Financial applications of blockchains and distributed ledgers

Master's program in Financial Engineering

Jiahua (Java) Xu

Session 2

Housekeeping

Time and venue

Three sessions: 15:15 – 16:10, 16:25 – 17:20, 17:35 – 18:30

Tuesdays, on Zoom, https://epfl.zoom.us/j/4897861984

To-do's

1. From a group.
2. Vote for the submission deadline.
3. (optional but appreciated) Contribute to the class discussion, on Moodle or live on Zoom.
4. (optional) The missing recording from last time . . .

From the previous lecture

Hyperinflation in Zimbabwe and Venezuela

1. Deficit government spending
2. National debt
3. Heavy money-printing

Special Drawing Right (SDR)

1. “IMF members can also use SDRs in operations and **transactions involving the IMF**, such as the **payment of interest on and repayment of loans, or payment for future quota increases**.”
2. Facebook’s Libra: “LBR will not be a separate digital asset from the single-currency stablecoins. Under this change, LBR will simply be a digital **composite of some of the single-currency stablecoins** available on the Libra network. It will be defined in terms of fixed nominal weights, such as the **Special Drawing Rights (SDR)** maintained by the International Money Fund (IMF). LBR can be used as an efficient **cross-border settlement coin** as well as a neutral, low-volatility option for people and businesses in countries that do not have a single-currency stablecoin on the network yet.”

Recap

1. Double spending
2. Digital signature
3. Cryptographically secure hash function
4. Proof of work

Bitcoin consensus algorithm (simplified)

Proof-of-Work

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. In each round, a random node gets to broadcast its block.
    - random: not selected, but through competition (**work**)
4. Other nodes accept the block only if all transactions in it are valid (unspent, valid signatures).
5. Nodes express their acceptance of the block by including its hash in the next block they create.

What do miners compete to solve?

Hash puzzle

$$H(nonce \| PrevHash \| tx1 \| tx2 \|) < target$$

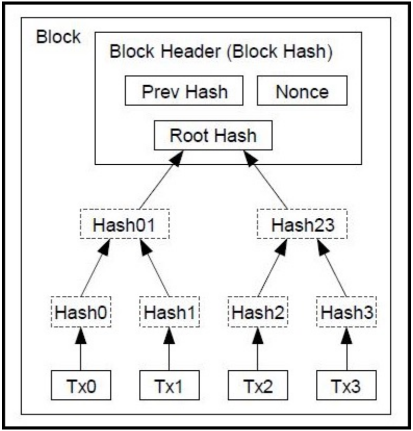


Figure 1: A block on the Bitcoin blockchain hased in a merkle tree

Benefit of using Merkle tree

Efficiency in data validation and storage: checking and downloading in branches

Solving hash puzzles is probabilistic, because nobody can predict which nonce is going to solve the hash puzzle.

recall: Sybil attack

51% Attack?

Attacker has to subvert not only **the consensus process** (by having 51% computing power) but also the cryptography!

Adjustable difficulty level

- Average block time: 10 min
- Target recalculated every 2,016 blocks – every two weeks.

Fork

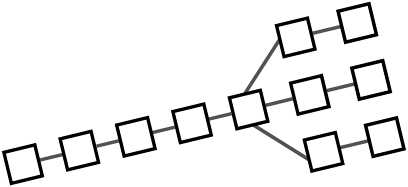


Figure 2: A blockchain fork

Miners diverge and start adding blocks to two chain branches

Heuristic

Follow the longest chain

Incentives

Block reward

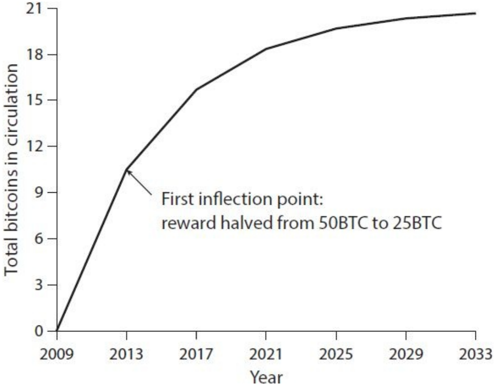


Figure 3: Total supply of bitcoins with time. The block reward is cut in half every 4 years, limiting the total supply of bitcoins to 21 million. This is a simplified model and the actual curve looks slightly different, but it has the same 21 million limit.

Transaction fee

- The initiator of any transaction can choose to make the transaction output(s) $<$ input(s).
- Whoever creates the block that first puts that transaction into the block chain gets to collect the difference, which acts a transaction fee.

One stone two birds:

1. Encourage block building
2. Encourage honest behavior

The economics of mining

$$\mathit{MiningReward} = \underbrace{\mathit{BlockReward} + \mathit{TransactionFee}}_{\text{Probablistic}}$$

$$\mathit{MiningCost} = \underbrace{\mathit{HardwareCost}}_{\text{FixedCost}} + \underbrace{\mathit{OperatingCosts}}_{\text{Variable Cost}}$$

If $\mathit{MiningReward} > \mathit{MiningCost}$, then the miner makes a profit.

Complications

- Other miners' hash rate?
- Denominations: USD/Bitcoin?
- Honest/dishonest?

Research question

Is the default miner behavior a *Nash equilibrium*? That is, does it represent a stable situation in which no miner can realize a higher payoff by deviating from honest behavior? (Narayanan et al. 2016)

Other consensus mechanisms

Proof of stake (PoS)

- Randomized block selection based on size of stake
  - Nxt
- Delegated proof of stake
  - EOSIO: Users stake `EOS` tokens to their favored block producers (BPs, 21 in total) and can choose to remove their stake at any time.
  - Tezos (Liquid Proof of Stake): number of consensus participants—or “delegates”—changes.

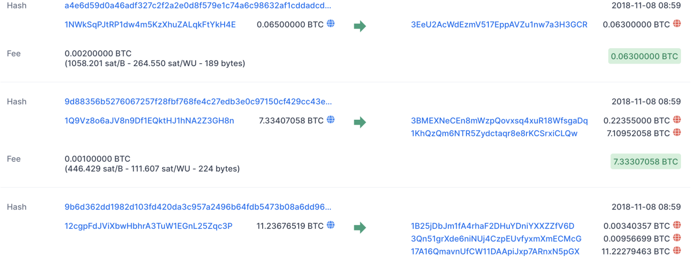
XRP Ledger Consensus Protocol (XRP LCP)

- Each user sets up its own unique node list of validators (UNL) that it will listen to during the consensus process. The validators determine which transactions are to be added to the ledger.

Bitcoin vs. Ethereum

Record-keeping model

BTC



Hash a4e6d59d0a46adf327c2f2a2e0d8f579e1c74a6c98632af1cddadcd... 2018-11-08 08:59

1NWkSqPJtRP1dw4m5KzXhuZALqkFtYkH4E 0.06500000 BTC → 3EeU2AcWdEzmV517EppAVZu1nw7a3H3GCR 0.06300000 BTC

Fee 0.00200000 BTC
(1058.201 sat/B - 264.550 sat/WU - 189 bytes)

0.06300000 BTC

Hash 9d88356b5276067257f28fbf768fe4c27edb3e0c97150cf429cc43e... 2018-11-08 08:59

1Q9Vz8o6aJV8n9Df1EQktHJ1hNA2Z3GH8n 7.33407058 BTC → 3BMEXNeCEn8mWzpQovxsq4xuR18WfsgaDq 0.22355000 BTC
1KhQzQm6NTR5Zydctaqr8e8rKCSrxiCLQw 7.10952058 BTC

Fee 0.00100000 BTC
(446.429 sat/B - 111.607 sat/WU - 224 bytes)

7.33307058 BTC

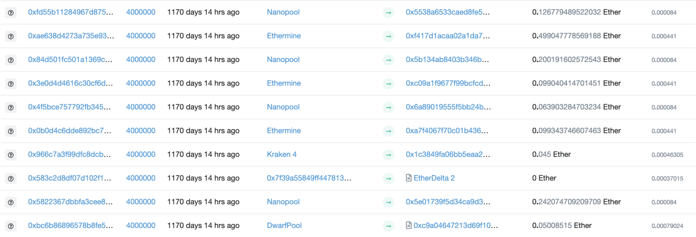
Hash 9b6d362dd1982d103fd420da3c957a2496b64fdb5473b08a6dd96... 2018-11-08 08:59

12cgpFdJViXbwHbhrA3TuW1EGnL25Zqc3P 11.23676519 BTC → 1B25jDbJm1fA4rhaF2DHuYDniYXXZZfV6D 0.00340357 BTC
3Qn51grXde6niNUj4CzpEUvfyxmXmECMcG 0.00956699 BTC
17A16QmavnUfCW11DAApiJxp7ARnxN5pGX 11.22279463 BTC

Figure 4: UTXO (Unspent Transaction Output)

Privacy through change addresses

ETH



?	0xfd55b11284967d875…	4000000	1170 days 14 hrs ago	Nanopool	→	0x5538a6533caed8fe5…	0.126779489522032 Ether	0.000084
?	0xae638d4273a735e93…	4000000	1170 days 14 hrs ago	Ethermine	→	0xf417d1acaa02a1da7…	0.499047778569188 Ether	0.000441
?	0x84d501fc501a1369c…	4000000	1170 days 14 hrs ago	Nanopool	→	0x5b134ab8403b346b…	0.200191602572543 Ether	0.000084
?	0x3e0d4d4616c30cf6d…	4000000	1170 days 14 hrs ago	Ethermine	→	0xc09a1f9677f99bcfcd…	0.099040414701451 Ether	0.000441
?	0x4f5bce757792fb345…	4000000	1170 days 14 hrs ago	Nanopool	→	0x6a89019555f5bb24b…	0.063903284703234 Ether	0.000084
?	0x0b0d4c6dde892bc7…	4000000	1170 days 14 hrs ago	Ethermine	→	0xa7f4067f70c01b436…	0.099343746607463 Ether	0.000441
?	0x966c7a3f99dfc8dcb…	4000000	1170 days 14 hrs ago	Kraken 4	→	0x1c3849fa06bb5eaa2…	0.045 Ether	0.00046305
?	0x583c2d8df07d102f1…	4000000	1170 days 14 hrs ago	0x7f39a55849ff447813…	→	📄 EtherDelta 2	0 Ether	0.00037015
?	0x5822367dbbfa3cee8…	4000000	1170 days 14 hrs ago	Nanopool	→	0x5e01739f5d34ca9d3…	0.242074709209709 Ether	0.000084
?	0xbc6b86896578b8fe5…	4000000	1170 days 14 hrs ago	DwarfPool	→	📄 0xc9a04647213d69f10…	0.05008515 Ether	0.00079024

Figure 5: Account/Balance Model

Simple, intuitive.

Language

BTC

Bitcoin scripting

- Simple, not Turing complete

$2 + 3 == 6$?

`2 3 OP_ADD 6 OP_EQUAL`

Transaction to Bitcoin address (pay-to-pubkey-hash)

`OP_DUP OP_HASH160 <371c...313> OP_EQUALVERIFY OP_CHECKSIG`

where

`<371c...313>`: pubKeyHash.

`OP_DUP`: Duplicates the top stack item.

`OP_HASH160`: The input is hashed twice.

`OP_EQUALVERIFY`: `OP_EQUAL` + `OP_VERIFY`

ETH

Solidity

- Sophisticated, Turing complete

Deposit to own account

```
function deposit() payable {
  deposits[msg.sender] += msg.value;
};
```

Decentralized autonomous organization (DAO)

Company vs. DAO

Company

- Rules enforced top-down
- Difficulty to change the rules depends on the management team

DAO

- Rules hard coded, enforced digitally
- Technically difficult to change the rules once they are *deployed*

The DAO

- Purpose: Crowd-funding
- Process
  - Investors pay ETH in exchange for DAO (representing voting rights)
  - Investors vote for projects and winning projects receive ETH from the DAO
- Vulnerability
  - Loophole: a smart contract retrieves ETH first and then update the balance
- Attack
  - retrieve ETH recursively before updating the balance
- Consequence
  - Hard fork: Ethereum vs Ethereum Classic

Decentralized finance

Decentralized exchange (DEX)

- DEXs on Ethereum
  - Automated market makers (AMM): Uniswap, Bancor . . .
- DEXs on XRPL
  - Ledger gateway

Cross-platform communication

Oracle

Oracles aredata feeds into smart contracts and by relying on some third party provide amechanism for accessing off-chain information.

Atomic swap

Hash Timelock Contracts

Thank you!

Contact

Jiahua (Java) Xu

Ecole Polytechnique Fédérale de Lausanne (EPFL)
EXTRA 249 (Extranef UNIL)
Quartier UNIL-Dorigny

jiahua.xu@epfl.ch

References I

Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. https://press.princeton.edu/titles/10908.html.