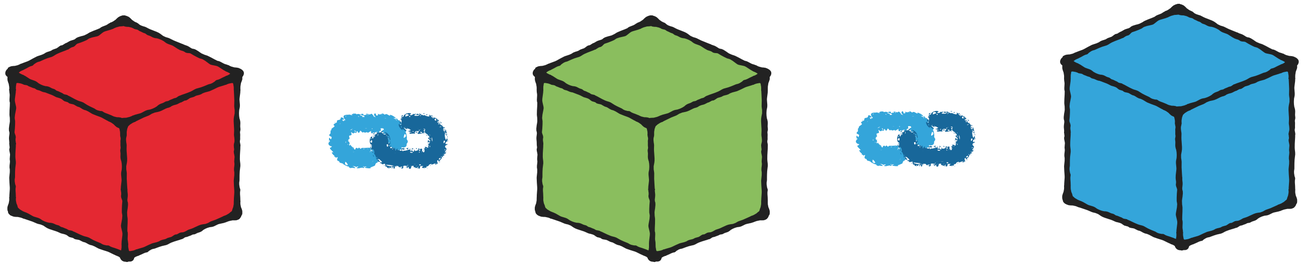


Dissecting Bitcoin and Ethereum Transactions:
On the Lack of Transaction Contention and Prioritization Transparency in Blockchains

Johnnatan Messias

@johnnatan_me

Joint w/ Vabuk Pahari, Balakrishnan Chandrasekaran, Krishna P. Gummadi, and Patrick Loiseau

Financial Cryptography and Data Security 2023

MAX PLANCK INSTITUTE FOR SOFTWARE SYSTEMS

UNIVERSITÄT DES SAARLANDES

VU VRIJE UNIVERSITEIT AMSTERDAM

Inria

UGA Université Grenoble Alpes

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 dramati- cally 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

грузовая компания 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.

THE INTERNET OF BLOCKCHAIN FOUNDATION

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 s contract-ba lockchain is be sed by In an I oup s a me of g cos easing spa

AIG

bitcoin

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 d in Ch a bl project th monitor afety.

IBM
Walmart

LTH
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

D REGISTRY
d registry titles now being stored 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 dramati- cally 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

грузовая компания 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.

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 s contract-ba lockchain is be sed by In an ro up s a me of g cos easing sp

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 d in Ch a bl project th monitor afety.

Walmart

LTH

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

D REGISTRY
d registry titles now being stored 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.

esse

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 stor g **certificates** of authenticity on the blockchain, it's possible to dramati- cally 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

грузовая компания 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

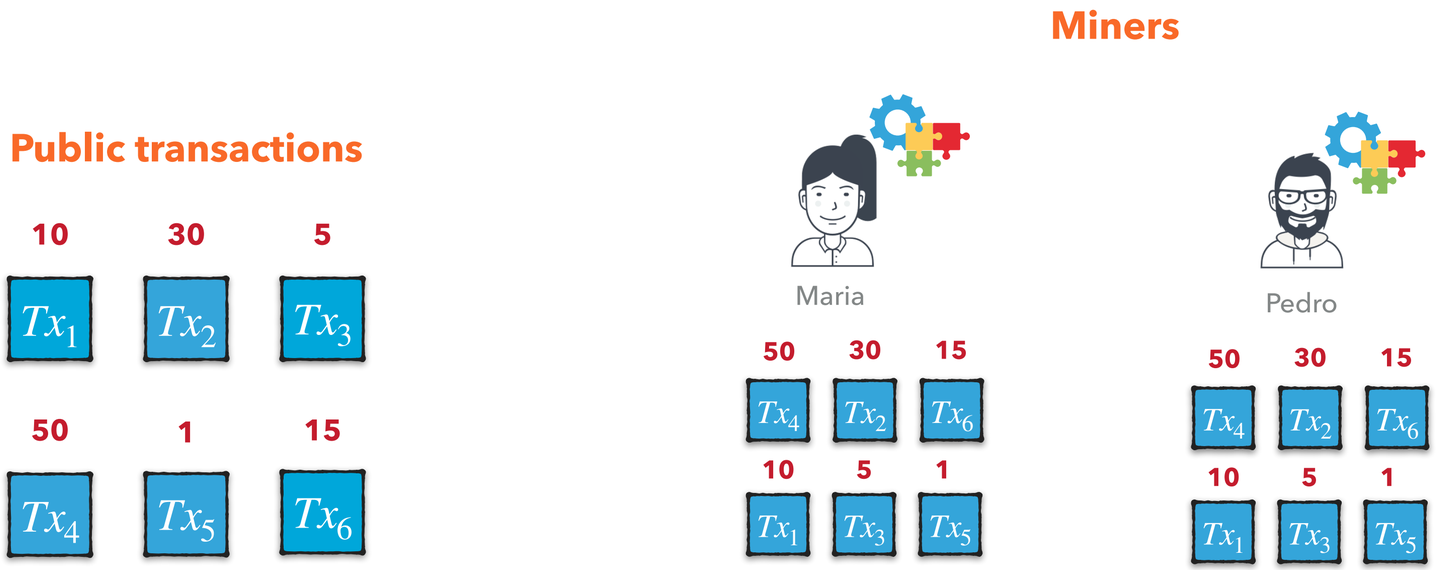
FISHING
Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.

bitcoin ethereum

THE INTERNET OF BLOCKCHAIN FOUNDATION

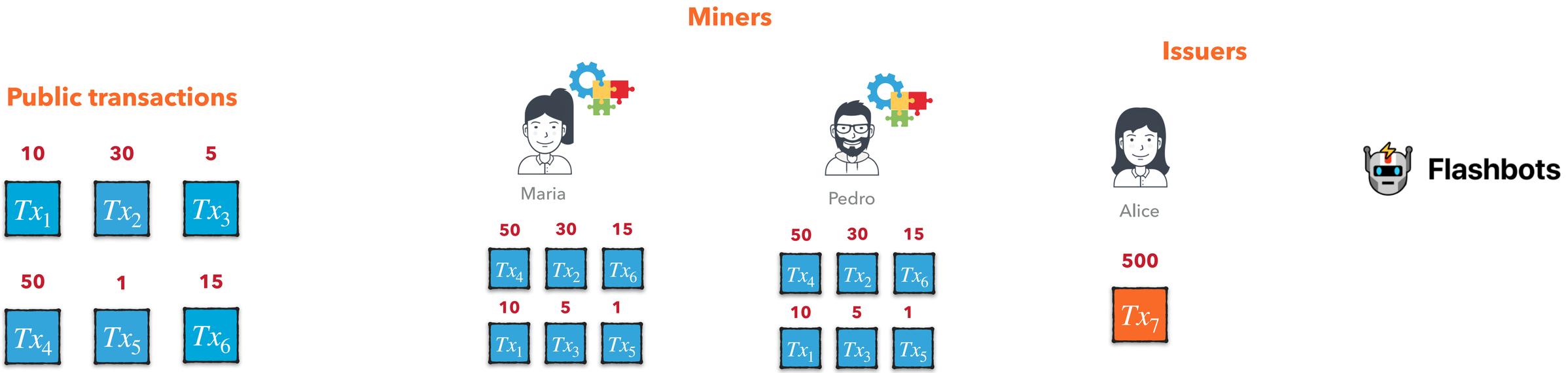
Lack of Transparency

- Contention transparency: Public and uniform view of all available transactions.



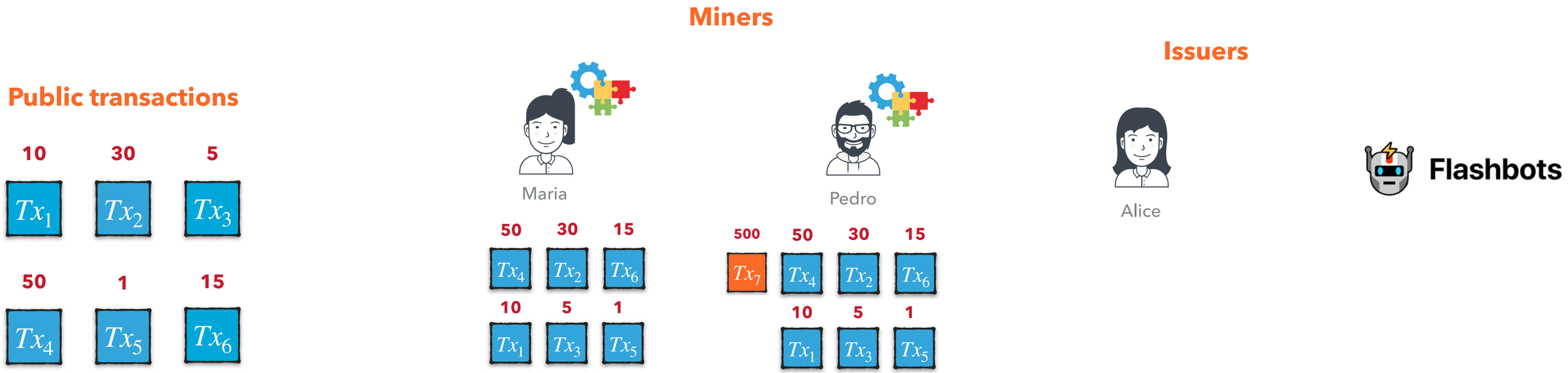
Lack of Transparency

- Contention transparency: Public and uniform view of all available transactions.



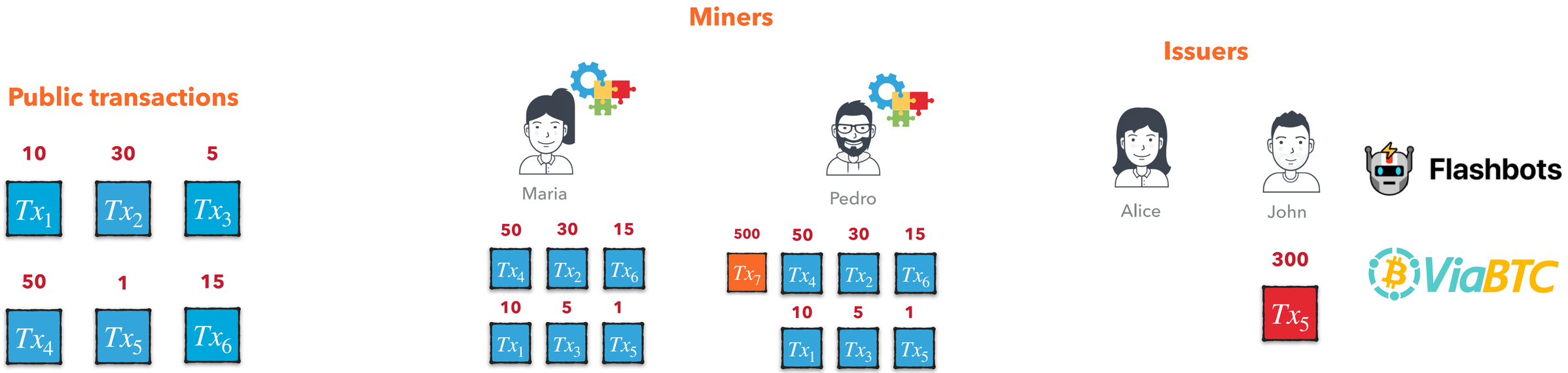
Lack of Transparency

- Contention transparency: Public and uniform view of all available transactions.



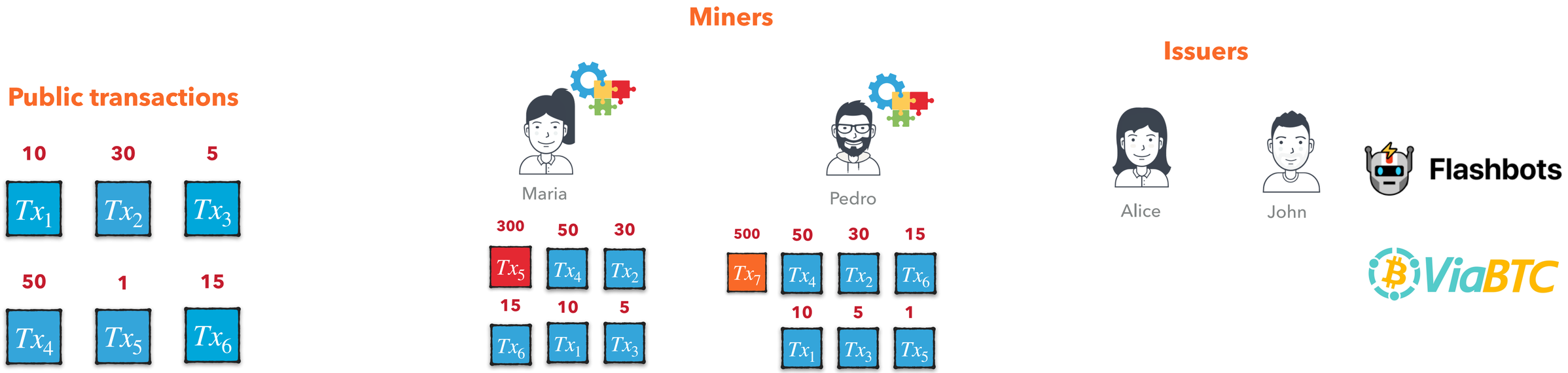
Lack of Transparency

- Contention transparency: Public and uniform view of all available transactions.
- Prioritization transparency: Fee offered by a transaction is only that publicly declared by that transaction.



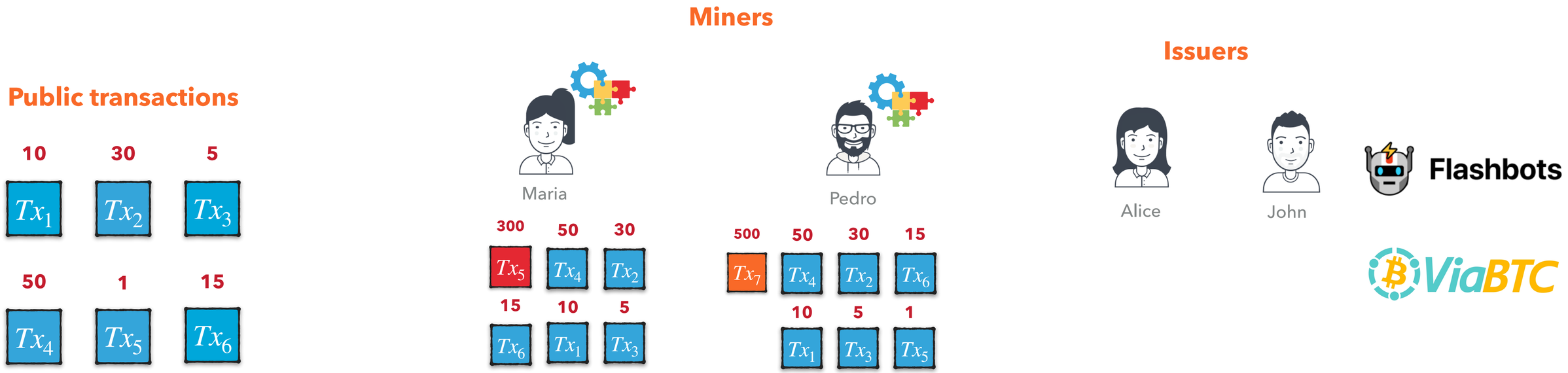
Lack of Transparency

- Contention transparency: Public and uniform view of all available transactions.
- Prioritization transparency: Fee offered by a transaction is only that publicly declared by that transaction.



Lack of Transparency

- Contention transparency: Public and uniform view of all available transactions.
- Prioritization transparency: Fee offered by a transaction is only that publicly declared by that transaction.
- The lack of transparency facilitates miners to collude and overcharge users.



Private Relay Networks: Flashbots

- Users can bundle their transactions and send them privately to miners.
  - Only participating miners and Flashbots know about these transactions.
  - The rest only after they are committed to a block.

- Miners are paid through a coinbase transfer.
  - Directly transfer to the miner's address.

- Miners "promise" to include bundles on the top of their blocks.
  - In case of competition: Miner includes the bundle with higher incentive.
  - The other bundle with all its transactions is discarded as it has never existed.

Private Relay Networks: Taichi Network

SPARK POOL

- Users can send their transactions privately to SparkPool and its patterns.
- Free to use.
- **No longer working.**

Bitcoin Transaction Accelerators

ViaBTC

ViaBTC cooperates with multiple mainstream mining pools to provide you with the fastest transaction acceleration service.

Remaining hourly FREE transactions	Total Accelerated Transactions
100	557499

Please enter Transaction ID

FREE Submission

Paid service

What is the difference between FREE and Paid?

✓ ViaBTC

✗ BTC.com

✓ f2pool

✗ Poolin

✓ bitcoinjumper

Among others

✓ **Available** ✗ **Unavailable**

Data Sets

Category	Bitcoin	Ethereum
Time period	Jan. 1st 2018 to Dec. 31st 2020	Sep. 8th 2021 to Jun. 30th 2022
# of blocks	161,954	1,867,000
Block number	501,951 to 663,904	13,183,000 to 15,049,999
# of transactions	313,575,387	347,629,393

Data Sets

Category	Bitcoin	Ethereum
Time period	Jan. 1st 2018 to Dec. 31st 2020	Sep. 8th 2021 to Jun. 30th 2022
# of blocks	161,954	1,867,000
Block number	501,951 to 663,904	13,183,000 to 15,049,999
# of transactions	313,575,387	347,629,393

Removed CPFP-txs
65,902,514 (21.01%)

Data Sets

Category	Bitcoin	Ethereum
Time period	Jan. 1st 2018 to Dec. 31st 2020	Sep. 8th 2021 to Jun. 30th 2022
# of blocks	161,954	1,867,000
Block number	501,951 to 663,904	13,183,000 to 15,049,999
# of transactions	313,575,387	347,629,393

Removed CPFP-txs
65,902,514 (21.01%)

Prior to the Merge

Data Sets

Category	Bitcoin	Ethereum
Time period	Jan. 1st 2018 to Dec. 31st 2020	Sep. 8th 2021 to Jun. 30th 2022
# of blocks	161,954	1,867,000
Block number	501,951 to 663,904	13,183,000 to 15,049,999
# of transactions	313,575,387	347,629,393

Removed CPFP-txs
65,902,514 (21.01%)

Prior to the Merge

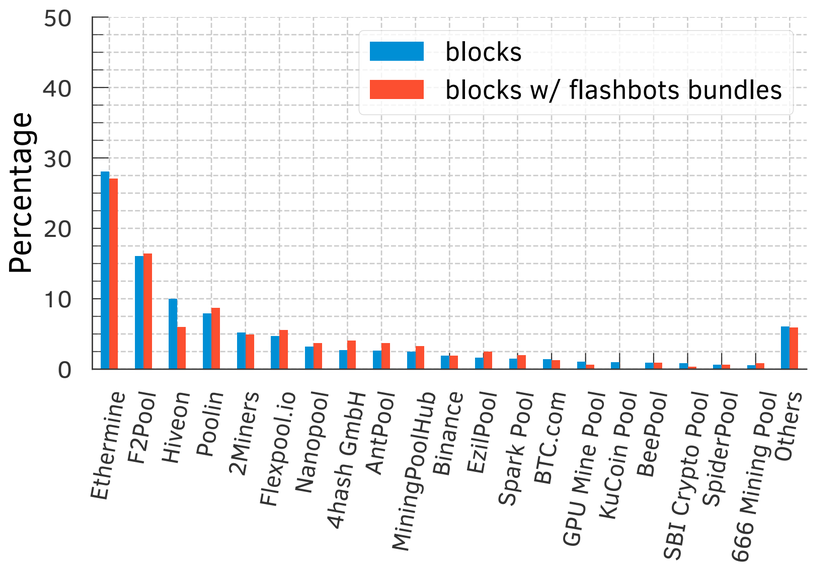
Flashbots data set
6,937,292 transactions in **3,284,886 bundles**

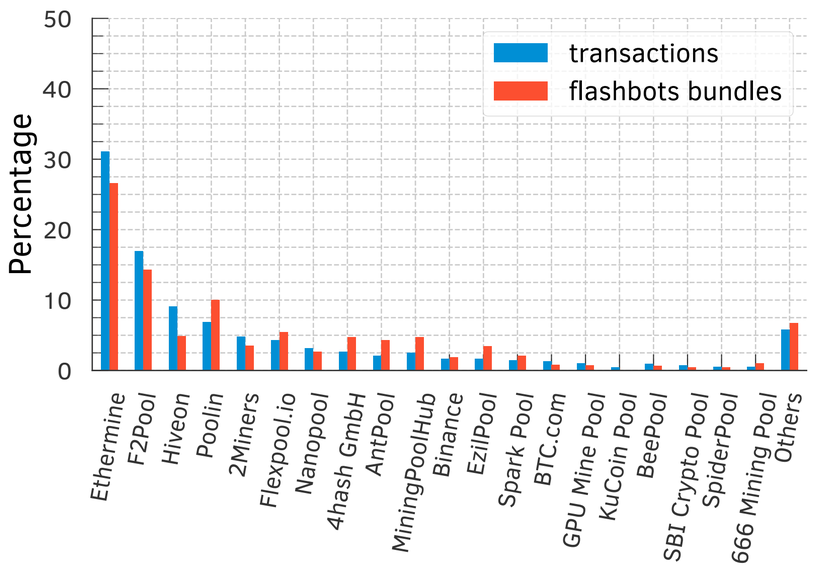
Prevalence of Bundling

Flashbots bundles are quite prevalent

Ethermine included 27.05% of all blocks with a Flashbot bundle and 26.63% of all Flashbots bundles, while mining around 28.05% and 31.11% of all blocks and transactions, respectively.

99.99% ETH hash-rate





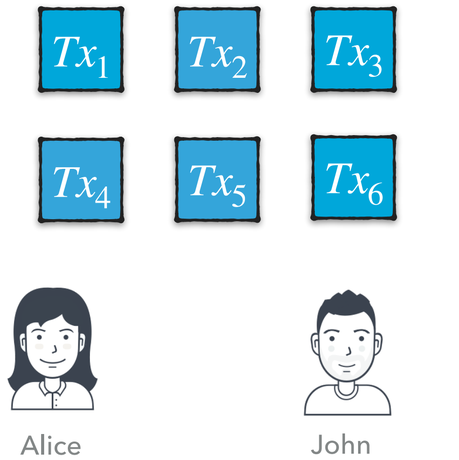
Contracts Most Frequently Called by Flashbots

- We focused on the 6 contracts calls: 0x Protocol, Balancer, Bancor, Curve, SushiSwap, and Uniswap V1 and V3.

- We find that 2,231,051 (67.92%) unique Flashbots bundles and 3,076,760 transactions (44.35%) called at least one of these contracts.
  - Uniswap and SushiSwap were the most bundled DEXes protocols.

Bundling Public Transactions

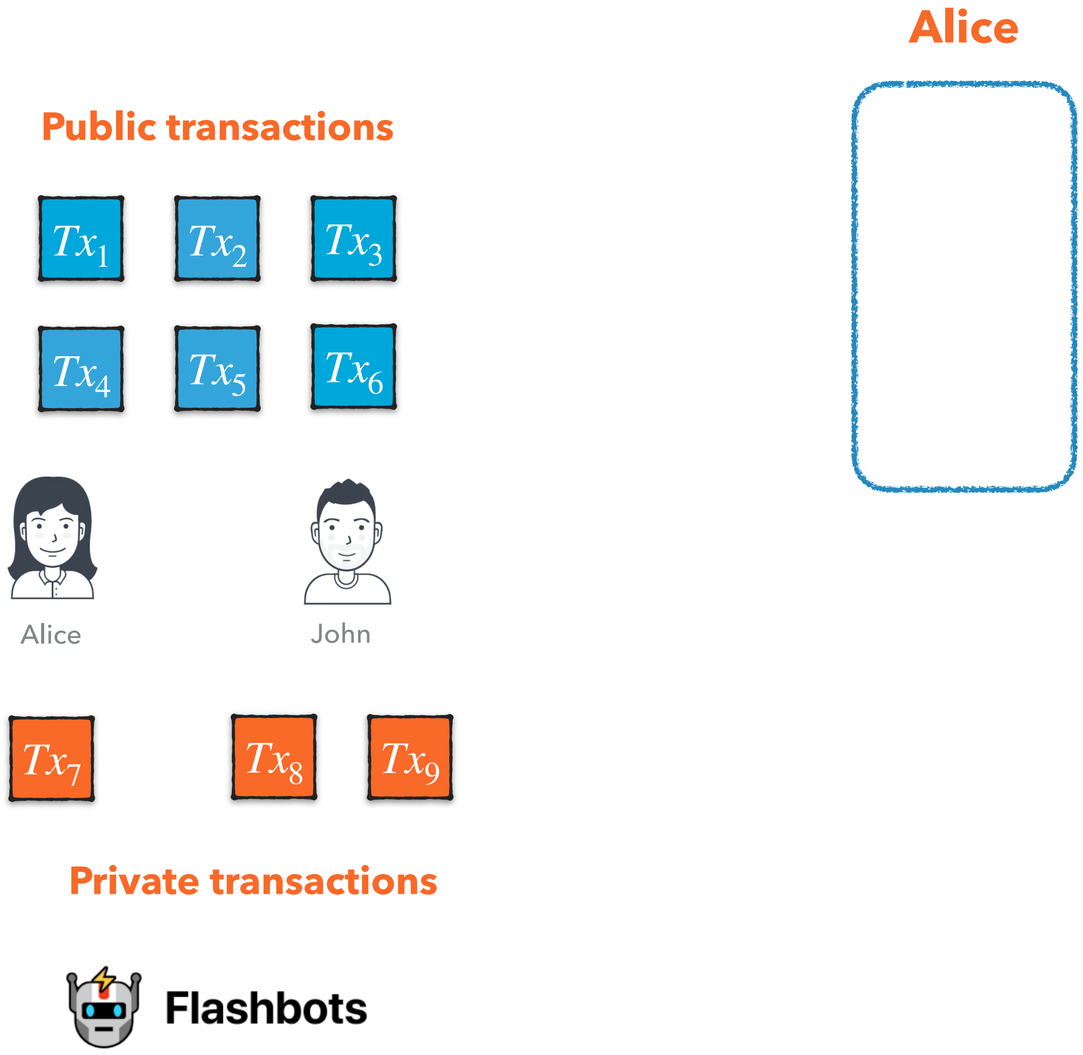
Public transactions



Private transactions

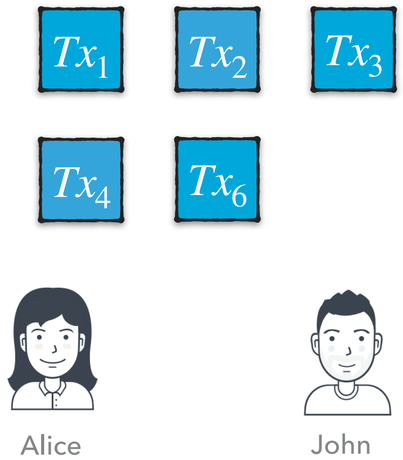
Flashbots

Bundling Public Transactions



Bundling Public Transactions

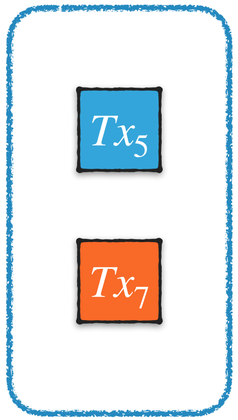
Public transactions



Private transactions

Flashbots

Alice



110,401 bundles

Bundling Public Transactions

Public transactions

Tx_1 Tx_2 Tx_3

Tx_4 Tx_6

Alice

John

Tx_8 Tx_9

Private transactions

Flashbots

Alice

Tx_5

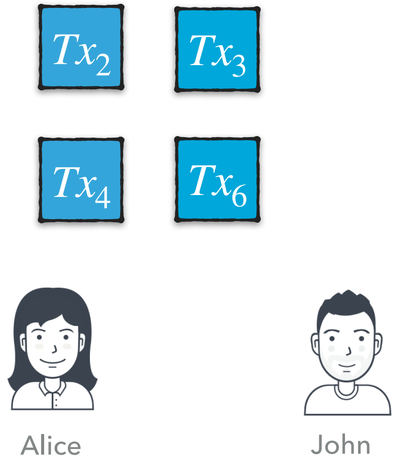
Tx_7

110,401 bundles

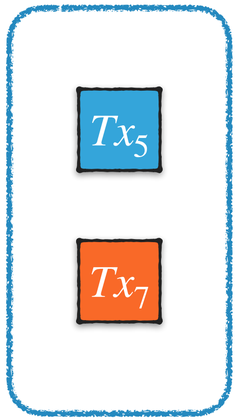
John

Bundling Public Transactions

Public transactions

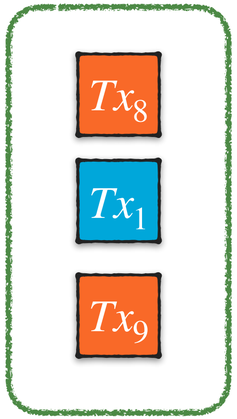


Alice



110,401 bundles

John



Sandwich attacks

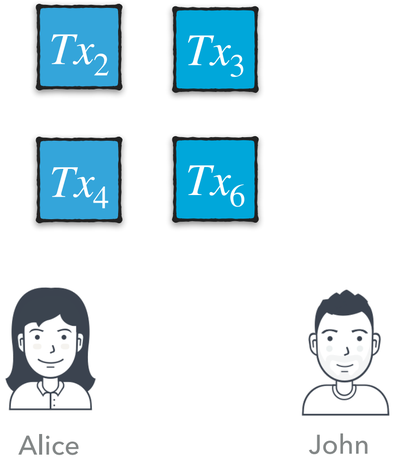
37,447 bundles

Private transactions

Flashbots

Bundling Public Transactions

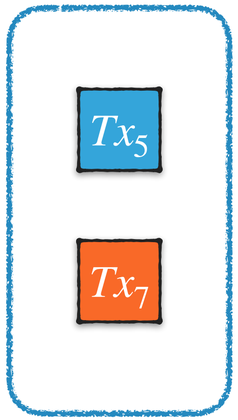
Public transactions



Private transactions

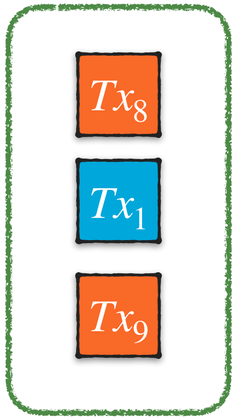
Flashbots

Alice



110,401 bundles

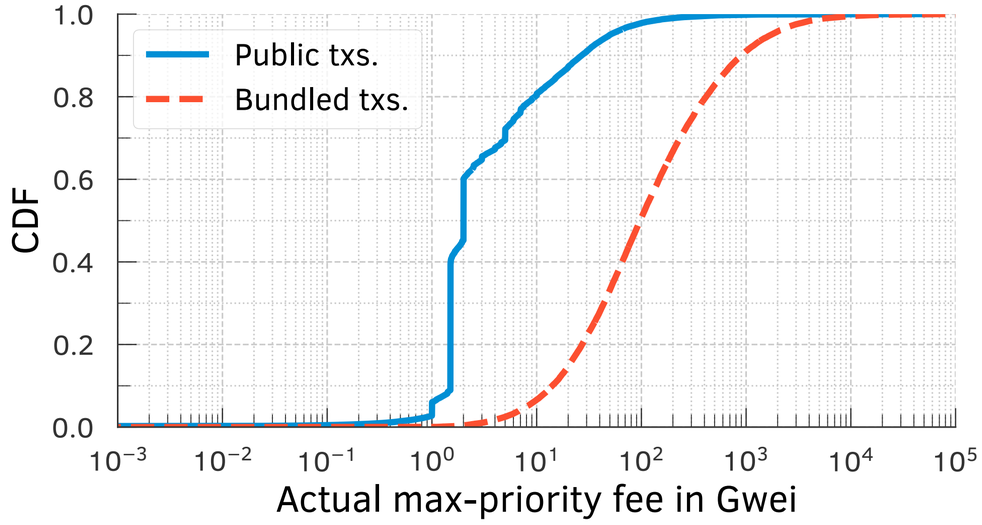
John



Sandwich attacks

37,447 bundles

Bundles typically offer a larger effective fee to the miners



Liquidation Through Bundling

- Over-collateralized lending protocols

	AAVE	Compound
	Liquidations	**Liquidations**
	16,418	6387
Flashbots	4863	2036

Liquidation With Bundled Chainlink Oracle Updates

- Over-collateralized lending protocols

AAVE

Liquidations

1165 in 1154 bundles

One Oracle update 994 bundles

Two Oracle updates 52 bundles

Followed by a liquidation

Flashbots

Compound

Liquidations

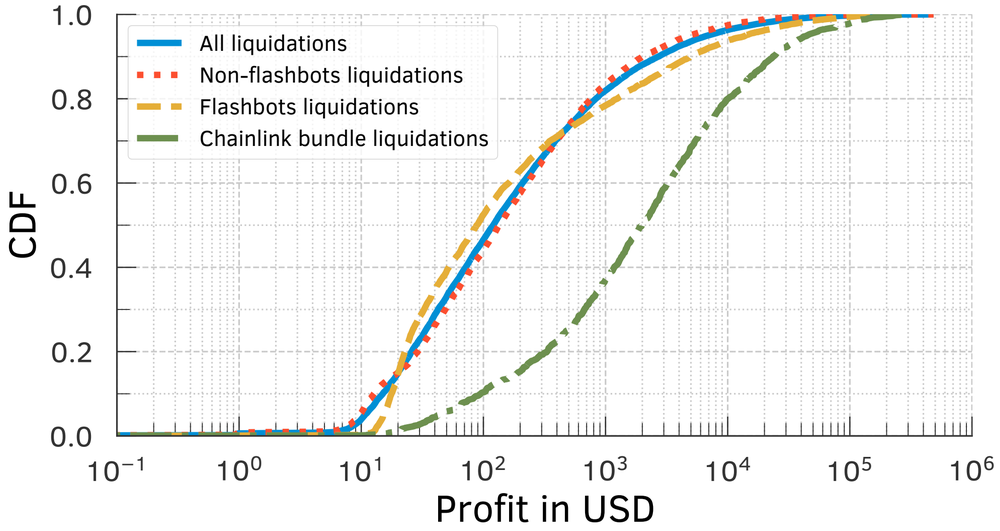
648 in 641 bundles

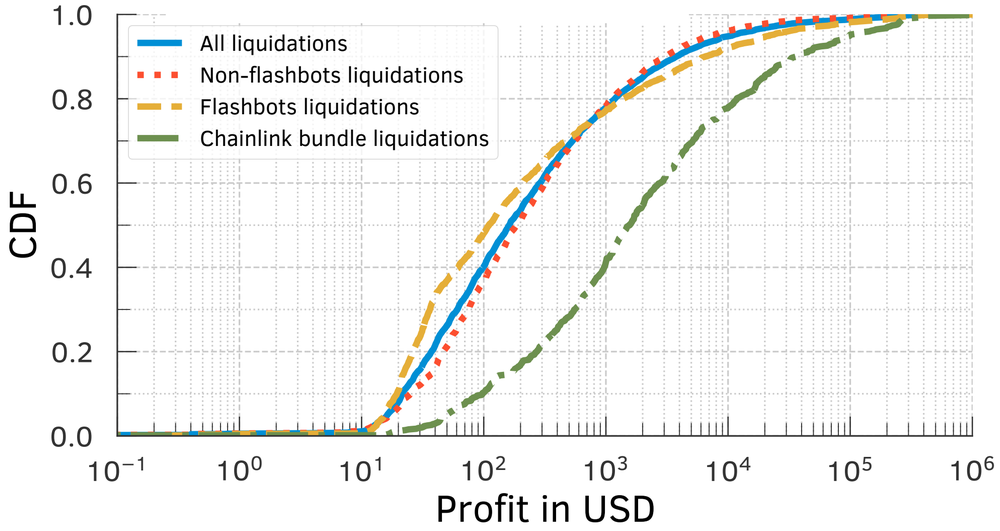
548 bundles

39 bundles

Liquidation With Bundled Chainlink Oracle Updates

- Over-collateralized lending protocols





Profits are ~15x higher when compared to all liquidations when bundling with a Chainlink update

Active Experiments

Taichi Network: Private Transactions

SPARK POOL

- Active experiment
  - We issued 8 transactions and sent them to the Ethereum blockchain.
    - 4 privately through Taichi Network and 4 publicly.

- While running the experiment, we checked if the popular blockchain explorers observed any of our private transactions.
  - if they did, it would imply that the Taichi Network leaked the transactions to the public.
  - Private transactions were only visible after they were committed.
    - Included in the expected block position based on the fees we offered.
  - SparkPool and Babel Pool included each 2 private transactions.

Bitcoin Dark-Fees Transactions

- Active experiment
  - We took 10 snapshots of our MemPool during periods of high congestion.
  - We randomly selected only low-fee rate transactions with a size of 101 bytes for accelerating using ViaBTC transactions accelerator services.
    - 212 in total transactions.
  - We paid ViaBTC 205 € to accelerate the 10 low feerate transactions.

Metrics	Delay in # of blocks		Perc. Position in a block	
	Acc.	Non-acc.	Acc.	Non-acc.
Minimum	1	9	0.07	17.47
25-perc	1	148	0.08	75.88
Median	2	191	0.09	87.92
75-perc	2	247	0.20	95.00
Maximum	3	326	4.39	99.95
Average	1.8	198.5	0.79	84.46

Bitcoin Dark-Fees Transactions

- Active experiment
  - We took 10 snapshots of our MemPool during periods of high congestion.
  - We randomly selected only low-fee rate transactions with a size of 101 bytes for accelerating using ViaBTC transactions accelerator services.
    - 212 in total transactions.
  - We paid ViaBTC 205 € to accelerate the 10 low feerate transactions.

Metrics	Delay in # of blocks		Perc. Position in a block	
	Acc.	Non-acc.	Acc.	Non-acc.
Minimum	1	9	0.07	17.47
25-perc	1	148	0.08	75.88
Median	2	191	0.09	87.92
75-perc	2	247	0.20	95.00
Maximum	3	326	4.39	99.95
Average	1.8	198.5	0.79	84.46

Bitcoin Dark-Fees Transactions

- Active experiment
  - We took 10 snapshots of our MemPool during periods of high congestion.
  - We randomly selected only low-fee rate transactions with a size of 101 bytes for accelerating using ViaBTC transactions accelerator services.
    - 212 in total transactions.
  - We paid ViaBTC 205 € to accelerate the 10 low feerate transactions.

Metrics	Delay in # of blocks		Perc. Position in a block	
	Acc.	Non-acc.	Acc.	Non-acc.
Minimum	1	9	0.07	17.47
25-perc	1	148	0.08	75.88
Median	2	191	0.09	87.92
75-perc	2	247	0.20	95.00
Maximum	3	326	4.39	99.95
Average	1.8	198.5	0.79	84.46

Bitcoin Dark-Fees Transactions

- Active experiment
  - We took 10 snapshots of our MemPool during periods of high congestion.
  - We randomly selected only low-fee rate transactions with a size of 101 bytes for accelerating using ViaBTC transactions accelerator services.
    - 212 in total transactions.
  - We paid ViaBTC 205 € to accelerate the 10 low feerate transactions.

Metrics	Delay in # of blocks		Perc. Position in a block	
	Acc.	Non-acc.	Acc.	Non-acc.
Minimum	1	9	0.07	17.47
25-perc	1	148	0.08	75.88
Median	2	191	0.09	87.92
75-perc	2	247	0.20	95.00
Maximum	3	326	4.39	99.95
Average	1.8	198.5	0.79	84.46

Bitcoin Dark-Fees Transactions

- Active experiment
  - We took 10 snapshots of our MemPool during periods of high congestion.
  - We randomly selected only low-fee rate transactions with a size of 101 bytes for accelerating using ViaBTC transactions accelerator services.
    - 212 in total transactions.
  - We paid ViaBTC 205 € to accelerate the 10 low feerate transactions.

Metrics	Delay in # of blocks		Perc. Position in a block	
	Acc.	Non-acc.	Acc.	Non-acc.
Minimum	1	9	0.07	17.47
25-perc	1	148	0.08	75.88
Median	2	191	0.09	87.92
75-perc	2	247	0.20	95.00
Maximum	3	326	4.39	99.95
Average	1.8	198.5	0.79	84.46

Bitcoin Dark-Fees Transactions

- These transactions were accelerated by 5 MPOs

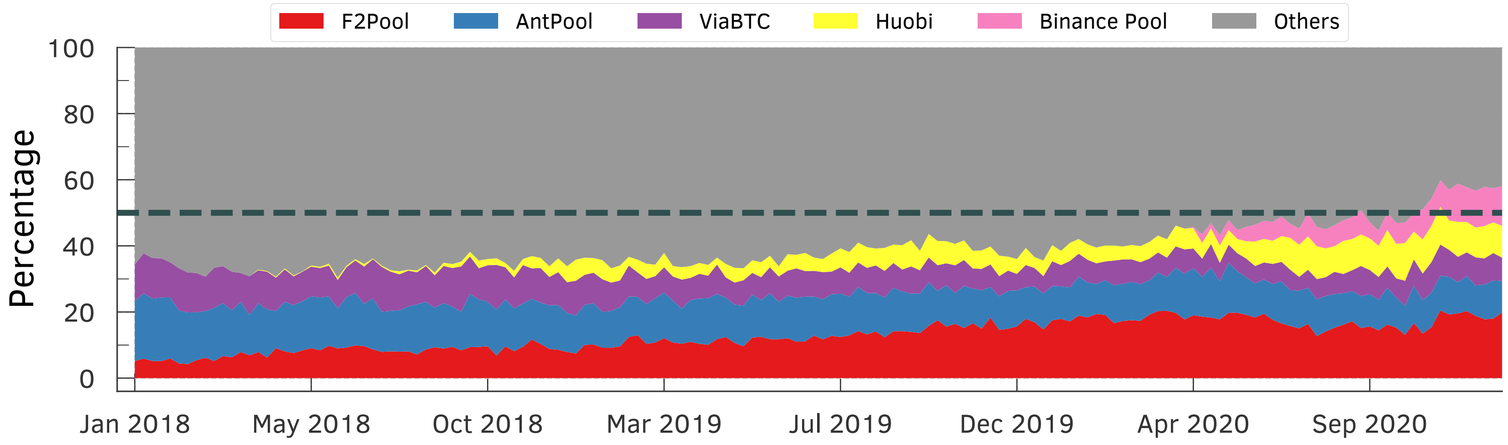
Mining Pool	Hash-rate		
	Last 24h	Last week	Last month
F2Pool	19.9 %	18.7 %	19.9 %
AntPool	12.5 %	10.6 %	10.2 %
Binance	9.6 %	10.3 %	10.0 %
Huobi	8.1 %	9.3 %	9.8 %
ViaBTC	5.1 %	7.1 %	7.7 %
Total	55.2 %	56 %	57.6 %

Mining pools with combined hash rates of over 50% were colluding to include these transactions!

Bitcoin Dark-Fees Transactions

- These transactions were accelerated by 5 MPOs

Mining Pool	Hash-rate		
	Last 24h	Last week	Last month
F2Pool	19.9 %	18.7 %	19.9 %
AntPool	12.5 %	10.6 %	10.2 %
Binance	9.6 %	10.3 %	10.0 %
Huobi	8.1 %	9.3 %	9.8 %
ViaBTC	5.1 %	7.1 %	7.7 %
Total	55.2 %	56 %	57.6 %



Mining pools with combined hash rates of over 50% were colluding to include these transactions!

Bitcoin Dark-Fees Transactions

- We use **SPPE** to measure the percentile deviation of transactions within a block.
  - Large SPPE values indicate that a transaction that should have been included at the bottom is included at the top of the block, confirming acceleration.

- **Accelerated transactions:** transactions with SPPE ≥ 99%.
  - Many large mining pools such as BTC.com, F2Pool, and ViaBTC are likely including accelerated transactions.
  - ViaBTC including them in over 40% of their blocks.

Summary

- Transaction ordering is an important topic to be considered!
- Through active experiments
  - Bitcoin miners collude when accelerating transactions.
  - It is hard to measure how prevalent private transactions are!
- Flashbots bundles are quite prevalent in Ethereum and are highly used for calling DEXes contracts to take advantage of MEV opportunities.
- Many large mining pools include accelerated transactions, with ViaBTC including it in over 40% of their blocks.
- Our observations still hold after the Merge.

Our Data Set and Scripts Are Available

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

thank you!

Dissecting Bitcoin and Ethereum Transactions:
On the Lack of Transaction Contention and Prioritization Transparency in Blockchains

Johnnatan Messias

@johnnatan_me

Joint w/ Vabuk Pahari, Balakrishnan Chandrasekaran, Krishna P. Gummadi, and Patrick Loiseau

Financial Cryptography and Data Security 2023

MAX PLANCK INSTITUTE FOR SOFTWARE SYSTEMS

UNIVERSITÄT DES SAARLANDES

VU VRIJE UNIVERSITEIT AMSTERDAM

Inria

UGA Université Grenoble Alpes