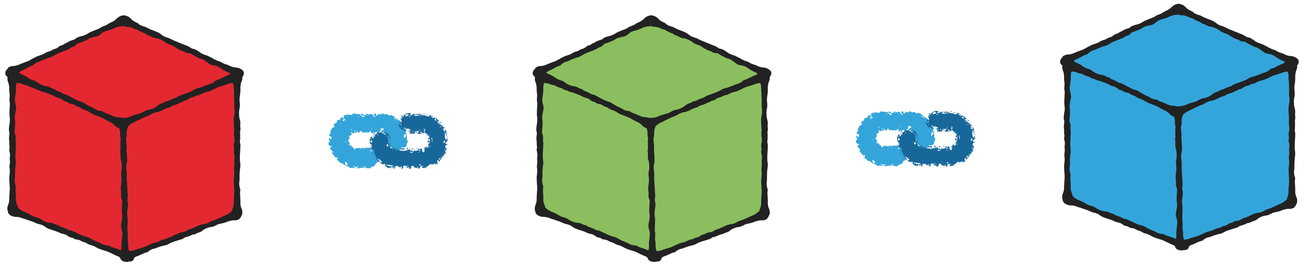


Selfish & Opaque Transaction Ordering in the Bitcoin Blockchain

The Case for Chain Neutrality

Johnnatan Messias

@johnnatan_me

Joint w/ Mohamed Alzayat, Balakrishnan Chandrasekaran, Krishna P. Gummadi, Patrick Loiseau, and Alan Mislove

MAX PLANCK INSTITUTE FOR SOFTWARE SYSTEMS

UNIVERSITÄT DES SAARLANDES

VU VRIJE UNIVERSITEIT AMSTERDAM

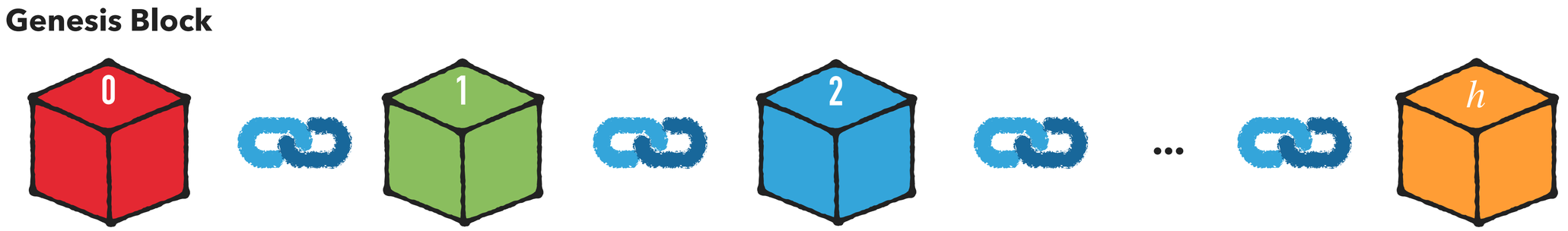
Inria

UGA Université Grenoble Alpes

Northeastern University

What's a Blockchain?

- ★ Decentralized ledger
- ★ P2P network
- ★ Tamper evident



50+ BLOCKCHAIN
REAL WORLD USES CASES

GOVERNMENT
Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government

essentia.one

IDENTIFICATION
Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by **Uport**.

uport

MOBILE PAYMENTS
The blockchain ledger that **Ripple** uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.

ripple

INSURANCE
A smart contract-based blockchain is being used by Insurer **American International Group Inc** as a means of saving costs and increasing transparency.

AIG

ENDANGERED SPECIES PROTECTION
The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.

CARBON OFFSETS
IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.

IBM HYPERLEDGER

ENTERPRISE
Ethereum's blockchain can be accessed as a cloud-based service courtesy of **Microsoft Azure.**

Microsoft Azure

BORDER CONTROL
Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.

essentia.one

SUPPLY CHAINS
IBM and **Walmart** have partnered in China to create a blockchain project that will monitor food safety.

IBM Walmart

HEALTHCARE
A number of healthcare systems that store data on the blockchain have been pioneered including **MedRec.**

MEDREC

SHIPPING
Shipping is a natural fit for blockchain, and **Maersk** have been trialling a blockchainbased project within the maritime logistics industry.

MÆRSK

REAL ESTATE
Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by **Propy**.

PROPY

ENERGY
Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.

essentia.one

LAND REGISTRY
Land registry titles are now being stored on the blockchain in Georgia in a project developed by the **National Agency of Public Registry**.

NATIONAL AGENCY OF PUBLIC REGISTRY

COMPUTATION
Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.

DIGITAL CURRENCY GROUP

ADVERTISING
New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.

NYIAX

BORDER CONTROL
Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.

essentia.one

JOURNALISM
Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as **Civil** has shown.

CIVIL

WASTE MANAGEMENT
Waltonchain is using **RFID** technology to store waste management data on the blockchain in China.

ENERGY
Food importation is another industry where blockchain is proving its worth, with **Louis Dreyfus Co** trialling a soybean importation operation using this technology.

LDC Louis Dreyfus Company

DIAMONDS
The **De Beers Group** is using blockchain to track the importation and sale of diamonds.

De Beers Group of Companies

FINE ART
By storing **certificates** of authenticity on the blockchain, it's possible to dramatically reduce art forgeries, as one blockchain project is proving.

NATIONAL SECURITY
For the past two years, the **US Department of Homeland Security** has been using blockchain to record and safely store data captured from its security cameras.

TOURISM
In a bid to boost its tourism economy, **Hawaii** is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.

TAXATION
In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by **Miaocai Network**.

ENERGY
Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.

CNE COMISIÓN NACIONAL DE ENERGÍA

RAILWAYS
Russian rail operator **Novotrans** is storing inventory data on a blockchain pertaining to repair requests and rolling stock

НОВОТРАНС

ENTERPRISE
Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by **Alphabet Inc**

Google Alphabet

MUSIC
Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.

arbit

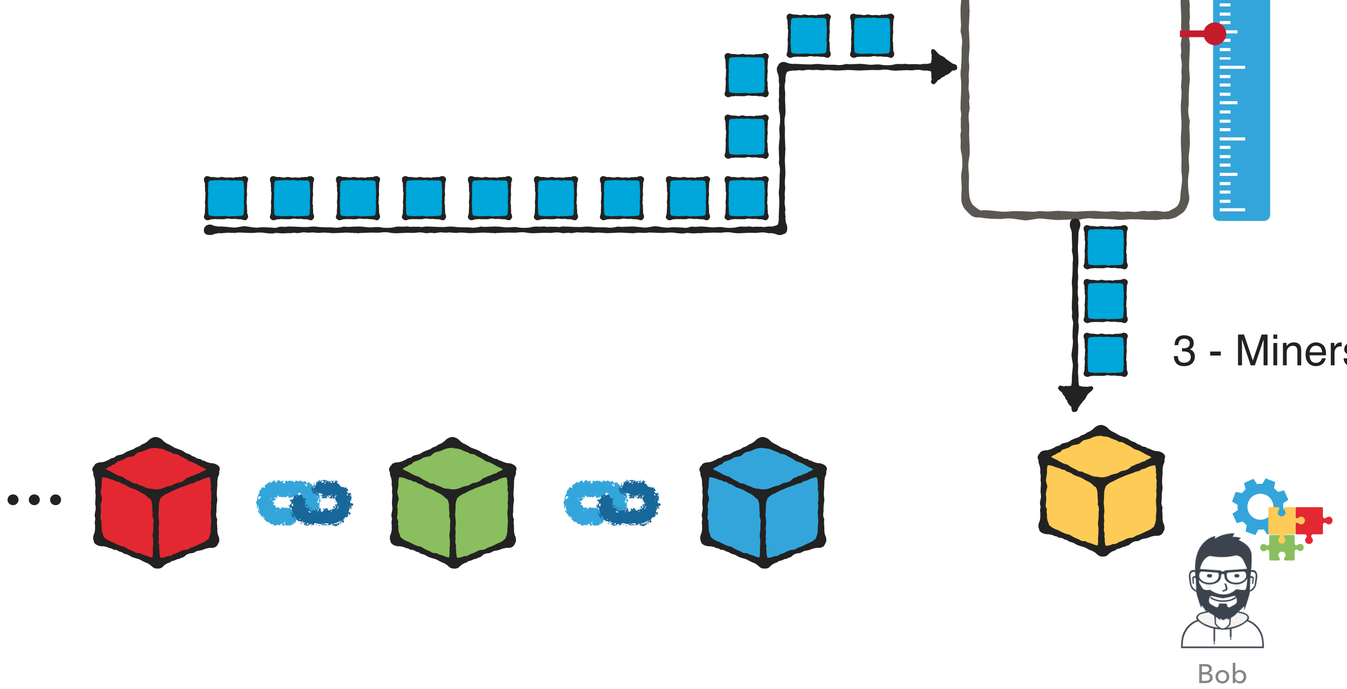
FISHING
Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.

How Transactions Are Ordered?

1 - Transactions arrive through P2P

Every transaction includes a fee-per-byte

2 - Transactions are included in the Mempool



3 - Miners select them to include in a block

4 - Miners/MPOs mine a block

5 - Miners relay the blocks to the P2P network

6 - Block and its transactions become part of the blockchain

There Are Three Norms Everyone Assumes Are Followed

- Which transactions are allowed or transmitted over the P2P network?
  - **Norm 1:** Fee-rate threshold for excluding transactions.

- Once they get into the Mempool, how are miners selecting them?
  - **Norm 2:** Fee-rate based selection when mining new blocks.

- Once miners selected these transactions, in what order do they get included within a block?
  - **Norm 3:** Fee-rate based ordering within blocks.

Analyzing Norm Adherence

Analyzing Norm Adherence

- **Norm 1:** Fee-rate threshold for excluding transactions
  - Bitcoin nodes filter out transactions with a fee-rate of less than 1 sat/byte.
    - But our node received in total 1084 low fee-rate transactions.

- **Norm 2:** Fee-rate based selection when mining new blocks.
  - A non-trivial fraction of transactions pairs **violates** the norm across all snapshots, clearly indicating that miners do not adhere to the norm.

- **Norm 3:** Fee-rate based ordering within blocks
  - We propose a useful metric Position Prediction Error (**PPE**) to measure how far away it is from the norm.
  - The mean PPE is **2.65%** with an std. of **2.89**. **20%** of all blocks have PPE higher than **4%.**

Analyzing Norm Adherence

- **Norm 1:** Fee-rate threshold for excluding transactions
  - Bitcoin nodes filter out transactions with a fee-rate of less than 1 sat/byte.
    - But our node received in total 1084 low fee-rate transactions.

Mostly it is followed, but there is a fraction that is not followed.

- **Norm 2:** Fe
  - A non-triv s all snapshots, clearly indicating that miners do not adhere to the norm.

- **Norm 3:** Fee-rate based ordering within blocks
  - We propose a useful metric Position Prediction Error (**PPE**) to measure how far away it is from the norm.
  - The mean PPE is **2.65%** with an std. of **2.89**. **20%** of all blocks have PPE higher than **4%.**

Investigating Norm Violations

Hypotheses That Might Explain Norm Violations

- Self-interest transactions
  - What if the miners have some vested interest in the transactions they are including (selfish-interest transactions)?
- Scam payment transactions
  - What if the miner was dropping some transactions because it's a scam payment?
- Dark-fees transactions
  - Are miners allowing users to pay a fee for prioritization via side-payment channels?

Hypotheses That Might Explain Norm Violations

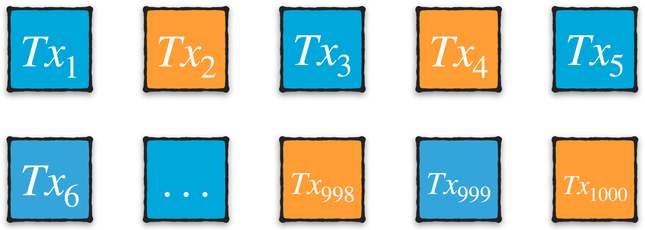
- Self-interest transactions
  - What if the miners have some vested interest in the transactions they are including (selfish-interest transactions)?
- Scam paym
  - What if th cam payment?
- Dark-fees transactions
  - Are miners allowing users to pay a fee for prioritization via side-payment channels?

Please, refer to our paper for more details!

Investigating Self-Interest Transactions

- How do we identify self-interest transactions?
  - We identified wallets that belong to the MPOs.
  - Transactions involving those wallets should be of interest to the MPOs.

- How do we detect selfish prioritization of those transactions?
  - We design a robust statistical test for differential prioritization to detect selfish prioritization.
  - Here is the key insight behind it on how the test works.



100 MPOs txs

30 txs **20 txs** **10 txs** **40 txs**

Deprioritization **Prioritization**

Investigating Norm Violations: Results

- Self-interest transactions
  - MPOs **prioritize** their **own** transactions and **other** MPOs **transactions.**

- Scam payment transactions
  - We did not observe any acceleration or deceleration.

- Dark-fees transactions
  - We confirm that a large fraction have been **accelerated** via side-channel payments.

SPPE ≥	*# transactions*	*# acc. transactions*	*% acc. transactions*
100 %	628	464	73.89
99 %	1108	720	**64.98**
90 %	5365	972	18.12
50 %	95,282	1007	1.06
1 %	657,423	1029	0.16

Summary and Discussion

Summary

- Transaction ordering is an important thing to be studied!

- There are three norms that everyone assumes are followed.
  - Fee-rate threshold for excluding transactions.
  - Fee-rate based selection when mining new blocks.
  - Fee-rate based ordering within blocks.

- Our study shows there are violations on all three.

- We expose some possible reasons behind them:
  - Selfish prioritization.
  - Non-transparent opaque dark-fees payments.

Discussion

- What are the **right prioritization** rules/norms?
  - Is it right for miners not to deprioritize scam transactions?
  - Should miners be allowed to accept payments through a side-channel?

- Should miners be allowed to differentiate transactions based on their data/content?
  - i.e., should miners maintain **chain neutrality?**

- How can blockchains **enforce the right prioritization** by miners?
  - How can we detect wrongful prioritization by miners?

Our Data Set and Scripts Are Available

https://github.com/johnnatan-messias/blockchain-transaction-ordering

Selfish & Opaque Transaction Ordering in the Bitcoin Blockchain

The Case for Chain Neutrality

Johnnatan Messias

@johnnatan_me

Joint w/ Mohamed Alzayat, Balakrishnan Chandrasekaran, Krishna P. Gummadi, Patrick Loiseau, and Alan Mislove

MAX PLANCK INSTITUTE FOR SOFTWARE SYSTEMS

UNIVERSITÄT DES SAARLANDES

VU VRIJE UNIVERSITEIT AMSTERDAM

Inria

UGA Université Grenoble Alpes

Northeastern University