



**crypto.com**

## **EIP-1559 and CBDCs**

**Analysing Ethereum's EIP-1559  
and MIT's Project Hamilton**

**March 2022**

# Research and Insights



Research Analyst  
William Wu PhD



Head of Research and Insights  
Henry Hon PhD, CFA

Research Intern  
Bowen Liu

## RESEARCH DISCLAIMER

This report alone must not be taken as the basis for investment decisions. Users shall assume the entire risk of any use made of it. The information provided is merely complementary and does not constitute an offer, solicitation for the purchase or sale of any financial instruments, inducement, promise, guarantee, warranty, or an official confirmation of any transactions or contract of any kind.

The views expressed herein are based solely on information available publicly, internal data or information from other reliable sources believed to be true. This report includes projections, forecasts and other predictive statements which represent [Crypto.com](https://crypto.com)'s assumptions and expectations in the light of currently available information. Such projections and forecasts are made based on industry trends, circumstances and factors involving risks, variables and uncertainties. Opinions expressed herein are our current opinions as of the date appearing on the report only.

No representations or warranties have been made to the recipients as to the accuracy or completeness of the information, statements, opinions or matters (express or implied) arising out of, contained in or derived from this report or any omission from this document. All liability for any loss or damage of whatsoever kind (whether foreseeable or not) which may arise from any person acting on any information and opinions contained in this report or any information which is made available in connection with any further enquiries, notwithstanding any negligence, default or lack of care, is disclaimed.

This report is not meant for public distribution. Reproduction or dissemination, directly or indirectly, of research data and reports of [Crypto.com](https://crypto.com) in any form, is prohibited except with the written permission of [Crypto.com](https://crypto.com). Persons into whose possession the reports may come are required to observe these restrictions.

# Contents

<b>Executive Summary</b>	<b>4</b>
<b>1. Empirical Analysis of EIP-1559</b>	<b>6</b>
1.1 Introduction	6
1.2 Methodology	8
Data Sources	8
1.3 Does EIP-1559 Affect Transaction Fee Dynamics?	8
1.4 Does EIP-1559 Affect Transaction Waiting Time?	10
1.5 Does EIP-1559 Affect Security?	12
Fork Rate	12
Network Load	12
Miner Extractable Value (MEV)	12
1.6 Conclusion	14
<b>2. Project Hamilton</b>	<b>15</b>
2.1 Introduction	15
2.2 System Performance Goals	16
2.3 System Model	17
System Roles	17
Security Properties	18
2.4 Transaction Design	19
Transaction Scalability Designs	19
2.5 Evaluation & Performance	21
Scalability	21
Fault Tolerance	23
2.6 Conclusion	24
<b>References</b>	<b>26</b>

# Executive Summary

This report gives an overview of two significant blockchain research papers, one on [Ethereum's EIP-1559](#), and the other on [Project Hamilton](#), a joint research project by Boston Fed and MIT DCI on central bank digital currencies (CBDCs).

## Empirical Analysis of EIP-1559: Transaction Fees, Waiting Time, and Consensus Security

This research paper answers three key questions on EIP-1559:

### 1. Does EIP-1559 affect transaction fee dynamics?

- EIP-1559 did not lower the transaction fee level itself, but it enabled easier fee estimation, resulting in less overpaying for users.

### 2. Does EIP-1559 affect transaction waiting time?

- Transaction waiting time significantly reduced after the London Hardfork.

### 3. Does EIP-1559 affect the security of the Ethereum blockchain?

- With existing evidence, the authors believe that "EIP-1559 does **not** make the Ethereum system substantially more insecure."

## A High Performance Payment Processing System Designed for Central Bank Digital Currencies

Project Hamilton builds on ideas from both cryptocurrency and electronic cash designs, and makes the following contributions:

1. Presenting a **flexible transaction processor design** that supports a range of models for a CBDC.
2. Proposing a **novel transaction format** that supports [modularity](#) (system components may be separated and recombined flexibly) and extensibility.
3. Designing **two architectures** to achieve high throughput and scalability (up to [1.7 million](#) transactions per second).
4. **Evaluating the performance** of the two architectures with different types of transaction workloads, as well as testing their ability to withstand failures. The architectures were able to recover from simulated failures within [15](#) seconds.

Unlike most CBDC research efforts to date, Project Hamilton is [open source](#). This allows results to be independently reproducible and helps to foster collaboration with external parties on continuing research.

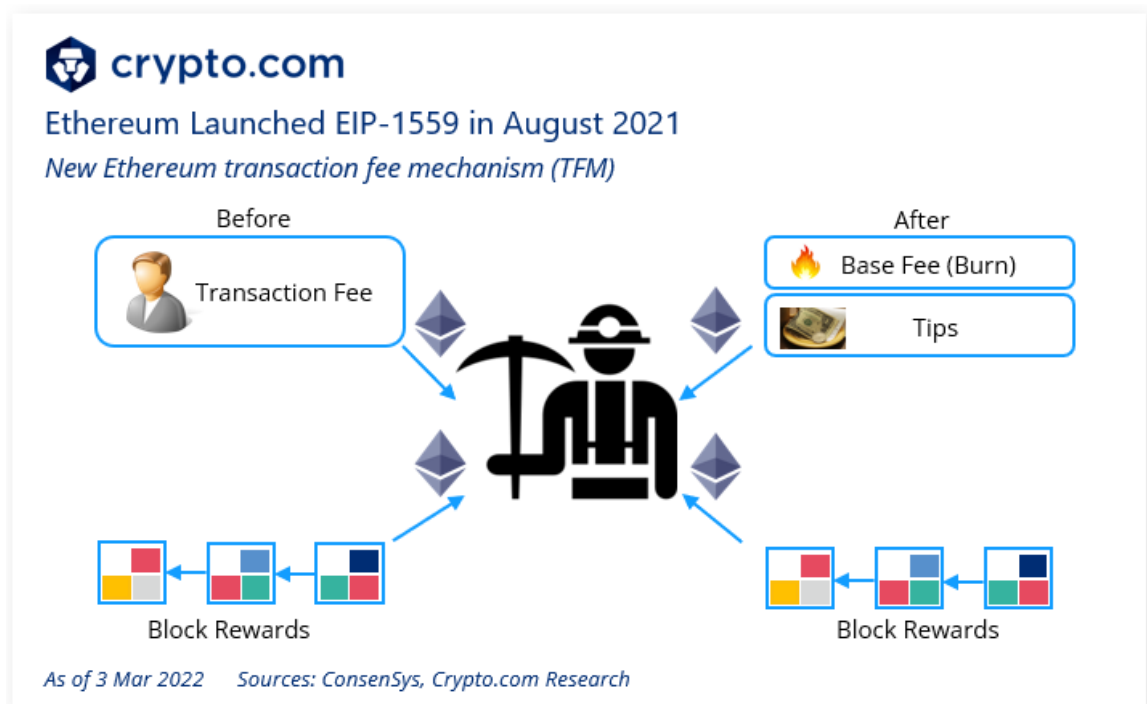
# 1. Empirical Analysis of EIP-1559

We give an overview of the paper '[Empirical Analysis of EIP-1559: Transaction Fees, Waiting Time, and Consensus Security](#)' by Yulin Liu et al. The authors of the paper are from Duke University, Peking University, as well as Bochsler Finance. The paper was highly praised by [Vitalik Buterin](#), co-founder of Ethereum. The paper has also been accepted for publication in [ACM Conference on Computer and Communications Security \(CCS\) 2022](#).

## 1.1 Introduction

[EIP-1559](#) is an 'Ethereum Improvement Proposal' that implements burning a portion of the gas fees on Ethereum transactions to improve the Ethereum fee market.


Fundamentally, EIP-1559 eliminated the [first-price auction](#) as its main gas fee calculator, where transaction senders bid a fixed amount of gas to pay for their transaction to be processed, with the highest bidder winning. **With EIP-1559, there would be a 'base fee' for transactions to be included in the next block. Users who wish to speed up their transaction can add a 'tip', which is essentially a 'priority fee' to pay a miner for faster confirmation.**



This research paper aims to answer three questions on the impact of this transaction fee mechanism (TFM) reform.




1. Does EIP-1559 affect transaction fee dynamics? For example, do the transaction fees become lower?
2. Does EIP-1559 affect transaction waiting time? That is, do transactions get processed (i.e. included in blocks) faster?
3. Does EIP-1559 affect the security of the Ethereum blockchain?

We give a lay summary of the paper in the infographic below. **Basically, EIP-1559 made Ethereum transactions cheaper (and more consistent), faster, and just as secure.**



### Lay Summary of the EIP-1559 Paper

*EIP-1559 made Ethereum transactions cheaper, faster, and just as secure*

	Cheaper ✓ (Indirectly)	• Users pay a lower fee due to less overpaying
	Faster ✓ (Indirectly)	• EIP-1559 lowers transaction waiting time
	Just as secure ✓	• No evidence that EIP-1559 made Ethereum more insecure

*As of 3 Mar 2022 Sources: Yulin Liu et al., Crypto.com Research*

To be precise, we have to add a disclaimer ‘indirectly’, because EIP-1559 “did not lower the transaction fee level itself”, nor did it increase the transactions per second (TPS) of Ethereum. Most experts believe that [sharding and layer two solutions](#) are the way forward to directly address these scalability issues. It is [theoretically known](#) that no transaction fee mechanism (including EIP-1559) can substantially lower transaction fees.

We give a simple ‘restaurant’ analogy to help the reader understand better: Imagine the Ethereum blockchain is a ‘restaurant’ and making transactions is like ‘buying food’. With EIP-1559, the cost of the food remains the same, but the extra surcharges (e.g. waiters’ tips or service charge) gets reduced, resulting in less overpaying and a lower bill. EIP-1559 also causes the queue system to be more efficient, resulting in diners spending less time waiting in the queue, even though the chef still cooks food at the same speed.

## 1.2 Methodology

### Data Sources

This research used three data sources. **Firstly**, the authors queried the blockchain data from [Google BigQuery](#), which contains block data and transaction data on Ethereum.

**Secondly**, the authors ran four [Ethereum full nodes](#) geographically distributed around the world (North Carolina, Los Angeles, Montreal, and Germany) to monitor the mempool of Ethereum constantly, so that it can capture a historical log of the Ethereum mempool. The Ethereum [mempool](#) is a waiting area for transactions that have not been added to a block and are still unconfirmed.

**Thirdly**, the authors queried ETH price data at a one-minute granularity from [Bloomberg Terminal](#). It used this data to compute minute level price volatility of ETH price as a control variable.

## 1.3 Does EIP-1559 Affect Transaction Fee Dynamics?

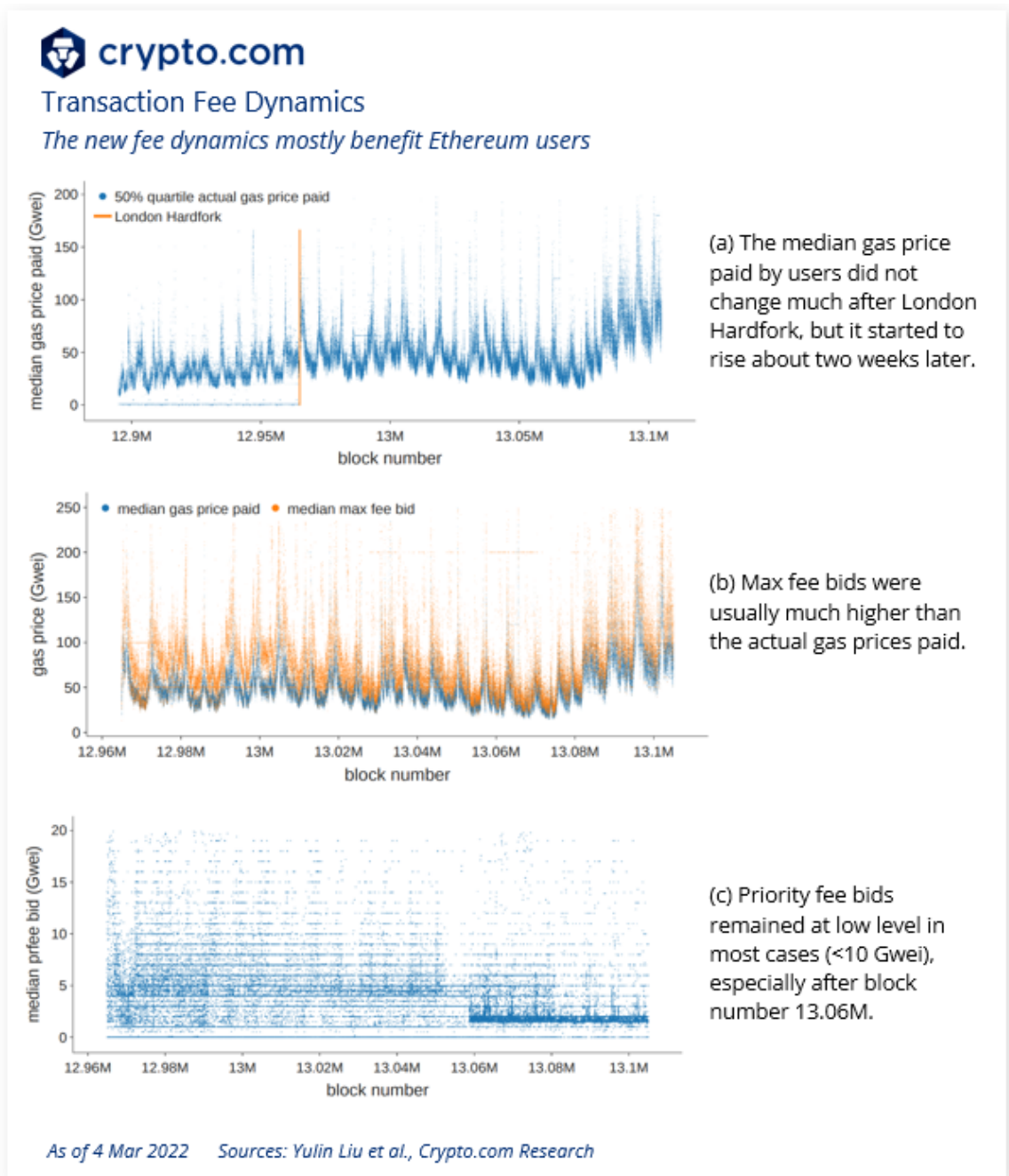
**The authors observed that EIP-1559 did not lower the transaction fee level itself in the data period, but it enabled easier fee estimation, resulting in less overpaying for users.** Notably, the intra-block gas price variance became significantly lower as more users adopted EIP-1559 transactions. **In layman's terms, gas prices became more consistent after EIP-1559.**

**Firstly, we take note that EIP-1559 occurred at block number 12.965M ([5 August 2021](#)).** Since EIP-1559 is backwards compatible, many users still adopted the legacy bidding style in the few weeks after the upgrade. By November 2021, around [40% to 60%](#) of all transactions used the new bid style proposed by EIP-1559.

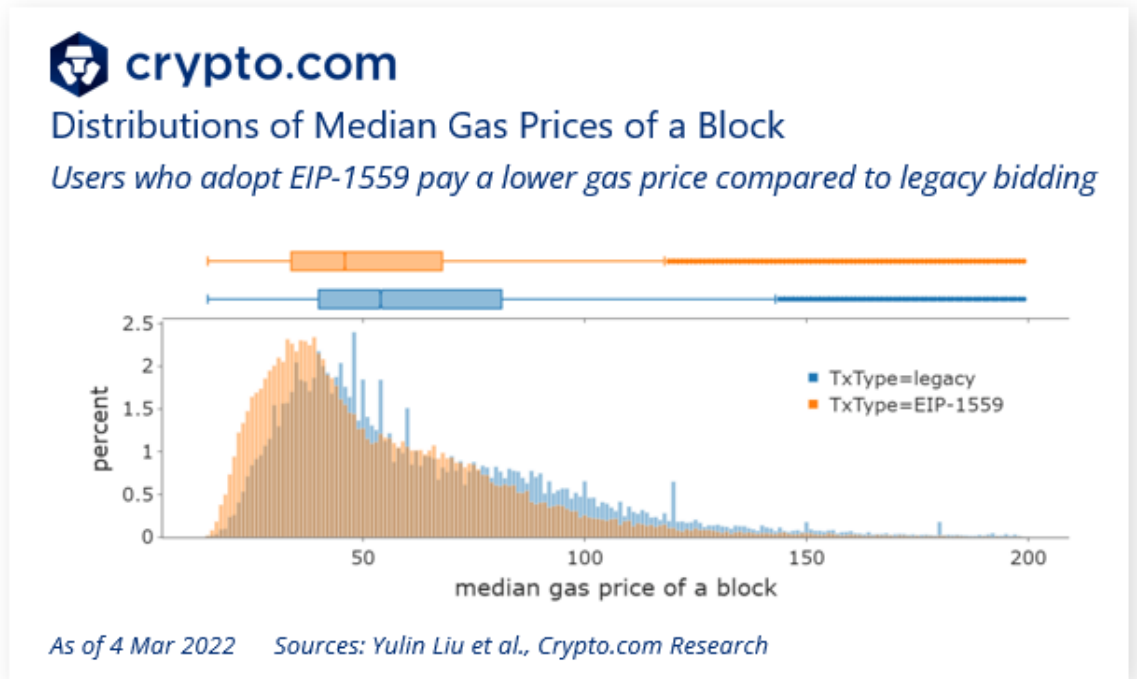
**In the diagram below, subfigure (a) shows the median gas price paid in each block before and after the London Hardfork.** The gas price level **did not change much before and immediately after** the London Hardfork. There were some oscillations due to differences in demand across time zones. The authors mentioned that it is 'unclear' whether the increase in gas price after block number 13.07M is caused by EIP-1559 or other factors.



Subfigures (b) and (c) further decompose different fee parameters in users' bids. Subfigure (b) shows that while the median gas price paid and median max fee bid are volatile and highly correlated to each other, the actual gas prices paid are usually lower than the max fee bids. **In practice, this benefits the Ethereum user because they would be refunded the difference between the max fee bid and the base fee (which is burned) and the priority fee (which goes to the miner).**



Meanwhile, subfigure (c) shows that the median max priority fee bid **remains at a low level** (almost always <10 Gwei throughout the period and <3 Gwei after block number 13.06M). **Again, this benefits Ethereum users as it helps to keep the total gas price (base fee + max priority fee) low.**



Moreover, the authors also compared the median prices for different transaction types. As shown above, the median gas price paid of the EIP-1559 transactions in a block **has a distribution shifted to the left** of that of the legacy transactions. The 50<sup>th</sup> percentile of the median gas price of EIP-1559 transactions in each block is 45 Gwei, while that of legacy transactions is 54 Gwei. **In short, this means that users who adopt EIP-1559 bidding overall pay less than those who stick to legacy bidding.**

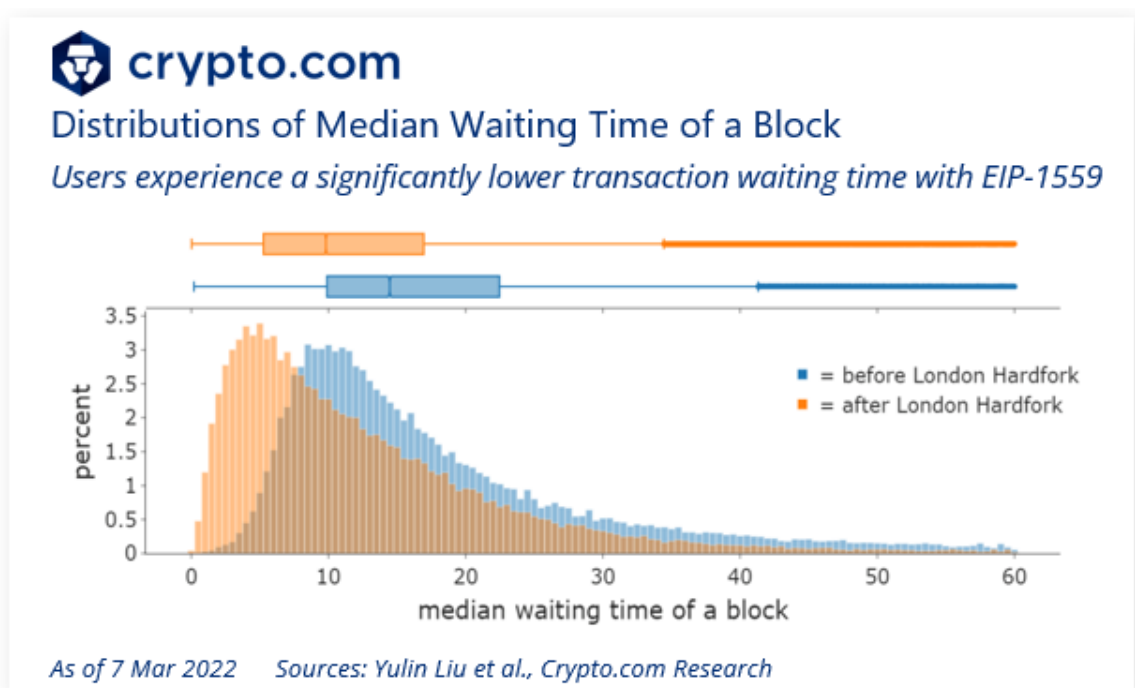
In conclusion, the findings imply that fee estimation is easier with the new gas fee bidding style, leading to less overpaying for users.

## 1.4 Does EIP-1559 Affect Transaction Waiting Time?

**Waiting time refers to the time difference between when a transaction is first observed in the mempool and when the transaction is mined.** When there are dependent transactions, users cannot submit new transactions until previous dependent transactions are successfully included in blocks or cancelled.

In time-sensitive situations, such as buying NFTs during [public mints](#), a lower waiting time would be very beneficial.

**The authors found that waiting time significantly reduced after EIP-1559, possible reasons include easier gas price bidding and variable-sized blocks.** This positively affects both the transactions that adopt EIP-1559 bidding and those that still use legacy bidding. **Hence, EIP-1559 improved the waiting time for transactions, despite the fact that not all users have adopted it.** The shorter waiting time might also be a result of the easier fee estimation after EIP-1559.



In the figure above, each observation represents a block and the median of transaction waiting times in that block. The 50<sup>th</sup> quartile of median **legacy-style** transaction waiting time across blocks is **9.4 seconds** after the London Hardfork, while that of median **EIP-1559-style** transaction waiting time across blocks is **8.9 seconds**.

**In simple terms, the typical EIP-1559-style transaction has a shorter waiting time.** This has the effect of making the Ethereum blockchain ‘faster’ in the sense that transactions get mined sooner, though technically EIP-1559 does not increase transactions per second (TPS). **This effect certainly helps to improve the user experience of Ethereum blockchain users.**

## 1.5 Does EIP-1559 Affect Security?

EIP-1559 alters crucial consensus parameters such as the block size and the incentive of miners and users. Hence, the effect of EIP-1559 on Ethereum's security is a valid concern.

### Fork Rate

It is known that larger blocks may take more time to propagate, resulting in more forks. For the case of EIP-1559, the block size is variable and dynamically adjusted, therefore its effect on fork rate is not well understood theoretically.

In general, the prevalence of forks (also called 'uncle blocks' in Ethereum) can lead to higher vulnerability due to [double-spend attacks](#) and [selfish mining](#). In simple terms, it is not good to have a high fork rate.

**The results empirically show that the London Hardfork increased block size on average, and it also led to an approximately 3% rise in fork rates.** According to the authors, this effect is negligible and would only have 'a small effect' on consensus security.

### Network Load

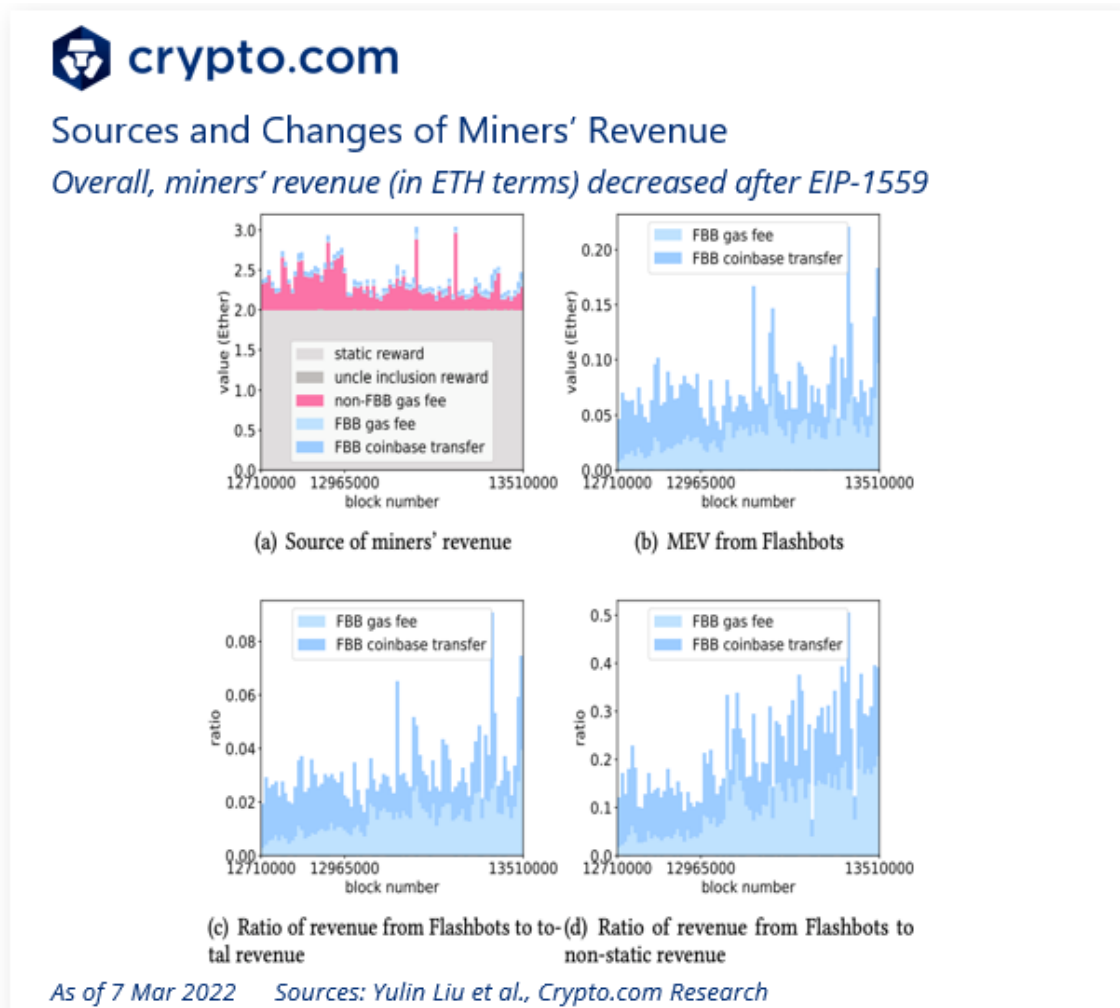
Network load refers to the amount of computational, networking, and storage work a node must perform to participate in the blockchain protocol. Since processing larger blocks uses more resources, previously the Ethereum community was concerned whether variable block sizes will increase the [network load](#).

**The results obtained by the authors show that EIP-1559 does not put the blockchain system under a significantly higher load.** The authors do observe load spikes (periods during which a higher-than-average amount of gas is consumed), but its frequency is not significantly different before or after the London Hardfork.

### Miner Extractable Value (MEV)

A miner can make profits by the arbitrary inclusion, exclusion, or re-ordering of transactions within the blocks they mine. This profit is known as MEV. [Researchers](#) have found that significant MEV can potentially incentivise miners to diverge from the consensus protocol (e.g., to maliciously fork, or rewind the blockchain to profit from MEV), thus negatively affecting consensus security.

Through the authors' empirical analysis, they find that MEV becomes a much larger fraction of miners' revenue after EIP-1559, primarily because the base fees are burnt. This may incentivise miners to invest more in MEV extraction.



Subfigure (a) shows the miners' total revenue and its composition. **Overall, miners' revenue (in ETH terms) decreased after EIP-1559, primarily because the base fees were burnt.** In fiat terms, other sources have noted that in the days following EIP-1559 activation, daily miner revenue in USD actually increased by [7.1%](#), due to ETH price increase.

For readers that are interested, 'FBB' in the diagrams above stands for '[Flashbots bundles](#)'. Essentially, it is a group of transactions bundled together, for the purpose of connecting directly to miners to avoid being [frontrun](#) in the public Ethereum mempool.

Subfigure (b) plots the revenue from MEV. **After a downturn for less than 50,000 blocks, MEV revenue quickly recovered to the level before the London Hardfork.** This may have been caused by the following reasons: Firstly, Flashbots

searchers needed to update their software after the London Hardfork in order to adapt to EIP-1559, and secondly, there was potentially high volatility of miner extractable value due to network instability in the short term after the London Hardfork.

Subfigures (c) and (d) show the ratio of MEV revenue to the total revenue and to the non-static revenue (i.e., miners' revenue minus the static block reward), respectively. **As the revenue from gas fees dropped greatly post London Hardfork while MEV revenue recovered rapidly, the ratio of MEV to total revenue increased significantly.** To be precise, as shown in subfigures (c) and (d), after the London Hardfork, miners' MEV revenue accounts for about **4% of the total revenue** and about **30% of the non-static revenue**. Previously before the London Hardfork, the MEV revenue was only about 3% of the total revenue and about 15% of the non-static revenue.

## 1.6 Conclusion

This paper presented several new findings that are absent from previously existing research. **The authors' results show that EIP-1559 improves the user experience by making fee estimation easier, mitigating the intra-block difference of gas price paid, and reducing users' waiting time.** These findings suggest new directions for improving transaction fee mechanisms.

## 2. Project Hamilton

### 2.1 Introduction

Central banks around the world are in various stages of progress with regards to central bank digital currencies (CBDCs). Some are in research and development phases, while others are running pilots or even launching products to the public. For instance, China's e-CNY has undergone [public trials](#) and was accepted as a payment method at the 2022 Winter Olympics in Beijing.

**Project Hamilton is a joint research project by the Federal Reserve Bank of Boston ([Boston Fed](#)) and the Massachusetts Institute of Technology's Digital Currency Initiative ([MIT DCI](#)).** The project is named after [Margaret Hamilton](#), an MIT computer scientist who developed flight software for NASA's Apollo program, and [Alexander Hamilton](#), who helped to establish the first two U.S. central banks.

The main findings of Project Hamilton were detailed in a [research paper](#) titled 'A High Performance Payment Processing System Designed for Central Bank Digital Currencies' by Lovejoy et al.

**Project Hamilton**  
Background of Project Hamilton

**Project Hamilton**  
A high performance payment processing system designed for CBDCs

Named after:

Margaret Hamilton      Alexander Hamilton

*As of 11 Mar 2022 Sources: Boston Fed, MIT DCI, Lovejoy et al., Crypto.com Research*

Project Hamilton builds on ideas from both cryptocurrency and electronic cash designs, and makes the following contributions:

1. Presented a **flexible transaction processor design** that supports a range of models for a CBDC and minimises data storage in the core transaction processor while supporting self-custody or custody provided by intermediaries (such as financial institutions, custodians, or payment service providers).
2. Proposed a **novel transaction format** that supports [modularity](#) (system components may be flexibly separated and recombined) and extensibility.
3. Designed **two architectures** to achieve high throughput and scalability (up to [1.7 million](#) transactions per second).
4. **Evaluated the performance** of the two architectures with different types of transaction workloads, as well as testing their ability to withstand failures. The architectures were able to recover from simulated failures within [15](#) seconds.

Unlike most CBDC research efforts to date, Project Hamilton is [open source](#). This allows results to be independently reproducible and helps to foster collaboration with external parties on continuing research. It also encourages global interoperability standards and provides a lower barrier to adoption. Contrary to other projects, Hamilton is designed to be administered directly by the central bank or a related entity.

## 2.2 System Performance Goals

In the current stage (1<sup>st</sup> phase), Project Hamilton's goal is to investigate the technical feasibility of a **high throughput, low latency, and resilient transaction processor** that provides flexibility for a range of eventual CBDC design choices.

In the blockchain context, transaction [throughput](#) refers to the rate at which valid transactions are committed by the blockchain. Throughput is usually measured in transactions per second (TPS). Transaction [latency](#) refers to the time taken for a transaction's effect to be usable across the network.

The targeted performance goals are as follows:

- **Speed** – To capture the benefits of faster or real-time payments, a target of **99% of transactions completing within 5 seconds** is set. Completion includes a transaction being validated, executed, and confirmed back to users.
- **Throughput and Scalability** – To support settlement finality and CBDC models which do not require intermediaries to aggregate transactions, Hamilton must be able to handle peak projected transaction volumes



produced by hundreds of millions of users. A minimum target of **100,000 transactions per second** is chosen based on existing cash and card volumes and expected growth rates.

- **Resilience** – To maintain trust in the digital currency, a CBDC must guarantee the ongoing existence and usability of funds. This phase currently focuses on continuing to provide system access and **preventing data loss even in the presence of multiple data centre failures**.

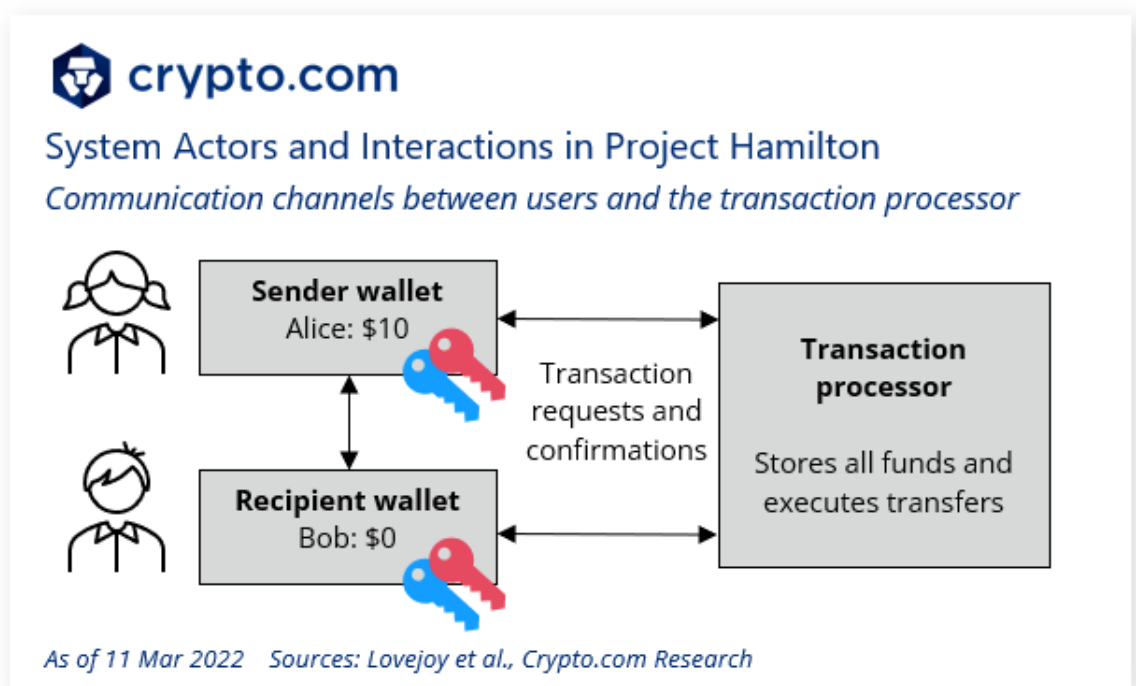
## 2.3 System Model

### System Roles

There are three types of [actors](#) (computational entities that take input, send output and perform functions) in Project Hamilton: the **transaction processor**, the **issuer**, and **users**.

- The transaction processor keeps track of funds that are owned by different users. Funds refer to an amount of money and a condition that must be satisfied to move this amount (for example, to other users).
- The funds enter and exit the system through acts of the issuer who can mint and redeem funds to add and remove them from the transaction processor, respectively.
- Users can execute transfer operations (transactions or payments) that change the ownership of funds, with the requirement that the total amount of funds stored in the transaction processor has not changed.

In layman's terms, the **transaction processor** is similar to a giant database keeping track of how much money each individual has. Meanwhile, the **issuer** is similar to a [central bank](#) or monetary authority in the sense that it can issue coins and control the money supply. Finally, **users** may refer to ordinary people who can send money or make payments.



A user executes transactions or payments by submitting their transaction to the transaction processor over the internet, which the processor then validates and executes. The implementation of offline transactions and transfers without internet connectivity will be left to a future phase.

The high-level system model and potential communication channels between users and the transaction processor are shown in the image above. Users run wallet software to manage cryptographic keys, track funds, and facilitate transactions. Wallets could run on a mobile phone or specialised hardware in [smart cards](#) (cards with smart chip technology).

## Security Properties

In general, the system must faithfully execute transactions, ensuring that each was authorised by the owner of the input funds, and also safeguard that transactions do not disturb the overall balance of funds (outside of minting and redemption). The transaction processor in Hamilton ensures this by satisfying the following four security properties.

1. **Authorisation** – Hamilton only accepts and executes *Mint* and *Redeem* operations authorised by the issuer, i.e., only the issuer can mint and redeem funds. Similarly, Hamilton only accepts and executes *Transfer* operations where [encumbrances](#) (spending conditions that have to be met in order to spend the funds) are satisfied (e.g., all three operations are covered by digital signature authorisation).

2. **Authenticity** – The [UTXO set](#) (the total supply of coins) of Hamilton only contains authentic funds. Only UTXOs (coins) created by authorised *Mint* operations are defined as authentic. Moreover, the system defines UTXOs created by *Transfer* operations to also be authentic as long as all inputs consumed by the transaction were authentic and the transaction preserves balance.
3. **Durability** – *Mint*, *Redeem*, and *Transfer* are the only operations in Hamilton that can change the UTXO set. As a consequence of the integrity properties defined above, the UTXO set always remains authentic and transactions in Hamilton cannot be reverted.
4. **Availability** – An authorised transaction spending authentic funds will always be accepted by the transaction processor.

## 2.4 Transaction Design

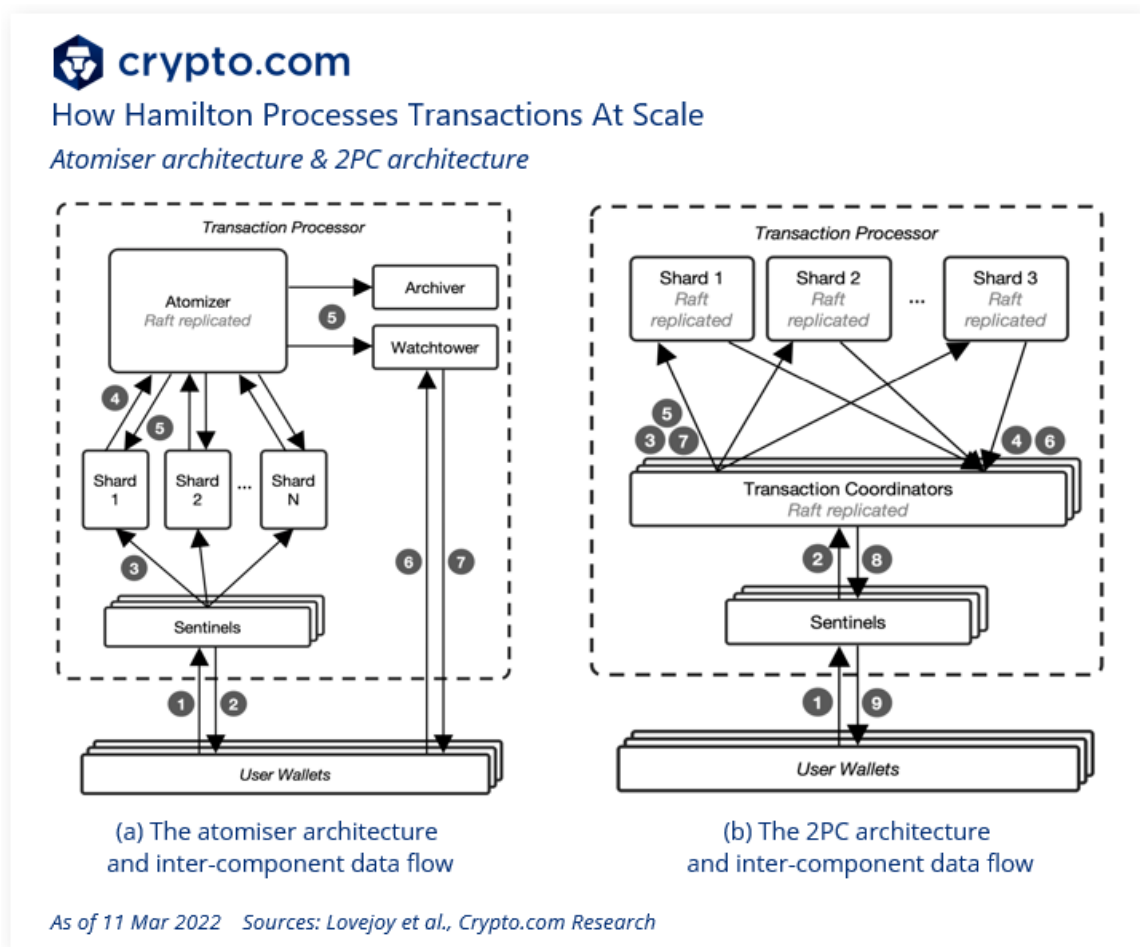
In Bitcoin or Ethereum blockchains, the entire set of transactions unfortunately needs to be stored on-chain. This has an effect on storage and bandwidth requirements (for instance, Bitcoin's UTXO state is over [4 gigabytes](#) and Ethereum's data size is over [600 gigabytes](#)).

Instead, Hamilton explored a design that does not require storing [encumbrances](#) (a 'locking' script that locks the output to a specific wallet address, which could identify users) and values in [cleartext](#) (i.e. not encrypted) in the transaction processor. In Hamilton, the transaction processor stores unspent funds as a set of [opaque](#) 32-byte cryptographic hashes of UTXOs, not entire UTXOs themselves. This design is clearly beneficial for privacy.

### Transaction Scalability Designs

Hamilton describes the two architectures (i.e., atomiser architecture and two-phase commit (2PC)) for processing transactions at scale.

- **Atomiser architecture** – uses an ordering server to create a linear history of all transactions.
- **2PC** – executes non-conflicting transactions (transactions that do not spend or receive the same funds) in parallel and does not create a single, ordered history of transactions.



The workflows of the two architectures are demonstrated above. Subfigures (a) and (b) show components in the atomiser and 2PC architectures respectively.

**According to the paper, there are two main differences between the 2PC and atomiser architecture.** Firstly, the 2PC architecture does not generate an immediately available total ordering of transactions, which the atomiser architecture does through a sequence of blocks. **In simple terms, for the 2PC architecture, unrelated transactions could execute in any order.**

Secondly, the atomiser uses **asynchronous** communication between components whereas the 2PC architecture uses typical **synchronous** remote procedure calls for inter-component communication.

In computer science, **asynchronous operations** mean that the program can move to another task before the previous one finishes. In this way, the program is able to deal with **multiple requests simultaneously**. Meanwhile, in **synchronous operations**, tasks are **performed one at a time** and only when one is completed, the following is unblocked. In other words, the program needs to wait for a task to finish to move to the next one.

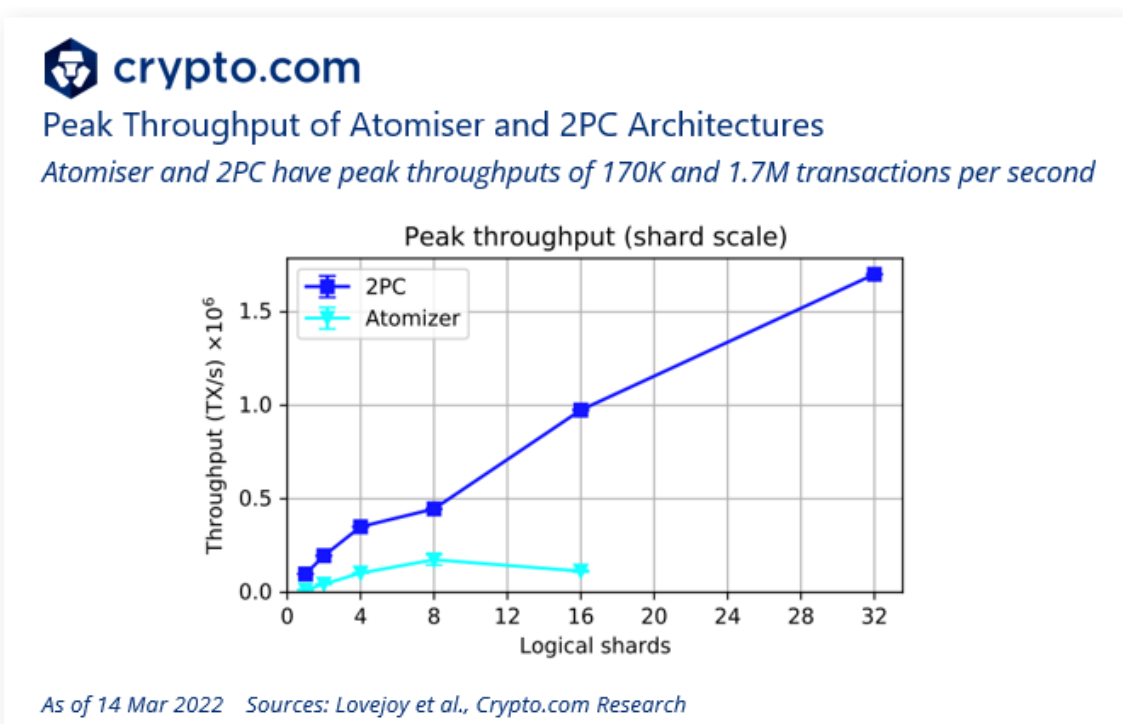
## 2.5 Evaluation & Performance

The open-source code of this research is available at [GitHub](#). The evaluations are based on the performance of the atomiser and 2PC architectures against original project requirements of high throughput and low latency, the ability to tolerate the failure of multiple data centre regions, and performance changes under a variety of workloads.

### Scalability

The figure below compares the peak transaction throughput between the **atomiser** and **2PC** as the number of shards increases. The **atomiser** architecture has a **peak throughput of 170,000 transactions per second**, beyond which adding additional shards fails to increase throughput, whereas the **2PC architecture** scales linearly as the number of shards increases, **up to 1.7 million transactions per second**, though the authors expect peak throughput would continue to increase with more shards.

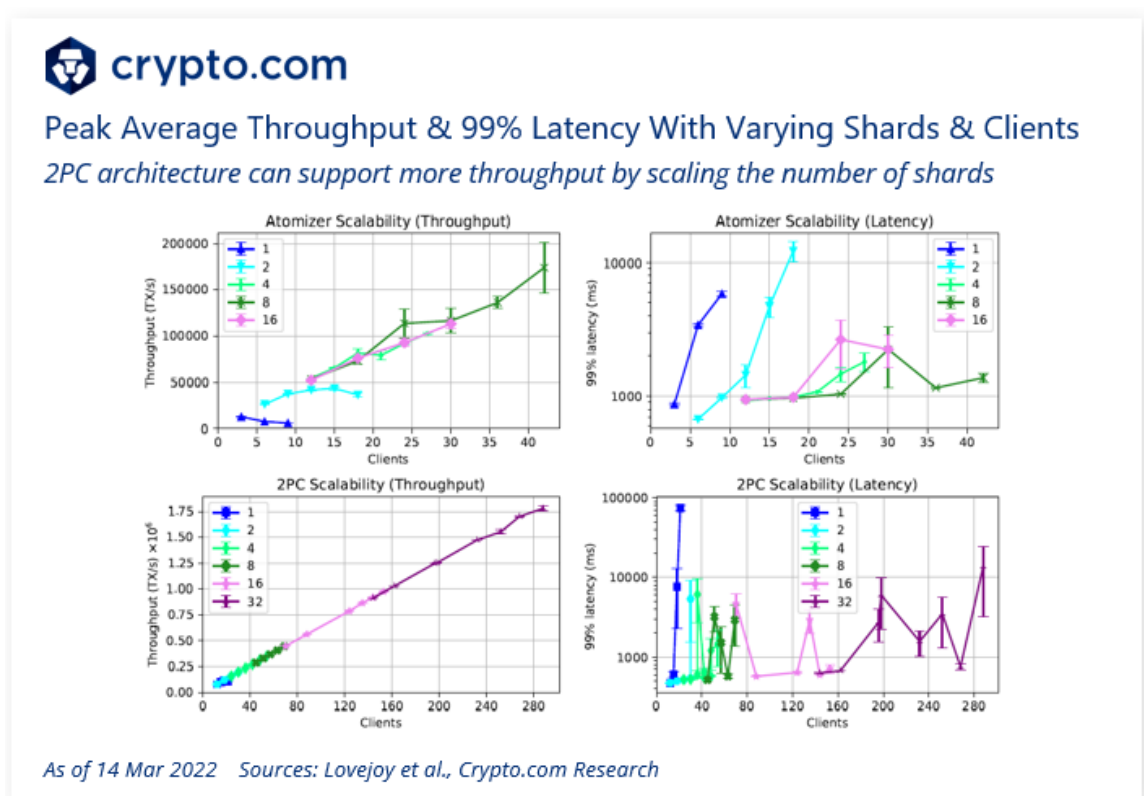
In the context of blockchains, [sharding](#) refers to the splitting of the blockchain into smaller pieces called 'shards'. The benefits of sharding include reducing network congestion and increasing transactions per second.



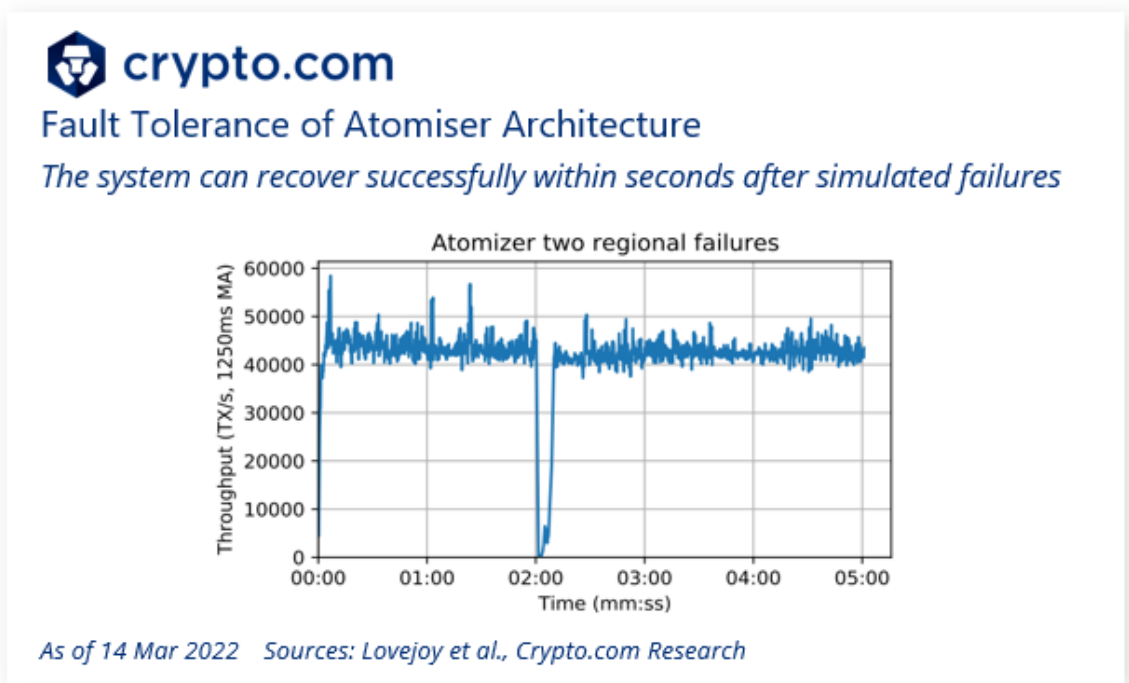
The authors further show the throughput and latency varying the number of clients for different shard counts for both architectures. Based on the experiments, the authors found that **2PC does not experience a drop off in performance**, supporting a greater offered load by increasing the number of shards. Additionally, if a lower tail latency is desired for a particular transaction throughput, increasing the number of shards can **decrease tail latency for the same offered load**.

Tail latency usually refers to the 98<sup>th</sup> or 99<sup>th</sup> percentile response times, i.e. the longest response times in comparison to the majority of other response times. Minimising tail latency is very important for improving the user experience.

Crucially, the 2PC architecture has **no experimentally demonstrated bottleneck** and can support more throughput without trading off tail latency by scaling the number of shards. By contrast, the **atomiser architecture has a clear peak throughput plateau with 8 shards**, whereby increasing to 16 nodes results in a drop in peak throughput.

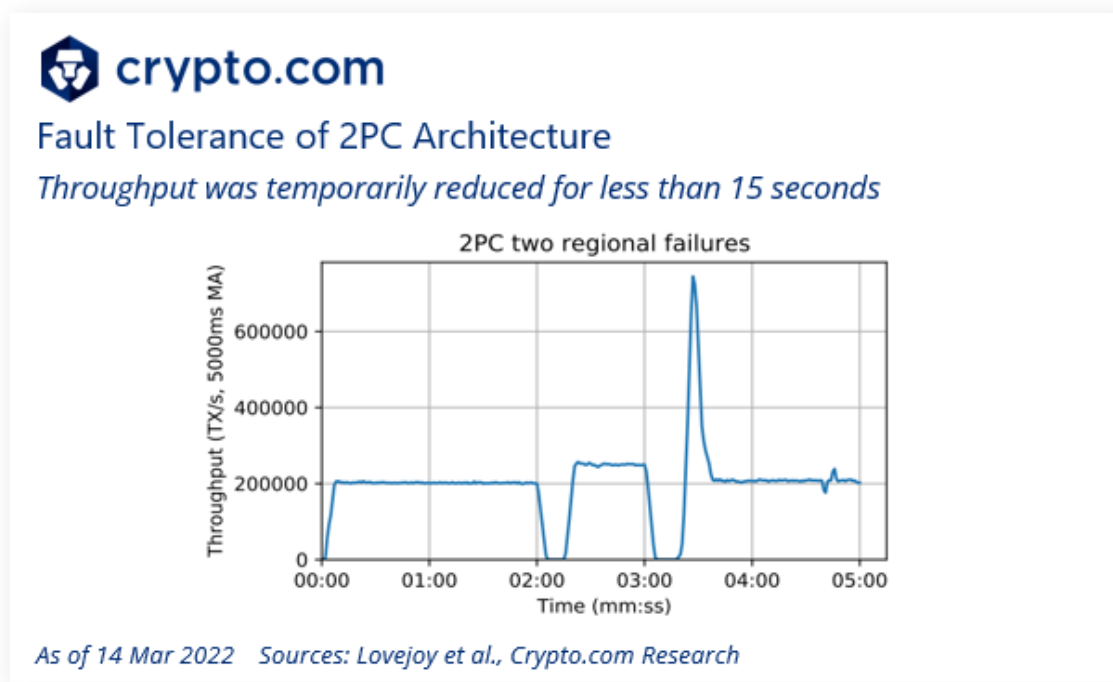


## Fault Tolerance



**It is crucial to analyse how the system responds to failures, such as random hardware failures, natural disasters, and network partitions.** The authors evaluate how both architectures handle up to two simulated regional data centre failures, and the scalability of each architecture as the number of supported failures increases.

The above figure shows the transaction throughput over time for the atomiser architecture when two simulated data centre failures occur. **The plot shows that the system can recover successfully and automatically restore the availability of the system in a matter of seconds.**



Similarly, the plot above shows that the 2PC architecture is successfully able to handle and recover from the failure of two entire data centres with minimal loss of downtime and no loss of system performance. For each failure, throughput was temporarily reduced for less than 15 seconds, before automatically recovering to the baseline.

## 2.6 Conclusion

**Project Hamilton presents a CBDC transaction processor design, implements two architectures to support transactions at scale, and achieve high performance and resilience.**

Through software design, development, and testing, Project Hamilton provides unique insights into technology relevant to implementing a CBDC. Furthermore, by designing a flexible research platform and issuing an open-source licence for the software, Project Hamilton aims to share its learnings with others and receive feedback and potential contributions from other experts.

**In the next phase (Phase 2) of Project Hamilton, the Boston Fed and MIT DCI will continue their CBDC infrastructure research and explore further in areas such as data privacy, programmability, and interoperability.** As the global CBDC landscape evolves, Project Hamilton aims to continue providing valuable insights to policymakers and the general public through its cutting-edge technical research.



## References

Liu, Yulin, et al. "Empirical Analysis of EIP-1559: Transaction Fees, Waiting Time, and Consensus Security." *arXiv preprint arXiv:2201.05574* (2022). *ACM CCS 2022*, forthcoming.

Lovejoy, James, et al. "A High Performance Payment Processing System Designed for Central Bank Digital Currencies."



**crypto.com**

e. [contact@crypto.com](mailto:contact@crypto.com)

© Copyright 2022. For information, please visit [crypto.com](https://crypto.com)