University of Basel
Center for Innovative Finance

Bitcoin, Blockchain and Cryptoassets

Incentives and Potential Consensus Attacks

Prof. Dr. Fabian Schär
University of Basel

```
Release Ver.:  (Local Release)
Version Hash:  (None)
Version Date:  (None)
```

Introduction

By now, we know about the fundamental role of consensus and the dangers of difficulties:

- Danger of permanent network splits.
- Uncertainty in case of temporary forks.

$\Rightarrow$ Both cases impact value of network to the users.

Focus of this lecture:

- General incentives for consensus relevant nodes (CRNs)
- Bitcoin specifics and incentives driving consensus.
- Consensus attacks in this context.

Economic Considerations of a CRN

To get participants to serve as compliant CRN and bear the corresponding cost, a Blockchain network typically offers revenues.

General CRN P&L categories

Cost	**Revenues**
Computation	Block-based (e.g., Coinbase tx)
(electricity, hardware, etc.)	Transaction-based (e.g., fees)
Cost of stake*	Attestation rewards*
Cost of maintaining Authority*	Miner Extracted Value (MEV)

*not applicable in Bitcoin context

$\Rightarrow$ With revenues in network currency and cost often in FIAT, CRNs have an incentive to keep network value - and consequently demand - high.

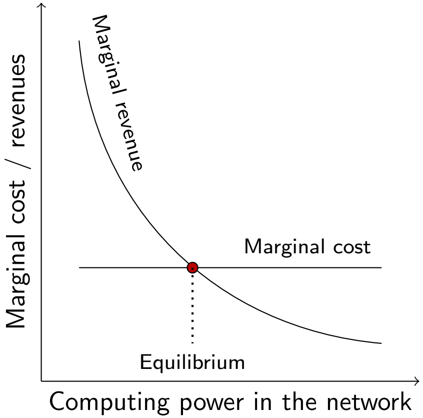
Computing Power Allocation

Mining Market:

- Competitive due to low entry barriers.
- Profits only through above average efficiency.

Underallocation: Miners add power to realize more profits.

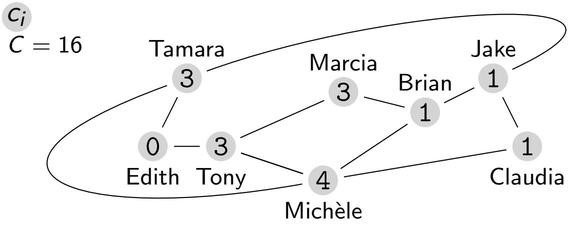
Overallocation: Miners remove power to avoid losses.



Bitcoin Mining: Probabilistic Reward Distribution

Under proof-of-work, probability of mining a block and earning the corresponding reward P is defined by a miner i's computing power relative to the network, i.e., $E(p_i) = P \cdot \frac{c_i}{C}$.

Illustrative example with P = 6.25 Bitcoin:

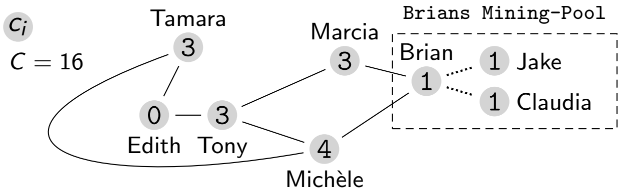


Jake's expected payout per block: $6.25 \cdot \frac{1}{16} = 0.391$ Bitcoin.

The Case for Mining Pools

1. Successful mining of a block follows a Poisson distribution.
2. Short- to mid-term actual payouts may deviate significantly.
3. Relatively small miners are disproportionally affected.

To address this, Jake, Brian and Claudia can form a **Mining Pool**:



$\Rightarrow E(p)$ per block: $6.25 \cdot \frac{1}{16}$ vs. $\frac{6.25}{3} \cdot \frac{3}{16}$.

$\Rightarrow \sigma_p$ per block: 1.523 vs. 0.813

Bitcoin Consensus Incentives: Basic Assumptions

CRN operators are:

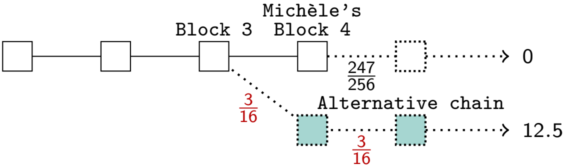
- Rational agents
  $\Rightarrow$ Effort is dedicated to chain with highest probability weighted payout.
- Independent (otherwise considered Mining Pools)

Value of payout is tied to network value:

- Consensus deviations impair trust in network and thus demand.
- Reduced demand is reflected in lower fees and devaluation of reward currency.

Bitcoin: Attraction of the Longest Chain

Situation: Michèle has successfully mined Block 4. Our Mining Pool is considering to continue mining it's own Block 4.

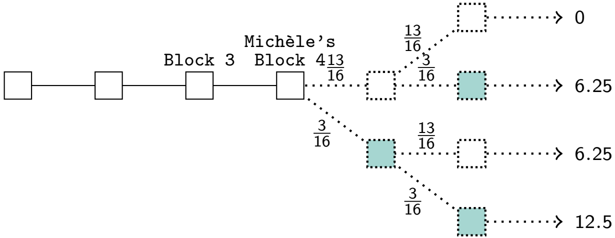


- Consensus compliant CRN's mine on top of Michèle's block.
- To become the longest chain, the Pool must mine two blocks before current consensus chain is extended.
- In case of success, the Pool receives two block rewards.

Expected Payout: $\frac{3}{16} \cdot \frac{3}{16} \cdot (6.25 \cdot 2) = 0.439$

Bitcoin: Attraction of the Longest Chain (cont.)

Expected payout over two blocks on top of Michèle's Block 4:



$\Rightarrow \frac{39}{256} \cdot 6.25 + \frac{39}{256} \cdot 6.25 + \frac{9}{256} \cdot 12.5 = \mathbf{2.344}$

Conclusion:

- Expected payouts strongly support compliance with consensus.
- Relative computing power thresholds for rational deviations are $\geq \frac{2}{3}$ over two blocks and $\geq \frac{1}{2}$ over long-term.

Longest Chain Incentives and Process-based Forks

Probabilistic Block Race

- Expected payout drives fast resolution along "winning" chain.
- Only miner of abandoned block has skewed incentives.

Block Withholding / Selfish Mining

- Risk of loosing block reward t vs. increased chances on $t+1$.
- Only rational for high relative computing power.

Forced Block Race

- Longest chain incentives do not discriminate "attack" chains.
- Only rational in case of computing power $\geq 51\%$.

$\Rightarrow$ Bitcoin incentives effectively protect consensus in absence of mining power concentration.

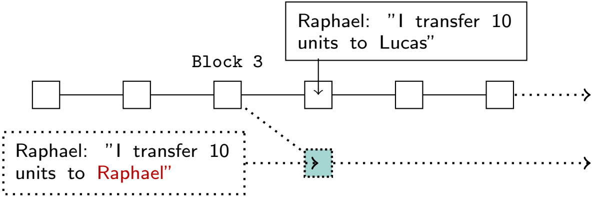
Other MEV: Double Spend Attack

Miners can choose which transactions to include in a block and thus can influence the consensus chain and, for example :

- Deliberately delay a transaction (blocking).
- Attack a block with conflicting transactions (double spend).

$\Rightarrow$ Situative other MEV may skew incentives for CRNs.

Example: Raphael pays 10 Bitcoin to Lucas and receives a car. Driving away, he attacks Block 4 spending the UTXO on himself.

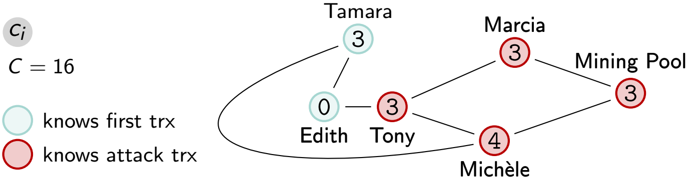


Double Spend Attack without Mining

Scenario

- Raphael buys take-away coffee, paying in Bitcoin.
- He receives the coffee against the - yet unconfirmed - trx.
- To another node, he sends a trx to himself with the same UTXO.

The faster the trxs are propagated through the network, the higher their relative chances to be included in a valid block first:



$\Rightarrow$ Relayed to a better connected node, the attack trx is probably getting confirmed first, leaving Raphael with coffee AND Bitcoin.

Double Spend Attack without Mining (cont.)

Double spend attacks do not require own mining power. The chances of success are not negligible, given enough time pressure in the exchange payment vs. goods.

The payee can take **cautionary measures** to minimize success probability of such attacks:

- If not waiting for confirmation, at least a minimal waiting time between relaying transaction and handing out goods.
- Maintaining a broad network connection to foster propagation of own transaction and increase chances of becoming aware of conflicting transactions.

References and Recommended Reading


Majority is not Enough: Bitcoin Mining is Vulnerable*

Ittay Eyal and Emin Gün Sirer

Department of Computer Science, Cornell University
ittay.eyal@cornell.edu, egs@systems.cs.cornell.edu

Abstract. The Bitcoin cryptocurrency records its transactions in a public log called the blockchain. Its security rests critically on the distributed protocol that maintains the blockchain, run by participants called miners. Conventional wisdom asserts that the mining protocol is incentive-compatible and secure against colluding minority groups, that is, it incentivizes miners to follow the protocol as prescribed.
We show that the Bitcoin mining protocol is not incentive-compatible. We present an attack with which colluding miners obtain a revenue larger than their fair share. This attack can have significant consequences for Bitcoin: Rational miners will prefer to join the selfish miners, and the colluding group will increase in size until it becomes a majority. At this point, the Bitcoin system ceases to be a decentralized currency.
Unless certain assumptions are made, selfish mining may be feasible for any group size of colluding miners. We propose a practical modification to the Bitcoin protocol that protects Bitcoin in the general case. It prohibits selfish mining by pools that command less than 1/4 of the resources. This threshold is lower than the wrongly assumed 1/2 bound, but better than the current reality where a group of any size can compromise the system.

1 Introduction

Bitcoin [23] is a cryptocurrency that has recently emerged as a popular medium of exchange, with a rich and extensive ecosystem. The Bitcoin network runs at over 42×10^{18} FLOPS [9], with a total market capitalization around 12 billion US Dollars as of January 2014 [10]. Central to Bitcoin's operation is a global, public log, called the blockchain, that records all transactions between Bitcoin clients. The security of the blockchain is established by a chain of cryptographic puzzles, solved by a loosely-organized network of participants called miners. Each miner that successfully solves a cryptopuzzle is allowed to record a set of transactions, and to collect a reward in Bitcoins. The more mining power (resources) a miner applies, the better are its chances to solve the puzzle first. This reward structure provides an incentive for miners to contribute their resources to the system, and is essential to the currency's decentralized nature.

The Bitcoin protocol requires a majority of the miners to be *honest*; that is, follow the Bitcoin protocol as prescribed. By construction, if a set of colluding miners comes to command a majority of the mining power in the network,

* This research was supported by the NSF Trust STC and by DARPA.

Majority is not Enough: Bitcoin Mining is Vulnerable
Ittay Eyal and Emin Gün Sirer
Online version