UNIVERSITY *of* NICOSIA

Session 5

Scalability

From block size limits to bottlenecks caused by DeFi & NFTs

BLOC 514: Emerging Topics in Blockchain and Digital Currency

Session Objectives

- To understand problems that may arise as digital currencies become more popular and distributed peer-to-peer networks reach their original design limits.
- To discuss the limits of current designs in terms of transaction rates, sizes of individual blocks and the size of the blockchain.
- To present the main arguments set forth in the current block size limit debate in Bitcoin.
- To present the major design proposals that have been suggested to improve the Bitcoin's resilience to scalability issues.
- To present the scalability issues related to the recent rise of DeFi and NFTs

Digital Currency Network Growth: Issues and Challenges

Scaling Bitcoin - The problem

- To achieve decentralization, Bitcoin was designed so that anyone would be able to run a node from a personal computer, without a need for specialized hardware or dedicated high-end servers.
  - In other words, an average home computer should be able to perform all tasks needed to constantly maintain consensus with other peers, such as verifying transactions and storing the entire blockchain.
  - The biggest problem is transaction verification, since hashing operations and signature verifications take time – this imposes processing and bandwidth issues.
  - Storing the entire blockchain imposes storage issues.
- To address some of these issues, the Bitcoin network limits the size of each block and, hence, the number of transactions it can carry.
  - The current limit stands at 1Mb per block.
  - At the time of writing this, average block sizes are quickly approaching to the limit.
  - As the network grows to reach the sizes of competing payment networks – the current limits are going to become problematic.

Transactions speeds: the case of FastFabric

SPECIAL ISSUE PAPER | Full Access

FastFabric: Scaling hyperledger fabric to 20 000 transactions per second

Christian Gorenflo, Stephen Lee, Lukasz Golab, Srinivasan Keshav

- According to the authors: "In this paper, we rearchitect a modern permissioned blockchain system, Hyperledger Fabric, to increase transaction throughput from 3000 to 20 000 transactions per second. We focus on performance bottlenecks beyond the consensus mechanism, and we propose architectural changes that reduce computation and I/O overhead during transaction ordering and validation to greatly improve throughput."
- Pre-print version in arxiv

Scaling Bitcoin – problems & solutions

- As long as Bitcoin popularity continues to increase, **design limits will eventually be reached** – perhaps very soon. If so, one should expect at least the following:
  - If blocks are not big enough to include all pending transactions, **miners will simply queue transactions** for the next available block.
  - The transactions with the highest fees per kilobyte will be favored and will be confirmed earlier.
  - **Low-fee, low-amount transactions will suffer most**.
- This can result in a **slow, unreliable** and **expensive** payment system.
- In order to overcome this problem **many solutions have been proposed**.
  - Most of them are suggesting to **increase the block size,** either **statically** (to a new limit, fixed or deterministically decided) or **dynamically** (continuously re-adjusting it, according to needs).
  - Other proposals are suggesting **off-the-blockchain transactions** that will ease the burden of many large blockchain transactions.

What if nothing is done?

- Bitcoin lead developers have offered a number of opinions on this issue:
  - Gavin Andresen believes that the "average transaction fee paid will rise, people or applications unwilling or unable to pay the rising fees will stop submitting transactions, people and businesses will shelve plans to use Bitcoin, stunting growth and adoption" (source)
  - Mike Hearn believes there would be "crashing nodes, a swilling transaction backlog, a sudden spike in double spending, skyrocketing fees" (source)
  - Jeff Garzik writes "as blocks get full and the bidding war ensues, the bitcoin user experience rapidly degrades to poor. In part due to bitcoin wallet software's relative immaturity, and in part due to bitcoin's settlement based design, the end user experience of their transaction competing for block size results in erratic, and unpredictably extended validation times" (source)
  - Pieter Wuille, replying to Andresen's comment above, notes: "Is it fair to summarize this as 'Some use cases won't fit any more, people will decide to no longer use the blockchain for these purposes, and the fees will adapt.'? I think that is already happening [...]" (source)

Debating on the block size

- Questions similar to "What is a reasonable upper bound of block size that would get us the scaling benefits without putting the decentralization of bitcoin at risk?" underlie the ongoing block size debate, which represents a trade-off between the number of transactions the Bitcoin network can handle and its decentralization.
  - The larger a block, the more transaction volume the network can handle.
  - But, larger blocks are harder to propagate, thus putting smaller miners at a disadvantage.

- In order to answer these questions, one must note two things:
  - The resources used by Bitcoin: Processing power, Storage, Bandwidth
  - Other related metrics
  - Technological evolution. Our thinking about what resources can be accommodated in the future must take into account Moore's Law – and its limitations.

- Related debate: Block size limit controversy

Basic metrics of Bitcoin

- **Cost per Confirmed Transaction (CPCT)**
  - The cost in USD of resources consumed by the entire Bitcoin system to confirm a single transaction. The CPCT encompasses several distinct resources, all of which can be further decomposed into operational costs (mainly electricity) and capital equipment costs.

- **Mining**
  - Expended by miners in generating the proof of work for each block.

- **Transaction validation**
  - The cost of computation necessary to validate that a transaction can spend the outputs referenced by its inputs, dominated by cryptographic verifications.

Basic metrics of Bitcoin

- **Bandwidth**
  - The cost of network resources required to receive and transmit transactions, blocks, and metadata.
- **Storage**
  - The cost (1) of storing all currently spendable transactions, which is necessary for miners and full nodes to perform transaction validation, and (2) of storing the blockchain's (much larger) historical data, which is necessary to bootstrap new nodes that join the network.
- **Bootstrap time**
  - The time it takes a new node to download and process the history necessary to validate the current system state.

Basic metrics of Bitcoin

- **Maximum throughput**
  - **Throughput** is the rate at which the blockchain can confirm transactions. Today, Bitcoin's maximum throughput is about 3.3-7 transactions/sec (depending on the assumptions made).
  - All scalability proposals aim at ultimately increasing Bitcoin's throughput. Otherwise, the network will not be able to scale up to compete with alternative payment channels (e.g. PayPal, Visa).

- **Latency**
  - **Latency** refers to the time it takes, on average, for a transaction to confirm.
  - A transaction is considered confirmed when it is included in a block. If all transactions are included in the first block that follows them, latency should be five minutes on average. In practice, it is much longer, as the scalability problem affects the ability of transactions to find space in blocks.

Processing power

- In Bitcoin terms, **the more processing power your computer has, the more transactions it can process**.
- Bitcoin utilizes processing power **mostly for verifying transactions**.
- To verify a transaction, a Bitcoin node needs to perform the following, computationally intensive, tasks:
  - **hashing** (sha256 and ripemd160)
  - **signature verifications** (ECDSA)
- According to a study, which also takes into consideration disk seek time, we cannot hope to scale beyond **200 transactions per second** (source) – based on the current generation of hardware.
- Theoretically, processing power when considered individually (as a technical specification) does not seem to be an obstacle for increasing the block size (e.g., up to 60Mb**)**

Storage

- Maintaining a full bitcoin node means storing every single transaction ever recorded on the blockchain.
  - Full nodes need at least **440+Gb** (as of Nov 2022 - source)

- If the network grows to the size of competing networks, storage requirements will skyrocket
  - For **200 transactions per second (tps)** – a reasonable target, given PayPal's current rate of 100 tps –nodes would require an additional storage space of 3Tb per year.
  - For credit card company-like throughput (**10,000 tps**), storage needs are increasing prohibitively, even for high-end servers.

- One might argue that storage is cheaper than processing power, but even so, storage needs might easily become a considerable burden for nodes – *remember that Bitcoin is designed to have the entire blockchain stored at **every** full node.*

Bandwidth

- Assuming that a bandwidth of 10Mbits/s is available, the rate with which nodes can receive transactions is limited to approximately 2,000 transactions per second.
  - Keep in mind that each node is informed about every transaction multiple times
  - Furthermore other non-transaction messages are broadcasted over the network
  - Of course, nodes might be used for other purposes, too

  - What happens if bandwidth is not enough
    - Peers won't be able to receive and validate transactions in time
    - As a result will become unable to synchronize with the rest of the network

Bandwidth

- Although transactions themselves don't seem to be causing any problem in regards to bandwidth, larger blocks would take **longer to propagate** over the network.
  - When a block solution is found, the new block is broadcast all over the network. As the block size grows to 1Mb, **a block takes several minutes to fully propagate**.
  - This may lead to a new block being created while another still propagates – remember, *blocks are supposed to be discovered every 10 minutes on average*.
  - When this happens, one of the two blocks will be discarded and, in effect, the network is **wasting hashing power** – this opens the possibility for less-than-50% (of the total hashing power) attacks.
  - **Increasing the block size** to accommodate more transactions will further degrade the security of the network and **will centralize mining** (as a miner does not need to wait to receive their own block).

Bitcoin Improvement Proposals

BIP

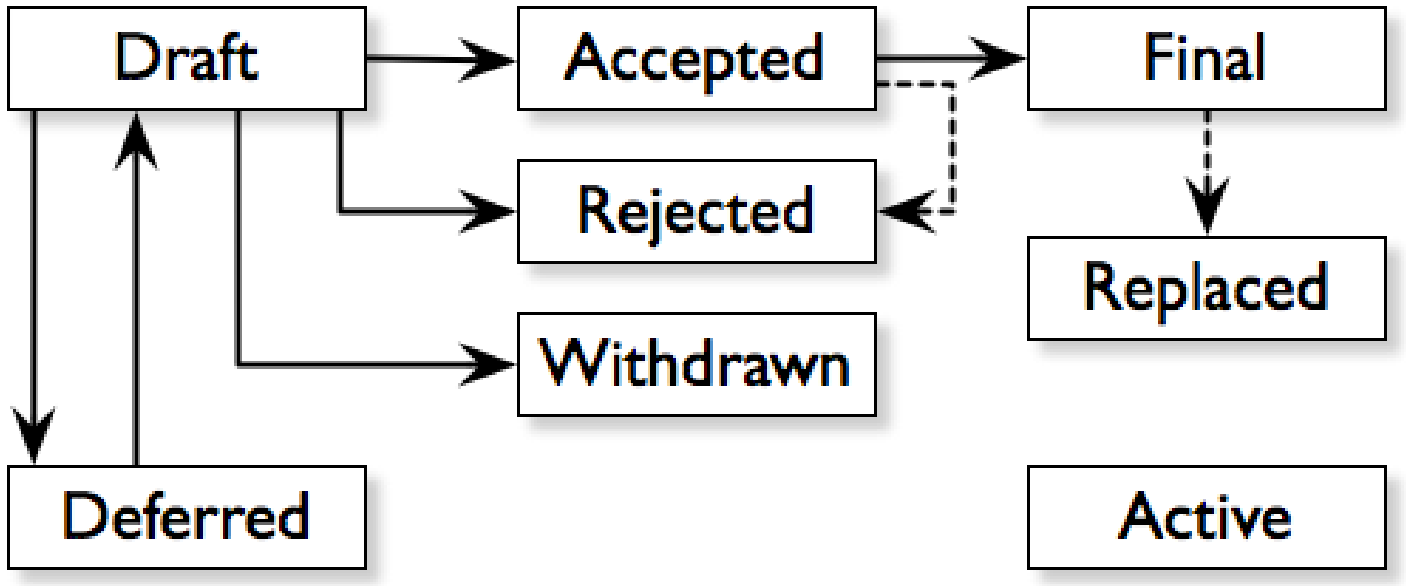
- A Bitcoin Improvement Proposal (BIP) is a design document providing information to the Bitcoin community, or describing a new feature for Bitcoin or its processes or environment. The BIP should provide a concise technical specification of the feature and a rationale for the feature (here).
  - Related short article
- Numerous BIPs
  - Complete list: https://github.com/bitcoin/bips

- There are three kinds of BIP:
  1. A **Standards Track BIP** describes any change that affects most or all Bitcoin implementations, such as a change to the network protocol, a change in block or transaction validity rules, or any change or addition that affects the interoperability of applications using Bitcoin. Standards Track BIPs consist of two parts, a design document and a reference implementation.
  2. An **Informational BIP** describes a Bitcoin design issue, or provides general guidelines or information to the Bitcoin community, but does not propose a new feature. Informational BIPs do not necessarily represent a Bitcoin community consensus or recommendation, so users and implementors are free to ignore Informational BIPs or follow their advice.

BIP

- There are three kinds of BIP (con't):
    3. A **Process BIP** describes a process surrounding Bitcoin, or proposes a change to (or an event in) a process. Process BIPs are like Standards Track BIPs but apply to areas other than the Bitcoin protocol itself. They may propose an implementation, but not to Bitcoin's codebase; they often require community consensus; unlike Informational BIPs, they are more than recommendations, and users are typically not free to ignore them. Examples include procedures, guidelines, changes to the decision-making process, and changes to the tools or environment used in Bitcoin development. Any meta-BIP is also considered a Process BIP.

BIP: Overall Process



Source: https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki

Indicative Examples: BIP102 - BIP103

- **BIP102**: Jeff Garzik proposed a **one-time block size increase from 1Mb to 2Mb**.

- **BIP103**: BIP103 (by Pieter Wuille) proposes a block size growth intended to accommodate for hardware and other technological improvements for the foreseeable future.
  - This is achieved by **replacing the current block size limitation with a function that allows a maximum increase in block size by 4.4% each time.**
  - The **average expected growth rate using the proposed function is 17.7% per year**, which seems to be consistent with the average growth rate of bandwidth during the last few years.
  - If over time, this growth factor is beyond what the actual technology enables, the intention should be to **soft fork a tighter limit**.

Indicative Examples: BIP105

- **BIP105**: BIP105 (by BtcDrak) is a method of **altering the maximum allowed block size of the Bitcoin protocol using a consensus-based approach**. The rationale behind the proposal is:
  - Predetermined block size increases are problematic because they attempt to predict the future.
  - Dynamic block size adjustments suffer from the potential to be gamed by large hash power.
- The specifications of BIP105 are:
  - The block size **cannot be below 1Mb or above 8Mb**.
  - **Each time a miner finds a block, they may vote to increase or decrease the block size**, by not more than 10% of the current size limit.
  - If a miner votes for an increase, the block hash must meet a difficulty target which is proportionally larger that the difficulty target base of the percentage increase they voted for. This is not required for votes proposing a decrease.
  - **Every 2,016 blocks, the block size limit is determined by the median of all votes.**

Indicative Examples: BIP106

- **BIP106**: Upal Chakraborty proposed **two different ways to dynamically control block size limits**.
  - The first proposal depends only on previous block size calculations, while the second considers the transaction fees collected by miners.
- **Proposal 1:**
  - If the majority of the last 2,000 blocks are more than 90% of the maximum block size limit then double the limit.
  - If 90% of the last 2,000 blocks are less than 50% of the maximum block size limit then halve the limit.
- **Proposal 2**:
  - This proposal will not increase the maximum block size if the transaction fee collection is not increasing.
  - In other words, **people using Bitcoin will be able to increase or decrease the block size** by giving more or less fees to the miners.

Indicative Examples: BIP107

- **BIP107**: Dr Washington Y. Sanchez proposed **a two-phase increase in the block size based on transaction volume**.
- **Phase 1**
  - Block size will be increased similarly to BIP101, as a safe runway prior to switching to phase 2, while network and protocol infrastructure is improved.
  - Maximum block sizes will be 2Mb per block in 2016, 4Mb in 2018 and 8Mb in 2020.
- **Phase 2**
  - After the last increase of phase 1 in 2020, **the maximum block size will keep increasing dynamically according to increases in transaction volume**.
  - Every 4,032 blocks, a check will be performed to determine if a raise in the max block size should occur. This can result to a maximum of 13 increases per year.
  - If the last 3,025 blocks were at least 60% full, the maximum block size will be increased by 10%.
  - Unlike other proposals, the maximum block size can only be increased, not decreased.

Indicative Examples: BIP141 & 144 (Segregated Witness)

- The Segregated Witness approach is **a method for minimizing the footprint of transactions inside blocks.**
- Originally presented by Pieter Wuile in December 2015, Segregated Witness is based on a concept used in sidechain Elements. **SegWit** has been proposed in BIP141 (Consensus Layer) by Eric Lombroso, Johnson Lau and Pieter Wuille and in BIP144 (Peer Services) by Lombrozo and Wuille.
- **How it works:**
  - Bitcoin transactions include one or more inputs, one more outputs and a signature that validates that the owner had the ability to execute the transaction.
  - The Segregated Witness approach **removes the signature from the transactions** and puts it into a Merkle tree in the **coinbase** component of the transaction (a coinbase transaction is the transaction created by a miner when finding a new block and contains the block reward).
  - This change would make transactions appear smaller to the network, thus allowing more transactions to be included on a block.
  - Unlike other proposed Bitcoin improvements, **Segregated Witness can be introduced to the network without the need of a hard fork**, thereby reducing risk.

Recent BIPs: Taproot (1/3)

- Taproot: regarded as the fist major upgrade since SegWit (2017)

- Timeline
  - Jan 2018: proposal Gregory Maxwell
  - June 2021: consensus for implementation
  - **Nov 2021**: activated (at at block 709,632 - see related article)

- What it is: Umbrella for 3 BIPs
  - BIP340 (BIP – Schnorr)
  - BIP341 (BIP – Taproot)
  - BIP342 (BIP – Tapscript)

Recent BIPs: Taproot (2/3)

- Extensive info [*] can be found in the respective BIP repository

```
BIP: 340
Title: Schnorr Signatures for secp256k1
Author: Pieter Wuille <pieter.wuille@gmail.com>
        Jonas Nick <jonasd.nick@gmail.com>
        Tim Ruffing <crypto@timruffing.de>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0340
```

```
BIP: 341
Layer: Consensus (soft fork)
Title: Taproot: SegWit version 1 spending rules
Author: Pieter Wuille <pieter.wuille@gmail.com>
        Jonas Nick <jonasd.nick@gmail.com>
        Anthony Towns <aj@erisian.com.au>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0341
```

```
BIP: 342
Layer: Consensus (soft fork)
Title: Validation of Taproot Scripts
Author: Pieter Wuille <pieter.wuille@gmail.com>
        Jonas Nick <jonasd.nick@gmail.com>
        Anthony Towns <aj@erisian.com.au>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0342
```

- [*] *Note: The tech details (as included in the above repository) are **not needed** for the final exam.*

Recent BIPs: Taproot (3/3)

- **BIP340 – Schnorr signature**
  - Implementation of a new cryptographic signature being smaller and more secure
  - Introduction of “key aggregation": handles multi-signature transactions as a single-signature transaction - enables data savings in the blockchain
- **BIP341 – Taproot**
  - Based o Segwit
  - Implementation of Merklized Alternative Script Trees (MAST)
  - MAST make only the satisfied (i.e., executed) conditions of a smart contract being recorded to the blockchain - enables advanced security
- **BIP342 – Tapscript**
  - Updates in the Bitcoin script supporting the aforementioned BIPs (BIP340&341)
- Also:
  - See current usage of the Taproot-based transaction: here

DeFi & NFTs Causing Parallelization Bottleneck

Scalability in the era of DeFi & NFTs

- Regarding Ethereum-based protocols, main approaches for tackling scalability issues include:
  - Layer 2 approaches
  - In general, integration with off-chain systems
  - Sharding
  - Transition from PoW to PoS
- However, the above approaches do not consider the fact that transactions are changing
  - From the early days to the current era of DeFi and NFTs
- Goal: Analyze, understand and improve(if possible) transaction parallelization
  - Why? Small number of smart contracts constitute parallelization obstacle
  - This holds especially for the case of applications related to DeFi and NFTs
- Recent study: "DeFi and NFTs Hinder Blockchain Scalability" by Heimbach et al. (2023)

Scalability in the era of DeFi & NFTs

[Submitted on 13 Feb 2023]

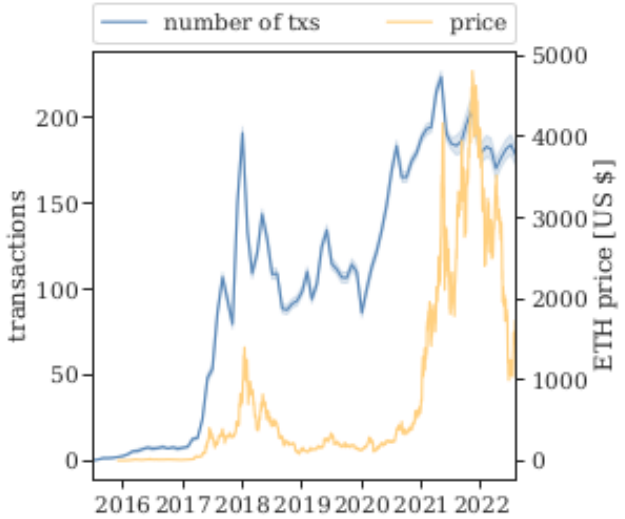
DeFi and NFTs Hinder Blockchain Scalability

Lioba Heimbach, Quentin Kneip, Yann Vonlanthen, Roger Wattenhofer

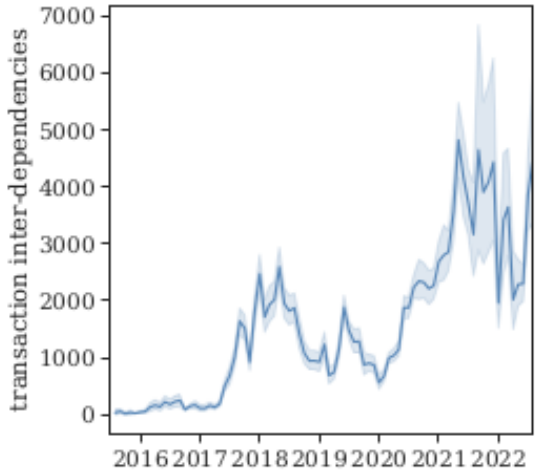
Many classical blockchains are known to have an embarrassingly low transaction throughput, down to Bitcoin's notorious seven transactions per second limit.Various proposals and implementations for increasing throughput emerged in the first decade of blockchain research. But how much concurrency is possible? In their early days, blockchains were mostly used for simple transfers from user to user. More recently, however, decentralized finance (DeFi) and NFT marketplaces have completely changed what is happening on blockchains. Both are built using smart contracts and have gained significant popularity. Transactions on DeFi and NFT marketplaces often interact with the same smart contracts. We believe this development has transformed blockchain usage. In our work, we perform a historical analysis of Ethereum's transaction graph. We study how much interaction between transactions there was historically and how much there is now. We find that the rise of DeFi and NFT marketplaces has led to an increase in "centralization" in the transaction graph. More transactions are now interconnected: currently there are around 200 transactions per block with 4000 interdependencies between them. We further find that the parallelizability of Ethereum's current interconnected transaction workload is limited. A speedup exceeding a factor of five is currently unrealistic.

Link to arxiv.org: https://arxiv.org/abs/2302.06708

Scalability in the era of DeFi & NFTs



(a) Historical development of the number of transactions per block on Ethereum mainnet and the Ether price.



(b) Historical development of the number of transaction interdependencies per block.

Fig. 1: Visualization of the average number of transactions per block (cf. Fig. 1a) and the average number of transaction interdependencies per block (cf. Fig. 1b). We randomly sample 65 blocks per day and plot the daily average along with the 95% confidence interval.

Source: "DeFi and NFTs Hinder Blockchain Scalability" by Heimbach et al.

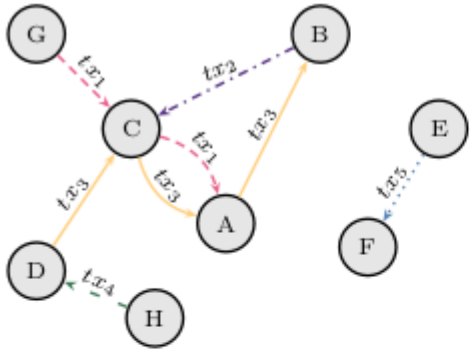
Scalability in the era of DeFi & NFTs

- Increase in avg number of transactions since 2020
  - Rise of DeFi and NFTs

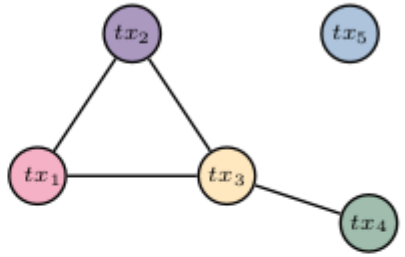
- Until late 2019
  - Mid-to-high correlation between avg number of transactions and gas
  - Specifically: 0.77 Pearson correlation coefficient

- Since 2020:
  - Mid correlation between avg number of transactions and gas
  - Specifically: 0.60 Pearson correlation coefficient

Scalability in the era of DeFi & NFTs



(a) Address-based graph representation of a sample set of Ethereum transactions, where vertices are addresses (contracts or wallets) and edges are calls. The color and style of an edge indicates which transaction the call belongs to.



(b) Transaction-based graph representation of a sample set of Ethereum transactions, where vertices are transactions and the edges indicate dependency between two transactions. Transactions that interact with the same address are dependent.

Fig. 2: Two types of graph representations of the same sample set of five Ethereum transactions. The edge colors indicate belonging to a transaction in the address-based graph representation (cf. Fig. 2a), the transaction-based graph representation has the same transaction set as vertices.

Source: "DeFi and NFTs Hinder Blockchain Scalability" by Heimbach et al.

Scalability in the era of DeFi & NFTs

- In general, graph-based representation and analysis is an important tool
  - Also, mentioned in previous session

- Two basic types of graphs
  1. Address-based (AG)
  2. Transaction-based (TG)

- In AG, transactions in proximity cannot be parallelized
  - Example: Tx4 can not be parallelized with Tx4
- In AG, transactions belonging to the same clique can not be parallelized
  - Example: Tx1, Tx2, and Tx3

Scalability in the era of DeFi & NFTs

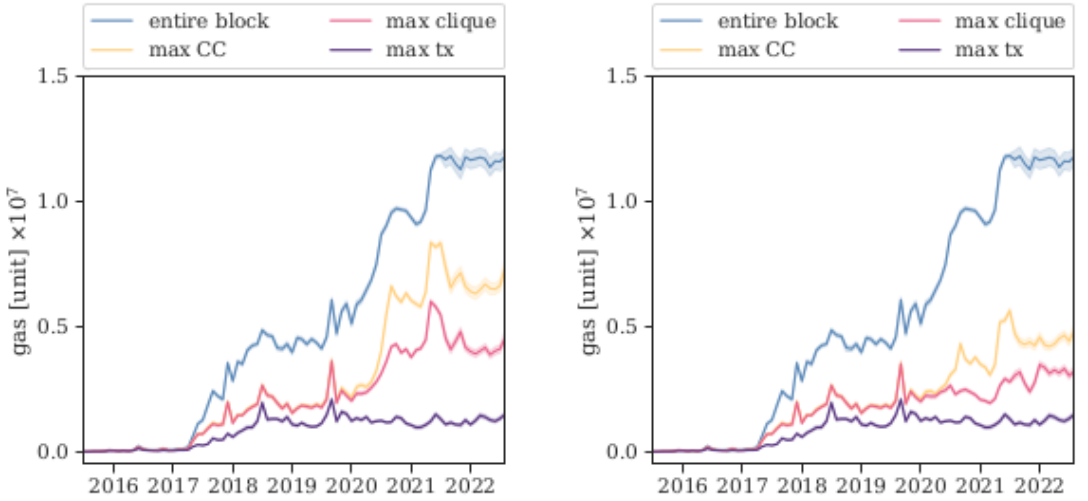


Fig. 5: We plot the gas used by: (1) the entire block, (2) the block's heaviest connected component (CC), (3) the block's heaviest clique, and (4) the block's heaviest transaction. Fig. 5a analyzes the original transaction data and Fig. 5b the disentangled transaction data. Note that we plot the monthly average along with the 95% confidence interval from randomly sampling 65 blocks per day.

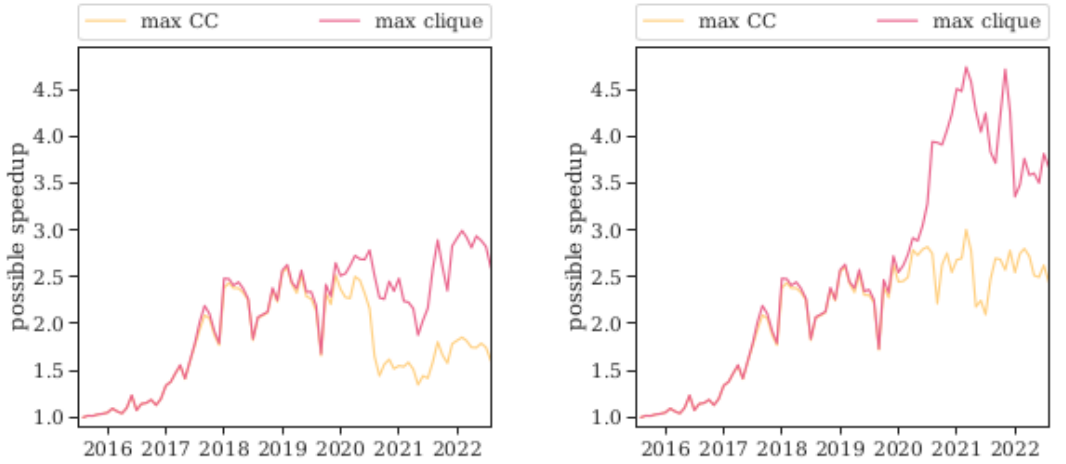
Source: "DeFi and NFTs Hinder Blockchain Scalability" by Heimbach et al.

Scalability in the era of DeFi & NFTs

- Heaviest connected component (max CC) has a dominant position
  - Specifically, responsible for more that 50% of blocks

- Difference between max CC and heaviest clique:
  - Increase since 2020
  - Related to the rise of DeFi and NFTs

Scalability in the era of DeFi & NFTs



(a) original transaction data (b) disentangled transaction data

Fig. 6: We visualize the achievable execution speedup (aggregated monthly) through parallelization for the original transaction data (cf. Fig. 6a) and the disentangled transaction data (cf. Fig. 6b). We obtain the lower bound for the parallelization potential through the identification of the heaviest connected component and the upper bound from the heaviest clique. Note both the heaviest connected component and clique are weighted by gas.

Source: "DeFi and NFTs Hinder Blockchain Scalability" by Heimbach et al.

Scalability in the era of DeFi & NFTs

- Two types of bounds:
  - Lower bound: Estimated by the size of heaviest connected component
  - Upper bound: Estimated by the size of the heaviest clique

- Both bounds refer to achievable improvement

- Before the DeFi (and NFTs) era (i.e., till 2020):
  - The gap between the two bounds was relatively small
- During the DeFi (and NFTs) era:
  - The gap between the aforementioned bounds has been increased

Scalability in the era of DeFi & NFTs

- Main finding: Parallelization is possible but limited

- Directions for improving parallelization:
  - Deeper study of dependencies
    - Even at the key-level
  - Put "attractive" incentive for “simple” transactions.
    - Plus, devise a scheme for not promoting heavy transactions
  - Improve the predictability of dependencies
    - In general, equivalent to the optimization of the translation of source code to machine code
    - Potential synergies with machine learning (aka AI) systems

Conclusions

Conclusions

- We expect to see digital currency networks to scale over time, allowing an increasing number of transactions, but:
  - **Scaling comes at a cost** for full nodes (processing power, bandwidth and storage)
  - **Scaling might hurt decentralization**
- A number of proposals have been put forward to address the block size limit issue, generating hot debates in the Bitcoin community
  - Most proposals suggest **methods for increasing the limit**, either deterministically or dynamically.
  - The introduction of such changes would require a **hard fork** and is therefore considered to be risky.
  - Other methods try to avoid the block size limit increase by **decreasing the footprint of transactions in the blockchain or making some transactions off-blockchain**.
- **Scalability-related questions will probably monopolize the interest of the community for some time.**

Bibliography

Bibliography (optional)

- Khan et al. **Systematic Literature Review of Challenges in Blockchain Scalability** (here)

- Kyle Croman et al. **On Scaling Decentralized Blockchains** (here)
  The authors analyze how fundamental and circumstantial bottlenecks in Bitcoin limit the ability of its current peer-to-peer overlay network to support substantially higher throughputs and lower latencies.

- Ittay Eyal et al. **Bitcoin-NG: A scalable Blockchain Protocol** (here)

UNIVERSITY *of* NICOSIA

Instructor’s Email:
iosif.e@unic.ac.cy