors, (iii) data protection &amp; custodial costs, (iv) data portability, (v) lack of control &amp; sovereignty over data, and the (vi) re-centralization of the Internet.</p> <p>~</p> <p>Blockchain networks and similar distributed ledgers use public-key cryptography for the identification of all network actors, but they are insufficient for a thriving tokenized economy. However, combined with DIDs, they can offer critical components for more “user-centric” identity solutions that are suitable for the Web3, and provide more privacy and control than “server-centric” solutions used in the Web2.</p> <p>~</p> <p>The user-centric identity process requires three actors: (i) identity issuers, (ii) identity owners, and (iii) identity verifiers. If set up correctly, anyone in a blockchain network can verify whether a piece of data (credential) is valid and which institutions attested to the validity of the data without revealing the data itself.</p> <p>~</p> <p>While plain text data should never be stored on a public ledger, a privacy-preserving identity management system can use distributed ledgers to allow a person to prove that their personal identity-related data fulfills certain requirements without revealing the actual data. In such a setup, distributed ledgers can be used to attest the authenticity of the data and attestations, only registering indirect “pointers” for the purpose of verification.</p> <p>~</p> <p>A user can create and register a DID when activating a blockchain wallet, which creates a pair of private and public keys. Public-key cryptography is used for authentication and encryption. Only the private key can prove one’s identity. The private key acts as your personal lock on the wallet.</p> <p>~</p> <p>Any DID can be linked to attestations (verifiable credentials) that are issued by other people and institutions attesting specific characteristics for an identity owner, such as name, address, email, age, existing diplomas, or other certifications such as a driver’s license. The credentials are signed by their issuers using public-key</p>

	<p>cryptography. Once signed by an issuer, credentials can be managed using the wallet of the identity owner directly.</p> <p>~</p> <p>The separation of the “identifier,” “authentication,” and “data” is crucial to a user-centric setup. It can be seen as a system of checks and balances in a data-driven economy that guarantees the level of autonomy and privacy over one’s digital footprint, and is very contrary to how the Internet is set up today. Using a public infrastructure such as a collectively maintained ledger as a unique source of truth, while splitting the roles in the identification management process, makes user-centric identity management systems “decentralized.”</p> <p>~</p> <p>The wallet acts as a personal container that allows you to control your digital identities. The wallet is the digital equivalent to a physical wallet, which usually acts as a container for all your ID cards, such as driver’s license, bank card, gym membership, national ID card, social security card, or loyalty cards, in addition to your money. While it is initially empty, over time, one can fill it with credentials that represent the digital version of your driver's license, bank card, gym membership, national ID card, social security card, loyalty cards, etc.</p> <p>~</p> <p>Just as you open your wallet to reveal your ID card, you need to activate your Web3 wallet to reveal your digital credentials to third parties (using a password). No one can see the contents of your Web3 wallet without your consent. You choose who to share these credentials with. The content of the wallet remains concealed until you choose to reveal something. The digital wallet is portable, as a dedicated hardware device, or an app in your mobile phone or your notebook.</p>
Chapter References And Further Reading	<p>Chapter References &amp; Further Reading * Allan, Christoper: “The Path to Self-Sovereign Identity,” March 1 2017, <a href="https://github.com/ChristopherA/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md">https://github.com/ChristopherA/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md</a> * Ellison, Carl: “Establishing Identity without Certification Authority,” 1996, <a href="https://irl.cs.ucla.edu/index.html">https://irl.cs.ucla.edu/index.html</a> * Feisthammel, Patrick: “Pretty good Privacy, PGP, Web of Trust,” Oct 7 2004, <a href="https://www.rubin.ch/pgp/weboftrust.en.html">https://www.rubin.ch/pgp/weboftrust.en.html</a> * Jordan, Ken; Hauser, Jan; Foster, Steven: “The Augmented Social Network,” White paper, 2000, <a href="https://firstmonday.org/ojs/index.php/fm/article/view/1068/988">https://firstmonday.org/ojs/index.php/fm/article/view/1068/988</a> * Kameron, Kim: “The Laws of Identity,” March 2007, <a href="https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/ms996456(v=msdn.10)?redirectedfrom=MSDN">https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/ms996456(v=msdn.10)?redirectedfrom=MSDN</a> * Kütt, Andres: "MyData Webinar #5: Identity in the Digital Era," Mydata Global, Youtube Video, retrieved from: <a href="https://www.youtube.com/watch?v=XjzJeys7PvM&amp;fbclid=IwAR0qMDGYuZVk0c6aDHOX46AdFQMGdsI24SSZ6-IMfj7XZY-TrbkbT5LFlqk">https://www.youtube.com/watch?v=XjzJeys7PvM&amp;fbclid=IwAR0qMDGYuZVk0c6aDHOX46AdFQMGdsI24SSZ6-IMfj7XZY-TrbkbT5LFlqk</a> * Many authors: “Rebooting the Web of Trust,” Papers and Specs, <a href="http://www.weboftrust.info/papers.html">http://www.weboftrust.info/papers.html</a> * Many authors: “Charta for Digital Human Rights,” Version: 01.12.2016 Unofficial English translation of the German original text, published by ZEIT-Stiftung Ebelin und Gerd Bucerius <a href="https://digitalcharta.eu/wp-content/uploads/2016/12/Digital-Charta-EN.pdf">https://digitalcharta.eu/wp-content/uploads/2016/12/Digital-Charta-EN.pdf</a> * Many authors: “Self-sovereign Identity A position paper on blockchain enabled identity and the road ahead,” October 23 2018, Identity Working Group of the German Blockchain Association, <a href="https://www.bundesblock.de/wp-content/uploads/2019/01/ssi-paper.pdf">https://www.bundesblock.de/wp-content/uploads/2019/01/ssi-paper.pdf</a> * Many authors: “The Respect Trust Framework, “ Version 2.1, Feb 2016, <a href="https://oixnet.org/wp-content/uploads/2016/02/respect-trust-framework-v2-1.pdf">https://oixnet.org/wp-content/uploads/2016/02/respect-trust-framework-v2-1.pdf</a> * Marlinspike, Moxie: “Sovereign Source Authority,” Moxytongue, Feb 2012, <a href="https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html">https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html</a> * Miller, Ron: "The Promise of managing identities on the blockchain,” Sep 10, 2017, <a href="https://techcrunch.com/2017/09/10/the-promise-of-managing-identity-on-the-blockchain/?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_recent_activity_details_all%3BknkLT7NkR5Cex9bx3zogKg%3D%3D&amp;gucounter=1">https://techcrunch.com/2017/09/10/the-promise-of-managing-identity-on-the-blockchain/?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_recent_activity_details_all%3BknkLT7NkR5Cex9bx3zogKg%3D%3D&amp;gucounter=1</a></p> <p>* Mire, Sam: “Blockchain Research Technologies Blockchain For Identity Management: 7 Possible Use Cases” Dec 5 2018, <a href="https://www.disruptordaily.com/blockchain-use-cases-identity-management/">https://www.disruptordaily.com/blockchain-use-cases-identity-management/</a> * N.N.: “Enterprise Ethereum Blockchain in Digital Identity,” Consensys website, <a href="https://consensys.net/blockchain-use-cases/digital-identity/#usecases">https://consensys.net/blockchain-use-cases/digital-identity/#usecases</a> * N.N.: “Identity Management with Blockchain: The Definitive Guide (2020 Update),” TYKN website: <a href="https://tykn.tech/identity-management-blockchain/">https://tykn.tech/identity-management-blockchain/</a> * Preukschat, Alex; Reed , Drummond: "Self-Sovereign Identity Decentralized Digital Identity and Verifiable Credentials" MEAP began December 2019 Publication in January 2021 (estimated) ISBN 9781617296598 300 pages (estimated), electronically retrieved from:<a href="https://www.manning.com/books/self-sovereign-identity">https://www.manning.com/books/self-sovereign-identity</a> * Reed, Drummond; Tobin, Andrew: “Sovereign White Paper,” Sept 29 2016, <a href="https://sovrin.org/wp-content/uploads/2017/07/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf">https://sovrin.org/wp-content/uploads/2017/07/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf</a> * Reed, Drummond; Sabadello, Markus: "Chapter 8 Decentralized identifiers" in Self Sovereign Identity, retrieved from on October 27, 2020: in <a href="https://livebook.manning.com/book/self-sovereign-identity/chapter-8">https://livebook.manning.com/book/self-sovereign-identity/chapter-8</a> * Ruff, Timothy: "When Explaining SSI, Start with the Wallet," Apr 21 2020, <a href="https://medium.com/@rufftimo/when-explaining-ssi-start-with-the-wallet-bee5d2af6696">https://medium.com/@rufftimo/when-explaining-ssi-start-with-the-wallet-bee5d2af6696</a> * Sabadello, Markus: “Human Rights in the Information Society,” 2011, <a href="https://danubetech.com/download/Human-Rights-in-the-Information-Society.pdf">https://danubetech.com/download/Human-Rights-in-the-Information-Society.pdf</a> * Shea, Michael;Smith,</p>

Samuel M.; Stöcker,Carsten, Caballero, Juan; Condon, Matt G.: “Decentralized Identity as a Meta-platform: How Cooperation Beats Aggregation a white paper from Rebooting the Web of Trust IX, <https://nbviewer.jupyter.org/github/WebOfTrustInfo/rwot9-prague/blob/master/final-documents/CooperationBeatsAggregation.pdf> \* Spike, Marlin: “Self Sovereign Identity, how the term has evolved,” Feb 2016, <https://www.moxytongue.com/2016/02/self-sovereign-identity.html> \* Smith, Samuel M.: "Key Event Receipt Infrastructure (KERI)", Cornell University, retrieved from: <https://arxiv.org/abs/1907.02143> \* Smolenski, Natalie: "The EU General Data Protection Regulation and the Blockchain," Aug 2 2017, <https://medium.com/learning-machine-blog/the-eu-general-data-protection-regulation-and-the-blockchain-1f1d20d24951> \* Stöcker, Carsten: “The Economic Value of Decentralized Identity — Part 2 Reimagining the economics of trust and reputation,” Mar 11 2020, <https://medium.com/spherity/the-economic-value-of-decentralized-identity-part-2-733aa977eaf8> \* Stöcker, Carsten: “Spherity’s Identity Tech Predictions for the decade of the 2020’s — Part 1,” Jan 16 2020 <https://medium.com/spherity/spheritys-identity-tech-predictions-for-the-decade-of-the-2020-s-part-1-410bc9b48be4> \* Stöcker, Carsten: “Spherity’s Identity Tech Predictions for the decade of the 2020’s — Part 2,” Feb 13 2020 <https://medium.com/spherity/spheritys-identity-tech-predictions-for-the-decade-of-the-2020-s-part-2-6e480d2a57ea> \* Stöcker, Carsten: “SSI201: Upgrading products with intelligent serial numbers and DIDs How smart can an object’s identifier be? How can it enable cradle-to-grave traceability and other innovative capabilities?” Nov 26, 2019 , <https://medium.com/spherity/ssi201-upgrading-products-with-intelligent-serial-numbers-and-dids-78da623b91dd> \* Stöcker, Karsten: "KERI: A more Performant Ledger for Trusted Identities Securing the control of decentralized identifiers at the root with ambient verifiability", Medium, Sperity Blog, July 2 2020, <https://medium.com/@cstoecker> \* Voshmgir, Shermin: “Identity as a Bottleneck for Blockchain,” Oct 17, 2017, <https://stories.jolocom.com/identity-blockchain-the-road-to-self-sovereign-identity-f9f4439c52cb> \* Voshmgir, Shermin: “Self Sovereign — Identity vs Data?” Feb 27 2018, <https://stories.jolocom.com/self-sovereign-identity-vs-data-5abe5947a62> \* Wikipedia contributors: "Pretty Good Privacy," Wikipedia, The Free Encyclopedia, [https://en.wikipedia.org/w/index.php?title=Pretty\\_Good\\_Privacy&oldid=959437666](https://en.wikipedia.org/w/index.php?title=Pretty_Good_Privacy&oldid=959437666) (accessed May 31, 2020). \* Zuboff, Shoshana: “ The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.” New York: PublicAffairs, 2019. \* Ageif: <https://age-ify.com/> \* Civic: <https://www.civic.com/wallet/> \* Edge: <https://edge.app/> \* General Data Protection Regulation (GDPR): <https://gdpr-info.eu/> \* Hu-manity.co: <https://hu-manity.co/> \* Jolocom: <https://jolocom.io/> \* Key: <https://key.io/> \* List of Blockchain & Identity Solutions: <https://github.com/peacekeeper/blockchain-identity> \* Madana: <https://www.madana.io/> \* Metadium: <https://www.metadium.com/> \* NewBanking Identity: <https://newbanking.com/#/> \* ObjectTech: <https://www.objectivetgg.com/> \* THEKEY: <https://www.thekey.vip/#/homePage> \* Trusti: <https://trusti.com/> \* PeerMountain: <https://www.peermountain.com/> \* PGP WOT: <https://www.linux.com/training-tutorials/pgp-web-trust-core-concepts-behind-trusted-communication/> \* Rebooting the Web of Trust:<http://www.weboftrust.info/papers.html> \* REMME: <https://remme.io/> \* Riddle & Code: <https://www.riddleandcode.com/> \* Spherity: <https://spherity.com/> \* SPKI/SDSI project: <http://world.std.com/~cme/html/spki.html> \* SoLid (Social Linked Data: <https://github.com/solid/solid-spec> \* uPort: <https://www.uport.me/> \* UniquID: <https://uniquid.com/> \* ValidatedID: <https://www.validatedid.com> \* WebIDs: <https://www.w3.org/2005/Incubator/webid/spec/tls/> \* WoTT: <https://wott.io/> \* W3C working group on verifiable claims: <https://www.w3.org/2017/vc/WG/> \* W3C Verifiable Claims Task Force FAQ: <https://w3c.github.io/webpayments-ig/VCTF/charter/faq.html> \* W3C initiative of Decentralized Identifiers (DIDs): <https://w3c.github.io/did-core>

Voshmgir, Shermin. Token Economy: How the Web3 reinvents the Internet (pp. 110-112). Token Kitchen. Kindle Edition.

Part 2a: Web3 Applications

Title	Contents
Smart Contracts	
Self-Enforcing Agreements	
Industry Use Cases	
Oracles	
USE Case Of Buying A Second-Hand Car	
History of Smart Contracts	
Chapter Summary	

Part 2b: Web3 Applications

Title	Contents

## Part 2c: Web3 Applications

Title	Contents

## Part 4a: Token Use Cases

Title	Contents
Asset Tokens & Fractional Ownership	Asset tokens allow the creation of a digital representative for any physical asset or securities and could introduce a range of new use cases that might not have been feasible before. They are the next step in the automation of the securities and asset markets, replacing entire back offices with smart contracts.
Use Case 1: Security Tokens	Security tokens provide a new form of representation, management, and distribution of existing securities. Paying out dividends could be conducted with a smart contract and on the fly, which is an upgrade for state-of-the-art financial settlement systems. From a regulator’s point of view, these tokens are traditional securities that are simply represented and managed by a new technology. They are not a new product, and therefore are fairly easy to regulate. Financial conduct authorities and similar regulatory bodies worldwide have concluded that any token that might be considered a security token is subject to regulatory bodies worldwide, like the Securities and Exchange Commision (USA), FMA (Austria), Monetary Authority of Singapore (MAS), BaFin (Germany), and FCA - Financial Conduct Authority (UK), just to name a few examples.
Use Case 2: Tokening Real Estate	
Use Case 3: Tokenizing Art	
Use Case 4: Collective Fractional Ownership	<p><b>Co-Working Space</b></p> <ul style="list-style-type: none"><li>Office building could be collectively owned by the members of a co-working space.</li><li>The tokens would grant voting rights. The co-working space could be tokenized based on usage rights, where members would have a right to use a certain share of the space.</li></ul> <p><b>NGO - Power Generation</b></p> <ul style="list-style-type: none"><li>A community of neighbors could buy and collectively operate a renewable energy–powered micro-grid, as it is more feasible for a collective of neighbors to cover the cost than for an individual.</li><li>The smart contract would send monthly revenues from the excess energy produced and sold to all members of the collective, in proportion to the shares they owned (read more: Part 2 - Institutional Economics of DAOs).</li></ul> <p><b>Taxi Drivers</b></p> <p>Such a setup could also be attractive for taxi drivers. Many drivers lack the money to invest in their own car, and thus work for a company to provide the infrastructure, sharing their revenues or paying a fixed rent to the vehicle’s owner. Fractional collective ownership tokens would allow several taxi drivers to collectively purchase a car, instead of renting it from someone, and split up the shifts as well as the costs and revenues involved with buying and maintaining the car for their rides. A smart contract could collect a portion of everyone’s revenues, allocated for the expenses involved.</p> <p><b>Community-Owned Assets</b></p>



	<p>The state of Alaska in the United States and Norway have already passed their residents a share of their oil sales, either directly or in the form of wealth funds. Such a process could be tokenized to reduce settlement costs, while increasing transparency and accountability.</p>
Chapter Summary	<p>Asset tokens allow the creation of a digital representative for physical assets or securities. They are the next step in the automation of the securities and asset markets, replacing entire back offices with smart contracts.</p> <p>The tokenization of an existing asset refers to the process of creating a tokenized digital twin for any physical object or financial asset. The token hereby represents the physical counterpart, collectively managed by a distributed ledger.</p> <p>“Asset token” is a general term that can include any assets, such as commodities, artwork, real estate, or securities. “Security tokens” are a specific type of asset tokens that are classified as securities under financial market regulations. The interpretation of what constitutes a security, however, is subject to local legislation.</p> <p>Security tokens provide a new form of representation, management, and distribution of existing securities. Paying out dividends could be conducted with a smart contract and on the fly, which is an upgrade for state-of-the-art financial settlement systems. From a regulator’s point of view, these tokens are traditional securities that are simply represented and managed by a new technology. They are not a new product, and therefore are fairly easy to regulate.</p> <p>Asset tokens are to financial markets what social media was to the publishing industry. They are much more likely to revolutionize our economy, and security tokens are the gateway drug to get there.</p> <p>~</p> <p>From a legal perspective, tokenization of (rights to) a physical asset and other (virtual) rights seems important. Tools that aim to represent virtual assets (such as paper certificates and other digital certificates) are likely to be substituted by tokens soon; for physical assets, possession seems likely to remain the most important link.</p> <p>~</p> <p>Depending on the regulatory environment and how the smart contract is set up, asset tokens may be eligible for global trading. Opening up global markets adds even more liquidity and provides new opportunities for entrepreneurs and investors alike. This trend might make it feasible to buy shares of assets in foreign countries that were previously much more difficult to obtain.</p> <p>~</p> <p>Smart contracts have the potential to facilitate rights management in the real estate industry, including the whole settlement process. Once real estate ownership is tokenized, it can be easily registered and managed on a public infrastructure and traded P2P, if it complies with regulation. The hashed data of each property could be recorded on a distributed ledger to provide a universally shared data set on all real estate–related activities, such as previous owner, repairs conducted, and amenities. Tokens could either be issued for existing real estate or for a real estate project under development.</p> <p>~</p> <p>In order to tokenize a real asset like an apartment, one generates a token with a smart contract, and associates a value of the real asset with that token. The ownership right in such an asset and its corresponding digital representation can be divided into parts and sold to several (co-)owners. Even if a token represents a physical asset that is not divisible, like a piece of art or real estate, the token itself is divisible.</p> <p>~</p> <p>One prerequisite for tokenizing real estate would be that the legal process of the real estate market is made Web3 compatible, from the land registry process to the general regulatory environment accepting smart contract processes.</p> <p>~</p> <p>Tokenizing the art and entertainment market could, potentially, resolve many of the inefficiencies of the current systems, from fractional ownership, provenance, digital rights management, and settlement to crowdfunding. Tokens could also enable new derivative artworks.</p> <p>~</p> <p>Asset markets, such as fine art or real estate, that usually have high economic buy-ins can be tokenized and fractionalized, potentially generating new use cases that were not feasible before. Instead of investing millions of Euros for an art piece, one can now buy a fraction of a painting. This allows for increased market depth and liquidity.</p> <p>~</p> <p>Any physical good or share in a small- or medium-sized enterprise can also be tokenized at a fraction of what it would cost in the client-server world and divided into representative tokens, which could be traded on an open market.</p>
Chapter References & Further Reading	


## Part 4: Basic Attention Token: Advertising Reinvented

Title	Contents
Basic Attention Token: Advertising Reinvented	<p>The idea of the Basic Attention Token project is to tokenize users’ attention and to create a more transparent and efficient advertising market. The Basic Attention Token reverses the roles of the players in the advertising industry, and redefines the question of who owns your attention and your web browsing experience, and who gets paid for what from whom.</p> <p>[...]</p> <p>As production started to surpass demand, markets became increasingly competitive, products commoditized, and sales and marketing became a way for companies to differentiate their products from the competition. What followed was a sales revolution (1920-1940). A marketing revolution followed (1940-1990), which then led into the finer-grained marketing revolutions of the late twentieth and early twenty-first century, focusing on relationship marketing and social media marketing. Free trade agreements and the emergence of the Internet allowed companies to increasingly outsource production and services to other countries and focus on product design, branding, and advertising.</p> <p>For the first time since the agricultural revolution, humans are approaching a stage where there is an abundance of resources like food, money, and knowledge. <b>Most modern-day shortages are due to allocation inefficiencies, and are rarely a product of real shortages.</b> In the age of information overflow, supply chain optimization, and algorithmic market mechanisms, this inefficiency can be further reduced. While the invention of the printing press in the 15th century can be seen as the first information revolution, the emergence of the Internet brought the second information revolution, and with that, the abundance of information. Data has become the fuel of this information economy, and attention is the scarce resource. <b>As we are approaching a “zero marginal cost society,”83 time and attention are becoming two of the most scarce resources.</b> The amount of time a person has to pay attention to advertising is limited.</p>
Attention Economy, Data Markets & Privacy	<p>Web2 platforms, in particular social media platforms and search engines, did not have a direct business model to generate income from the services they provided. The only thing they had was user data, which served as a basis for targeted advertising based on user behavior. This revolutionized the advertising industry forever. The current ad-tech ecosystem has been developed and is predominantly controlled by two companies: Alphabet (Google) and Facebook. Anything from web-browsing history to location-based data, our everyday movement is being tracked by the companies whose services we use, and then resold to the data brokers of the marketing industry. The data brokers analyze and resell this data to advertisers. Algorithmic methods extract information from this raw data to evaluate which customers are the most relevant for which advertiser. Users today have little or no direct control over what happens with their personal data behind the walled gardens of the servers of the Web2 service providers.</p>
Basic Attention Token (BAT)	<p>The idea is to use cryptographic tokens and a privacy-preserving browser to create a decentralized advertising system. Advertising is performed P2P, directly in the “Brave” browser, a decentralized application that communicates with the Ethereum network and manages two tokens: BAT (Basic Attention Token) and BAM (Basic Attention Metrics).</p> <p>BAT</p> <p>The BAT token can be used as a transfer of value between publishers, advertisers, and users in a way that:</p> <ol style="list-style-type: none"><li>1. users are compensated for viewing ads in a privacy-preserving manner</li><li>2. publishers receive a bigger stake of the ad revenue than they would today</li><li>3. advertisers could gain a better return on investment, as well as more accurate data.</li></ol>

	<div>4. Users can opt to see certain ads from companies they are genuinely interested in, or pay a fee to not see any advertisements at all.</div> <div>BAM</div> <div>Basic Attention Metrics (BAM) allows for the accurate tracking and reporting of user attention directly in the browser. In spite of the fact that the browser constantly tracks one’s attention, this data is anonymized, as it never leaves the browser software locally running on one’s device. In-device machine-learning algorithms determine relevant content for personalized advertising. The “attention value” for each ad depends on how long the ad is viewed and other metrics such as the number of ad pixels that are visible in proportion to relevant content, etc. Data analysis is performed directly on the browser for the sake of serving targeted advertising without revealing the base data to the company that delivers the ad (advertiser). Advertisers have direct access to trustful metrics without the need for third-party tracking and without compromising the privacy of the user. Such a level of disintermediation can improve the effectiveness of targeted advertising.</div> <div>How BAT Works (in detail)</div> <div><ul style="list-style-type: none"><li>• Anyone who downloads the app receives an initial amount of BAT tokens.</li><li>• Advertisers pay publishers BAT tokens to display personalized ads, which are filtered by the algorithm in the Brave browser, based on locally collected data only. This means that users maintain ownership and control over their data. When delivering an ad, the advertisers send BAT tokens in a locked state using a smart contract.</li><li>• If and when users view the ads, the smart contract unlocks the BAT tokens, which compensate the user with up to 70 percent of the advertising revenue. The publisher hosting the advertisement receives the rest, which could incentivize them to deliver relevant quality content instead of random spamming with irrelevant ads. Users can get compensated for their time and attention, and in turn, spend these tokens for other online activities, such as tipping artists and content creators for their free online content.</li><li>• <b>Tipping:</b> This tipping option works in a similar way to services such as “Patreon,” but eliminates the need for third-party services such as Patreon. One could also use BAT tokens to pay for subscriptions, digital goods, and other services in the future. At the time of writing the book, BAT tokens can be used for charity donations to over 1000 organizations, such as the Red Cross or the World WildLife Fund. BAT has partnered with the TAP Network, a rewards-as-a-service tech company, which has more than 250,000 commercial partners such as Amazon, Apple, Walmart, American Airlines, Starbucks, and HBO. Users will also be able to redeem their BAT tokens for rewards from any of those companies, which could be a further incentive for users to adopt Brave and BAT. Furthermore, there are over 28,000 Brave-verified publishers where BAT tokens are also accepted, such as Vimeo, Vice, Washington Post, The Guardian, and MarketWatch.</li></ul></div> <div>Outlook &amp; Challenges</div> <div><ul style="list-style-type: none"><li>• Centralized</li><li>• <b>Fiat Peg.</b> BAT token is pegged to fiat currencies. BAT tokens are not minted upon proof of certain behavior, but were initially funded with fiat money in a token sale. The token flow and value creation in the BAT model seem to be reflecting old-school value creation models, and are based on a pool of pre-mined BAT tokens.</li><li>• <b>Poor Ad Units.</b> While they offer advertisement options in-line with their newsfeed or search results, BAT currently only offers display ads, which is not as attractive to advertisers.</li><li>• <b>Value Transfer In Road Map.</b> The BAT project has it on their roadmap to implement BAT usage beyond advertising use cases, for any in-browser value transfer. Whether they will be able to succeed at implementing this plan remains unclear.</li><li>• Competitors: AdEx (video ads)</li></ul></div> <div>Not From Book</div> <div><ul style="list-style-type: none"><li>• Over 3.8M Monthly Transacting Users have used BAT tokens in the platform, with over 13M Brave/BAT rewards wallets created to date. (January 2021)</li><li>• BAT is one of the most widely utilized tokens, with over 1M verified publishers accepting BAT from Brave Rewards users.</li><li>• <b>Brave Wallet:</b> The foundation for mass adoption and use of crypto and DeFi will be the Brave Wallet, which will unify Brave Rewards, custodial accounts, and best-in-class non-custodial (i.e., the user owns their private key, best stored in a hardware device) accounts in Brave.</li><li>• <b>Brave Search Engine:</b> Brave acquires search engine to offer the first private alternative to Google Search and Google Chrome on both mobile and desktop (March 3, 2021)</li></ul></div>
--	---

Part 4: Token Curated Registries —The New Search?

Title	Contents
Token Curated Registries —The New Search?	Token Curated Registries provide a market mechanism for content curation that could complement centralized curation services. Tokens are hereby used as economic incentives to curate lists, or rank information in such a list, including content feeds in a social network or recommendation algorithms for e-commerce platforms.
How TCRs Work	<p>Token Curated Registries (TCRs) are a market mechanism introduced by Mike Goldin for collectively curating lists in the absence of third-party coordination. Tokens provide an economic incentive to curate lists that are valuable to consumers. Transactions are settled and cleared autonomously by a distributed ledger. TCRs are designed to represent a public good. Anyone can participate.</p> <p><b>Prerequisites:</b> In order to set up a TCR, one needs to</p> <ol style="list-style-type: none"><li>1. Define a purpose for the list</li><li>2. A native token</li><li>3. A governance mechanism that makes sure that all token holders are incentivized to maintain a high-quality list.</li></ol> <p><b>Stakeholders:</b></p> <ol style="list-style-type: none"><li>1. Candidates provide content for the list</li><li>2. Consumers use the list</li><li>3. Curators collectively manage the quality of the list (token holders)</li></ol> <p><b>Process:</b> Candidates have to deposit a certain amount of tokens to apply for the list. Any token holder can participate in the curation process, and has a certain time to cast a vote on whether or not the candidate's application should be included in the list. If they think that the application should be excluded, they can challenge the listing. To do so, they must make a deposit of a certain amount of tokens into a smart contract, locking a part of their network stake. Once a challenge has been initiated, all other token holders can vote by also staking their tokens. If at the end of the voting period, the application is rejected by the majority of token holders, the applicant's deposit is split between the challenger and all other token holders who voted to reject the application. Otherwise the listing of the candidate is added to the registry, and the smart contract distributes the challenger's deposit between the applicant and all token holders who voted for accepting the listing. It is advised that TCRs divide the voting process into two phases, the commit phase and the reveal phase. Results are only openly broadcasted after the commit phase is completed to avoid “coordination attacks,” where one curator could have influence over the voting process of other curators. Tokens are locked in the commit phase and unlocked during the reveal phase.</p> <p><b>Token:</b> Tokens are designed to be transferable and fungible (all tokens are designed to be equal). It is assumed that each list needs their own token to give a reliable signal of the quality of the list and the value of the network. The price of a token is a result of supply and demand, and as such, assumed to be a performance indicator for the collective actions of all token holders. If a TCR would accept a non-native token as a means of payment, such as BTC or ETH, the collective performance of the token holders would not reflect performance of the list and the economic incentive mechanisms would therefore not work. Mechanism Design: The incentive mechanism needs to align incentives in a way to make sure that it pays off for token holders to vote truthfully, and that it does not pay to cheat the system. Candidates who believe they will be rejected are not likely to apply; otherwise, they would lose their tokens. Token holders, on the other hand, could theoretically reject every candidate, but that would collide with their interest to increase the value of their tokens. An empty list is not interesting for anyone. Profitability and quality of all stakeholders need to be well-aligned, so that objective and high-quality lists can be produced.</p> <p><b>Design assumptions:</b> The concept of a TCR is based on the assumption that a free market for listings could potentially provide a better mechanism for quality curation of lists than centrally managed lists and data feeds. It is also assumed that economic actors want to maximize their profits and act rationally at all times. Candidates are assumed to have an interest to be included on the list for advertising purposes, and be willing to pay a listing fee, as placement on such a list serves as validation of quality of their services. Curators, who also have a stake in the network in the form of network tokens, would make more money from well-maintained lists with a lot of traction, which means that they have an incentive to curate the list truthfully. The vote of token holders is proportional to the number of tokens they own, or stake. Proportional voting rights are based on the idea that those who have the most at stake are most incentivized to act in the network's best interest. Consumers, on the other hand, seek high-quality information and use lists to make decisions. If the quality of the listing is good, consumers will be interested in consulting the listing, which will make it more attractive for candidates to apply to be listed and strengthens the overall economy of that list.</p>
Attack Vectors	

Criticisms Of TCRs	However, critics argue that TCRs that use token-weighted votes (i) cannot provide nuanced curation, (ii) cannot replace subjective reputation systems, and (iii) have a problem with “minimum economy” size. They claim that having a stake in a system alone cannot build quality curation, as token holders are more likely to maximize short-term profits, since they can sell their tokens any time and exit the system, which is harmful to the collective quality of the list in the long run. Furthermore, any TCR will need a minimum market size to resist manipulation attempts, which means that new lists have a chicken-and-egg problem. Also, consumers will not be interested in a small or half-empty registry, and candidates won’t be interested to apply to a registry that is not visited by anyone. Another issue is that TCRs are not useful for all types of registries. Bulkin, for example, is an outspoken critic and distinguishes between “subjective TCRs” and “objective TCRs.” In his opinion, a TCR can only be successful if (i) an objective answer to the listing question exists and if (ii) the answer is publicly observable, such as air temperature in a certain geographic area.

Part 2: Web3 Basics

Title	Contents

Part 4c: Social Media

Title	Contents
SteemIT	<p>Steemit is a decentralized social network where contributions to the network get rewarded with network tokens. It runs on the \Steem blockchain, a special-purpose blockchain that provides a public infrastructure for the decentralized social network.</p> <p>----</p> <ul style="list-style-type: none"><li>• SteemIT did a hard fork into Hive</li><li>• As opposed to Web2-based social media applications, Steemit has (i) no advertisements; (ii) all data is public on the ledger, which means that no single institution owns your transaction data; and (iii) contributors to the network are rewarded with network tokens. How much you get paid is a function of the number of your contributions, and the popularity of your contributions. Steemit is permissionless, allowing any user to join for free. Sign up is either by email or phone number and manually verified by an administrator. Alternatively, one can pay a fee to create the account. Both procedures intend to create an effort/cost for account creation, in order to combat spam, bots, and name squatters.</li><li>• <b>History:</b> first and longest-running decentralized application. It was conceptualized in 2015 and has been operational since 2016.</li><li>• <b>Activity:</b> At the time of writing this book, the network has over one million registered users, 25,000 posts, and 100,000 comments, and 1.4 million transactions on the Steem blockchain per day. (Michael note: On May 7, there were 50,000 posts on Bitclout)</li></ul>
Reddit	<p>In May 2020 two subreddits - <a href="#">r/Cryptocurrency</a> and r/FortNiteBR - with over 2.4 million users announced the launch of their own subreddit tokens - MOON and BRICK - that will each be managed by the Ethereum</p>



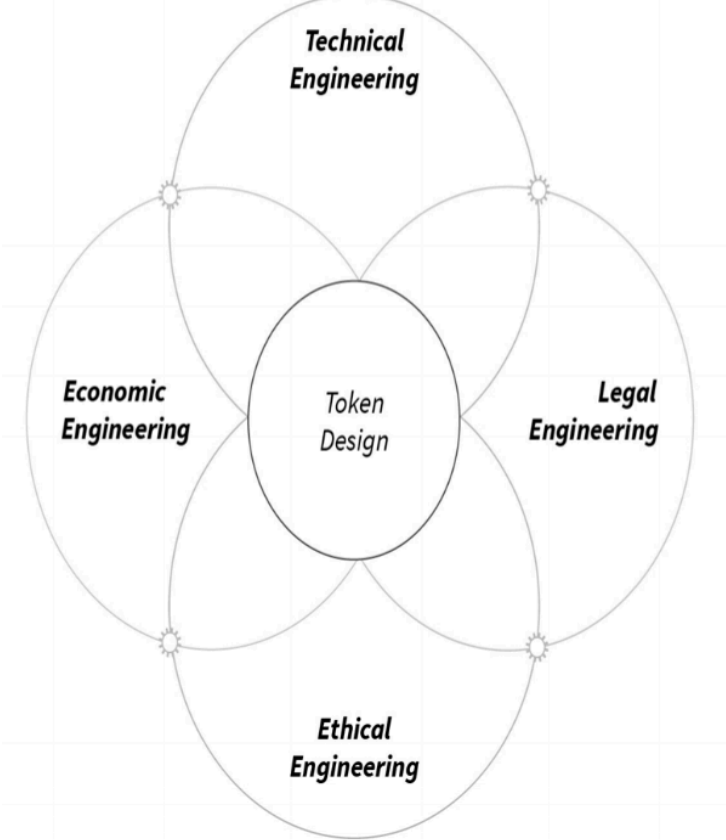
	<p>network. Both tokens could be seen as a test use case for tokenizing all subreddits with their special purpose community tokens. The tokens will be initially managed by the Ethereum testnet “Rinkeby” for a few months before migrating to Ethereum’s mainnet. “Reddit Vault” is an Ethereum wallet integrated into Reddit’s mobile apps and communications with the Ethereum network. Both tokens are designed to be transferable, and users can send their MOON and Brick tokens to any other ERC-20 compatible wallets. The tokens also come with special voting rights within the community, however, it is still unclear how such a voting process will look like. In this initial design, the tokens can be used to animated emojis, exclusive badges and to reply to Reddit comments using gifs. The monetary policy of the tokens varies and can be determined by the community of each subreddit, at least to some extent. This means that each subreddit community will have certain control over the properties and function of the token (issuance rate, minting process, voting rights, transferability, utility properties.)</p> <p>“r/Cryptocurrency” announced that MOON tokens have a fixed issuance rate per month, 5 million MOONs, which will decrease by 2.5% every month until a total of 250 million is reached. “r/FortNiteBR” has not specified an issuance rate for their BRICKS tokens. At the time of writing this book it is still unclear if or when exchanges will list the token. With this move, Reddit is the first Web2 based social media network that has officially announced to tokenize their social media activities. It is likely that other existing social media networks will follow soon. The greatest challenge will be to design the token so the desired purpose of the economic system created by the token cannot be gamed.</p>
--	---

Part 4c: Token Curated Registries

Title	Contents
Token Curated Registries - The New Search?	Token Curated Registries provide a market mechanism for content curation that could complement centralized curation services. Tokens are hereby used as economic incentives to curate lists, or rank information in such a list, including content feeds in a social network or recommendation algorithms for e-commerce platforms.
How TCRs Work	
Attack Vectors	The economics behind the registry needs to be designed in a way that it accounts for all possible attack vectors. A number of attack vectors have been identified, such as “trolling,” “madman attacks,” “registry poisoning,” or “coin flipping.” A solution to each of these potential attacks needs to be reflected in the governance rules of the TCR to guarantee high-quality listings.
Criticism of TCRs	However, critics argue that TCRs that use token-weighted votes (i) cannot provide nuanced curation, (ii) cannot replace subjective reputation systems, and (iii) have a problem with “minimum economy” size. They claim that having a stake in a system alone cannot build quality curation, as token holders are more likely to maximize short-term profits, since they can sell their tokens any time and exit the system, which is harmful to the collective quality of the list in the long run. Furthermore, any TCR will need a minimum market size to resist manipulation attempts, which means that new lists have a chicken-and-egg problem. Also, consumers will not be interested in a small or half-empty registry, and candidates won’t be interested to apply to a registry that is not visited by anyone. Another issue is that TCRs are not useful for all types of registries. Bulkin, for example, is an outspoken critic and distinguishes between “subjective TCRs” and “objective TCRs.” In his opinion, a TCR can only be successful if (i) an objective answer to the listing question exists and if (ii) the answer is publicly observable, such as air temperature in a certain geographic area.
Examples	<ul style="list-style-type: none"><li>• <a href="#">Relevant</a>, Founder <a href="#">Slava Balasano</a> (26,000 members)</li><li>• AdChain</li><li>• <a href="#">Distric0x</a></li><li>• Messari - <a href="https://messari.io/article/token-curated-registries-tcr">https://messari.io/article/token-curated-registries-tcr</a></li><li>• <a href="#">Kleros</a></li></ul>

Part 4d: How To Design A Token System

Title	Contents
-------	----------

<div>How To Design A Token System</div>	<div>If you would like to tokenize your business or community and make it Web3 ready, how do you need to approach your token design? Which questions do you have to ask yourself? What know-how do you need in your team to be able to properly “design” or “engineer” these tokens? The aim of this chapter is to understand what questions are relevant in the design and engineering process of a new token system, depending on what type of token you want to create.</div> <div><div>Token Engineering</div></div>
<div>Technical Engineering</div>	
<div>Economic Engineering</div>	
<div>Ethical Engineering</div>	
<div>Chapter Summary</div>	<div>The terms “design” and “engineering” are closely related but not the same. Rather, they complement each other. While the term “design” might be a more known and intuitive term, carrying a more subjective, creative, and even artistic meaning, the term “engineering” tends to bring to the forefront the technical aspects, the composition of inert parts to create a predictable and robust whole.</div> <div>Design is a part of an engineering process. The term “engineering design” is used to describe the part of the engineering process which is open ended and ultimately more subjective. Similar to electrical engineering and public policy design, token engineering is about rigorous analysis, design, and verification of systems and their assumptions. Their assumptions need to be assisted by tools that reconcile theory with practice. As opposed to electrical engineering, designing human behavior is much more similar to steering national economies, and public policy design, as it requires much more “fuzzy” modeling techniques.</div> <div>With the emergence of AI and better simulation tools, we might be able to design and deploy more effective purpose-driven tokens that also factor in unknown probability distributions, unknown or adversarial behaviors of agents, potential network externalities, and “tragedy of the commons” incurred to other parts of society.</div> <div>Engineering is the practice of creating a technology that ultimately always has a social goal. Looking at engineering though a purely technological lens perpetuates a reductionist mindset on why and how we build technology. There seems to be a growing understanding for the need of using the term “engineering” in the broader sense when designing a token system.</div> <div>Technical engineering relates to the technical questions of creating an infrastructure token or an application token, and how to technically implement the token system: Infrastructure tokens or application tokens? Security aspects address the design of the cryptoeconomic mechanisms to provide the level of security</div>

needed. Scalability aspects address the trade off between security, decentralization, and scalability. Privacy aspects address the questions of what type of cryptography should be used to allow for the right “privacy by design.”

Legal Engineering of tokens is the predominant task when we deal with “simple token systems.” The term “simple” is commonly used in the complex systems domain. In the context of token engineering, the term “simple” refers to the fact that the dynamics of the business or governance models of a potential token are well known, as in the case of (i) central bank money, (ii) securities and other assets, (iii) identification and certification processes, (iv) voting rights, (v) vouchers and coupons, or (vi) entry tickets and other access rights. Tokenizing known business/governance processes requires making the tokenization of existing assets, access rights, and voting rights legally compliant with local legislation.

Economic engineering is predominantly required when designing “complex token systems.” The incentives and governance rules of the community are tied to “purpose-driven tokens” that steer collective action of the community through automated mechanisms. The tools that are necessary to design such systems can be found in economics, network science, cyber-physical systems, and sociotechnical systems. The main questions that need to be answered in such design processes deal with the following questions: What kind of system do you want to create? How many different token types do you need? Purpose? Properties: Transferability, fungibility, expiry date?

The design of token systems also requires ethical and political thinking. What type of system we want to create is not a technological question but a socio-economic and political question. Questions of politics, morals, and ethics will need to be answered, ideally before the design of such systems, the most important of which revolve around the questions of “transparency vs. privacy” and “power structures.” If we fail to incorporate ethical questions in the design thinking process of such systems, we will create “protocol bias.”

Having lawyers, economists, and social scientists as part of the team in addition to the technical engineers, on executive level and below, will be paramount to developing resilient token systems. However, interdisciplinary work takes time and effort, as all four categories overlap and communication between the disciplines requires some ramp-up efforts.



## Highlights

### Kindle Popular

The Bitcoin network and other distributed ledgers all represent a collectively maintained public infrastructure and are the backbone of the next generation Internet, what the crypto community refers to as the Web3.

**If we assume that the WWW revolutionized information, and that the Web2 revolutionized interactions, the Web3 has the potential to revolutionize agreements and value exchange.** The Web3 changes the data structures in the backend of the Internet, introducing a universal state layer, often by incentivizing network actors with a token. The backbone of this Web3 is represented by a series of blockchain networks or similar distributed ledgers.

While the Web2 was a front-end revolution, the Web3 is a backend revolution.

### Web3 Protocols

Apart from computation we need file storage, messaging, identities, external data (oracles) and many other decentralized services. A blockchain network is simply the processor for decentralized applications that operate on top of the Web3. It serves as a distributed accounting machine recording all token transactions and performing computation.