CrushCrypto

What is blockchain technology?

Educational Series

September 2, 2018

Introduction

- The most significant achievement in the early stages of the internet was the ability to transfer data in the form of messages, pictures, music, and more. This advancement ushered in a new era of civilization, one where people had access to an ever-growing collection of knowledge and ideas.
- However, because data can be copied and distributed by anyone on the internet, there was no way to digitally transfer money between two parties in a secure way. Transactional data could easily be copied or falsified, meaning transfers of value required a third party for verification.
- The invention of blockchain tackled this issue – it allows for the secure transfer of value between any two parties with an internet connection.

Overview

- A **blockchain is a distributed ledger of data that is maintained and updated by a network of computers across the globe**. The data is packaged into blocks, and each one contains a timestamp and a cryptographic link to the previous block.
- The first widespread implementation of blockchain technology came along with the release of Bitcoin in 2009 by an anonymous person/entity named Satoshi Nakamoto.
- The Bitcoin blockchain is used as a ledger containing all wallet balances and transactional data, keeping records that are secure and immutable – effectively impossible to change once they are stored on the blockchain.
- After Bitcoin, more projects have been released that explore the possibilities of blockchain beyond wallet balances and transactional data. Blockchain technology has the potential to optimize processes in industries such as insurance, healthcare, real estate, and more, and the use cases are just starting to be explored.

How does it work?

- A blockchain is a distributed database where data is packaged into blocks and added to the database by computers (called nodes) across the world. These nodes work together to achieve a consensus on new data that is being added to the blockchain.
- A new block contains a timestamp of when it was created, and a hash of all the data (transactions, difficulty target, etc.) in the previous block.

How does it work? (continued)

- Hashing is a cryptographic process where a big chunk of data is converted into a much smaller string of numbers and letters. The process creates a completely different hash for every unique set of data, even if the change is just one letter or number.
- Therefore, each block contains a hash of the data in the previous block, and that block contains the hash of the data from 2 blocks ago, which includes the hash of the data from 3 blocks ago… and so forth. Each new block of data is cryptographically connected to the block before it, securing the entire chain together.

Consensus protocol

- There are many protocols that regulate how nodes achieve consensus, but the most popular is proof-of-work. Proof of work was implemented into the Bitcoin blockchain at its inception and is the consensus mechanism of many other large networks such as Ethereum.
- While data is being added to the current block, other computers called miners are attempting to crack a code that validates the block. After validation, the “winning” miner broadcasts the result at which point the block is sealed and miners move on attempting to guess the next block’s code.
- The mining process is comparable to guessing a random long password – the more computing power you have, the faster you can make guesses thus giving you a better chance to validate the current block.

Consensus protocol (continued)

- People are incentivized to use their computers as miners through automatically distributed block rewards, where the first miner that correctly guesses the next block's code receives an allocation of new coins.
- The inflation rate is programmed into the blockchain and there is no other way to mint new coins. This incentivization is extremely important because miners are the main actors in protecting the network from malicious actors.
- However, to beat the rest of the network in mining the block and continue beating them afterwards, at least 51% of all the network's computing power is required. This is called a 51% attack and is the main security vulnerability in a proof-of-work blockchain system. It's also the reason why a blockchain is more secure as the number of miners and difficulty of mining go up.

Wallets

- The main way to interact with a blockchain is through wallets, which allows users to own, send, and receive assets.
- Each wallet has a public address and an associated private key, where both are strings of numbers and letters. The public address can be generated from the private key, but the process is not reversible as a private key can never be derived from a public address.
- The public address can be thought of as a physical home address; it is public for anyone to see and used to receive mail or packages – but in this case it is assets on the blockchain.
- The private key is like your house key in the sense that only you, the home owner, should ever have access to it. If you give away your house key, anyone can enter your home and steal the contents of your house. If you give away or have your private key stolen, that person then has full access to move funds out of your blockchain wallet.

Summary

- Blockchain technology is a distributed database that solves two of the major hurdles facing the internet: (1) transferring assets in a P2P fashion and (2) immutable data.
- A blockchain works by utilizing nodes and miners to validate and update the data being added to the database. Miners are incentivized to contribute their computing power to the network through block rewards, where new coins are minted.
- Each block of data is cryptographically linked to the previous block, connecting from the current block to the first block ever created. This mechanism secures the data on the network and ensure malicious actors cannot change a blockchain's data at will.
- Wallets are the main interface for interacting with the blockchain and are comprised of a public address and private key. The public address can be seen by anyone and is used for receiving coins, while the private key is the only way to send coins out of your wallet.

CrushCrypto