Increased block size and Bitcoin blockchain dynamics

J. Go¨bel, Department of Informatics, University of Hamburg 22527 Hamburg, Germany

A.E. Krzesinski, Department of Mathematical Sciences, Stellenbosch University 7600 Stellenbosch, South Africa

중앙대학교 소프트웨어학과
20150249 김용재

Contents

1. Introduction

2. Increasing the block size & transaction rate

3. Blockchain Simulation Experiments

4. Bitcoin-NG (Next Generation)

5. Conclusion

Introduction

- Bitcoin transactions have an average size of **250 bytes.**

- The **maximum block size** was set at **1 MB** which can contain up to **approximately 4,000 transactions.**

- It implies an average transaction rate of some **7 transactions per second** (TPS).
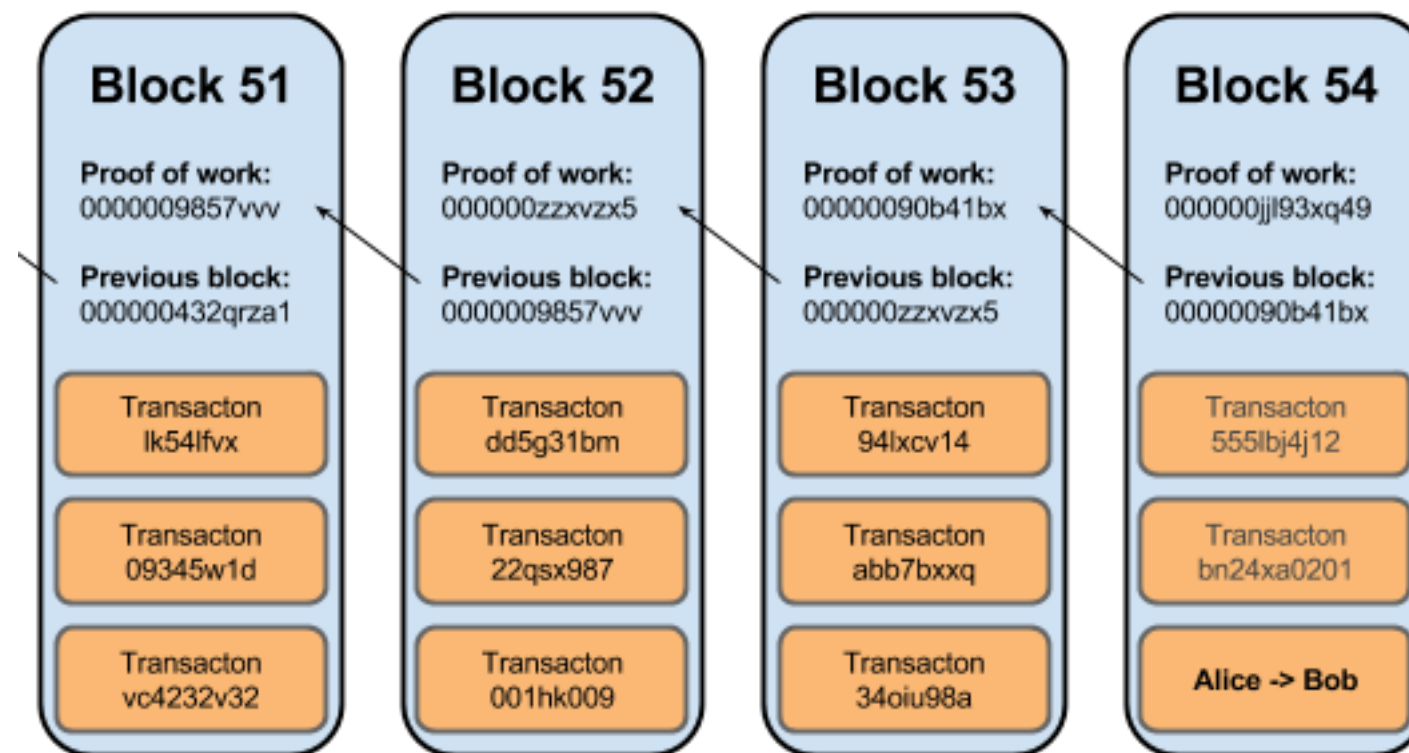
Compared to Other Services

- Currently Bitcoin is **not on par with VISA** which has an average transaction rate of some **2,000 transactions per second (TPS)** with a **peak of 56,000 TPS.**
- Bitcoin is also **not on par with PayPal** which has **170 TPS.**
- Unfortunately, Bitcoin network can handle a sustained rate of some **2.8 TPS** which is far less than commonly assumed because of **increasing average transaction size to 600 bytes.**

In this paper..

- It Investigates **whether larger block sizes can achieve higher transaction processing rates** in Bitcoin.

- It presents a **simulation analysis of Bitcoin-Next Generation** where blocks stripped of transactions propagate rapidly through peer-to-peer network.

- *< Bitcoin-NG: A Scalable Blockchain Protocol >* : Bitcoin NG is a new blockchain protocol designed to scale.

Increasing the Block size & Tx rate

Bitcoin network can handle a transaction rate of some 3 TPS and this has given **rise to investigations about how to increase the transaction throughput.**

- **Decreasing the block mining interval** would require adjustments to the reward model of mining, which **would compromise the profitability of Bitcoin mining.**
- The **only obvious method** for increasing the transaction rate is to **increase the block size.**
- There are many examples of proposed increases in the block size include.

Effect of the block size

- Croman et al. investigated the **effect of the block size and the block mining interval on the performance** of the P2P overlay network in terms of the *X % effective throughput* which blocks propagate within an average block mining interval.
- They reported that for a **block mining interval of 10 min or less,**
  1. **4 MB : 10 % of the nodes** do not receive the blocks before the next block (on average) is mined.
  2. **38 MB : 50 % of the nodes** do not receive.

Blockchain Simulation Experiments

- This study models a small number of nodes, some of which are **miners** and some of which are **relay nodes.**

- In this Bitcoin network model the miners and relays are co-located with randomly selected Bitcoin full nodes.

- **Relay nodes do not mine blocks** and ensure that the **TCP connections don't exceed some 4,000 km apart from the trans-Pacific route.**
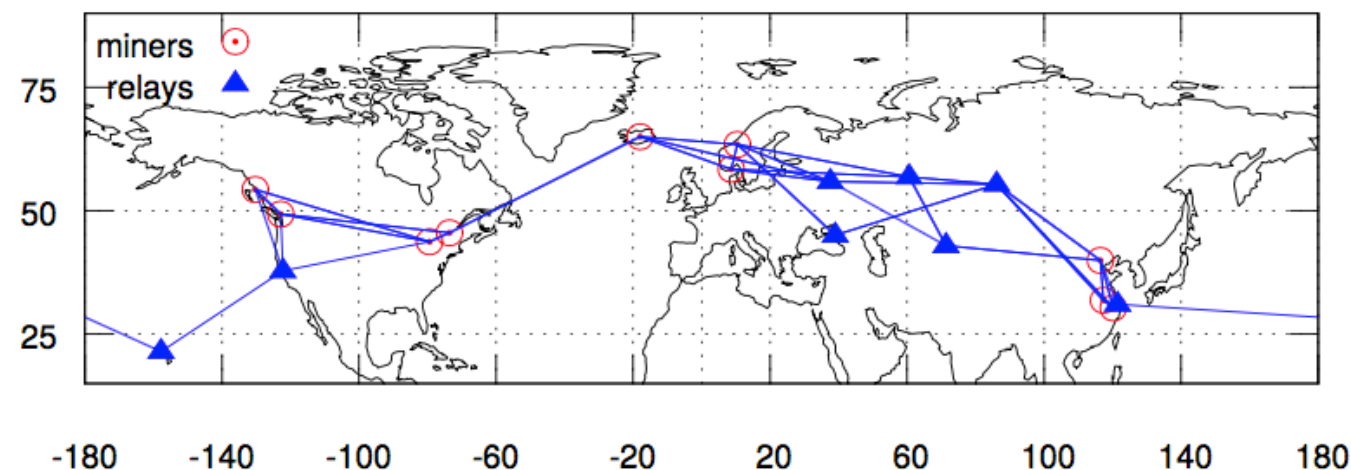
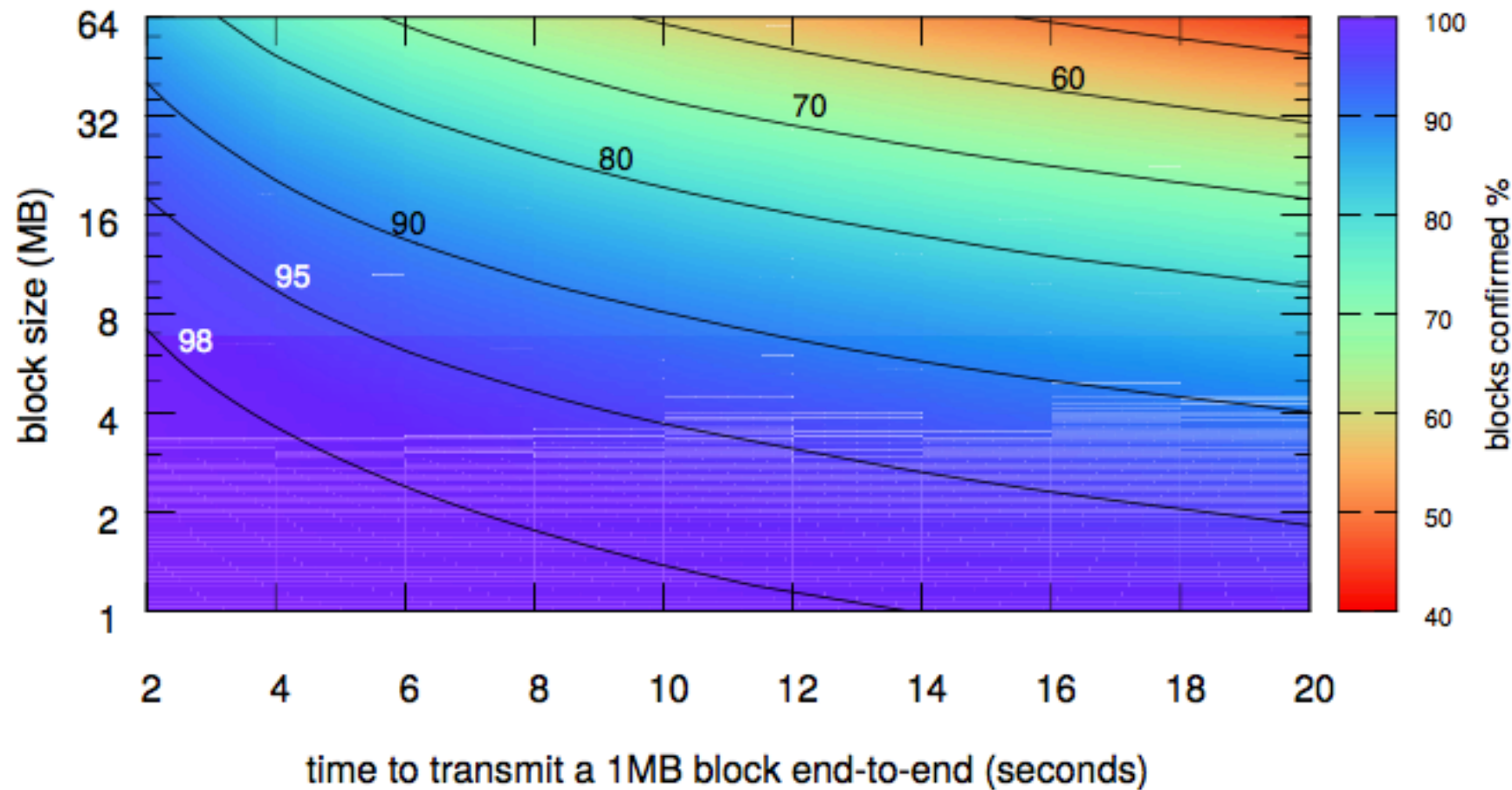- The relays also provide a measure of route diversity.

Figure 1: A random configuration of 10 miners and 10 relays.

Block success probability

Figure 2: Block success probability.

Fig 2 shows that the percentage of blocks admitted to the long-term blockchain becomes unacceptably low as the block size and the basic delay increase.

Consensus mechanism

– **If blocks are mined by different miners within close succession of each other**, the **blockchain splits**, and the **consensus mechanism** is used to determine which **leaf of the blockchain to mine upon.**

– Eventually, all the miners will obtain successors to the blocks they are mining on, so that **one branch of the blockchain becomes longer than the others and this branch become the main branch.**

Splits per day
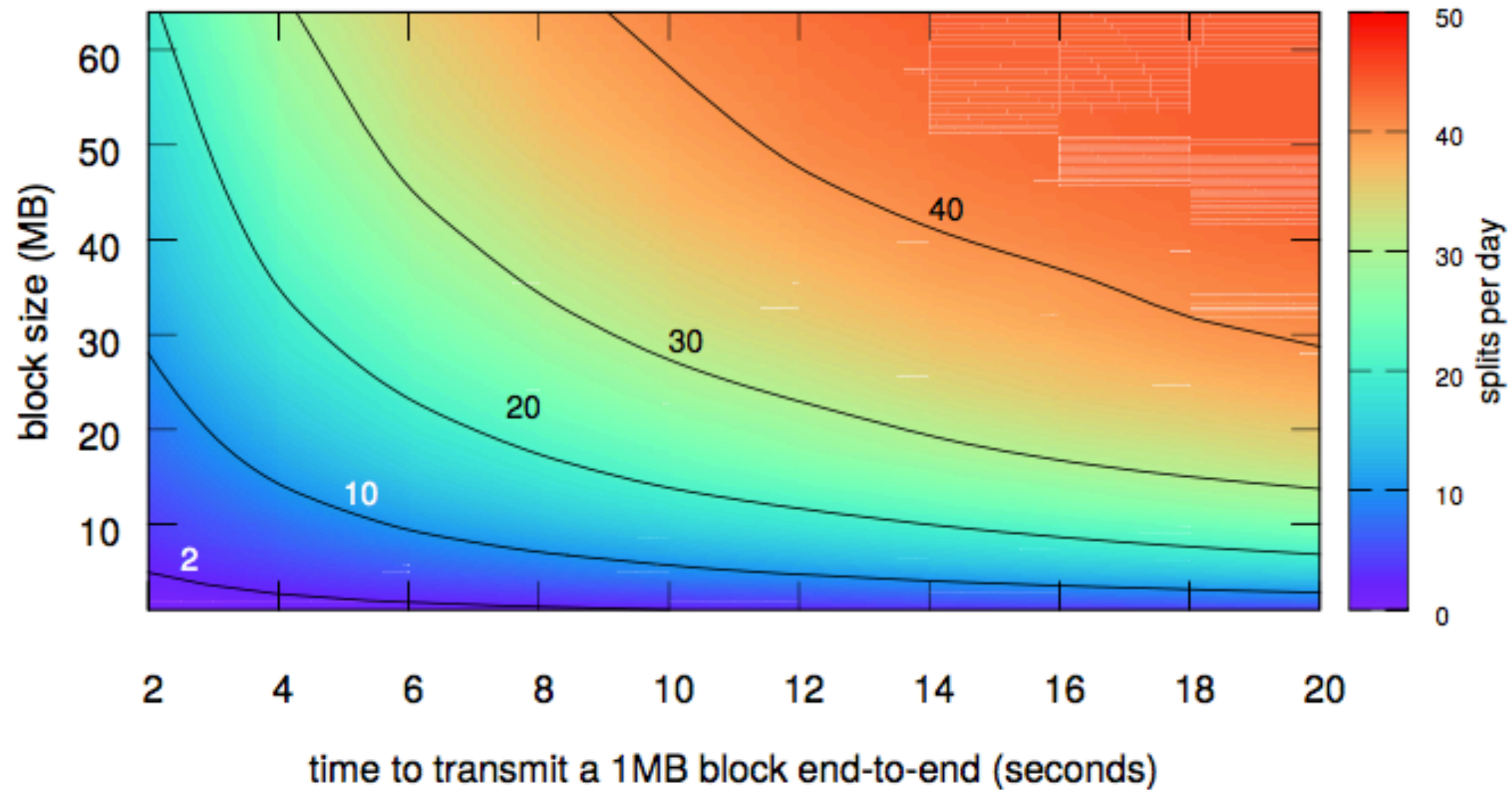
(a) The total number of blockchain splits per day observed at a node.

Highest split order
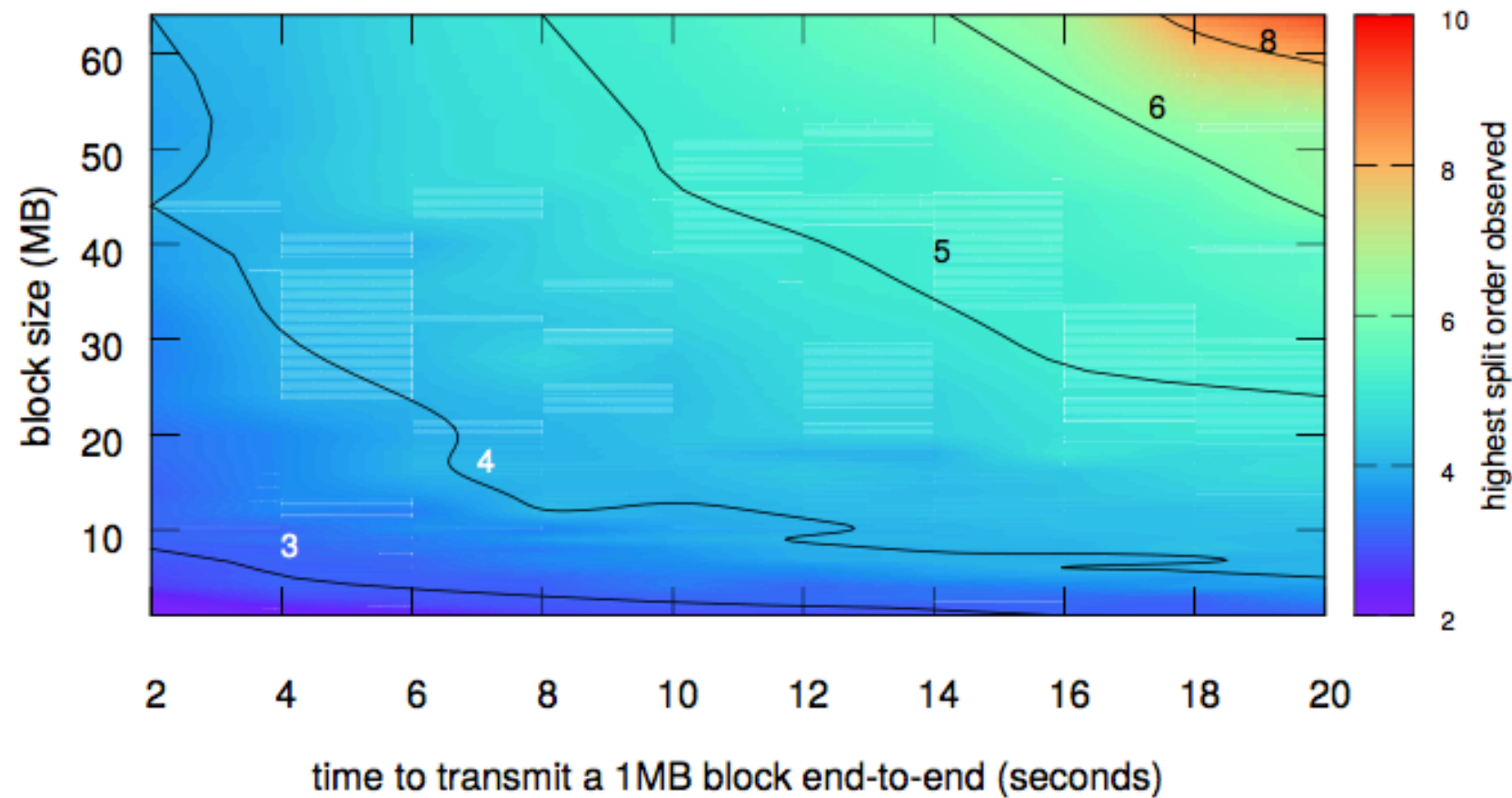
(b) The highest split order observed at a node.

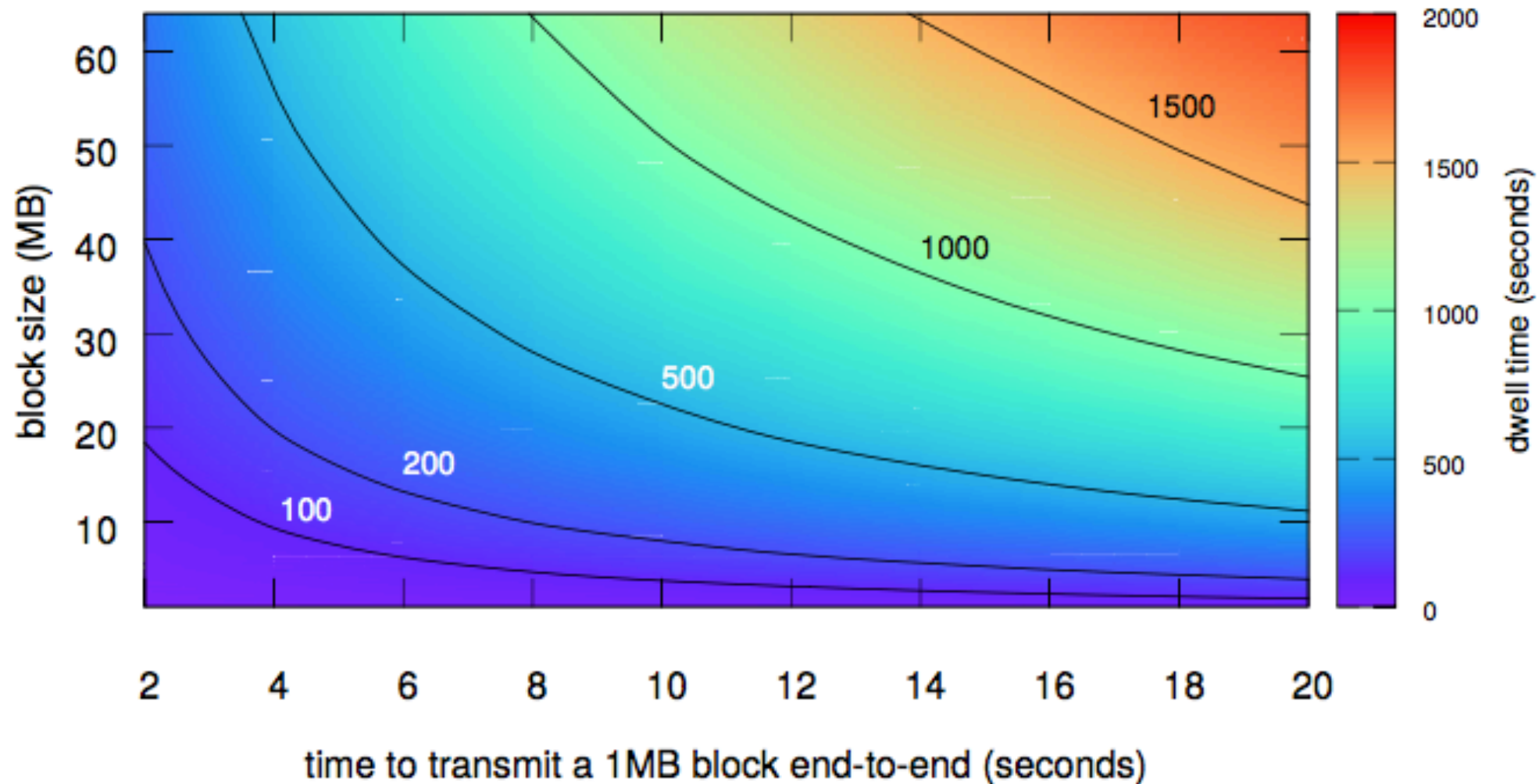Figure 3: Blockchain split behaviour.

The figure shows that larger end-to-end delays and larger block sizes give rise to more splits, and to higher-order splits.

Dwell time

Suppose there is a mechanism that can simultaneously inspect the **blockchains at all the nodes and report if each blockchain has a single leaf.** If this condition occurs then the network is said to be **split-free.**

t0   t   *dwell time*   t'

split-free   split-free   split-free

Dwell time

Figure 4: Blockchain split behaviour.

The figure shows that as the block size and the basic delay increase, the dwell time greatly exceeds the average time taken to mine a block.

Ethereum

- Ethereum is a P2P network and protocol backed by a decentralized repository stored using a blockchain.
- Ethereum is designed to out-perform Bitcoin in its ability to **encode smart contracts into blockchain.**
- **The validation of the correct execution** of such contracts becomes **part of the block mining process.**
- Since block arrivals happen on the order of the block propagation time, **blockchain splits are more likely in Ethereum than in the Bitcoin network.**
- The Bitcoin protocol requires that the longer branch be retained and the shorter branch(es) be discarded. In contrast, The Ethereum blockchain protocol **deletes the lightest subtree.**
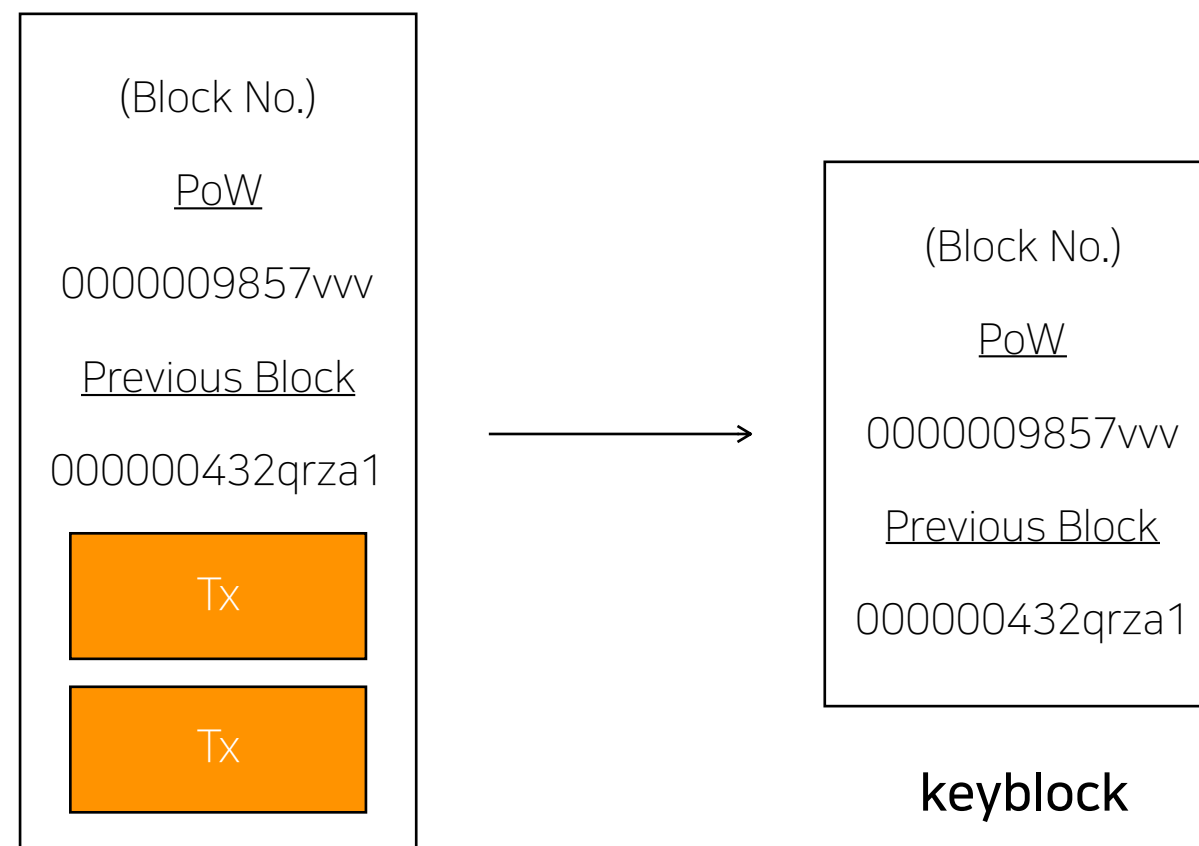
Bitcoin-NG

- Bitcoin-NG is a new blockchain protocol that is designed to scale.
- Bitcoin-NG partitions blockchain operations into two activities namely **leader election** and **transaction serialisation.**
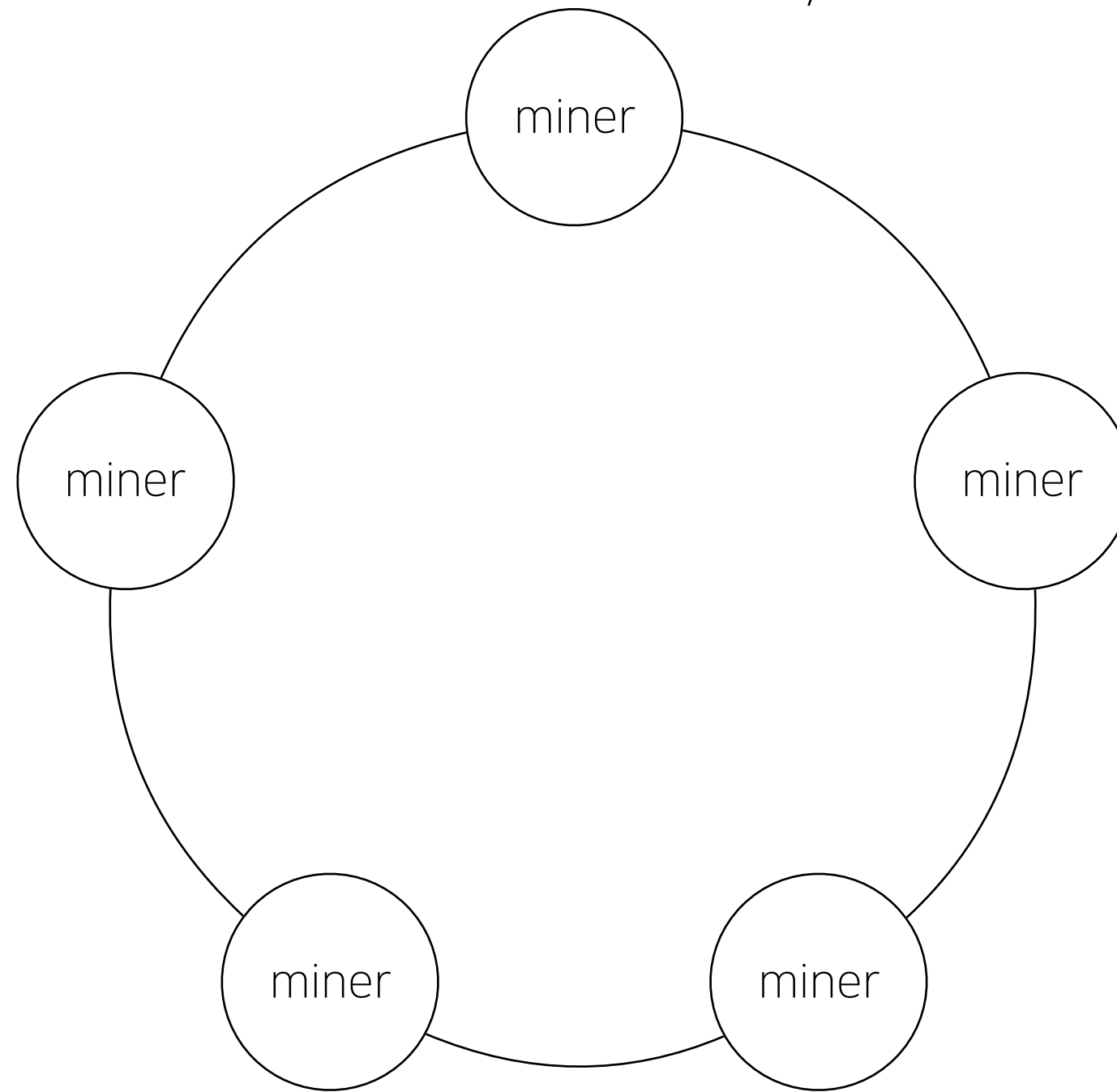
Leader election

- Transactions contribute the most to the payload of a block.
- **Blocks when stripped of transactions are much smaller** and are transmitted end-to-end **much faster.**
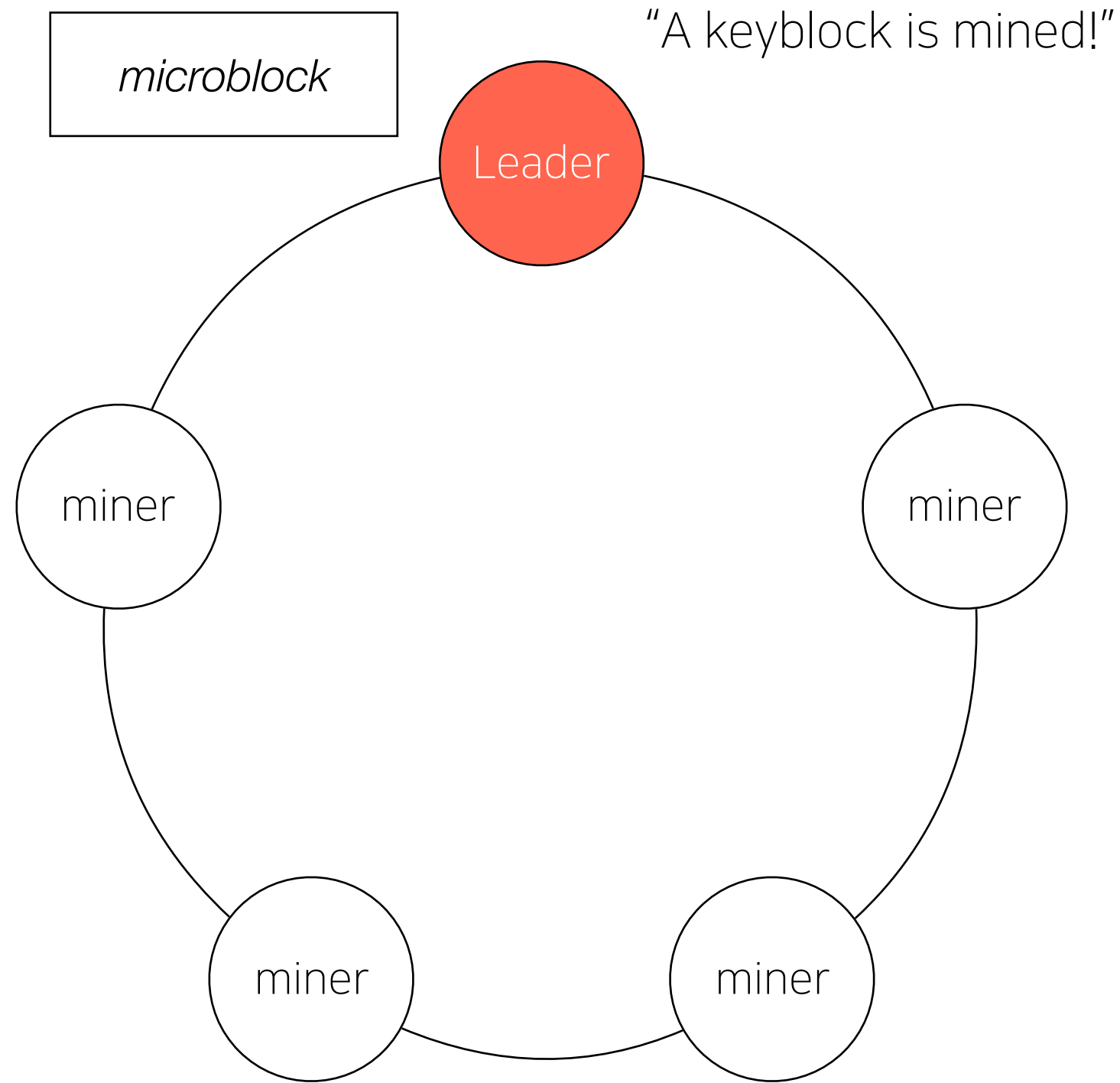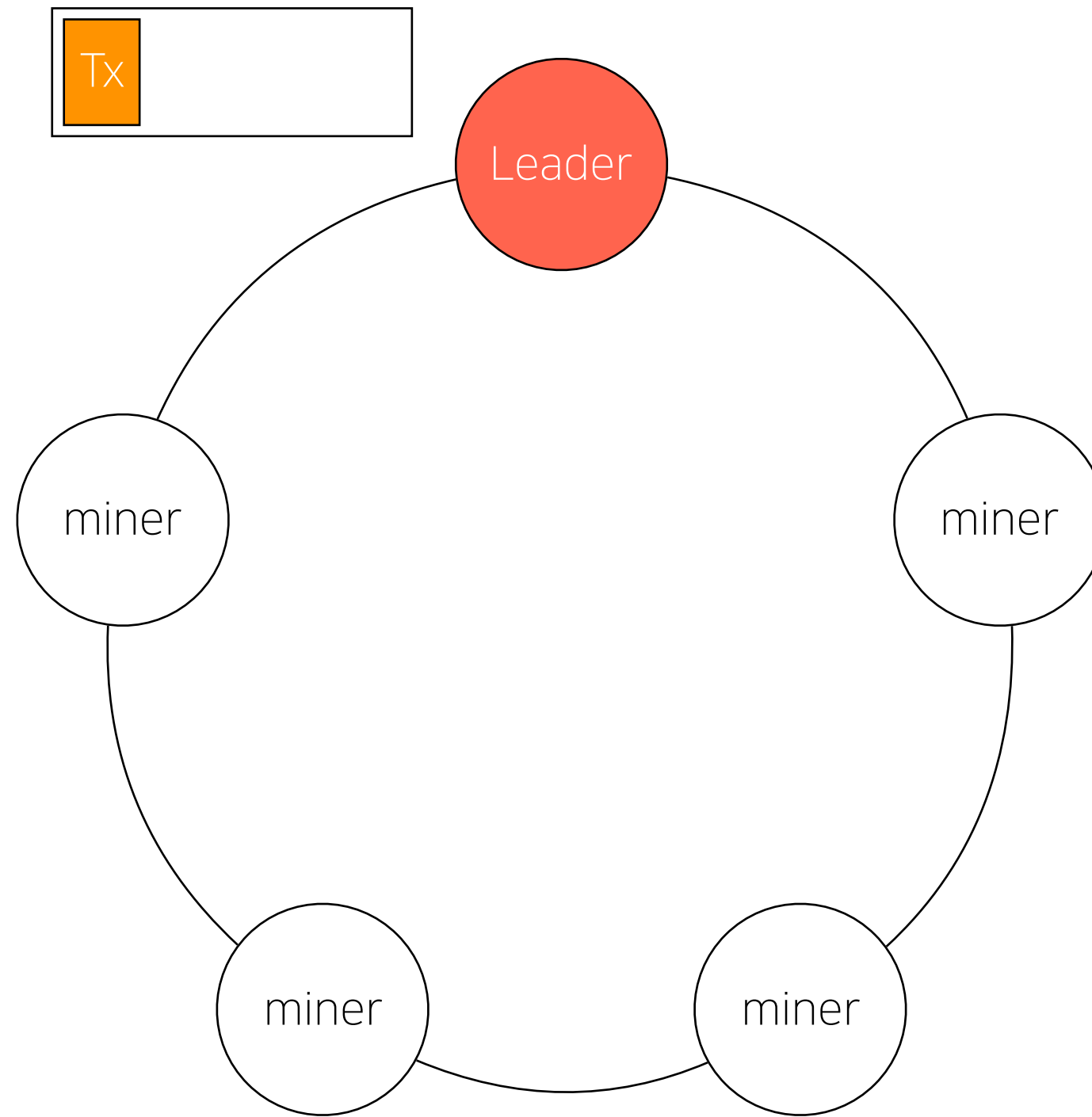- Bitcoin-NG transmits such stripped **keyblocks** end-to-end in **one second on average.**

(Block No.)

PoW

0000009857vvv

Previous Block

000000432qrza1

Tx

Tx

→

(Block No.)

PoW

0000009857vvv

Previous Block

000000432qrza1

keyblock

Leader election

"A keyblock is mined!"

Leader election

microblock
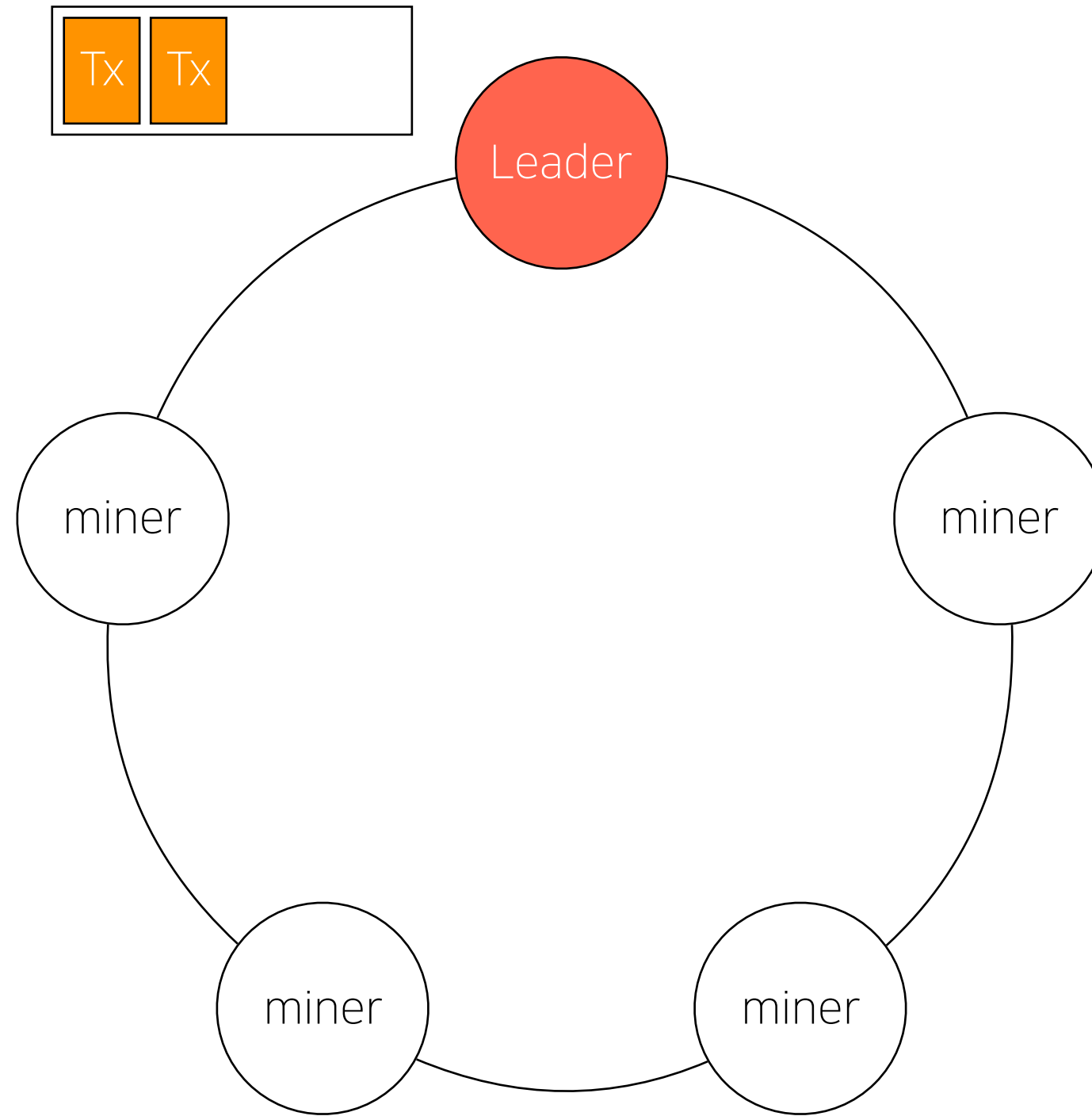
"A keyblock is mined!"
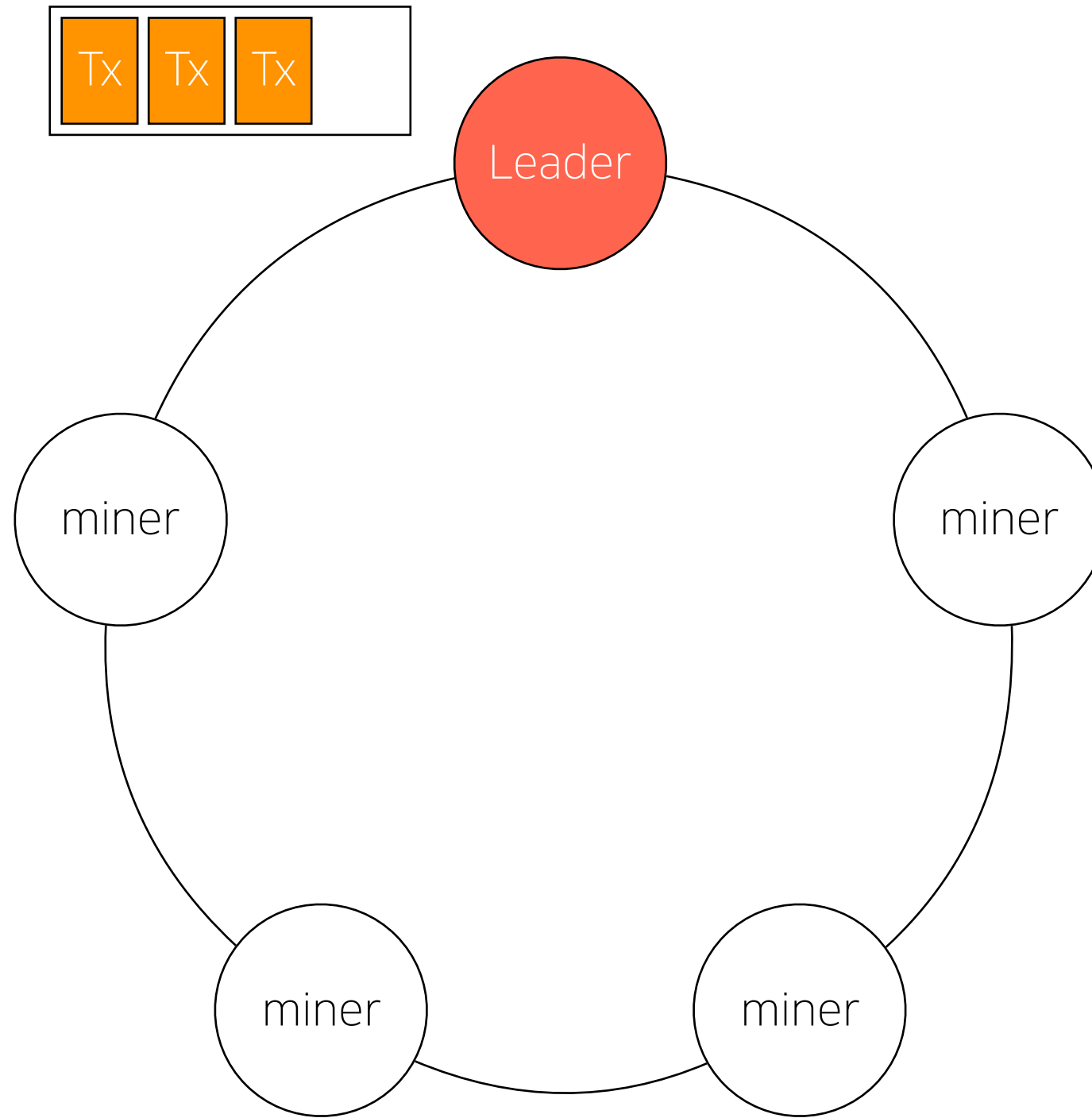
Leader

miner

miner

miner

miner

Leader election

Leader election

Leader election

Leader election
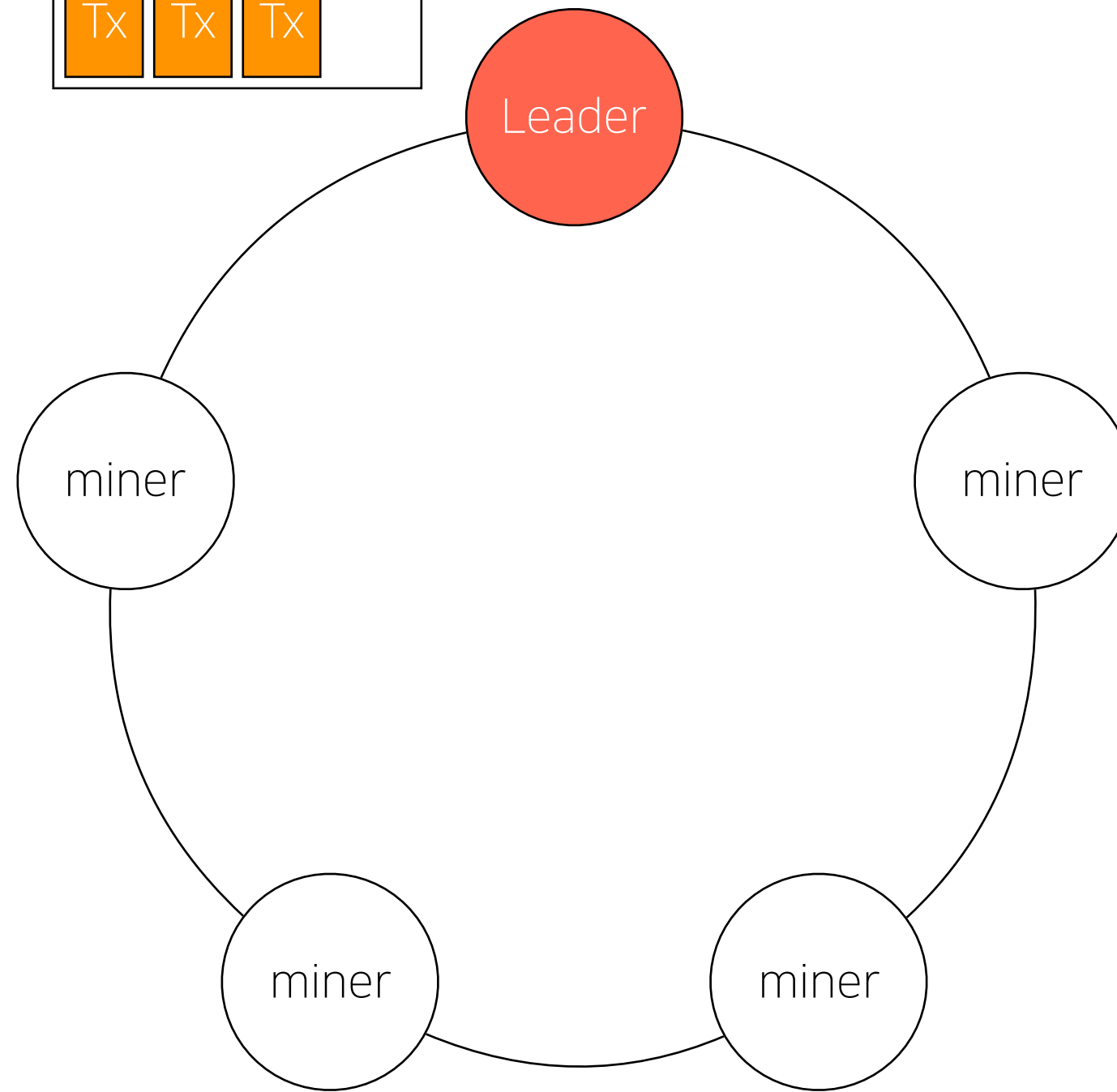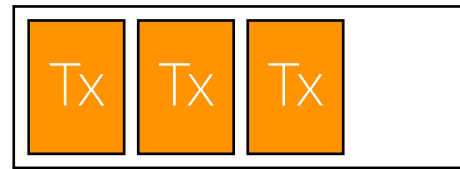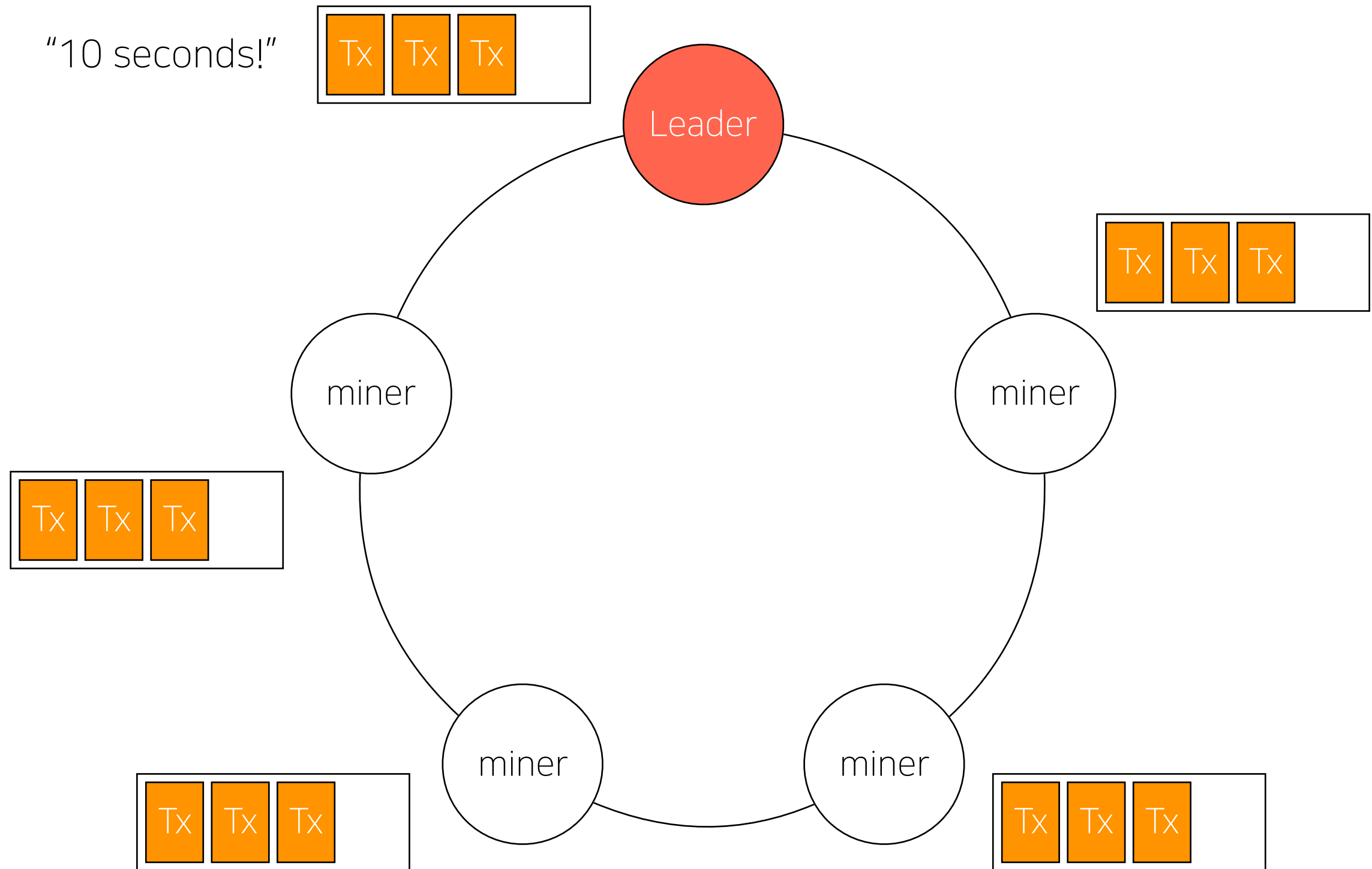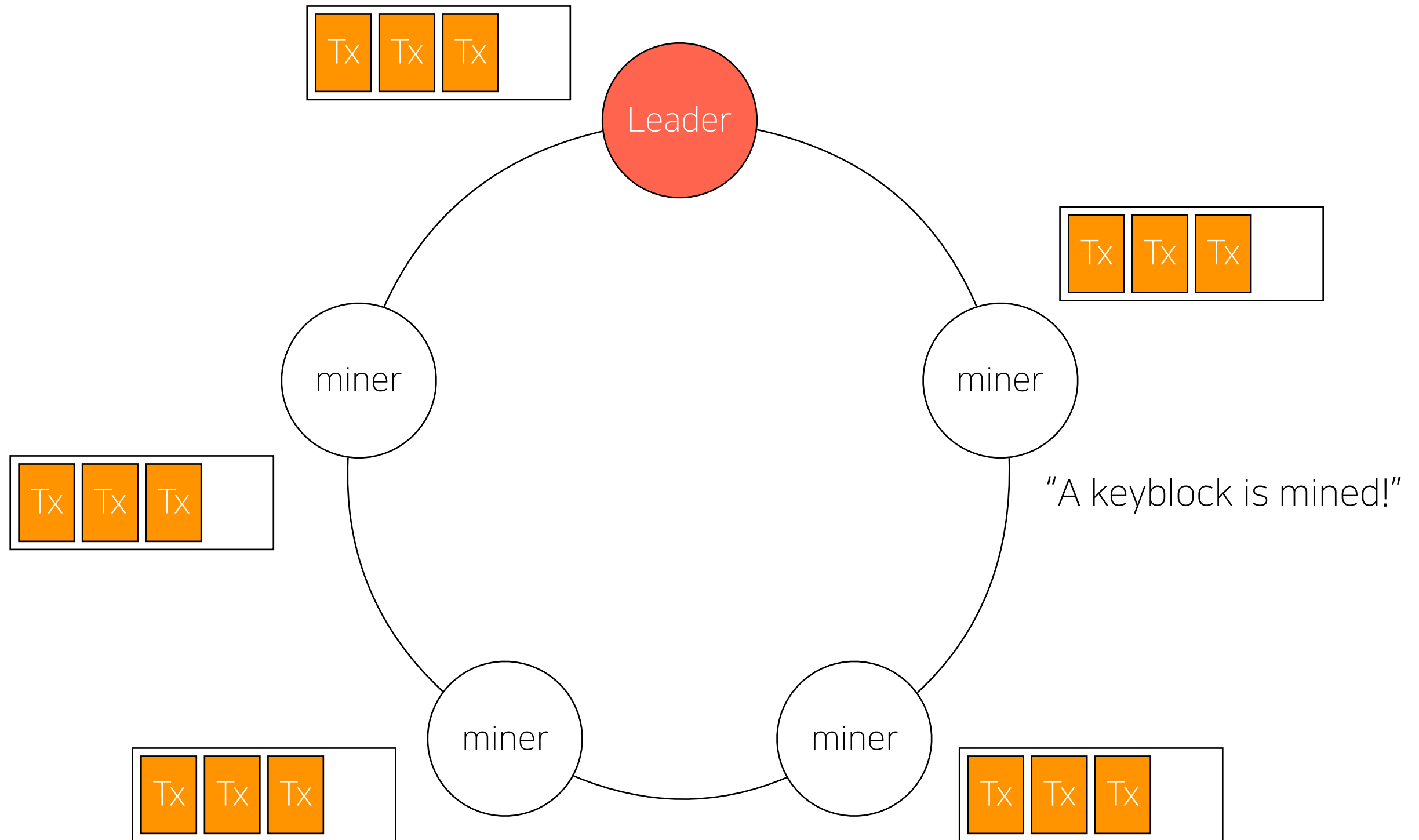
"10 seconds!"

Tx Tx Tx

Leader

miner

miner

miner

miner

Leader election
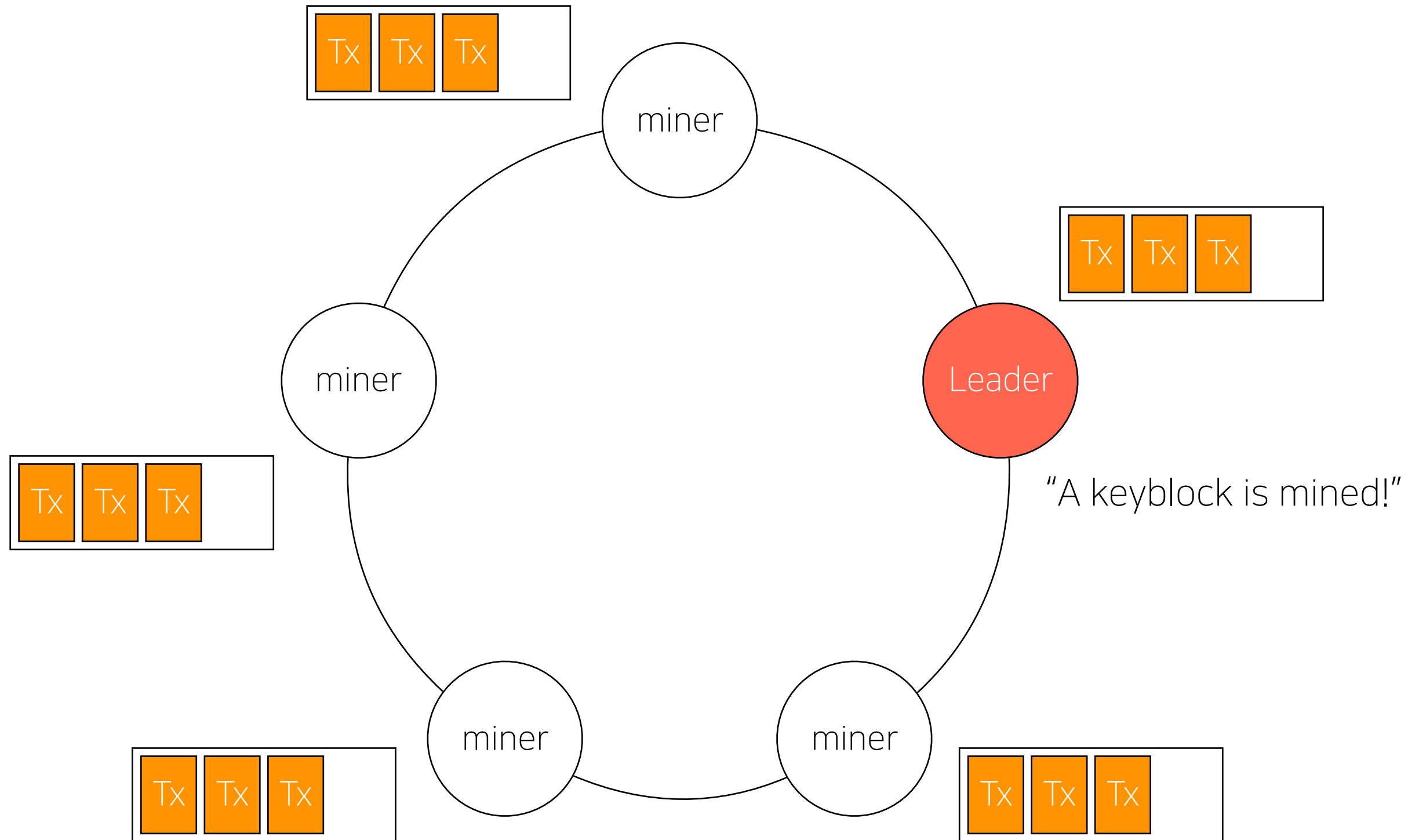
Leader election

Leader election

"A keyblock is mined!"

Transaction serialisation

- The **keyblock header** contains **the same fields as a standard Bitcoin block header**, and **in addition contains a public key** to be used in subsequent microblocks.
- The **microblock header** contains a **reference to the previous block,** the **merkle root of the transactions** in the microblock, and a **cryptographic signature of the header** using the private key of the leader.

Standard Bitcoin Block Header
🔑
public key

keyblock

Microblock Header
.
.
.

microblock

previous block
merkle root
signature of header

microblock header
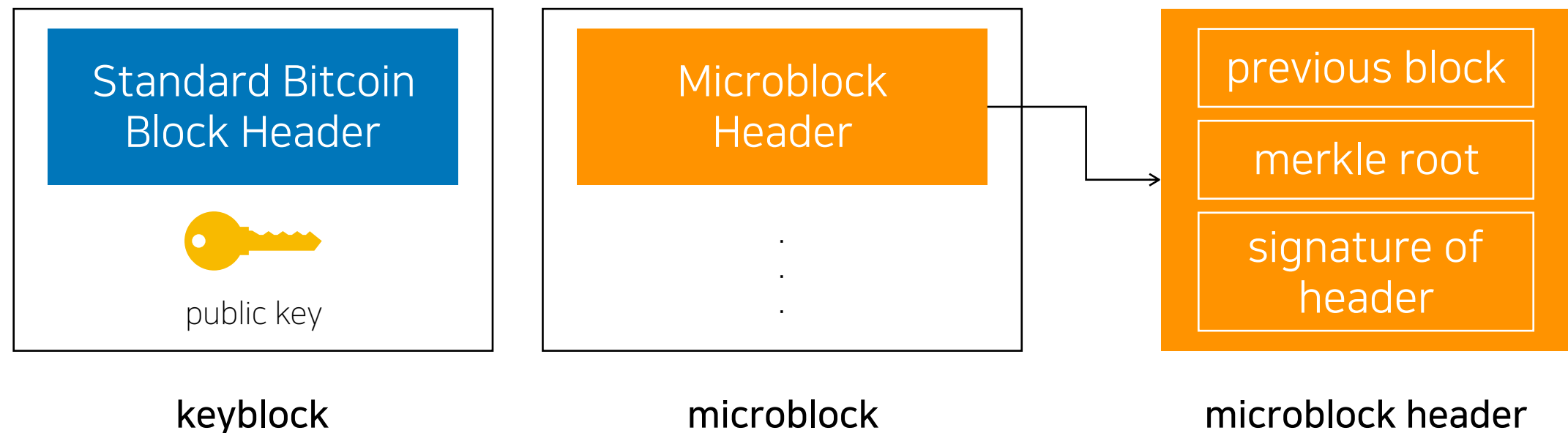
Performance

Table I: Bitcoin, Ethereum and Bitcoin-NG performance.

1 MB delay	payload 10 mins	TPS MAX	TPS Bitcoin-600	TPS Bitcoin-10	TPS Ethereum	TPS Bitcoin-NG
2 sec	1	2.9	2.9 ± 0.0	2.9 ± 0.0	2.9 ± 0.0	2.9 ± 0.0
	8	23.3	22.9 ± 0.2	22.8 ± 0.1	22.8 ± 0.1	23.5 ± 0.0
	64	186.4	159.1 ± 0.9	158.3 ± 1.1	159.9 ± 1.0	187.4 ± 0.1
10 sec	1	2.9	2.9 ± 0.0	2.9 ± 0.1	2.0 ± 0.0	2.9 ± 0.0
	8	23.3	21.0 ± 0.2	20.9 ± 0.1	21.1 ± 0.6	23.5 ± 0.0
	64	186.4	112.4 ± 0.7	112.9 ± 0.4	112.3 ± 0.6	185.3 ± 0.1
20 sec	1	2.9	2.8 ± 0.0	2.0 ± 0.0	2.8 ± 0.0	2.9 ± 0.0
	8	24.0	19.3 ± 0.2	19.3 ± 0.1	19.3 ± 0.1	23.4 ± 0.0
	64	186.4	117.8 ± 10.4	122.1 ± 11.4	102.3 ± 9.1	182.6 ± 0.1

It would appear that **Bitcoin-NG** can attain **PayPal-class** transaction rates.

Conclusion

- The Bitcoin transaction rate is currently limited to about **3 TPS.**

- This is **much less than the transaction rate offered by competing financial transaction processing systems.**

- In this paper, They used discrete event simulation to investigate the consequences of large block sizes.

- **Larger block sizes will not provide VISA-class transaction throughput rates.**

- In general, **Bitcoin-NG perform better than Ethereum and Bitcoin** and it would appear that **Bitcoin-NG can attain PayPal-class transaction rates.**