Ethereum Mainnet Use Case Analysis v1

Publish date: July 24, 2020

Prepared by: The EEA Mainnet Working Group Use Case Task Force

Introduction

Members of the Enterprise Ethereum Alliance – Mainnet Working Group formed a task force in early 2020 to study enterprise application use cases involving Ethereum Mainnet, and to identify major barriers or challenges that enterprise architects and developers face when they consider building on Mainnet. The results of this survey will be used as a starting point for designing and building technical solutions to fill any existing functional gaps.
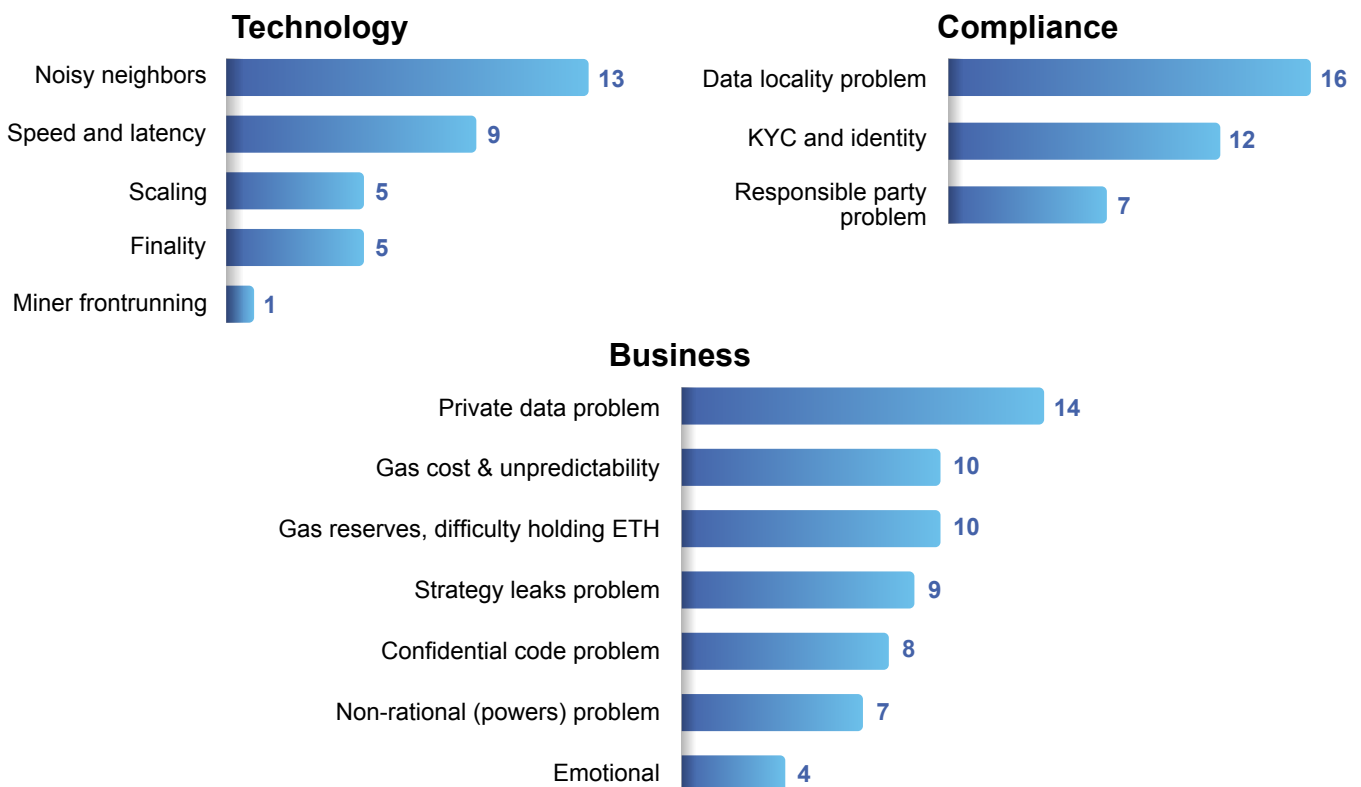
About the Survey

- Conducted in April and May 2020
- 26 responses
- Consisted of 21 questions, supplemented by background information
- Topics included general information about the applications/use cases being considered, barriers and challenges to building on Ethereum Mainnet, benefits, and performance requirements. See questions at https://forms.gle/x8GbL8KRR1WksHmU7.
- Promoted through EEA and other email lists and social media

Respondents were asked to "Please think about a potential application involving Ethereum Mainnet that are very familiar with when filling out this survey. Note that your application does not have to be technically feasible today! We are just as interested in understanding applications that won't work on Mainnet (yet), and why they won't work."

Barriers

What are the barriers to implementing applications on Mainnet?

Technology

Noisy neighbors	13
Speed and latency	9
Scaling	5
Finality	5
Miner frontrunning	1

Compliance

Data locality problem	16
KYC and identity	12
Responsible party problem	7

Business

Private data problem	14
Gas cost & unpredictability	10
Gas reserves, difficulty holding ETH	10
Strategy leaks problem	9
Confidential code problem	8
Non-rational (powers) problem	7
Emotional	4

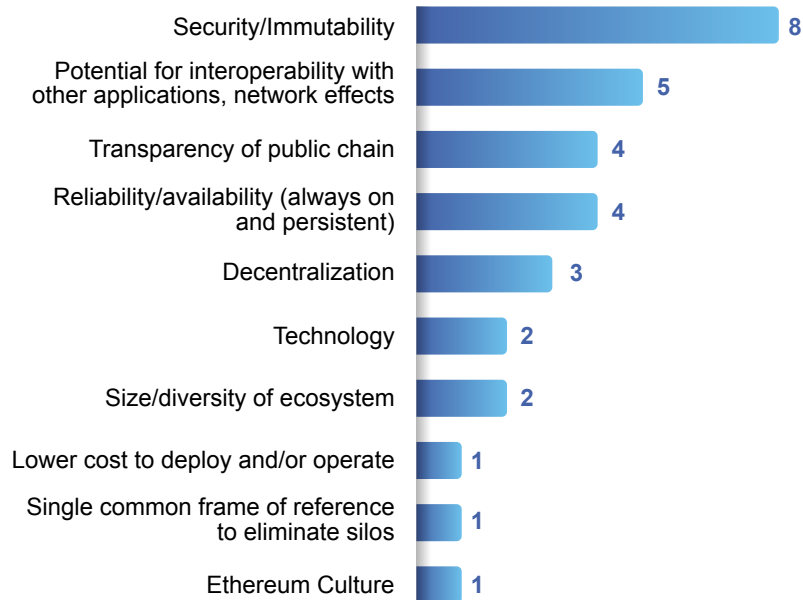*See Appendix 1 for the exact verbiage.*

Applications

Which applications involve Ethereum Mainnet?

- Medical records and medication lists
- Procurement
- E-Commerce vendor reputational score
- Tracking and rating environmental impact of companies
- Tokenizing goods in a supply chain
- Loyalty points
- Factoring invoices
- Health insurance market
- B2B process integration
- Real estate finance
- Supply chain track and trace
- Agricultural seed to sale tracing
- COVID-19 contact tracing
- Finance/securities
- Healthcare research
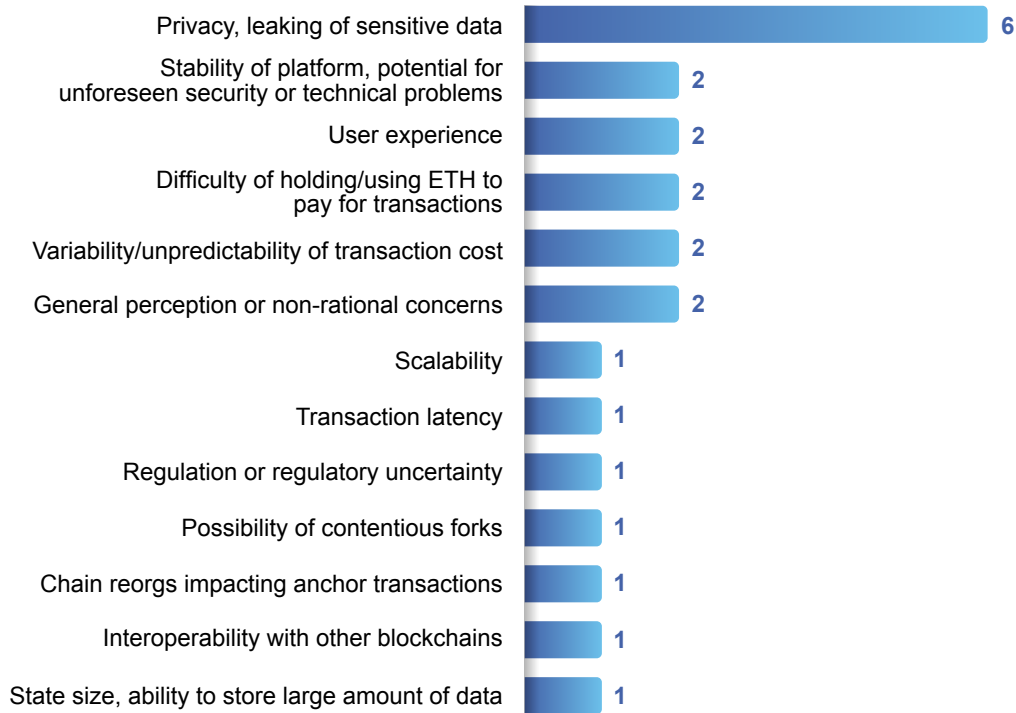- Content management
- Anchoring private chain transactions

Benefits

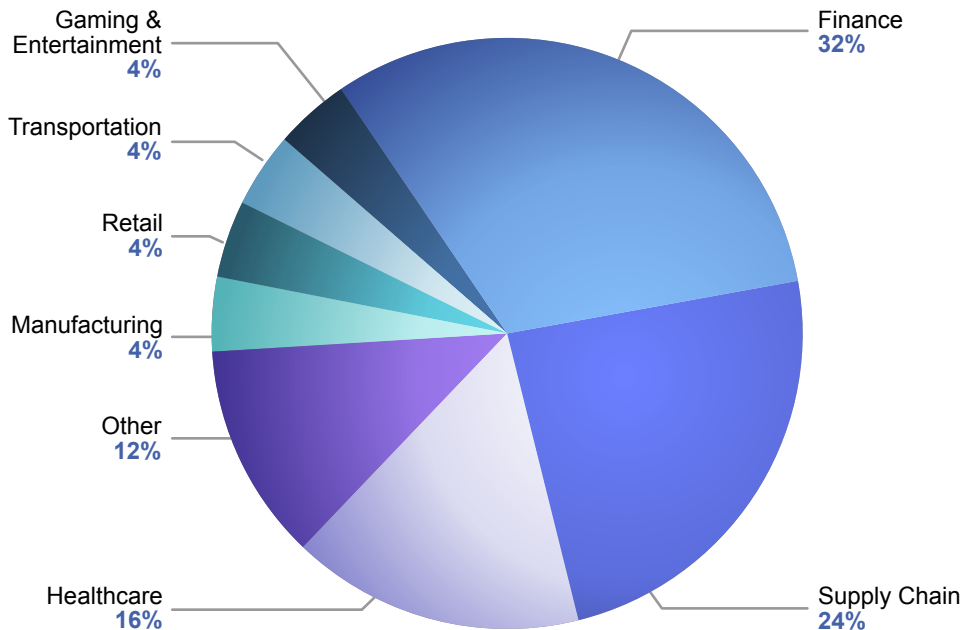**What are the benefits of using Ethereum Mainnet or another public permissionless blockchain?**

Benefit	Count
Security/Immutability	8
Potential for interoperability with other applications, network effects	5
Transparency of public chain	4
Reliability/availability (always on and persistent)	4
Decentralization	3
Technology	2
Size/diversity of ecosystem	2
Lower cost to deploy and/or operate	1
Single common frame of reference to eliminate silos	1
Ethereum Culture	1

Concerns

What are your concerns about using Ethereum Mainnet or another public permissionless blockchain?

Concern	Count
Privacy, leaking of sensitive data	6
Stability of platform, potential for unforeseen security or technical problems	2
User experience	2
Difficulty of holding/using ETH to pay for transactions	2
Variability/unpredictability of transaction cost	2
General perception or non-rational concerns	2
Scalability	1
Transaction latency	1
Regulation or regulatory uncertainty	1
Possibility of contentious forks	1
Chain reorgs impacting anchor transactions	1
Interoperability with other blockchains	1
State size, ability to store large amount of data	1

Industry Breakdown

Of the industries most likely to benefit from Ethereum Mainnet solutions, finance, healthcare, and supply chain were the most frequently mentioned.

Industry	Percentage
Finance	32%
Supply Chain	24%
Healthcare	16%
Other	12%
Manufacturing	4%
Retail	4%
Transportation	4%
Gaming & Entertainment	4%

Performance Requirements

Most respondents (>75%) did not have specific performance requirements or mention transaction latency or throughput as a concern. Of those that did, responses varied widely. For example:

- ~95%+ finality within 15-20 seconds
- 10,000+ TPS
- [latency] should be less than 0.5 sec
- +/- 10-seconds. 30-seconds max
- 1 second maximum
- 40k transactions per day
- 8,100 Transactions per minute

From this and other statements made by respondents, we infer that most of the applications being considered do not exceed the performance capabilities of Ethereum Mainnet. However, it is possible that some potential respondents did not even consider Mainnet in this context for high throughput applications, or that they are focusing on low throughput applications until the technology has evolved further.

Conclusions

Security and interoperability were the top perceived benefits of building on Mainnet.

Data locality and privacy were the most frequently mentioned challenges/barriers. These must be addressed via design patterns and proper choice of technology, as they are not something that can be addressed directly on layer 1.

We were slightly surprised by how few respondents mentioned scalability as a challenge. This suggests that **most of the enterprise use cases involving Mainnet that are under consideration today have relatively low transaction throughput,** which is consistent with our prior experience from personal discussions with community members. However, it is possible that there are many such applications requiring high throughput, but those are not the ones that people are focusing on today. It may be useful to gather additional data on this topic.

The "noisy neighbors" problem was the next most frequently mentioned barrier. The perceived risk that network congestion caused by others may impact an enterprise application is understandable. There are several possible ways to address this.

- Using layer 2 scaling solutions can minimize the number of transactions on layer 1, and the risk and impact and cost of network congestion. There is more educational work to be done in this area to inform developers of their options.
- Developers should use appropriate dynamic gas pricing mechanisms to ensure that critical transactions are not delayed excessively when network utilization fluctuates.
    1. There may be an opportunity for someone to develop a gas price hedging system so that those who want predictability can have it.
    2. There may be more educational work to be done in this area as well.
    3. EIP-1559 should make it easier to determine the appropriate amount of fees to pay at any given time.
- Sharding in Eth2 will increase overall network capacity, and congestion in one shard should not affect the others.

- Finally, this risk exists with many publicly available systems including the Internet, but as they demonstrate their reliability over time, people grow to trust them.

- **Identity/KYC was also at the top of the list, being mentioned by half of respondents.** Identity is a complex topic, and requirements for one application may be extremely different from another. There are many companies and projects working in this space, but still many unsolved problems.

- **Gas cost, difficulty of buying and holding ETH for gas, and variability/unpredictability of gas cost were also top concerns.** Approaches to addressing these interrelated issues include:

  – As mentioned above, there may be an opportunity for someone to develop a gas price hedging system so that those who want predictability can have it.

  – There may be an opportunity for someone to offer a transaction relayer (aka gas station) service aimed at enterprise applications. It would broadcast transactions to the Ethereum network on behalf of its clients, and collect payment in fiat currency. It may also implement dynamic gas price estimation and even hedging.

- **Respondents who had performance requirements were often concerned with transaction latency in addition to throughput.** For certain applications, layer 2 technologies such as plasma and rollups may help meet these requirements. There may be an opportunity to educate enterprise developers about these design patterns.

Acknowledgements

About The EEA

The Enterprise Ethereum Alliance (EEA) is a member-driven standards organization whose charter is to develop open blockchain specifications that drive harmonization and interoperability for businesses and consumers worldwide. Our global community of members is made up of leaders, adopters, innovators, developers, and businesses who collaborate to create an open, decentralized web for the benefit of everyone. To join the EEA, please reach out to membership@entethalliance.org.

If you would like to contribute information about your enterprise use cases involving Ethereum Mainnet to the Use Case Task Force to help guide our future work, please use this link: https://forms.gle/UGMjeBDJm8AWfy77A

Appendix 1 – Barriers

Technology Barriers

- Scaling Problem: My application requires hundreds or thousands of transactions per second, which public chains can't handle.

- Speed and Latency Problem: Our CRM and ERP systems don't need the kind of Transaction Per Second speeds of a Visa or Mastercard (and even they get those TPS rates through parallelization… can't fool me). But long wait times for round-trip + consensus makes things I might do with mainnet a bad user experience.

- Noisy Neighbors must not disrupt my operations: As an enterprise conducting mission-critical operations that rely on predictable operation timing, I need to be comfortable that a "cryptokitty" event isn't a possibility. I need to know that, even though the Mainnet is a public utility, there is reasonable assurance by some means that the reads, writes and computations I need to conduct business on the Mainnet will not be reduced to a crawl by the activities of others.

- Finality Problem: Ethereum is an "eventual consistency". If that's changing with Eth2.0, I don't understand it… something about a magical fast finality something. I dunno. What I do know is that all my systems are ones where a change to data is final the second it's written.

Compliance Barriers

- Data Locality Problem: GDPR requires that I can account for where PII data is stored, even when it is encrypted. And I need to be able to delete that data permanently upon request.

- If the data is sitting permanently on any number of nodes not controlled by me everywhere...yeah.

- Responsible Party Problem: My legal structure requires that there be a responsible party handling all aspects of my data and business logic. If I put data on the Mainnet, I lose a key responsible party.

- Opt-In KYC: I need to know who I'm transacting with, and to register an Ethereum address/identity with KYC/AML: "TSA Precheck" for Identity

Business Barriers

- Cost Problem: It's not about how much it costs per transaction or that our company isn't yet set up to hold ETH for "gas." It's also about the unpredictability of the cost. And I don't want to have to go back for my degree in finance to understand stablecoins just to manage IT.

- Gas Reserves: As a company whose treasury still isn't comfortable holding cryptocurrency, I need an easy and safe way to maintain gas reserves necessary to conduct operations. (This does not include custodianship of coins and tokens held as assets or currency, but rather as a commodity needed to run non-financial operations, store data and proofs, generate shield contracts and other cryptographic methods, and power transactions that may or may not be conducting financial transfers.).

- Private Data Problem: Eighty percent of our data is considered sensitive, internal or personally identifiable client, customer or user data. Encryption isn't enough. Any data can be deanonymized and decrypted given time. And anyone with a full node has forever to crunch the bits on the ledger. So I don't like putting even encrypted data on a public chain.

- Strategy Leaks Problem: Transaction metadata can be used to game the system or collect / analyze for strategic counterintelligence or corp. espionage. In the age of AI, any trace activity done on a permanent, public ledger can be used to figure out who is doing what, even if it's just little changes to Merkle tries.

- Confidential Code Problem: You can't just hide the data with something like ZK-SNARKS and think that everything is ok from a corporate perspective. Many business agreements are embodied in code... business logic. If a machine can execute a smart contract, it can decompile and look at the logic, and that can leak sensitive info.

- Non-Rational (Power) Problems: IBM, Oracle, SAP and others are telling me what to use. They have intimated that if I don't promote their version of private, permissioned blockchain, they might be less interested in selling my offerings to their customers, and we rely on that. [Or any number of other reasons why one might not choose Ethereum Mainnet, even if one believed it was a good technical fit.].

- Emotional: Bitcoin and Ethereum are for criminals and terrorists. I don't want to be associated with that, and I'm afraid of what might happen if government cracked down on public blockchains.