Stefanie Boss[*]
Balázs Bodó[*]

SPECIAL SECTION

DECENTRALISED LAW ENFORCEMENT: A CASE STUDY OF ETHEREUM'S PROOF OF STAKE MECHANISM FOR MODERATION PRACTICES

Abstract
This paper examines the evolving role of the Ethereum blockchain's consensus layer as a potential tool for decentralised law enforcement, with a focus on its Proof-of-Stake (PoS) mechanism and its implications for moderation practices. While it was traditionally designed for credible neutrality, Ethereum's consensus layer is now facing increasing pressure to assist in regulatory enforcement, particularly concerning the U.S. OFAC sanction list. This shift raises fundamental questions about whether a decentralised platform can effectively meet regulatory requirements without compromising its core principles of transparency, security, decentralisation and censorship resistance.
This paper dives into the roles and incentives of actors in the consensus mechanism, with a main focus on builders, relays and validators. It also looks into the complexities introduced by Maximal Extractable Value (MEV) and the Proposer-Builder Separation (PBS). The paper critically assesses Ethereum's potential to function as a regulatory enforcement tool by discussing its inherent limitations, the current stance on adhering to OFAC sanction lists, and other relevant decision-making factors. It also considers the risks associated with leveraging this decentralised platform for regulatory purposes, including the potential for unintended consequences such as privacy and security concerns, and the erosion of core values.
Ultimately, this paper aims to provide insights into whether Ethereum can effectively be leveraged as a regulatory enforcement technology while maintaining its fundamental attributes. We find that Ethereum can leverage compliance to a certain degree, particularly through mechanisms that incentivise validators to exclude sanctioned transactions, and with simple regulation to adhere to. However, the platform's decentralised nature and commitment to censorship resistance means that complete alignment with traditional regulatory frameworks is unlikely. This highlights the fundamental trade-offs that are inherent to attempting to impose centralised control on a decentralised system.

JEL CLASSIFICATION: K42

[*] PhD Candidate at the Institute for Information Law, Institute for Informatics and the Data Science Centre at the University of Amsterdam.
[*] Full Professor at the Institute for Information Law, University of Amsterdam.

DOI 10.13135/2785-7867/12272

SUMMARY

1 Introduction

"Gatekeepers wield silent power, embedded within the very architecture of systems. They determine who gets included and who is excluded, often without those affected even realizing the criteria. Control is not always visible, but it shapes access and opportunity at every step."

– Adapted from Langdon Winner, The Whale and the Reactor: A Search for Limits in an Age of High Technology

This observation encapsulates the essence of gatekeeping. The term *gatekeeper* can be understood as a 'person or organisation that controls whether people can have or use a particular service'.[1] The consensus layer of the Ethereum blockchain fits the description of a gatekeeper, due to its moderating role. Actors in the consensus mechanism decide upon the ordering, inclusion and exclusion of transactions in the Ethereum ecosystem, thus having decisive power over whether certain transactions – or all transactions from a certain user – will enter the ecosystem.

From a regulatory perspective, gatekeepers are non-state actors who can alter the behaviour of others in circumstances where the state has limited capacity to do so.[2] These properties make gatekeepers excellent potential candidates for taking part in the law enforcement domain. Therefore, there has seemingly been an increased interest among administrative authorities to involve private parties – the gatekeepers – in law enforcement activities that are traditionally a task of public regulators, particularly when it comes to content moderation.[3] In some contexts, such as content moderation on large social media platforms and internet service providers, this shift has now reached a point where it no longer merely involves assisting with compliance; instead, it requires these gatekeepers to take a proactive role in balancing the conflicting rights and freedoms of their users, and it may even risk holding them accountable for their users' actions.[4] This extent may also be characterised as responsibilisation, which indicates that these private

[1] 'Gatekeeper' (*Cambridge Dictionary*) <https://dictionary.cambridge.org/dictionary/english/gatekeeper>.
[2] Emily B Laidlaw, 'A Framework for Identifying Internet Information Gatekeepers' (2010) 24 International Review of Law, Computers & Technology 263.
[3] Orla Lynskey, 'Regulating 'Platform Power'' (2017) 1 LSE Law, Society and Economy Working Papers 1 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2921021> accessed 20 June 2025.
[4] Stanisław Tosza, 'Internet Service Providers as Law Enforcers and Adjudicators. A Public Role of Private Actors' (2021) 43 Computer law & security review 1.

parties - the gatekeepers - can now be held responsible for a task that would previously have been the duty of another actor – the state - and sometimes even imposes liability on them.[5] This emerging trend of including technical infrastructures in compliance strategies aligns with broader EU strategies aimed at enhancing digital compliance and enforcement, particularly under frameworks like the Digital Services Act (DSA). However, this form of decentring of regulation may raise concerns, since these gatekeepers that now execute public law functions normally do not serve the public interest, and may not adhere to the relevant public values, such as openness, fairness, participation, consistency, rationality and impartiality of decision-making.[6]

This regulatory debate also strikes the Ethereum blockchain due to recent developments in the context of its consensus mechanism. Lately, there appears to be a tendency among its actors to voluntarily assist regulators in the enforcement of sanction lists by excluding transactions from sanctioned addresses. The Ethereum consensus layer was initially designed to be credibly neutral, meaning that it would be a system designed to validate and order transactions based on objective rules, whilst treating all users and data equally. However, recent developments have shown how the system may be shifting away from neutrality towards a more ambiguous gatekeeping system. First, a recent update to the Ethereum network introduced a new consensus mechanism and strengthened economic incentives for participants in its consensus layer.[7] Second, when the United States' Office of Foreign Asset Control added Ethereum addresses to its sanction list and included Tornado Cash in a more particular fashion, the debate around Ethereum's regulatory capabilities and responsibilities started to gain attention.[8] This shift has raised a fundamental question: Can Ethereum, despite its inherent decentralisation, be effectively leveraged as a regulatory enforcement technology?

Ethereum's inherent design relies on autonomy and decentralisation. Blockchain technology underpins these features, relying on a network of interconnected nodes that

[5] Aleksandra Kuczerawy, 'Private Enforcement of Public Policy: Freedom of Expression in the Era of Online Gatekeeping' (PhD thesis, KU Leuven 2018).

[6] Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World' (2001) 54 Current legal problems 103; Jody Freeman, 'Private Parties, Public Functions and the New Administrative Law' in Steven Cann (ed), *Administrative Law* (Routledge 2018); Kuczerawy (n 5); Tosza (n 4).

[7] Burak Öz and others 'Time Moves Faster When There Is Nothing You Anticipate: The Role of Time in Mev Rewards,' *Proceedings of the 2023 Workshop on Decentralized Finance and Security* (ACM 2023) <https://doi.org/10.1145/3605768.3623563> accessed 20 June 2025.

[8] Zhipeng Wang, Xihan Xiong and William J Knottenbelt, 'Blockchain Transaction Censorship:(In) Secure and (In) Efficient?' *The International Conference on Mathematical Research for Blockchain Economy* (Springer Nature Switzerland 2023) <https://doi.org/10.1007/978-3-031-48731-6_5> accessed 20 June 2025; U.S. Department of the Treasury, 'U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash' *U.S. Department of the Treasury News* (Washington, 8 August 2022) <https://home.treasury.gov/news/press-releases/jy0916#:~:text=WASHINGTON%20%E2%80%93%20Today%2C%20the%20U.S.%20Department,since%20its%20creation%20in%202019.> accessed 20 June 2025; Anders Brownworth and others, 'Regulating Decentralized Systems: Evidence from Sanctions on Tornado Cash' (Federal Reserve Bank of New York 2024) <https://doi.org/10.59576/sr.1112> accessed 20 June 2025.

maintain a shared, immutable ledger of transactions.[9] This structure theoretically eliminates the need for centralised authorities, fostering trust and transparency.[10] However, the very nature of a blockchain—its capacity to record and validate transactions—also raises the possibility of utilizing it to enforce regulatory mandates. While the current dynamics within Ethereum's consensus mechanism present opportunities for the system to take part in regulatory compliance, the prospect of it acting as an enforcement technology is complex, demanding a nuanced understanding of its mechanism design, the motivations of its participants, and the potential implications for its core principles. This paper explores these opportunities and challenges through a critical assessment of Ethereum's ability to be leveraged for regulatory enforcement while preserving its fundamental attributes, such as decentralisation. To achieve that, this paper will take the following approach. First, we will provide some background on the concept of the Ethereum consensus mechanism and its properties. Thereafter, we will discuss Ethereum's potential to function as a tool for regulatory enforcement by discussing its (limiting) properties, the current stance of its regulatory capability through the discussion of its adherence to the OFAC sanction list, other relevant decision-making factors, the sanction effectiveness, and the risks that come with this approach. To understand the real-world implications, we mostly rely on empirical and experimental literature for these sections. Lastly, we will conclude with recommendations and insights into Ethereum's ability to be effectively leveraged as a regulatory enforcement technology.

2 Ethereum's consensus mechanism

2.1 Blockchain technology and Ethereum

Blockchain technology refers to data structures that are used to record transactions in a peer-to-peer network, and are oftentimes built on principles such as decentralisation, immutability, distribution, privacy, security, scalability, reliability and transparency.[11] Blockchains can be categorised as either permissionless or permissioned. Permissionless blockchains, such as Bitcoin and Ethereum, are open to anyone and rely on deterministic consensus rules, rather than on trusted intermediaries to validate transactions. These consensus rules also determine the procedure to add transactions to the blockchain.[12] In

[9] Lorenzo Ghiro and others, 'A Blockchain Definition to Clarify Its Role for the Internet of Things' *2021 19th Mediterranean Communication and Computer Networking Conference (MedComNet)* (IEEE 2021) <https://doi.org/10.1109/medcomnet52149.2021.9501280> accessed 20 June 2025; Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' [2008] SSNR <http://dx.doi.org/10.2139/ssrn.3440802> accessed 20 June 2025.
[10] Ghiro and others (n 9).
[11] ibid, Nakamoto (n 9).
[12] Ghiro and others (n 9).

contrast, permissionless blockchains require specific authorisation for access or participation.[13]

The Ethereum blockchain operates as a permissionless, decentralised blockchain that supports both transaction processing and the deployment of smart contracts – self-executing code that facilitates decentralised applications.[14] The Ethereum network consists of interconnected nodes (computers or servers) that keep a copy of the blockchain and perform various functions, including validating transactions, executing transactions and supporting the consensus mechanism.[15] The aim is to find a consensus on the inclusion and order of transactions that have been requested to be added to the blockchain by its network's users.[16]

On 15 September 2022, Ethereum transitioned from the computationally heavy Proof-of-Work (PoW) consensus mechanism to the more open and energy-efficient Proof-of-Stake (PoS) consensus mechanism.[17] This upgrade is commonly referred to as "*The Merge*". The PoS system relies on verifiable stake, which means that participants must prove that they own a specific stake in Ethereum's native currency to become validators, which currently stands at 32 ETH (approx. 80,000 USD).[18] Validators are responsible for proposing and confirming blocks of transactions. Each validator is randomly assigned a proposing task every once in a while, with a likelihood that equals the proportion of tokens that have been put in stake.[19]

When zooming in on the PoS mechanism, it is structured around slots and epochs. A slot lasts 12 seconds, while an epoch consists of 32 slots (a total of 6.4 minutes). During each slot, a proposer is randomly selected to propose a block, while the other validators vote on which block is best. At the end of an epoch, at least two-thirds of the validators must support the epoch for the blocks therein to be justified. If the two-thirds majority persists in the next epoch, the blocks in the epoch become immutable.[20] Once the blocks are immutable, they cannot be altered, unless an attacker gains control over more than two-

[13] ibid.
[14] Anton Wahrstätter and others, 'Blockchain Censorship' *Proceedings of the ACM Web Conference 2024* (ACM 2024) <https://doi.org/10.1145/3589334.3645431> accessed 20 June 2025.
[15] Davide Mancino and others 'Exploiting Ethereum after" The Merge": The Interplay between PoS and MEV Strategies' *Proceedings of the Italian Conference on Cyber Security (ITASEC 2023)* (CEUR-WS 2023) <https://ceur-ws.org/Vol-3488/> accessed 20 June 2025; Benjamin Kraner and others, 'Agent-Based Modelling of Ethereum Consensus' *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (IEEE 2023) <https://doi.org/10.1109/icbc56567.2023.10174948> accessed 20 June 2025.
[16] Stefanie Boss and Balázs Bodó, 'Censorship-Resistance and Compliance Behavior in the Ethereum Consensus Mechanism' *2025 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (IEEE 2025) (forthcoming).
[17] Mancino and others (n 15); Anton Wahrstätter and others, 'Time to Bribe: Measuring Block Construction Market' [2023] arXiv preprint arXiv:2305.16468 <https://arxiv.org/abs/2305.16468> accessed 20 June 2025; 'The Merge' (*Ethereum.org*, 13 June 2024) <https://ethereum.org/en/roadmap/merge/> accessed 28 June 2024; Kraner and others (n 15).
[18] Ethereum (n 17); Kraner and others (n 15).
[19] Ethereum (n 17); Mancino and others (n 15).
[20] 'Gasper' (*Ethereum*, 15 August 2023) <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/gasper/> accessed 20 June 2025.

thirds of the validators – a scenario known as a 67% attack.[21] This makes the PoS inherently more secure than the PoW system, where an attacker would only need 51% control to alter blocks.[22]

2.2 Stake as an incentive

The PoS system operates on the principle that users with the largest stake have the largest interest in maintaining a properly functioning and secure network. This is because they would lose the most if the value or the reputation of the network's native currency were to diminish.[23] The stake also serves as collateral for incentivising responsible behaviour and for disincentivising malicious actions through a process called *slashing*. Slashing refers to the situation where collateral can be lost as a penalty for misconduct, such as excessive downtime (failing to sign transactions) or double signing (signing multiple conflicting blocks).[24] These penalties can result in the partial or total loss of staked collateral, ensuring that validators adhere to their responsibilities and protect the network's integrity.[25] Despite its benefits, critics argue that this system may lead to wealth centralisation. Wealthier participants can stake their assets, earn rewards, and compound their wealth over time, potentially creating a centralising force.[26] Additionally, there are concerns that a small number of token holders may validate a disproportionately large share of blocks, further concentrating power within the network.[27]

The introduction of *liquid staking* and *staking pools* added another layer of complexity to the consensus mechanism. Liquid staking is a mechanism that allows participants to receive tokenised representations of their staked assets, which enables them to retain access to their funds while still earning staking rewards.[28] These challenges the assumption that high stakes inherently incentivise network care, as users can spend or trade their liquid tokens strategically. However, liquid staking also increases accessibility

[21] Ulysse Pavloff, Yackolley Amoussou-Guenou and Sara Tucci-Piergiovanni, 'Ethereum Proof-of-Stake under Scrutiny' *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing* (ACM 2023) <https://doi.org/10.1145/3555776.3577655> accessed 20 June 2025; Lucas Nuzzi, Kyle Waters and Matias Andrade, 'Breaking BFT: Quantifying the Cost to Attack Bitcoin and Ethereum' [2024] SSNR <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4727999> accessed 20 June 2025.
[22] Pavloff, Amoussou-Guenou and Tucci-Piergiovanni (n 21); Nuzzi, Waters and Andrade (n 21).
[23] Mancino and others (n 15); Ethereum (n 19).
[24] Alpesh Bhudia and others, 'Extortion of a Staking Pool in a Proof-of-Stake Consensus Mechanism,' *2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS)* (IEEE 2022) <https://doi.org/10.1109/coins54846.2022.9854946> accessed 20 June 2025; Krzysztof Gogol and others, 'Empirical and Theoretical Analysis of Liquid Staking Protocols' [2024] arXiv preprint arXiv:2401.16353 <https://arxiv.org/abs/2401.16353> accessed 20 June 2025.
[25] Bhudia and others (n 24); Gogol and others (n 24).
[26] Mancino and others (n 15); Ethereum (n 19).
[27] Mancino and others (n 15); Ethereum (n 19).
[28] Dominic Grandjean, Lioba Heimbach and Roger Wattenhofer, 'Ethereum Proof-of-Stake Consensus Layer: Participation and Decentralization' *International Conference on Financial Cryptography and Data Security* (Springer Nature Switzerland 2024) <https://link.springer.com/chapter/10.1007/978-3-031-69231-4_17> accessed 20 June 2025.

by removing the need for participants to fully lock up their collateral.[29] *Staking pools*, such as Lido and Rocket Pool, further democratise staking by allowing users to combine their resources and collectively meet the 32 ETH requirement for running a validator node.[30] Participants in these pools share both the rewards and the responsibilities of staking. This reduces the barriers to entry for smaller stakeholders and simplifies the staking process, because it allows participants to delegate tasks to pool operators.[31] While this pooled model improves accessibility, it raises concerns about decentralisation and security. A staking pool centralises control over multiple validators, making it an easier target for malicious actors compared to individually operated nodes.[32] Despite the challenges of both liquid staking and staking pools, they have still benefited the consensus mechanism by significantly broadening the inclusivity of the system, and by providing opportunities for smaller investors to contribute to the PoS system.[33]

2.3 Proposer builder separation and maximal extractable value

The complexity of transaction ordering in Ethereum's consensus layer is primarily influenced by two key concepts: maximal extractable value (MEV) and proposer builder separation (PBS).

MEV refers to the value that users can extract within a blockchain network beyond standard protocol incentives. This phenomenon manifests itself on many of Ethereum's layers, but in the context of the consensus mechanism, MEV opportunities arise when certain actors take advantage by strategically including or excluding transactions, or by ordering a block in a certain way.[34] A key concept in consensus layer MEV is *gas*, which is the maximum price that a user is willing to pay to have their transaction included in the blockchain. Gas is calculated as the computational cost of executing a transaction on the network.[35] Each user can determine their own maximum and express this in the form of a bid. Within this specific MEV realm, there are a few common MEV strategies[36]:

[29] Apostolos Tzinas and Dionysis Zindros, 'The Principal-Agent Problem in Liquid Staking' *International Conference on Financial Cryptography and Data Security* (Springer Nature Switzerland 2023) <https://doi.org/10.1007/978-3-031-48806-1_29> accessed 20 June 2025; Gogol and others (n 24); Krzysztof Gogol and others, 'SoK: Liquid Staking Tokens (LSTs) and Emerging Trends in Restaking' [2024] arXiv preprint arXiv:2404.00644 <https://arxiv.org/abs/2404.00644> accessed 20 June 2025.
[30] Bhudia and others (n 24).
[31] ibid.
[32] ibid.
[33] ibid.
[34] Wang, Xiong and Knottenbelt (n 8); Mancino and others (n 15); Wahrstätter and others (n 14); Öz and others (n 7); Simona Ramos and Joshua Ellul, 'The MEV Saga: Can Regulation Illuminate the Dark Forest?' *International Conference on Advanced Information Systems Engineering* (Springer International Publishing 2023) <https://doi.org/10.1007/978-3-031-34985-0_19> accessed 20 June 2025.
[35] Wahrstätter and others (n 14).
[36] Ramos and Ellul (n 34).

- *Front-running*: an MEV-seeking party pays a gas price that is higher than a targeted other transaction, so that the MEV-seeker's transaction can be included in the blockchain before the targeted transaction.[37]
- *Back-running:* an MEV-seeking party places its transaction directly after a targeted transaction.[38]
- *Sandwich attacks:* an MEV-seeking party places its transaction both before and after a targeted transaction.[39]

While these MEV strategies seem lucrative at first glance, they have caused several issues. A main issue is the competitive advantage that it gives to larger validator pools and validators with successful MEV strategies, because it makes staking less accessible for smaller or individual validators.[40] Other issues included gas fee inflation, network congestion, excessive block space usage, compromised consensus security, unfairness, and problematic competition between MEV-seekers.[41] Studies have also shown significant MEV increases during times of crisis, such as the FTX collapse, with spikes between 400 and 1000%.[42] MEV on the consensus layer may also lead to undesired censorship of transactions and market manipulation practices.[43]

To address these issues, Ethereum introduced the proposer-builder separation (PBS). PBS separates the block building and the block proposal tasks, which were previously performed by validators alone.[44] This division enables competitive block construction while ensuring that block proposal and validation remain neutral, as block proposers cannot view the transaction content before signing the blocks.[45] To allow the parties to trust each other while also benefiting economically, algorithms called 'MEV-Boost relays' have been introduced as intermediaries between builders and proposers.[46] This is part of the *MEV-Boost* architecture, an opt-in mechanism that block proposers voluntarily use to access profitable blocks by proficient entities, and is adopted approximately 90% of the time[47].

When zooming out, there are a few key actors in the Ethereum consensus layer under PBS: users, searchers, builders, relays, and validators. They all have different roles and

[37] Wahrstätter and others (n 14).
[38] ibid.
[39] ibid.
[40] Yan Ji and James Grimmelmann, 'Regulatory Implications of MEV Mitigations' *International Conference on Financial Cryptography and Data Security* (Springer Nature Switzerland 2024) <http://link.springer.com/chapter/10.1007/978-3-031-69231-4_21> accessed 20 June 2025.
[41] Wahrstätter and others (n 14); Sebastian Wunderlich, 'Current State of MEV in the Ethereum Ecosystem' *Konferenzband zum Scientific Track der Blockchain Autumn School 2023* (Hochschule Mittweida 2023); Ji and Grimmelmann (n 40).
[42] Wahrstätter and others (n 14).
[43] Ramos and Ellul (n 34).
[44] Öz and others (n 7).
[45] Ji and Grimmelmann (n 40).
[46] Mancino and others (n 15); Wang, Xiong and Knottenbelt (n 8); Öz and others (n 7); Ramos and Ellul (n 34).
[47] Wahrstätter and others (n 14).

have different opportunities to deviate from remaining neutral for varying reasons, including economic or legal reasons. *Users* request transactions and specify a maximum gas fee that they are willing to pay. By bidding higher gas fees, users can potentially push through transactions that might otherwise be deprioritised or sanctioned.[48] Transaction requests flow either through a public mempool, which is a repository of pending transactions, or through a private order flow directly to block builders. *Searchers* monitor the mempool, identify MEV opportunities, restructure transactions, and submit bundles of transactions to builders through private order flow.[49] They have discretion over which transactions to include in their bundles, giving them some influence over the inclusion of sanctioned or less profitable transactions.[50] *Builders* aggregate transactions from the mempool and from private order flow sources to construct the most profitable blocks.[51] They can optimise transaction ordering by using algorithms and market-driven strategies.[52] Builders can employ inclusion or exclusion lists based on various factors, including economic incentives or compliance. This gives them medium to high influence over which transactions are included or excluded from blocks.[53] After constructing the blocks, they submit the blocks to *relays*, who act as intermediaries between builders and proposers. Relays verify the validity of the blocks that they received from builders.[54] Importantly, they can decide to enforce policies that filter out illicit transactions through their algorithm, such as those associated with sanctioned addresses.[55] This gives relays medium to high influence over transaction inclusion. Afterwards, relays send the most profitable block to the proposing validator in a blind manner, which means that the transaction contents are not revealed.[56] The proposing validator selects the most profitable block received from the relays that it is signed up to, signs it and sends it back to the relay, who verifies the signature and sends the full block to the proposer.[57] Because the blocks are blind, proposers have minimal direct autonomy over the transaction inclusion.[58] However, proposers can choose which relays they work with, thereby indirectly influencing transaction inclusion by favouring relays that filter or prioritize certain transactions.[59] When the proposer has received the full block from the relay, it propagates the block to the attesting validators in the peer-to-peer network.[60] The validators will then attest to the blocks they receive, which includes confirming the

[48] Wang, Xiong and Knottenbelt (n 8); Wahrstätter and others (n 14); Boss and Bodó (n 16).
[49] ibid.
[50] ibid.
[51] ibid.
[52] Wang, Xiong and Knottenbelt (n 8).
[53] ibid, Wahrstätter and others (n 14); Boss and Bodó (n 16).
[54] Wang, Xiong and Knottenbelt (n 8); Wahrstätter and others (n 18); Boss and Bodó (n 16).
[55] ibid.
[56] ibid.
[57] ibid.
[58] ibid.
[59] Brownworth and others (n 8).
[60] Wang, Xiong and Knottenbelt (n 8); Wahrstätter and others (n 14); Boss and Bodó (n 16).

validity and the accuracy of the data contained within a block.[61] This occurs every epoch. These validators have limited direct influence on transaction inclusion because they primarily validate blocks that are already constructed and proposed. While refusing to attest to certain blocks could theoretically allow validators to censor illicit blocks, this comes with risks of penalties like slashing.[62] Once in a while, validators may have to participate in the sync committee, for which they must create signatures to attest to the chain's head. Sync committee participation lasts 27 hours.[63] Validators receive rewards for their tasks, including consensus layer rewards (for block proposal, attestation, and sync committee participation)[64] and execution layer rewards[65] (priority fees and direct user payments).[66] They can also receive a whistleblower reward if they provide evidence of dishonest validators.[67] After a block is backed by two-thirds of the attestors, it will be added to the blockchain. All in all, the system looks as follows (figure 1).[68]

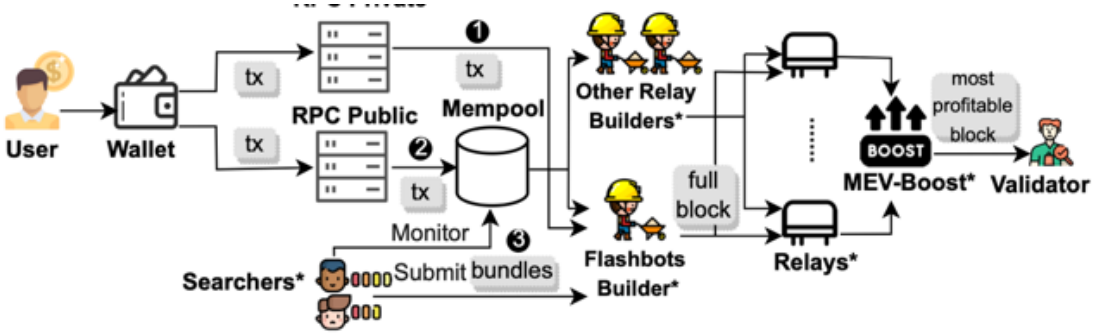

Figure 1: PBS workflow[69]

The introduction of PBS enhances efficiency by delegating block construction to specialised builders who optimise transaction selection.[70] Validators are only required to select the highest-paying block, reducing computational costs and improving network efficiency. [71] Despite its benefits, PBS also introduces new centralisation risks. The current landscape is dominated by a few relays, resulting in a degree of centralisation, with an oligarchic character.[72] Empirical studies suggest that, rather than decentralising

[61] ibid.
[62] ibid.
[63] ibid.
[64] Currently, a validator receives approximately 0.04 ETH for a successful proposal and 0.00001 ETH for a successful attestation.
[65] This is approximately 0.1 ETH per block that they propose.
[66] Grandjean, Heimbach and Wattenhofer (n 28).
[67] ibid.
[68] Wang, Xiong and Knottenbelt (n 8).
[69] ibid.
[70] ibid.
[71] ibid.
[72] Boss and Bodó (n 16); Fei Wu and others, 'From Competition to Centralization: The Oligopoly in Ethereum Block Building Auctions' [2024] arXiv preprint arXiv:2412.18074 <https://arxiv.org/abs/2412.18074> accessed 20 June 2025.

transaction inclusion, PBS has now introduced risks surrounding power concentration with a small set of block builders and relays.[73] Essentially, the issues found with dominant validators pre-PBS, such as entry barriers due to the competitive advantages, seem to have shifted towards builders and relays under PBS.[74] Additionally, entities like private RPCs, MEV searchers, builders, and relays may censor transactions based on economic incentives or regulatory compliance.[75] The upcoming section dives deeper into the censorship dilemma.

2.4 Ethereum's values: content agnosticism, credible neutrality and censorship resistance

Converse to most gatekeeping systems, such as on social media platforms where proactive moderation practices are often practiced,[76] the Ethereum consensus mechanism is designed to be content agnostic and censorship resistant. This essentially comes down to a system where filtering of any kind is not prescribed or encouraged. Actors shall, in principle, accept and include all transactions that comply with the technical standards of the network, and that are consistent with the transaction history.[77] Traditional, neutral, rules for transaction inclusion can therefore be found in network rules, and the availability of sufficient funds to complete the transaction.[78] This design promotes open participation, and provides a degree of protection against state-level enforcement.

While this standard practice does not directly open doors for Ethereum Consensus as an enforcement technology, recent developments are indicating a shift towards more complex and elaborate moderation practices. There are indications of consensus layer actors engaging in more elaborate moderation practices, where both economic incentives and regulatory incentives are playing an increasingly important role.[79] The Merge has altered the reward structure, and may have led to an intensified profit-driven nature of consensus layer participants' actions.[80] Nonetheless, the biggest shift has come from the sanctions on Ethereum addresses issued by the U.S. Office of Foreign Assets Control (OFAC), particularly the Tornado Cash sanctions in August 2022.[81] Addresses on this sanction list are considered illegal to interact with. While the sanctions have eventually

[73] Lioba Heimbach and others, 'Ethereum's Proposer-Builder Separation: Promises and Realities' *Proceedings of the 2023 ACM on Internet Measurement Conference* (ACM 2023) <https://doi.org/10.1145/3618257.3624824> accessed 20 June 2025; Sen Yang, Kartik Nayak and Fan Zhang, 'Decentralization of Ethereum's Builder Market' *2025 IEEE Symposium on Security and Privacy (SP)* (IEEE 2025) <https://www.computer.org/csdl/proceedings-article/sp/2025/223600b456/26hiUkhZyfK> accessed 20 June 2025.
[74] Wahrstätter and others (n 14); Heimbach and others (n 73).
[75] Wang, Xiong and Knottenbelt (n 8).
[76] Tosza (n 4).
[77] Michael Nofer and others, 'Blockchain' (2017) 59 Business & Information Systems Engineering 183.
[78] ibid, Boss and Bodó (n 16).
[79] Boss and Bodó (n 16).
[80] Öz and others (n 7).
[81] Wang, Xiong and Knottenbelt (n 8); Brownworth and others (n 8); U.S. Department of the Treasury (n 8).

been overturned in November 2024,[82] they have raised important questions about the extent to which legal compliance and accountability (should) influence consensus-level decisions and around the balance between these factors and other considerations.[83]

This discussion has opened the door to questions around Ethereum's ability to enforce regulation, and in what way the consensus layer could play a role in and be responsible for regulatory enforcement. This discussion centres around two key perspectives. One perspective is that it is required to be compliant with regulation, or to at least try to enforce the law, while the other perspective uses the shield of credible neutrality to argue that they shall not engage in censorship behaviour that follows from regulatory pressure. Those against censorship tend to compare the situation to internet governance and net neutrality. In both systems, the base layer participant solely engages in the recording of data. Some other actors argue that record-keeping on the blockchain is no different than financial messages being transmitted through – for instance – internet service providers, routers, network switches, email and chat programs, and that they should be granted the same neutrality exceptions.[84] Therefore, there runs a sentiment that validators should not have to monitor or censor transactions according to the law.[85]

3 Ethereum's efficacy in compliance and enforcement

To be able to assess whether and to what extent the Ethereum consensus mechanism would be able to deal with regulatory enforcement in the context of European regulation, it is important to dive into empirical evidence regarding its current state of compliance practices. We will first establish a few prerequisites for the evaluation framework. Then, we will discuss evidence for compliance with the OFAC sanction lists. In the later sections, we will discuss economic, reputational and jurisdictional factors and risks that may influence the decision-making process of the consensus layer participants, which could potentially be considered when evaluating potential improvements of the system design or incentivisation in the context of regulatory compliance. Thereafter, we will discuss the sanction effectiveness, and the risks associated with Ethereum as a regulatory enforcement tool.

3.1 Prerequisites and system limitations

It is first relevant to make a distinction between direct and indirect censorship. Direct censorship refers to the explicit exclusion of specific transactions by validators to, for

[82] Nate Raymond, 'Court Overturns US Sanctions against Cryptocurrency Mixer Tornado Cash' (*Reuters*, 27 November 2024) <https://www.reuters.com/legal/court-overturns-us-sanctions-against-cryptocurrency-mixer-tornado-cash-2024-11-27/> accessed 20 June 2025.
[83] Wang, Xiong and Knottenbelt (n 8).
[84] Rodrigo Seira, Amyaixizhang and Dan Robinson, 'Base Layer Neutrality' (*Paradigm*, 8 September 2022) <https://www.paradigm.xyz/2022/09/base-layer-neutrality> accessed 20 June 2025.
[85] ibid.

instance, comply with regulations such as OFAC sanctions.[86] For instance, a validator might refuse to broadcast a received transaction, sign an attestation, or include a transaction in a block. Indirect censorship involves a 'coincidence' kind of censorship, as it results from economic optimisation strategies, such as MEV exploitation, where transaction selection is biased for profit, rather than for explicit rules.[87] Indirect censorship may also occur due to transaction delays that originate from external entities like relays or RPC providers.[88]

There are also some limitations to consider. Ethereum's consensus mechanism design plays a pivotal role in shaping how different actors approach transaction censorship, but comes with its own instructions and limitations in the context of compliance. The system's architecture creates a nuanced landscape where participants' abilities to influence transaction inclusion vary significantly based on their roles.[89] At the forefront of this dynamic are builders and relays, because their direct access to transaction details empowers them to make informed decisions about which transactions they include or exclude from blocks. This position allows for more deliberate choices, potentially balancing profit motives against regulatory compliance.[90] In contrast, proposers and validators operate in a more constrained environment. Proposers interact with opaque blocks, unable to scrutinise individual transactions before proposing or validating. This more or less 'blind' approach inherently limits their capacity for targeted transaction censorship, shifting the balance of power in the censorship ecosystem to block builders and relays.[91] Attesting validators face constraints as well, as they are most at risk of facing negative consequences for censorship behaviour with the slashing risks.

It is further important to notice that Ethereum's consensus mechanism is fundamentally designed to make binary decisions about transaction inclusion or exclusion, based on predefined rules. The design, as outlined in section 2, may struggle to deal with nuanced regulatory requirements. This limitation is particularly evident when considering the time constraints of Ethereum's 12-second slot time, due to which most actors use algorithms to execute their tasks. They pre-program their desired decision-making path, which necessitates that all regulatory compliance is algorithmically programmable. While such algorithms can effectively implement straightforward rules, such as blocking transactions from specific blacklisted addresses, it likely lacks the sophistication to handle complex compliance scenarios that often require contextual interpretation. This limitation is particularly problematic when dealing with European digital regulations, which frequently demand nuanced understanding and application. The evaluation of such regulatory criteria

[86] Heimbach and others (n 73); Wahrstätter and others (n 14).
[87] Wu and others (n 72); Zihao Li and others, 'Demystifying Defi Mev Activities in Flashbots Bundle' *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (ACM 2023) <https://doi.org/10.1145/3576915.3616590> accessed 20 June 2025.
[88] Wu and others (n 72); Li and others (n 87).
[89] Boss and Bodó (n 16).
[90] ibid.
[91] ibid, Yang, Nayak and Zhang (n 73).

requires human interpretation, especially when navigating evolving regulations or grey areas in compliance. However, the 12-second timeframe for block creation makes human intervention impossible, and programming such complex decision-making into an algorithm that must also optimise for economic factors is highly challenging. Another complicating factor is the diverse and sometimes conflicting nature of international regulations. As it is often impossible to determine the country of origin for a transaction, any implemented regulation must be universally applicable or at least not directly conflict with rules from other jurisdictions. Given these constraints, it's crucial to recognise that Ethereum's consensus mechanism would only be effective for regulatory enforcement if the rules in question are binary, universal or simple enough to be programmed into an algorithm. In the following sections, we will therefore evaluate the enforcement capabilities based on the premise that the regulation in question is a programmable, straightforward rule, such as the OFAC sanctions list.

3.2 Direct censorship: OFAC sanction list enforcement

Due to the increased attention for regulatory compliance-related censorship in Ethereum, several empirical studies have investigated the extent to which regulatory compliance is followed in this realm. These studies show that compliance-based censorship in Ethereum is not incidental, but is systemically enforced by major relays and builders, with behaviour varying among different consensus layer participants. Interestingly, compliance appears to be an important factor in the inclusion or exclusion of sanctioned transactions: the fees offered for blocks that include sanctioned addresses are lower than those that exclude them, indicating that non-compliance may be a conscious, philosophical choice, rather than a monetarily driven choice.[92]

Some large relays, including Flashbots, Eden and bloXroute Regulated, explicitly state that they exclude sanctioned transactions.[93] These relays indeed demonstrate the lowest inclusion percentages of sanctioned addresses, albeit not being 0%, regardless of how many blocks they are involved in.[94] This compliance suggests these actors are likely trying to mitigate legal repercussions, potentially in jurisdictions with a strong regulatory enforcement culture, indicating that legal considerations play a significant role for some participants.[95] A similar suspicion holds for block builders, as a study reveals that regulatory pressure may potentially alter the structure of the block-building market and, to some extent, intensify transaction censorship tendencies.[96]

When zooming in on the transactions themselves, studies show that transactions from Tornado Cash addresses were included significantly less often in blocks after their

[92] Brownworth and others (n 8).
[93] Wang, Xiong and Knottenbelt (n 8); Brownworth and others (n 8).
[94] Boss and Bodó (n 16); Heimbach and others (n 73).
[95] Boss and Bodó (n 16).
[96] Brownworth and others (n 8).

sanctioning, and that the inclusion is largely dependent on a single larger block builder.[97] Further, it was found that all OFAC-sanctioned addresses are significantly less likely to be included in PBS-produced blocks, with a 50 percent lower likelihood compared to non-PBS-produced blocks.[98]

The consequences of censorship are evident, with Tornado Cash transaction volume plummeting by 84% within two months of the sanctions that were announced in August 2022.[99] Additionally, studies have identified that censorship not only relates to exclusion but may also manifest as delayed inclusion when not every builder, proposer, or validator is censoring, making transaction inclusion a matter of time and luck rather than a full ban.[100]

3.3 Indirect censorship: economic factors

Some consensus layer participants may be driven to make decisions based on factors other than compliance. A key alternative factor lies in economic thinking. Literature highlights a complex relationship between economic incentives, censorship behaviour, and network stability within Ethereum's consensus mechanism. Simulation findings suggest that when staking incentives are insufficient, validators may resort to censorship strategies to safeguard their economic interests.[101] In contrast, well-structured staking reward mechanisms can strengthen censorship resistance.[102] Similarly, game-theoretic analyses of transaction fees reveal that sufficiently high fees incentivise builders to accept all transactions rather than engage in censorship, indicating that effective market pricing mechanisms can influence whether builders would be incentivised to engage in censorship for compliance purposes. [103] Empirical evidence confirms this by showing that block builders consistently prioritise MEV-profitable transactions, sidelining lower-value transactions that fail to meet profitability thresholds.[104] This creates an environment where financial incentives dominate decision-making. A similar dynamic exists with relays, which often prioritise revenue-maximising transactions over ensuring fairness and accessibility, deepening economic censorship in Ethereum's block-building process.[105]

[97] ibid.
[98] Heimbach and others (n 73); Wahrstätter and others (n 14).
[99] Wahrstätter and others (n 14).
[100] ibid.
[101] Letterio Galletta and others, 'Resilience of Hybrid Casper under Varying Values of Parameters' (2023) 2 Distributed Ledger Technologies: Research and Practice 1.
[102] ibid.
[103] Elijah Fox, Mallesh Pai and Max Resnick, 'Censorship Resistance in On-Chain Auctions' *5th Conference on Advances in Financial Technologies* (AFT 2023) (Leibniz-Zentrum für Informatik 2023) <https://doi.org/10.4230/LIPIcs.AFT.2023.19> accessed 20 June 2025; Agostino Capponi, Ruizhe Jia and Sveinn Olafsson, 'Proposer-Builder Separation, Payment for Order Flows, and Centralization in Blockchain' [2024] SSNR <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4723674> accessed 20 June 2025.
[104] Bruno Mazorra, Michael Reynolds and Vanesa Daza, 'Price of Mev: Towards a Game Theoretical Approach to Mev' *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security* (ACM 2022) <https://doi.org/10.1145/3560832.3563433> accessed 20 June 2025; Wunderlich (n 41); Ramos and Ellul (n 34).
[105] Ramos and Ellul (n 34).

The temporal dynamics of transaction censorship in Ethereum's consensus mechanism add another layer of complexity. The temporal patterns are closely tied to economic incentives, particularly those related to MEV. Studies show fluctuations in validators' block proposal frequency and their treatment of censored transactions over time, with censorship rates showing periodic surges.[106] These fluctuations appear to be driven by a complex interplay of factors, including validator market concentration, MEV-based economic incentives, and governance structures.[107] Time series analyses further demonstrate how MEV extraction patterns ebb and flow with market cycles, manifesting in changing block-building profits and evolving MEV strategies, such as sandwich attacks and liquidations.[108] Moreover, during periods of high MEV rewards, Proof-of-Stake validators have been observed strategically adjusting their block proposal timing to optimise earnings, leading to noticeable shifts in block production patterns.[109] Collectively, these findings paint a picture of a dynamic censorship landscape in Ethereum, where economic incentives, particularly those driven by MEV, play a crucial role in shaping transaction inclusion patterns over time. This suggests that optimizing transaction fee structures and staking reward mechanisms could be key to influencing censorship and compliance incentives.

3.4 Jurisdictional concerns

Ethereum's censorship landscape is closely intertwined with regulatory complexity. A recent study found that a significant portion of Ethereum's nodes, including 34% of consensus nodes and 44% of execution nodes, are located in the United States.[110] This geographic concentration raises the question whether the United States and its regulations may significantly influence the behaviour of consensus layer participants surrounding regulatory compliance, and whether they may mostly adhere to the United States' regulations, rather than to European regulations. A complicating factor in this question is the concept of "regulatory complication," which stems from blockchain's inherent design. The pseudonymous or anonymous nature of many actors on the network makes it difficult—and costly—for regulators to identify and trace those behind questionable or illegal transactions. This lack of accountability can incentivise certain actors to engage in illicit activities, particularly when there are financial rewards, such as higher transaction fees, to be gained. These actors may perceive themselves as autonomous from legal frameworks, further complicating enforcement efforts. This sense of autonomy is reinforced by blockchain's reliance on code, which allows the system to function

[106] Pavloff, Amoussou-Guenou and Tucci-Piergiovanni (n 21).
[107] ibid.
[108] Heimbach and others (n 73).
[109] Öz and others (n 7).
[110] Simon Brown, 'Measuring the Concentration of Control in Contemporary Ethereum' [2023] arXiv preprint arXiv:2312.14562 <https://arxiv.org/abs/2312.14562> accessed 20 June 2025.

independently of legal oversight—at least in theory. As a result, validators may not always prioritise compliance with legal rules when processing transactions.

3.5 Reputation

Reputation may also play a role in the decision-making process of consensus layer participants. If an actor takes part in compliance, this may in some contexts benefit their reputation – in jurisdictions that are highly regulated or at risk of regulation – or damage your reputation if you are not established in a region where regulation does not form a major risk. Further, if the majority of the network stands for neutrality, a voluntary compliant validator may risk being perceived as weak or not in accordance with the network's values. Another aspect of reputation comes in when a validator engages in self-serving behaviour.[111] If a validator obstructs the stability of the consensus system by waiting long periods to validate a block or transactions to extract value from that action, it might encounter reputation damage.[112]

3.6 Sanction effectiveness

The decentralised architecture of Ethereum poses unique challenges to the enforcement of sanctions. While sanctions aim to restrict illegal transactions, their effectiveness in such systems is inherently limited due to the network's design, which allows transactions to bypass certain layers of enforcement. The complexity arises from the decentralised nature of Ethereum's consensus system, combined with a system design that obscures the true nature of transactions for certain actors in the consensus layer.[113] Another complexity arises if a larger entity in the system decides to let sanctioned addresses through, as it permits the transaction to be added to the blockchain, with an inclusion delay as the largest consequence.[114]

While sanctions can delay the inclusion of blacklisted transactions, studies show that these transactions often find pathways to eventual inclusion in blocks. This highlights the limitations of partial enforcement, where only some actors or layers implement sanctions. Empirical observations suggest that blacklisted transactions tend to occur more frequently after their sanction date, potentially indicating attempts to move funds before sanctions are fully implemented or adopted by all actors.[115] Further, transaction volumes associated with sanctioned addresses often drop before sanctions are announced, but remain at non-zero levels after enforcement begins. This suggests that sanctions may have a limited

[111] Öz and others (n 7).
[112] ibid.
[113] Zeinab Alipanahloo, Abdelhakim Senhaji Hafid and Kaiwen Zhang, 'Maximal Extractable Value Mitigation Approaches in Ethereum and Layer-2 Chains: A Comprehensive Survey' (2024) 1 IEEE <https://espace2.etsmtl.ca/id/eprint/30326/1/Zhang-K-2024-30326.pdf> accessed 20 June 2025.
[114] Heimbach and others (n 73).
[115] Boss and Bodó (n 16).

impact on restricting the address activity in its entirety.[116] When a transaction is eventually delayed, studies show that these censored transactions experience an average delay of 20.6 seconds compared to uncensored ones, following a normal distribution pattern. [117] The average confirmation time for censored transactions (e.g., Tornado Cash-related transactions) increased from 15.8 ± 22.8 seconds in August 2022 to 29.3 ± 23.9 seconds in November 2022. Non-censored transactions maintained significantly lower confirmation times (8.7 ± 8.3 seconds).[118] Such extended delay increases failure rates and raises the likelihood of censored transactions being dropped entirely. [119]

These findings underscore the limitations of partial enforcement in decentralised systems, where sanctioning often results in delays or a 'waiting game', rather than an absolute ban. While sanctions can delay the inclusion of blacklisted transactions, these transactions often find pathways to eventual inclusion in blocks, highlighting the limitations of partial enforcement where only some actors or layers implement sanctions. Effective regulation may require a coordinated, system-wide approach involving all actors to ensure consistent enforcement.[120]

3.7 Risks

While transaction censorship for regulatory purposes could potentially provide more legal certainty in the Ethereum blockchain, it also introduces significant risks. Studies have shown that time differences in transaction acceptance may lead to de-anonymisation, compromising network privacy.[121] Furthermore, censorship behaviours have cascading effects on Ethereum's security and decentralisation. Selective transaction exclusion results in mempool congestion, reduced throughput, and increased vulnerability to attacks.[122] Adversaries may introduce complex "tainted transactions" that force miners or block builders to perform additional computations, degrading network performance.[123] Most critically, if more than 50% of validators engage in censorship, Ethereum's censorship resistance is severely compromised, threatening decentralisation by concentrating decision-making power among a few entities.[124] Decentralisation plays a crucial role in mitigating these adverse effects; higher decentralisation reduces validator manipulation risks, distributes decision-making power more evenly, and makes the network more

[116] ibid.
[117] Wahrstätter and others (n 14).
[118] ibid.
[119] Ji and Grimmelmann (n 40).
[120] Boss and Bodó (n 16).
[121] Shan Wang and others, 'Deanonymizing Ethereum Users behind Third-Party RPC Services' *IEEE INFOCOM 2024 - IEEE Conference on Computer Communications* (IEEE 2024) <https://doi.org/10.1109/infocom52122.2024.10621236> accessed 20 June 2025.
[122] Heimbach and others (n 73); Grandjean, Heimbach and Wattenhofer (n 28); Wahrstätter and others (n 14).
[123] Wang, Xiong and Knottenbelt (n 8).
[124] Wahrstätter and others (n 14).

resilient to single-point failures.[125] These risks highlight the delicate balance between regulatory compliance and preserving the core principles of blockchain technology. They also suggest that if Ethereum fully embraces legal compliance, its decentralisation mechanisms must be carefully considered, potentially requiring design upgrades to mitigate the risks of centralisation.

3.8 Can Ethereum's consensus layer assist in regulatory enforcement?

This section has explored the current state of regulatory compliance within the Ethereum consensus mechanism, particularly focusing on the enforcement of OFAC sanctions. Several empirical papers demonstrate that direct censorship, while present, is not absolute, with sanctioned transactions often experiencing delays rather than outright exclusion. This partial enforcement stems from the decentralised architecture of Ethereum, where different actors have varying degrees of control over transaction inclusion. The system's architecture creates a nuanced landscape where participants' abilities to influence transaction inclusion vary significantly based on their roles. At the forefront of this dynamic are builders and relays, because their direct access to transaction details empowers them to make relatively informed decisions about which transactions to include or exclude from blocks. This position allows for more deliberate choices, potentially balancing profit motives against regulatory compliance. In contrast, proposers and validators operate in a much more constrained environment, with proposers even interacting with opaque blocks and unable to scrutinise individual transactions. This limits their capacity for targeted transaction censorship, shifting the balance of power in the censorship ecosystem to block builders and relays.

Design features, economic incentives, jurisdictional concerns, and reputational factors further complicate the landscape, as they are simultaneously influencing the decision-making processes of consensus layer participants. Ethereum's consensus mechanism is designed to make relatively quick decisions about transaction inclusion or exclusion, based on predefined rules. The design may struggle to deal with nuanced regulatory requirements, especially with the time constraints of Ethereum's 12-second slot time, due to which most actors use algorithms to execute their tasks. Such algorithms can effectively implement straightforward rules, such as blocking transactions from specific blacklisted addresses, but they likely lack the sophistication to handle complex compliance scenarios that often require contextual interpretation. Additionally, the diverse and sometimes conflicting nature of international regulations poses a challenge, especially if several regulations may conflict with each other.

Economic factors also play a significant role, as there exists a complex relationship between economic incentives, censorship behaviour, and network stability within

[125] Christoph Mueller-Bloch and others, 'Understanding Decentralization of Decision-Making Power in Proof-of-Stake Blockchains: An Agent-Based Simulation Approach' (2022) 33 European journal of information systems 267.

Ethereum's consensus mechanism. Several studies suggest that when staking incentives are insufficient, validators may resort to censorship strategies to safeguard their economic interests, while well-structured staking reward mechanisms can strengthen censorship resistance. Relays often prioritise revenue-maximising transactions over those designed to ensure fairness and accessibility, deepening economic censorship in Ethereum's block-building process. Jurisdictional concerns also influence Ethereum's censorship landscape. A significant portion of Ethereum's nodes is located in the United States, which raises the question whether the United States and its regulations may significantly influence the behaviour of consensus layer participants surrounding regulatory compliance. This is further complicated by the difficulty in identifying and tracing actors that allow questionable or illegal transactions in the system, due to the pseudonymous or anonymous nature. This can incentivise certain actors to engage in illicit activities, particularly when there are financial rewards, such as higher transaction fees, to be gained. Reputation may also play a role in the decision-making process of consensus layer participants, as validators may risk reputational damage if a validator engages in self-serving behaviour or obstructs the consensus system.

As to the actual censorship of sanctioned addresses, it was found that all OFAC-sanctioned addresses are significantly less likely to be included in PBS-produced blocks, with a 50 percent lower likelihood compared to non-PBS-produced blocks. Censorship may also manifest as delayed inclusion, occurring when not every builder, proposer, or validator is censoring, making transaction inclusion a matter of time and luck rather than a full ban. Such extended delay increases failure rates and raises the likelihood of censored transactions being dropped entirely.

Ultimately, the effectiveness of sanctions is mostly limited by the network's design, leading to a "waiting game" where blacklisted transactions often find eventual pathways to inclusion. The inclusion is sometimes even largely dependent on a single larger block builder or relay that refuses to exclude a sanctioned transaction. The findings further underscore the challenges of achieving consistent regulatory enforcement in decentralised systems and highlight the need for a coordinated, system-wide approach to ensure effective compliance, while acknowledging the inherent risks to privacy, security, and decentralisation. Therefore, careful consideration of these risks is essential when evaluating the potential for Ethereum to serve as a regulatory enforcement technology within the European regulatory framework.

3.9 Key implications and recommendations

Addressing the challenge of promoting EU-based compliance without compromising Ethereum's core values requires a nuanced and multi-faceted approach. First, it is essential to acknowledge the inherent limitations of consensus layer participants, particularly in terms of their decision-making speed and system design features. The 12-

second time slot limitation is crucial to this consideration, as it creates a reality where decisions are typically executed algorithmically. Such algorithms cannot be overly complicated, as they must be able to reach a decision within 12 seconds. This makes it unrealistic to expect them to interpret or implement complex or ambiguous regulatory requirements in real time. Therefore, it is important that regulatory requirements for consensus layer participants are sufficiently simple to program into an algorithm – or ideally, binary.

To promote compliance with European regulations, which extend beyond their current efforts that are mainly based on the OFAC sanction list, it is essential to cooperate, rather than adopting a merely restrictive approach. Developing a simple overview of requirements from EU-based sanction lists and regulations that are feasible to comply with could encourage them to cooperate. Policymakers could also consider developing such an overview in a machine-readable format, making it easy and feasible for consensus layer participants to implement it in their operational processes.

Another important avenue is incentive alignment. Because consensus layer participants are strongly motivated by economic incentives, it could be a powerful tool for aligning regulatory compliance with these incentives. Developers could explore system-level upgrades to incentivise compliance, such as through renewed reward or penalty structures. Policymakers, on the other hand, could investigate whether a provision of additional rewards for compliance would be feasible or desirable. However, caution should be taken in this approach: overly centralised or unilateral incentive schemes could undermine Ethereum's decentralised nature. Any such optimisation should therefore be carefully evaluated, ideally through technical research and community consultation.

A final recommendation is governance-related. The decentralised nature of Ethereum makes it difficult to adopt a necessary unilateral compliance approach. To tackle this issue, consensus layer participants could experiment more intensively with decentralised governance mechanisms - such as community voting, working groups, and forum discussions - to collectively decide on compliance strategies. These options could enable consensus participants to express their compliance preferences, engage in discussions about trade-offs, and establish new norms or rules that balance regulatory requirements with Ethereum's core values.

4 Conclusions

This paper has navigated the complex terrain of Ethereum's evolving role as a potential regulatory enforcement technology. While the initial promise of a credibly neutral, decentralised system held appeal, the realities of economic incentives, regulatory pressures, and the intricacies of its consensus mechanism reveal a far more nuanced picture. Ethereum's journey toward Proof-of-Stake and the rise of mechanisms like MEV-Boost, intended to optimise network efficiency, but has inadvertently opened the door to

regulatory influence, blurring the lines between a neutral infrastructure and a potential tool for censorship and control.

However, simply classifying this shift as a betrayal of the system's ideals is an oversimplification. The Ethereum community finds itself on a tightrope of decentralisation, where it must balance the demands of regulatory compliance with the imperative to preserve the network's core principles of openness, transparency, and censorship resistance. The willingness of validators to consider OFAC sanctions, for example, highlights a pragmatic approach to ensuring the network's long-term viability in the face of legal and political pressures. This is not necessarily a sign of giving up on the original principles, but potentially a strategic adaptation to a complex and evolving regulatory landscape.

The critical challenge lies in ensuring that any form of regulatory enforcement within Ethereum remains transparent, accountable, and subject to community oversight. The risk is that unchecked regulatory capture, driven by economic incentives or external pressures, could transform Ethereum into a permissioned system in disguise, eroding the very foundations upon which it was built. The ongoing discussions around proposer-builder separation and maximal extractable value (MEV) are crucial in this regard. They represent attempts to mitigate the potential for malicious actors to exploit the network for their gain, but also to address concerns about fairness, censorship, and market manipulation.

Ultimately, the question of whether Ethereum can be effectively leveraged as a regulatory enforcement technology remains open. Its success hinges on the ability of its community to develop and implement governance mechanisms that safeguard its decentralised nature while addressing legitimate regulatory concerns. This requires a commitment to ongoing dialogue, experimentation, and a willingness to adapt to the ever-changing dynamics of the digital landscape. The future of Ethereum, and perhaps the broader blockchain ecosystem, may depend on it.

The transparent nature of blockchain technology could also offer regulators a unique tool to monitor and enforce compliance without undermining the decentralised ethos of these systems. Though, regulators that consider the Ethereum consensus mechanism as a gateway to the enforcement of their regulations must think of a few things first. If they consider adopting this strategy, they must emphasise the clarity and simplicity of the rules. We see that while Ethereum may not be suitable for enforcing complex or nuanced regulations that require human interpretation, it could potentially be used for enforcing straightforward, algorithmically programmable rules, such as the enforcement of sanctions lists. However, regulators must be aware of and deal carefully with the potential for unintended consequences, such as the chilling effect on legitimate transactions, privacy violations stemming from increased surveillance, and the increased vulnerability to targeted attacks if compliance mechanisms create new attack vectors. Another consideration is the proper incentivisation of the actors that operate the consensus mechanism. To incentivise these actors to follow regulatory guidelines, there must be

incentives that align with their usual approach, such as economic incentives or rewards for adherence. This could enhance the effectiveness of sanctions and other regulatory measures while maintaining the competitive dynamics that drive innovation within the Ethereum ecosystem. By leveraging mechanisms like MEV strategically, regulators could encourage compliant behaviour. This dual focus on compliance incentives and decentralised innovation could help bridge the gap between blockchain governance and the EU's regulatory objectives.

Future research should focus on exploring innovative approaches to decentralised compliance that address existing challenges and leverage the unique capabilities of blockchain technology. This includes exploring the development of more sophisticated incentive mechanisms that align the interests of validators with regulatory objectives, the implementation of privacy-preserving technologies that protect user autonomy, and the establishment of clear legal and ethical frameworks for the use of blockchain technology in regulatory enforcement.

The consensus layer, a ‘fractured gatekeeper’ with fractured incentives across its participants, presents both a risk and an opportunity: a risk of overreach and a loss of core principles, but also an opportunity to create a more accountable and transparent digital world. Ultimately, navigating this fractured landscape demands a commitment to preserving decentralisation while pragmatically addressing legitimate regulatory concerns. The key lies in finding this equilibrium.