Token Economy

Author	Goodreads Link	Rating
Shermin Voshmgir	https://www.goodreads.com/book/show/54222022-token-economy?ac=1&from_search=true&qid=3FPinqzG2r&rank=1	***

Overview

Tokens - often referred to as cryptocurrencies - can represent anything from an asset to an access right, such as gold, diamonds, a fraction of a Picasso painting or an entry ticket to a concert. Tokens could also be used to reward social media contributions, incentivize the reduction of CO2 emissions, or even ones attention for watching an ad. While it has become easy to create a token, which is collectively managed by a public Web3 infrastructure like a blockchain network, the understanding of how to apply these tokens is still vague.

The industry keeps referring to "Blockchain" as different from "Bitcoin," creating an artificial divide that is often misleading. There seems to be too little understanding about the fact that Bitcoin is a blockchain network, which is (a) globally managed by people who mostly do not know each other, and (b) enabled by the consensus protocol that (c) incentivizes all network actors for their contributions with a native token. The governance rules are tied to the minting of a native blockchain token. The Bitcoin token can, therefore, be seen as the currency of a distributed Internet tribe, called the Bitcoin network, where network actors are rewarded with Bitcoins, just as the Ether is the currency of the distributed Internet tribe Ethereum network, or Sia is the native currency of the Sia network. 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.

This book attempts to summarize existing knowledge about blockchain networks and other distributed ledgers as the backbone of the Web3, and contextualize the socio-economic implications of the Web3 applications such as smart contracts, tokens, and DAOs to the concepts of money, economics, governance and decentralized finance (DeFi).

Notes

Part1: Web3 Basics

In this context, blockchain networks seem to be a driving force of the next-generation Internet, what some refer to as the Web3. They reinvent the way that data is stored and managed over the Internet, providing a unique set of data—a universal state layer—that is collectively managed by all nodes in the network. This unique state layer, for the first time, provides a native value settlement layer for the Internet in the absence of intermediaries. It enables true P2P transactions, and it all started with the emergence of Bitcoin.

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

In the Web3, values are represented by cryptographically secured tokens.

If you can't hold state in the Internet, you cannot transfer value without centralized institutions acting as clearing entities.

As a result of this, users are paying for services with their private data.

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.

People and institutions who do not know or trust each other, reside in different countries, are 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.

Decentralized & Autonomous Organization (DAO): The ledger is collectively managed by autonomous network nodes, which is why it is also heralded a new form of organizational infrastructure often referred to as Decentralized Autonomous Organization

The underlying challenge of a P2P network with a set of anonymous network nodes is how to deal with malicious network nodes in the absence of centralized parties securing the system. One must always assume that there will be bad actors trying to disrupt any open and public network. How can such a distributed network reach consensus about which data is correct or which is not correct, or which process is true or false in such an untrusted setup? This is referred to as the "Byzantine Generals Problem."

Before the emergence of Bitcoin, it was believed to be impossible to achieve fault-tolerant and attack-resistant consensus among untrusted nodes in a P2P network.

Cryptoeconomics can be defined as the study of economic interaction in untrusted environments, where every actor could potentially be corrupt.

The Bitcoin network is the first practical instance of cryptoeconomics. It produces "trust by math" rather than "trust by legal contract."

Proof-of-Work is designed in a way that (i) if you spend money and play by the rules, you can earn network tokens; (ii) it doesn't pay to cheat because mining requires special-purpose computer hardware and consumes large amounts of power.

The Bitcoin network is (i) open source, (ii) public, and (iii) permissionless.

A Proof-of-Work network is safe as long as more than 50 percent of the work is being put in by miners who are honest.

Online tool to check what it would cost to attack the Bitcoin network: https:// gobitcoin.io/ tools/ cost-51-attack/

What a 51 percent attack cannot do is change existing transactions or fake transactions, like: (i) changing the amount sent in an existing transaction; (ii) changing the recipient of an existing transaction; or (iii) sending someone’s tokens without their approval. This is because all transactions need to be signed with the private key of the token owner, which cannot be revealed by majority agreement of the network.

The “length of the blockchain” refers to the network branch with the most cumulative Proof-of-Work, not the one with the most blocks.

Furthermore, alternative distributed ledger systems have emerged with completely different types of consensus mechanisms, such as directed acyclic graphs (DAGs) that do not require the creation of a chain of blocks anymore, and instead use alternative cryptoeconomic mechanisms to reach consensus. Examples of networks that use DAGs as a consensus mechanism are “IOTA,” “Byteball,” or “Nano.”

An analog example for a public key would be the example of a padlock. If Bob wants to send a message to Alice, but is scared that somebody might intercept and read it, he will ask Alice to send her padlock (unlocked) over to him, and to keep her key to that padlock. Bob can now put his letter in a small box and lock it with the padlock that Alice sent him, closing it with a simple push. The letter can now be sent around the world without being intercepted by an unauthorized person. Only Alice, who has the key to her padlock, can open the letter.

Hashing in the Bitcoin network is part of the following processes: (i) encoding wallet addresses; (ii) encoding transactions between wallets; (iii) verifying and validating the account balances of wallets; and for the consensus mechanism (iv) Proof-of-Work.

Alice now broadcasts this transaction to any computer in the network: she sends out both the plaintext transaction and the signed hash (automatically performed by her wallet software).

KERI (Key Event Receipt Infrastructure) is a novel technology-a type of consensus network-that allows to move certain functions of decentralized identity-management systems off-chain to a different layer, and minimize the role of the distributed ledger. The aim is to provide a simple, scalable, more modular, identity-management system that is more interoperable across different blockchain networks and other distributed ledgers.

One of the most interesting future use cases will be the digital identification of objects. Currently, most Internet-of-Things (IoT) devices have no secure digital identity and access management capabilities. A DID-powered serial number can make any object in the Web3 addressable. Once we start tagging objects with mini computers (crypto accelerators) that come with a DID-powered serial number and communicate with a distributed ledger network, any object along the supply chain can prove ownership and credentials to others in the network using cryptographic proofs.

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.

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 cryptography. Once signed by an issuer, credentials can be managed using the wallet of the identity owner directly.

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.”

Part 2: Web3 Applications

A more complex example of a smart contract is the use case of a 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.

Token holders running full nodes and developers might prefer upgrades that result in lower transaction fees. Miners will find such a proposal unattractive, since transaction fees are a source of income for them. They might favor protocol upgrades that would yield larger block rewards, which would increase the inflation rate and thus would probably not be in the long-term interest of any of the stakeholders involved.

Part 4: Token Use Cases

networks. The most important design questions in

The quick and dirty approach of the Web1 and Web2, where the development process was rather “hack now and pivot later” oriented, does not play out well in the Web3.

#books #booksummaries #web3