

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

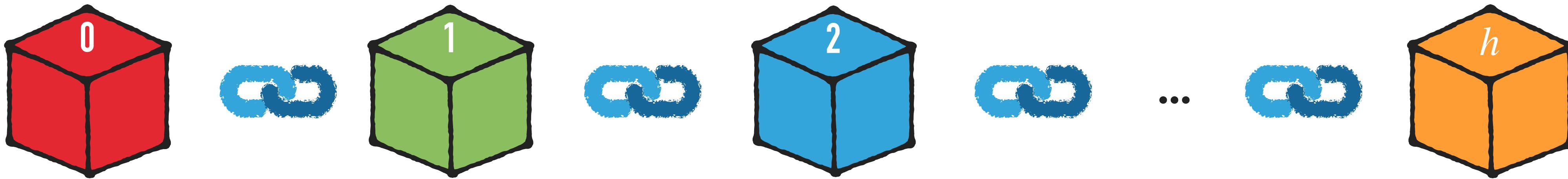


UNIVERSITÄT
DES
SAARLANDES



What's a Blockchain?

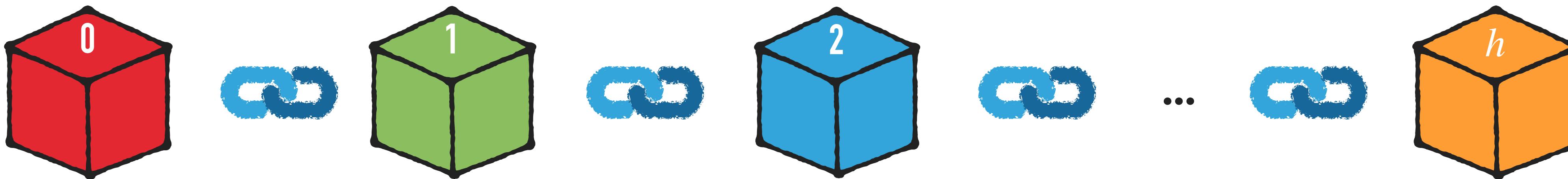
Genesis Block



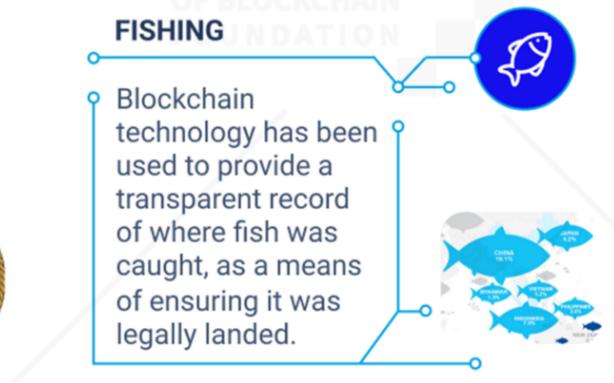
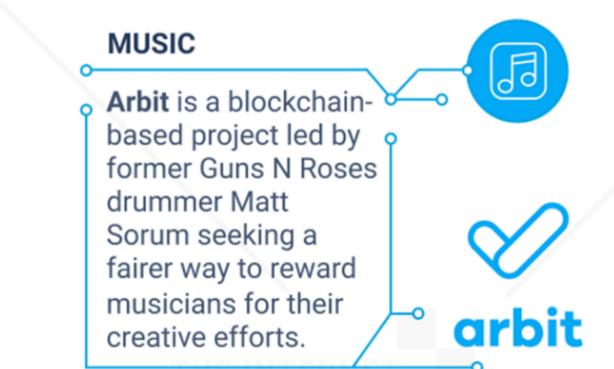
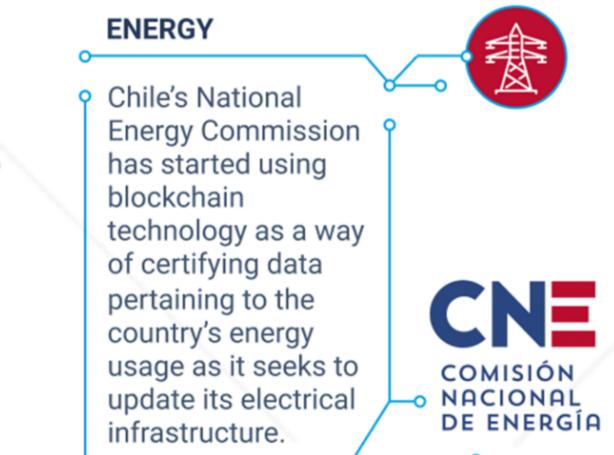
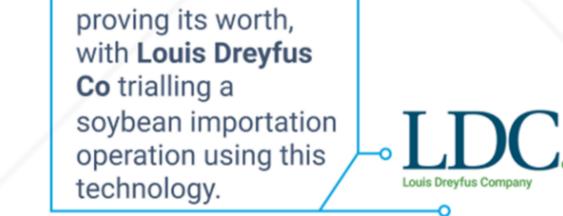
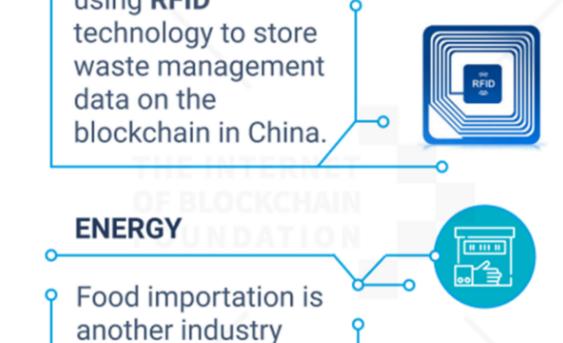
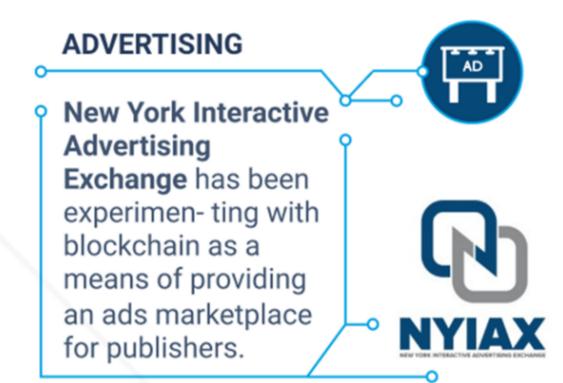
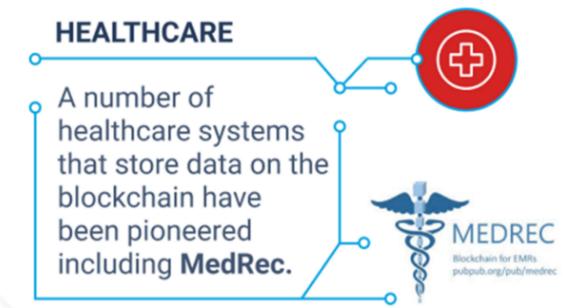
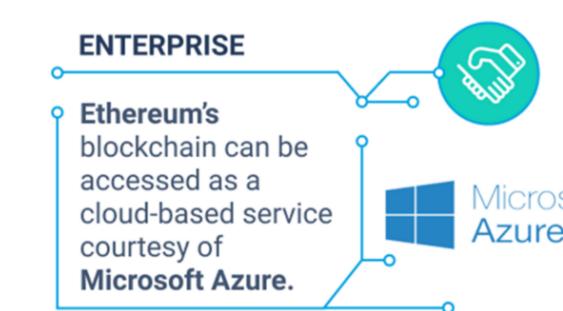
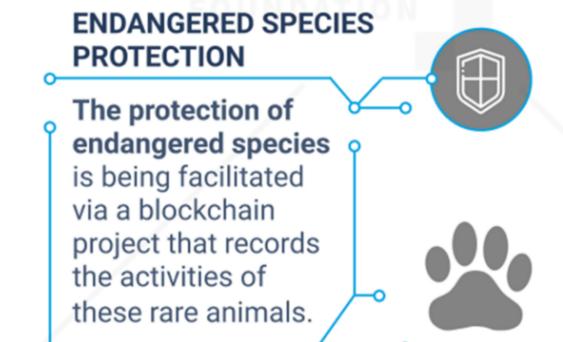
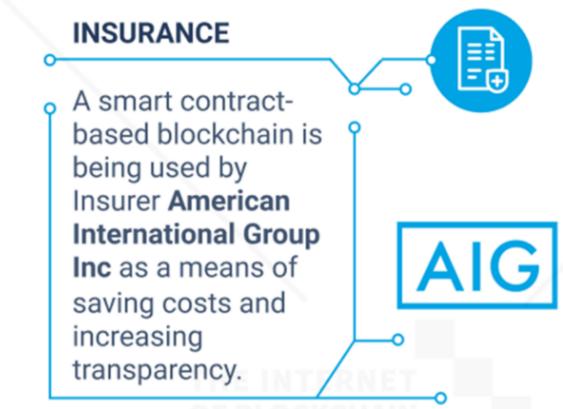
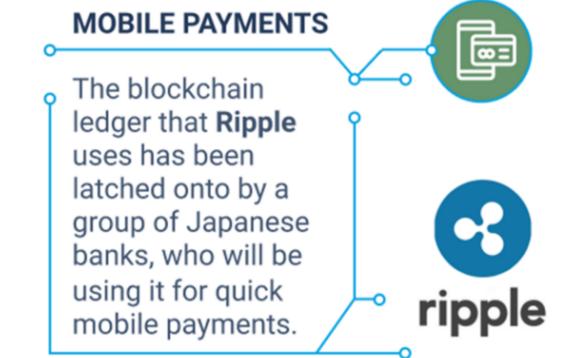
What's a Blockchain?

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

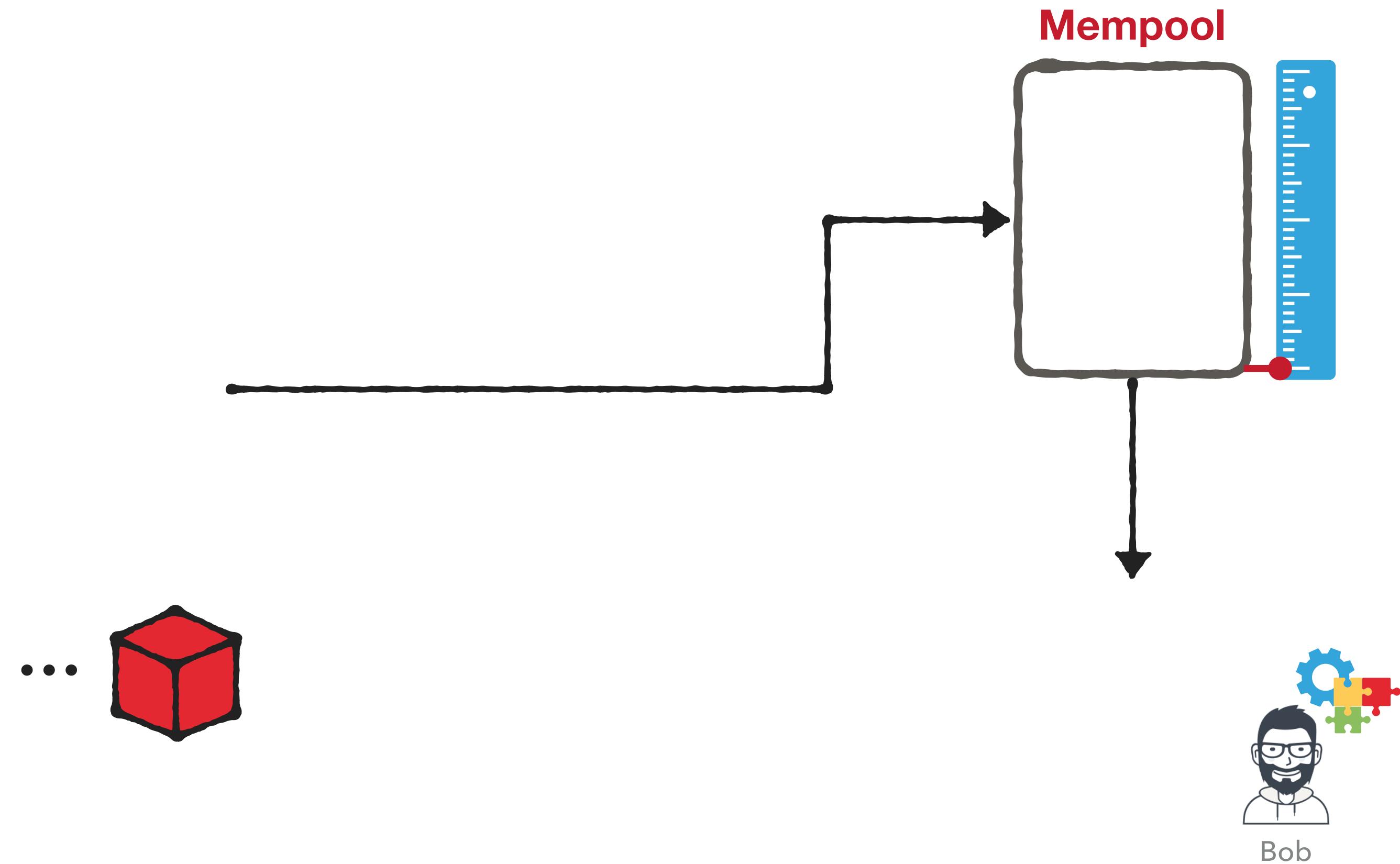
Genesis Block



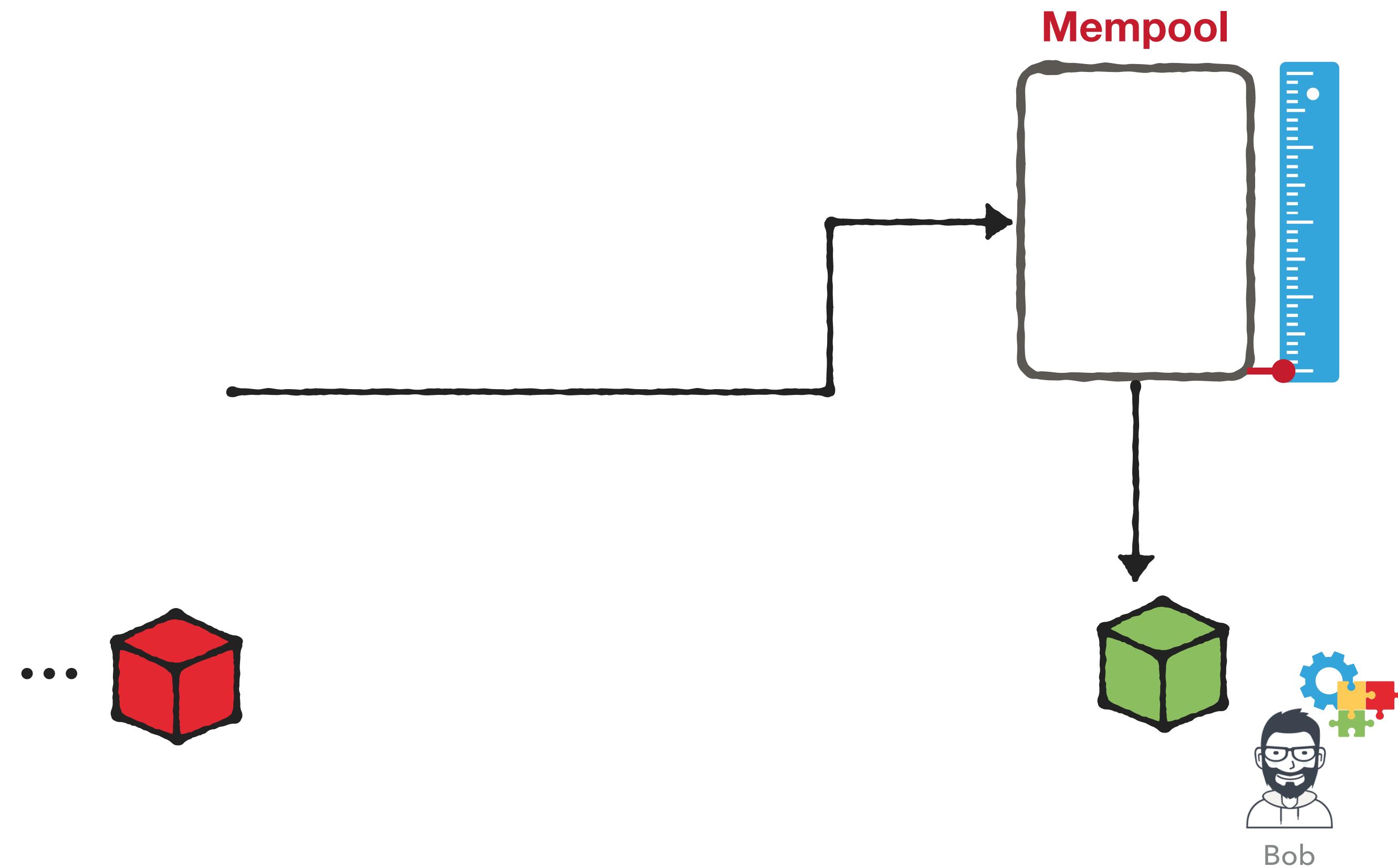
50+ BLOCKCHAIN REAL WORLD USES CASES



How Transactions Are Ordered?



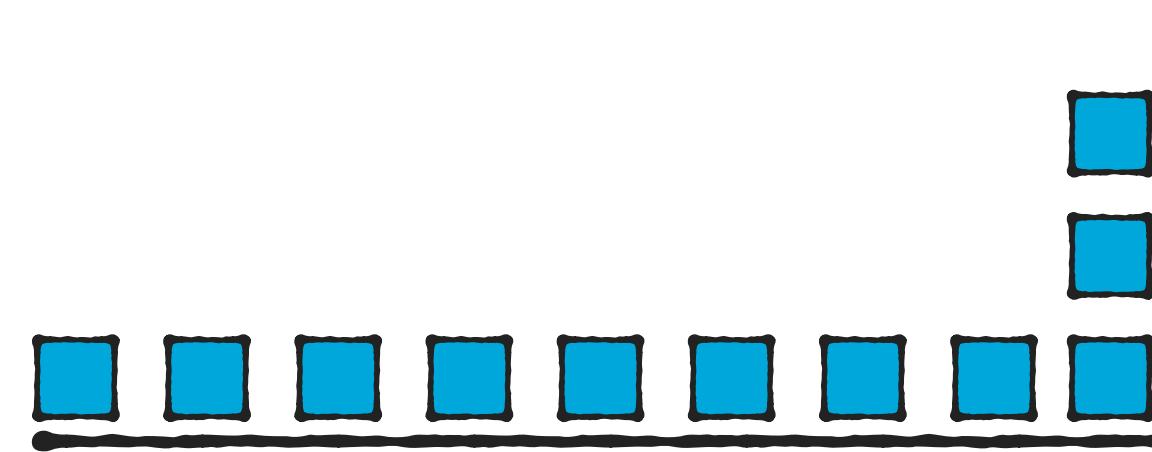
How Transactions Are Ordered?



How Transactions Are Ordered?

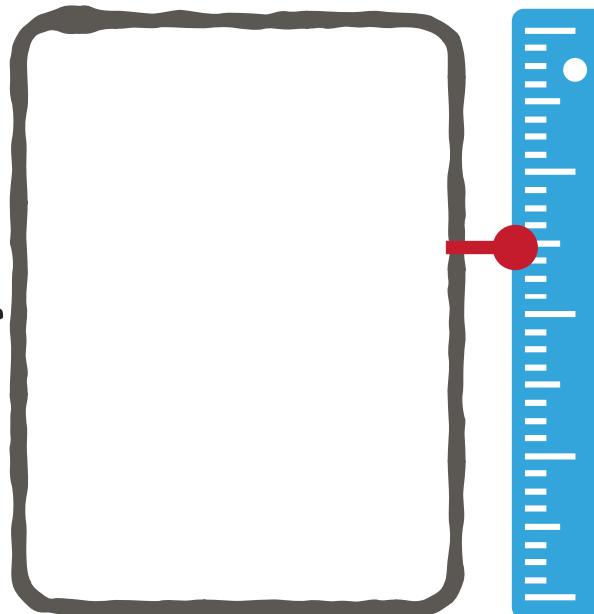
1 - Transactions **arrive** through P2P

Every transaction includes a fee-per-byte

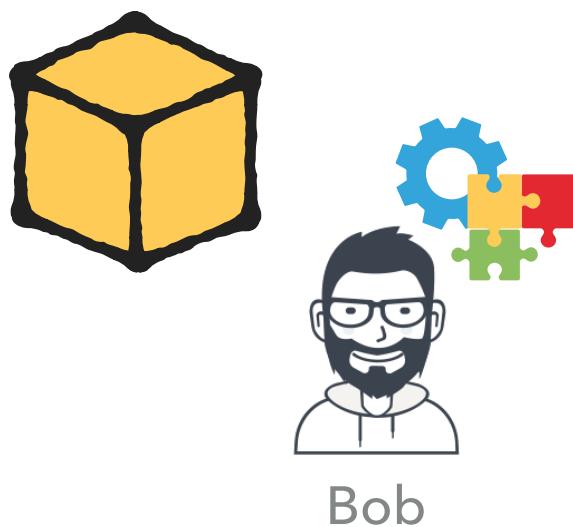
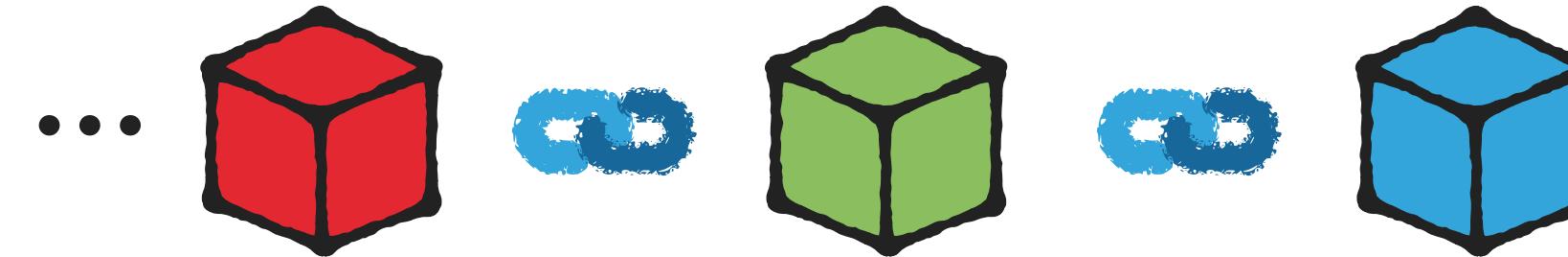


Mempool

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.

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.

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.

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.

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.
- ▶ **Norm 2:** Fee-rate based ordering within blocks
 - ▶ A non-trivial fraction of all transactions do not follow this 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%**.

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)?

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?

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 payment
 - ▶ What if the miners are accepting scam 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

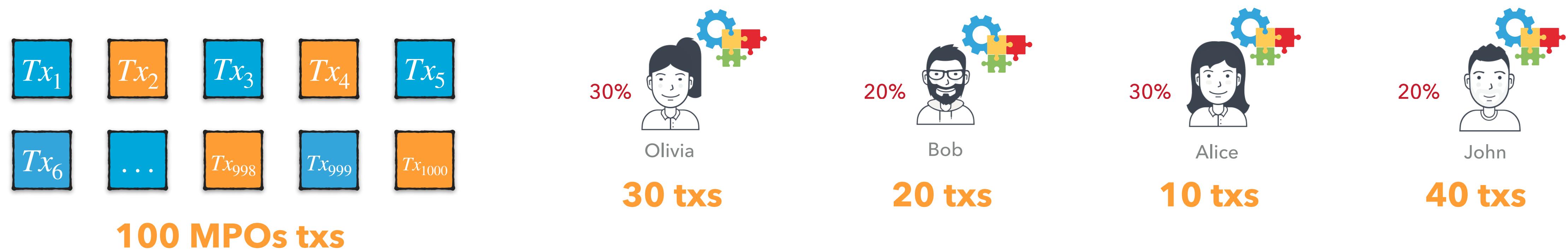
- ▶ How do we identify self-interest transactions?
 - ▶ We identified wallets that belong to the MPOs.
 - ▶ Transactions involving those wallets should be of interest to the MPOs.

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.

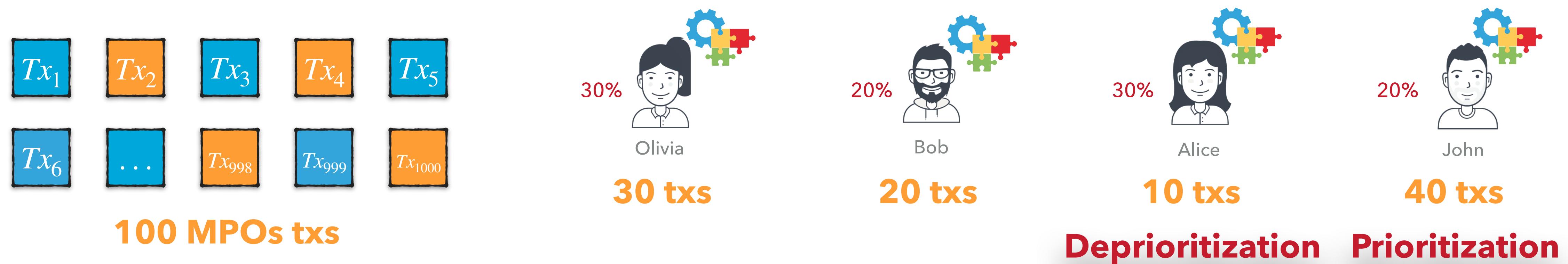
Investigating Self-Interest Transactions

- ▶ 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.



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.



Investigating Norm Violations: Results

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

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.

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.

| $SPPE \geq$ | # 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!

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.

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.

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?

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?**

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>

thank you!



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

