Unit 2: Bitcoin Intro

SI 486I: Randomized and Blockchain Technology

Assoc. Prof. Daniel S. Roche
United States Naval Academy

Spring 2022

Goals of this unit

We want to understand at a high level:

- Blockchain
- Mining
- Transactions
- Bitcoin and friends

Details will come later — this is "big picture" time.

Brief history

- David Chaum: "Blind Signatures for Untraceable Payments", CRYPTO 1982.
- Cyntha Dwork & Moni Naor: "Pricing via Processing or Combatting Junk Mail", CRYPTO 1992.
- Adam Back: Hashcash, Cypherpunks mailing list, 1997
- Satoshi Nakamoto: "A peer-to-peer electronic cash system", 2009
- Vitalik Buterin: Etherium white paper, 2013
- Total market cap of cryptocurrencies exceeds $1 trillion USD, January 2021

Blockchain

The blockchain is...
A **distributed**, **immutable linked list** of **data blocks**.

Blockchain

The blockchain is...
A **distributed**, **immutable linked list** of **data blocks**.

Key Technology: Cryptographic hash

How do we make immutable links between blocks?

A cryptographic hash turns any data into a digest that is always:

- The same length (such as 32 bytes)
- Unique*
- Random*

*Technically false, but we act like these are true

Mining: Adding blocks

- "Immutable" blockchain means removing or altering blocks is impossible
- Adding blocks is slow but possible.
- **Crucial**: "mining" a new block is very slow, but *checking* it is fast!

Key Technology: Cryptographic puzzles

How do we make mining slow but verification fast?

Motivation: puzzles like Sudoku (or other NP-complete problems. . .)

Cryptographic puzzle properties:

- Puzzle instance randomly generated from previous block hash and current block contents.
- Only way to solve: many "guess-and-check" iterations
- The first to solve the puzzle gets to mine the next block!

(As it turns out, the puzzles also use cryptographic hash functions.)

Transactions: the contents of blocks

Transactions are "ledger entries" like:

```
Send 20.3 BTC from account 4f58e3 to account 7cc201
```

- Each transaction is signed by the sender
- The signatures are easy to check, impossible to forge
- Not complete until a miner adds it to a block.

Key Technology: Digital signatures

Properties of a cryptographic digital signature:

- Can add signature to any amount of digital data
- The signature has fixed size (e.g., 64 byte)
- Anyone can easily verify a signature matches a given identity
- Only someone with the corresponding secret key can make a signature
- Prevents someone else from spending your BTC!

Notice, kind of similar to hash except you need a secret key to compute it

Verifying a block

What do all network nodes check when a miner submits a new block?

- Block has link (hash digest) back to end of existing blockchain (*)
- Miner has solved the cryptographic puzzle
- All transactions are signed by the senders
- All transaction "inputs" haven't been spent before

Fees

- Transaction not complete until added to a new block
- Only miners are able add new blocks...

Comparison

Similarities to Venmo:

- All transactions are public
- . . . but don't reveal the actual human behind each account.
- The system doesn't know what the payment is for
- Impossible to get a refund once the transaction goes through
- Users must (separately) transfer $USD in and out of the system

Differences:

- Bitcoin is not run by a single entity (decentralized)
- Value of BTC vs USD fluctuates (wildly!)

Useful as money?

Recall the properties money should have:

- Scarce
- Easy to store
- Divisible
- Hard to forge
- Easy to trade