CPSC 467: Cryptography and Security

Michael J. Fischer

Lecture 24b
December 1, 2020

- Blockchains

- Bitcoins

Blockchains

Blockchains

The theoretical concept of a *Blockchain* is a distributed database built using cryptography. It has several nice properties:

- It is a decentralized, anonymous and public digital *ledger*, managed by collectively trusted servers.
- Entries are indelible, that is permanent and unchangeable.
- Additions to the blockchain are immediately visible to everyone.
- A blockchain gives a unique, public, global, and consistent view of its data.

The problem is that real implementations cannot fully implement the theory.

How a blockchain works

A blockchain (*ledger*) is a record of transactions.

- It consists of a list of *blocks*, linked together using cryptographic hash functions.
- Each block contains a list of *transactions*, the author ID, and a cryptographic hash of the prior block in the chain.
- The chain is managed by a peer-to-peer network of maintainers (often called *miners*) who follow a protocol for communication and validation.
- Once recorded, the data in a block cannot be changed without changing the prior-block hashes of all subsequent blocks.
- As time passes and more blocks are added, it becomes very unlikely, but not impossible, that a given block will change.

How blockchains grow

From time to time, a miner will process a batch of properly signed transaction requests by placing them in a new block and attaching that block to the current blockchain, thereby *extending* it.

The miner checks the validity of the transactions before placing them in the block, and anyone can subsequently do the same in order to verify the validity of the new chain.

The miner then sends the updated chain to all other miners.

Any miner receiving a valid chain that is longer than the one it currently knows about will discard the current chain and accept the new one as current.

Forking

- A *fork* happens when two different blocks (call them A and B) are created at the same time in different parts of the network. Both will be used to extend the current chain, and both will be propagated to the other miners.
- Propagation across the net takes time. During that time, both new blocks are circulating among the miners. Some miners will receive A first; other will get B first.
- At this point in time, some miners have the new chain ending in block A, whereas others have the new chain ending in block B.
- The chain has thus forked into two parts that differ in their last block.

Reaching consensus

To achieve a single consistent ledger, the miners must somehow agree on which of the new chains to accept as genuine.

There are two different mechanisms in use for doing so.

1. They can run a *consensus protocol* in order to agree among themselves which of the two chains to accept as valid.
2. They can do nothing and hope that the next time one of the forks is extended (either A or B), the new longer chain will reach all miners before another block is added. In this case, all miners will adopt the new chain and discard all shorter chains. This only works if the rate of adding new blocks is sufficiently low.

Transaction commitment

A transaction to a database is said to be *committed* if it is permanently in the system and cannot be rolled back.

If a transaction appears in block A of a fork but not in block B, then the transaction might not be committed to the ledger and could later disappear from the blockchain altogether.

If the miners reach consensus, then the transactions in the agreed-upon block are committed.

But if the miners simply hope agreement happens because one chain overtakes all the others, no one can ever be assured that a transaction has committed.

Bitcoins

Bitcoin history

- Bitcoin was invented by an unknown person writing under the pseudonym Satoshi Nakamoto. A link to his original whitepaper can be found here.
- Bitcoin was the first popular cryptocurrency; Ethereum branched from it and uses slightly different protocols. Many current cryptocurrencies use the same or similar software protocols.
- Blockchains were introduced along with *Bitcoin* and are used to implement it. They address the forking problem by using a mechanism called *proof of work*.

Some properties of Bitcoin

Bitcoins are a kind of virtual digital currency based on cryptography.

- They exist only in the cloud.
- Their supply is limited.
- Like commodities, their value goes up and down depending on market forces.
- They can be used for online transactions without involving a central party, but most users transact with a Bitcoin exchange.
- Bitcoin transactions are (in some circumstances) anonymous and are a favored medium of exchange for illegal transactions.

Bitcoin exchange

Bitcoins are bought and sold on exchanges such as CEX·IO or coinbase, where today's bitcoin price is around $19,000 USD.

Bitcoins are volatile. The next slide shows the price for Bitcoin (BTC) since Aug 16, 2010.

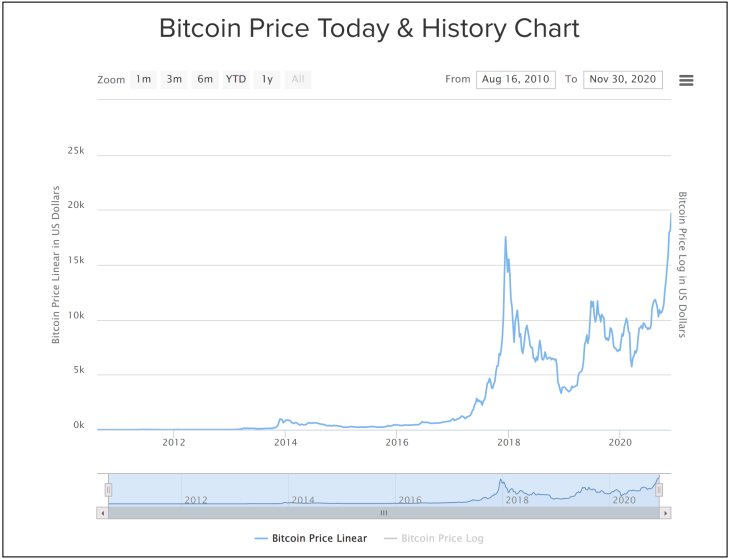

Image from https://www.buybitcoinworldwide.com/price/