Smart Contracts and Blockchain Technology

Lecture 4. Consensus Formation

Christian Ewerhart

University of Zurich

Fall 2022

Introduction and overview

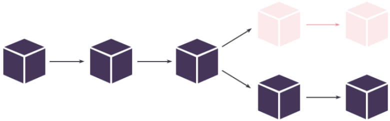
Last lecture: Model of crypto mining (equilibrium, activity analysis, mining pools)

This lecture: Consensus formation (forks, model of the blockchain, conservative mining, longest-chain rule, selfish mining)

Formal model of the blockchain (1)

Forks

A **fork** occurs if a single block has two or more child nodes:



Forks can be quite problematic:

- Loss of liquidity (e.g., in decentralized exchanges)
- Value of a stablecoin after the fork?
- NFTs are no longer unique
- Etc.

Formal model of the blockchain (2)

Examples of forks

Bitcoin (BTC) vs. Bitcoin Cash (BTH):

- The fork was caused on August 1, 2017 due to a disagreement on how to scale the network up to accommodate the strong demand for transactions.[1]
- As of October 2022, BTC is valued USD 20'000, BCH is valued USD 110.

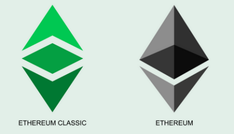
[1] Bitcoin has a block size of 1 MB at the cost of dropping the electronic signature of transactions (so-called Segregated Witness technology, SegWit2x), while Bitcoin Cash has a block size of 8 MB, at the cost of larger disc space requirements.

Formal model of the blockchain (3)

Examples of forks (continued)

Ethereum (ETH) vs. Ethereum Classic (ETC):

- Investors in the DAO had lost USD 70m due to an exploit in the smart contract. To revert the hack, Ethereum was hard-forked in 2016.[2]
- The legacy chain became Ethereum Classic.
- As of October 2022, ETH is valued USD 1'300, ETC is valued USD 24.



[2] For the full story, see https://medium.com.

Formal model of the blockchain (4)

Some popular terminology

Accidential forks. Two or more miners broadcast a new block at nearly the same time. An accidential fork is resolved as subsequent blocks get added and one of the branches becomes longer than the other. Miners will tend to ignore the blocks that are not in the longest chain (**orphaned blocks**).[3]

Intended forks may result from updates of the software used by nodes of the peer-to-peer network:

- So-called **soft forks** may (but need not) result from backwards-compatible updates.
- **Hard forks** may (but need not) result from backwards-incompatible updates.

[3] Note the potentially confusing terminology. An orphaned block always has a parent block (unless it is the genesis block). Moreover, orphaned block are defined by the property that they have no child blocks.

Formal model of the blockchain (5)

Definition

Suppose there are $n \geq 2$ **miners**, collected in a set $N = \{1, \ldots, n\}$.

A **blockchain** $\mathbb{B}$ consists of:

(i) a **sequence of blocks** $B = \{b_0, b_1, \ldots, b_T\}$, where $T \geq 0$;

(ii) a **parent-child relation** $\Lleftarrow$ on B;

(iii) an **assignment map** $\iota : B \backslash \{b_0\} \rightarrow N$.

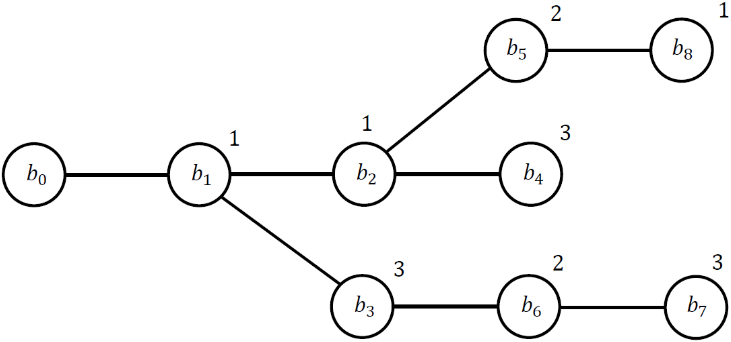
It is required that:

(a) each block except the **genesis block** b_0 has precisely one parent, i.e., for any $t' > 0$, there is precisely one t such that $b_t \Lleftarrow b_{t'}$

(b) the parent has a lower index than the child, i.e., $b_t \Lleftarrow b_{t'}$ implies $t < t'$.

Formal model of the blockchain (6)

Example



An example of a 3-miner blockchain with $T = 8$; the numbers at the circles refer to the values of the assignment map.

Formal model of the blockchain (7)

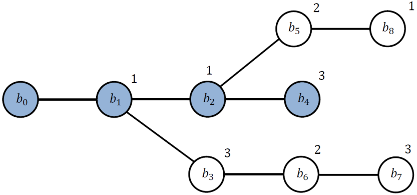
Chains

Length: nr. of parent-child relationships

A **chain** of length $K \geq 1$ in the blockchain $\mathbb{B}$ is a set $C = \{b^{(0)}, \ldots, b^{(K)}\}$ such that $b^{(k-1)} \Leftarrow b^{(k)}$ for $k = 1, \ldots, K$.

The **original chain** starts at b_0 and, if there is more than one child to a given parent, continues with the child with the lowest index.

E.g., in the example, the original chain is $C^{\text{org}} = \{b_0, b_1, b_2, b_4\}$.



Formal model of the blockchain (8)

Blockchain game, initial stage

Suppose the n miners incrementally construct a blockchain $\mathbb{B}$ by interacting over $T \geq 1$ stages. We denote the intermediate blockchains as $\mathbb{B}_0, \mathbb{B}_1, \ldots, \mathbb{B}_T$.

At the start of the game, $\mathbb{B}_0$ consists only of the genesis block, so that $B_0 = \{b_0\}$, and both $\Leftarrow_0$ and ι_0 are empty.

Formal model of the blockchain (9)

Blockchain game, intermediate stages

Next, at any intermediate stage $t \in \{1, 2, \ldots, T\}$, $\mathbb{B}_t$ is constructed from the existing blockchain $\mathbb{B}_{t-1}$ as follows.

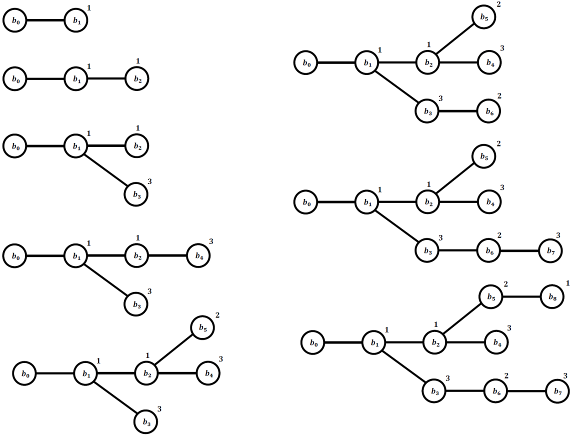
Each miner $i \in N$ selects a block $\widehat{b}_{t-1}(i) \in B_{t-1}$ from the existing set of blocks B_{t-1}.

Then, a fair random draw, just as in Dimitri's (2017) mining model, selects the winning miner $i_t^* \in N$ of stage t.

The new block b_t is assigned to i_t^*. Moreover, it is appended as a child to the block $\widehat{b}_{t-1}(i_t^*)$ chosen by the winning miner.

Formal model of the blockchain (6)

Example

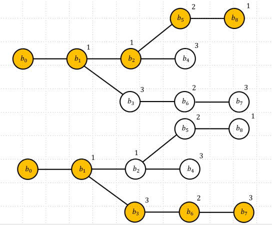


b_0 b_1 1
b_0 b_1 1 b_2 1
b_0 b_1 1 b_2 1 b_3 3
b_0 b_1 1 b_2 1 b_4 3 b_3 3
b_0 b_1 1 b_2 1 b_5 2 b_4 3 b_3 3
b_0 b_1 1 b_2 1 b_5 2 b_4 3 b_3 3 b_6 2
b_0 b_1 1 b_2 1 b_5 2 b_4 3 b_3 3 b_6 2 b_7 3
b_0 b_1 1 b_2 1 b_5 2 b_8 1 b_4 3 b_3 3 b_6 2 b_7 3

Formal model of the blockchain (10)

Payoffs

After stage T, one of the longest chains C in the blockchain $\mathbb{B}_T$ is drawn with equal probability.



Each miner $i \in N$ receives one *token* for each block $b \in C \backslash \{b_0\}$ assigned to her. Miners are risk-neutral and maximize the number of tokens they receive.

Note: There are efficiency gains from coordination...

Formal model of the blockchain (11)

Nash equilibrium

Definition.

- We say that miner *i* is *conservative* if she always chooses the last block of the original chain.
- We say that miner *i* follows the *longest-chain rule* if she always chooses the last block of one of the longest chains.

Note: *Conservative mining is a strategy, whereas the longest-chain rule is a class of strategies.*

Proposition. *Conservative mining constitutes a symmetric Nash equilibrium. Any combination of mining strategies consistent with the longest-chain rule forms a Nash equilibrium.*

Formal model of the blockchain (12)

Proof (for conservative mining)

We assume that all miners $j \in N \backslash \{i\}$ are conservative. We have to show that miner i likewise wishes to be conservative.

Suppose first that i is conservative. Then, the blockchain develops into a single chain consisting of $T + 1$ blocks, and miner i receives one token for each block that she mines.

Suppose, instead, that miner i deviates and works on a block that is not the last block of the original chain. Then, miner i creates a fork with positive probability. As a result, she does not necessarily receive one token for each block that she mines.

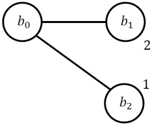
Thus, miner i potentially lowers, but never raises her payoff. Therefore, a deviation from conservative mining can never lead to a strictly higher expected payoff for miner i.

Formal model of the blockchain (13)

Subgame perfection

Conservative mining need not constitute a subgame-perfect equilibrium.

Example 1. Let $n = 2$ and $T = 3$, and consider the blockchain $\mathbb{B}_2$:



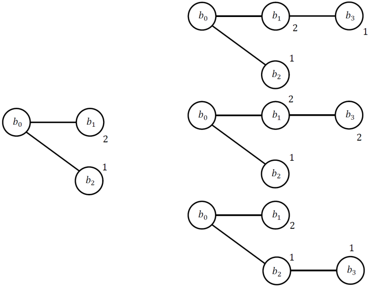
Thus, miner 1 mined b_2, not following the conservative strategy.

Formal model of the blockchain (14)

Subgame perfection (continued)

At stage $T = 3$, the last block of the original chain is b_1.

However, it is optimal here for miner 1 to work on b_2 because this allows her, with probability $1/2$, to realize a token for the block b_2.



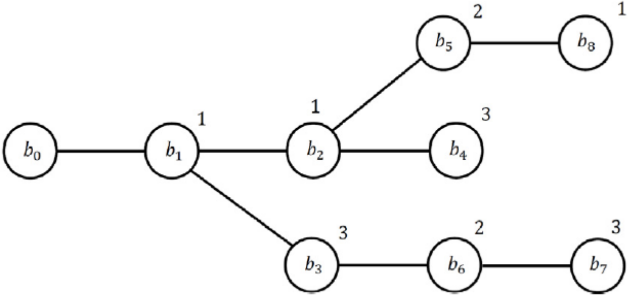
Thus, conservative mining is **not subgame-perfect**.

Formal model of the blockchain (15)

Subgame perfection (continued)

Longest-chain mining need not constitute a subgame-perfect equilibrium either.

Example 2. Let $n = 3$ and $T = 6$, and consider the blockchain $\mathbb{B}_5$:



Formal model of the blockchain (16)

Discussion

The model captures the **interplay between two forces**:

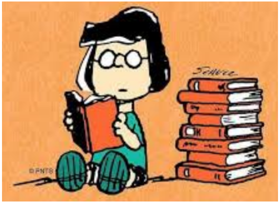
- Coordination problem between players
- Problem of vested interests

Formal model of the blockchain (18)

Bibliographic notes

The framework introduced above is a simplified version of the model used by Biais et al. (2019). See Ewerhart (2020).

Eyal and Sirer (2018) show with the help of a Markov chain model that selfish mining can be profitable.



Formal model of the blockchain (17)

References

Biais, B., Bisiere, C., Bouvard, M., Casamatta, C. (2019), The blockchain folk theorem, *Review of Financial Studies* **32**, 1662-1715.

Ewerhart, C. (2020), Finite blockchain games, *Economics Letters* **197**, 109614. (link)

Eyal, I., Sirer, E.G. (2018), Majority is not enough: Bitcoin mining is vulnerable, *Communications of the ACM* **61**, 95-102.