CS5412 / BLOCKCHAIN CONTENT (ENRICHMENT/REVIEW)

Ken Birman

Fall, 2022

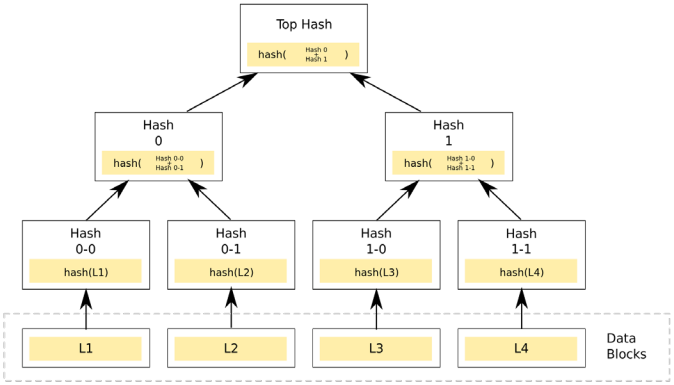
RECAP: BLOCKCHAINS

Blockchains are just append-only logs holding records. However, unlike Paxos and Derecho, they normally are used in Byzantine settings.

The term means "adversarial". A blockchain is designed to operate well even under a moderate attack.

Two important forms of attack are denial of service (DDoS) and Sybil attacks. A Sybil attack is one where some single user mimics a big data center by running lots of VMs, hoping to "outnumber" the other users.

WHAT IS IN A RECORD?

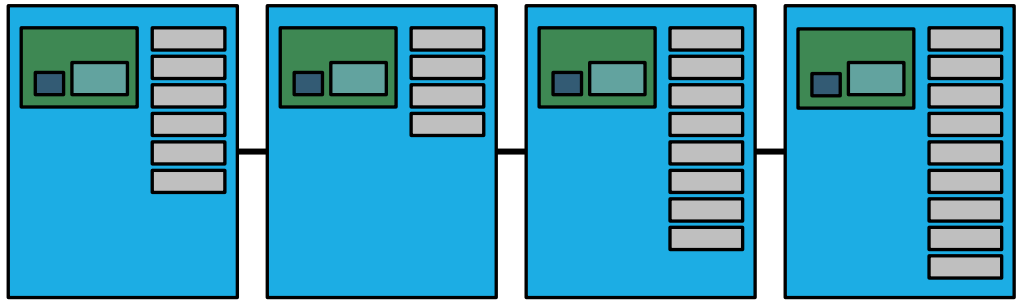


A Merkle tree of signatures… each entangles two integer "hashes"

Leaf nodes are transactions encoded as smart contracts in Ethereum or Hyperledger or a similar language

The root of the Merkle tree also has a field for the hash of the tail record of the current blockchain, and for an integer "nonce" (random value).

GROWING A BLOCKCHAIN

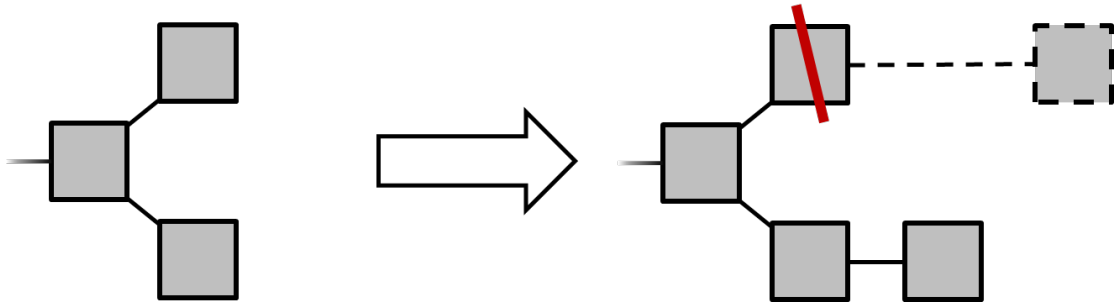


Typically, you first collect the transactions you wish to place into the block

Now you construct the Merkle tree by hashing the transactions and combining the hashes in a binary manner

Fill in the field that holds the hash of the last block on the current chain. Now search for a nonce value such that the hash of your block is smaller than some target value (an integer with some number of leading zeros).

FORKS



Rule: Adopt the longest chain your system learns about. A fork arises when two miners concurrently discover candidates for the next block. Some adopt one, some adopt the other.

When an extension to one chain is found, the shorter chain is abandoned (unless someone shows up with an even longer extension that builds on the short one).

Block "buried" under six other blocks is stable: Rollback unlikely, safe to trust it.

THE SLOW LEMONADE ISSUE

In lecture 14, two children sold delicious lemonade

This woman bought a cup using a bitcoin, but then she had to wait for an hour before her purchase was considered stable.

This is a problem with proof-of-work. **Proof-of-stake eliminates rollback: A majority "vote" finalizes the position of a block.** But it favors rich participants. Many blockchain users reject proof of stake.

ENTANGLEMENT, AND OTHER CRYPTO TOOLS

We say that the blocks on the chain are *cryptographically entangled*

This is one of several uses of cryptography. We also learned about

- Hash functions. They take a block of data and reduce it to an integer
- Encryption/decryption, especially with RSA
- Blinded signatures where a record can be "notarized" yet with its content hidden from the system that signs it.

SOME BASIC USE CASES

Other than for entanglement this allows us to:

- Send a message from A to B, such that only A could have sent it
- Send a message from A to B, such that only B can read it
- Create a blockchain record that has hidden content, but that can be revealed later (e.g. in the event of a dispute)
- Confirm that A owns bitcoin X or NFT X
- … etc

ANONYMITY

In blockchain, this means “nobody knows who I am”

Normally, a user will create one or many (public-key,private-key) pairs

The public keys are anonymous names of this user. The private keys allow the user to “prove” ownership of the public key. Then a coin, for example, can be “owned by public-key X”. Only Y, who has the private key for X, can spend this coin.

BUT THIS IS NOT THE SAME AS ANONYMITY IN A PUBLIC SETTING

In the real world, you are anonymous if nobody knows your identity

But with blockchain, the main uses are *financial*

- Create or purchase coins, sell them, wallets (like bank accounts), etc
- The blockchain can be anonymous, but when you convert cash to coins or coins to cash, that links the chain to the outside world
- A smart sleuth can link the two "graphs" and deduce a lot about you. Tax evasion or money laundering could actually be traced.

THREE FORMS OF BLOCKCHAIN

Permissionless, anonymous: Like Bitcoin. This approach uses a fully distributed and anonymous model, with proof-of-work to prevent Byzantine attacks from disrupting the system.

Permissioned, anonymous: Like Hyperledger. Uses proof-of-stake records in the blockchain itself to authorize mining for new blocks. Majority approval by the current set of witnesses needed to append a new record.

Permissioned, not anonymous: Paxos or Derecho are in this category. They don't normally entangle blocks… but they could! No need for "proof-of-xxx"

TODAY'S LIMITATIONS

You can use your crypto coins to buy an NFT of Banksy's **Love isin the Air**!

Blockchains work well for basic financial tasks, NFTs

But they are hard to use for records from IoT settings, or collaborating companies that hoped the chain could be a shared ground truth

- Rollback can be problematic
- Huge energy costs of proof of work are a concern
- The blockchain isn't a "database" but companies want to treat it as one

VEGVISIR, EMR CASES

We also looked at the idea of using BlockChain for farming, or for a hospital collaborating with other hospitals.

These are *good* questions, and worth exploring.

But they are also complex projects that require a lot of thought and many questions arise that go beyond what BlockChain can do today. They are really research topics, not yet mature business opportunities.