8/8/2022

Mr. Daniel J. Harty
Director, Office of Capital Markets
Department of the Treasury
1500 Pennsylvania Avenue NW Washington, DC 20220
Re: Responsible Development of Digital Assets, Request for Comment 87 FR 40881

Dear Mr. Harty:

We welcome the opportunity to provide the U.S. Department of the Treasury with our feedback to the Request for Comment titled Responsible Development of Digital Assets in line with Executive Order 14067 of March 9, 2022[1]. We want to express our appreciation for your efforts in seeking to better understand the impact of digital assets on the U.S. economy, and we appreciate the Administration's approach to improving the regulation of this emerging industry with a whole-of-government approach that starts with collecting relevant details, often from industry participants such as ourselves, which we are more than happy to provide.

The Hedera Council ("Council")[2] is a coalition of twenty-six (26) independent and unaffiliated organizations who collectively operate and govern a distributed public ledger (the "Hedera Network"[3] which is an example of Distributed Ledger Technology ("DLT") based on the hashgraph consensus algorithm). As with other distributed public ledgers, the Hedera network provides a network-native digital asset for application developers and users to utilize when making the micropayments required whenever they consume a Hedera Network service, i.e. whenever their application makes an API call. In the case of the Hedera Network, that digital asset is the HBAR. This is a fundamental requirement of any public implementation of digital asset technology because anyone can use these APIs to build Web3 applications with high throughput, fair ordering, and low-latency consensus finality in seconds without relying on centralized infrastructure, but only if there is a cryptographically secure method of fairly

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

[2] https://hedera.com/council

[3] https://hedera.com

compensating all of the decentralized infrastructure providers responsible for making these services available to the public. In the case of the Hedera Network, our coalition of independent network node operators provides these services in an environmentally and financially sustainable manner, as documented in a recent study from University College London[4]. This is partially due to the fact that the Hedera Network uses a proof-of-stake security model, which is an increasingly popular and environmentally sustainable method of securing a distributed public ledger.

While we commend the comprehensive nature of the Request for Comment, we have chosen to focus our response on questions where we could provide details on competitive aspects of a distributed ledger technology that we are especially familiar with, such as fair timestamping, fair ordering, and settlement finality. We believe these details are critical in recognizing both how this new technology could underpin our financial markets in a competitive and fair, equitable manner. Thank you for your consideration and please reach out to us with any questions.

Sincerely,

Brett McDowell, Chair
Hedera Hashgraph LLC

[4] http://blockchain.cs.ucl.ac.uk/blockchain-energy-consumption/

Question (4): Risks and Mitigating Factors

Question four of the Request for Comment on Ensuring Responsible Development of Digital Assets asks respondents to "identify and describe any risks arising from current market conditions in digital assets and any potential mitigating factors" that directly relate to market transparency, accuracy and reliability of market data, technological risks, including attacks, bugs, and network congestion, smart contract design and security, settlement and custody, and jurisdictional and legal conditions.

While the consensus protocols of many distributed ledger technologies offer significant improvements over traditional settlement methods and processes, such as reducing (a) settlement risk through disintermediation, (b) settlement time from days to minutes or seconds, and (c) settlement cost to fractions of a percent of the notional value of the transaction, the protocols may also present challenges with respect to (i) fair timestamping of transactions, (ii) fair ordering of transactions, and (iii) clear technological and legal definitions of settlement finality. Each of these issues may bring a set of risks to market participants and have varying levels of severity of potential for mitigation.

Before elaborating on these issues, it is important to note that these challenges are not unique to distributed ledger technology and are present to certain degrees within traditional and intermediated settlement systems, which is outside the scope of this comment. The existence of risks within a distributed ledger network should not be assumed to disqualify the technology or to be worse than other settlement networks without careful comparison and consideration.

Fair Timestamping and Fair Ordering[5]

Timestamping is the process of establishing a consensus date and time a transaction is received by a network. Ordering is the process of placing transactions received by a network into a sequence. Many applications require knowing either the time at which a transaction happened (e.g., submitting federal taxes before the deadline) and/or its order relative to other transactions (e.g., competing bids in markets or auctions). A fair transaction time and order is essential for users of any finance application and exchange, as variations or manipulations can affect the profitability of a transaction or render it invalid, but achieving fair transaction time and order is a non-trivial computer science challenge for many distributed ledger technologies. In many scenarios, *when* a transaction is executed is far more important than whether it was executed at all.

Self-interested or malicious actors may be able to manipulate or influence the timestamp of a transaction, or the order of a series of transactions, on a given network – specifically, from the time the network first receives transaction instructions to the time the transaction is validated by the network, it may be possible to delay validation or reorder transactions. If present, this capability could allow for frontrunning on the knowledge of pending transactions by introducing

[5] https://hedera.com/blog/fair-timestamping-and-fair-ordering-of-transactions

new transactions to the network that are validated more quickly. Additional information, discussion, and examples of frontrunning on distributed ledger networks is available in academic papers here[6] and here[7]. In addition, new types of order manipulation such as backrunning[8], where a transaction sender wishes to have their transaction ordered immediately after some unconfirmed target transaction, should be considered.

Different consensus protocols utilized by different networks will have varied levels of vulnerability to such order-manipulation attacks. For example, the consensus protocol underlying the Hedera network, a directed acyclic graph called "hashgraph[9]," is computationally "fair" because there is no leader node or miner given special permissions for determining the consensus timestamp assigned to a transaction (a technique commonly used by other DLT networks who must make this compromise in order to deliver speed and scale to their users). Instead, the consensus timestamps for transactions on the Hedera Network are calculated via an automated voting process in the algorithm through which all of the nodes collectively and democratically establish the consensus of all transactions submitted to the network, each node "voting" with the level of influence (aka "weight") they have, which is derived from how many HBAR network participants have chosen to stake to any given node). Fairness is a complex topic in a public distributed ledger context. We can distinguish between three aspects of fairness.

First, fairness on a network requires fair access. Hashgraph is fundamentally fair because no individual node can stop a transaction from entering the system, or even delay it by a material amount of time. If one or a few malicious nodes attempt to prevent a given transaction from being delivered to the rest of the network and so be added into consensus, the random nature of the hashgraph gossip protocol through which nodes communicate messages to each other will ensure that the transaction flows around that blockage.

Second, fairness on a network requires fair timestamping. Hashgraph gives each transaction a consensus timestamp that is based on when the majority of the network nodes received that transaction. This consensus timestamp is fair, because it is not possible for a malicious node to corrupt it and make it differ by a material amount from the original time. Every transaction is assigned a consensus time, which is the median of the times at which each node says it first 'received' it. Received here refers to the time that a given node was first passed the transaction from another node through gossip. This is part of the consensus, and so has all the guarantees of being Byzantine[10]. If more than two thirds of participating nodes are honest and have reliable

[6] https://arxiv.org/abs/1902.05164

[7] https://ieeexplore.ieee.org/document/9152675

[8] https://github.com/ethereum/go-ethereum/issues/21350

[9] https://hedera.com/learning/hedera-hashgraph/what-is-gossip-about-gossip

[10] https://hedera.com/learning/hedera-hashgraph/what-is-asynchronous-byzantine-fault-tolerance-abft

clocks on their computer, then the timestamp itself will be honest and reliable, because it is generated by an honest and reliable node or falls between two times that were generated by honest and reliable nodes. Because hashgraph takes the median of all these times, the consensus timestamp is robust. Even if a few of the clocks are a bit off, or even if a few of the nodes maliciously give times that are far off, the consensus timestamp is not significantly impacted, if at all. This consensus timestamping is useful for things such as a legal obligation to perform some action by a particular time. There will be a consensus on whether an event happened by a deadline, and the timestamp is resistant to manipulation by an attacker. In earlier generations of blockchain technology, each block contains a timestamp, but it reflects only a single clock: the one on the computer of the miner who mined that block.

Third, fair order on a network requires fair timestamping. On hashgraph, transactions are put into order according to their timestamps. Because the timestamps assigned to individual transactions are fair, so is the resulting order. This is critically important for some use cases. For example, imagine a stock market, where Alice and Bob both try to buy the last available share of a stock at the same moment for the same price. In earlier generations of blockchain technology, a miner might put both of those transactions in a single block and have complete freedom to choose in what order they occur. Or the miner might choose to only include Alice's transaction, and delay Bob's to a future block. In hashgraph, there is no way for an individual node to unduly affect the consensus order of those transactions.

Settlement Finality[11]

Settlement finality is the moment in time when the property involved in a transaction becomes irrevocably and unconditionally the legal possession of the receiving party. Settlement finality can be further broken down into operational finality and legal finality, defined below. Finality is critical in all financial applications, as without definitive finality, one participant's insolvency could undermine transactions considered settled and unleash a host of liquidity and credit problems for other participants in the payment system.

Operational finality is the process by which a transaction is physically settled. Distributed ledger networks, depending on their consensus mechanisms, generally have either probabilistic or deterministic operational finality. Probabilistic operational finality means true finality may never be reached, but the participants can become increasingly (or decreasingly) confident the transaction cannot be revoked after certain events occur. For example, in the context of "Proof-of-Work" (PoW) consensus mechanisms like Bitcoin, the longest confirmed chain of transactions is considered to be the valid log. There is always a finite possibility that a longer chain will be revealed, and that counterparties who had believed their transaction to be confirmed by the network, will see their transactions discarded and their settlement revoked. In fact, it is expected behavior as each PoW node races to confirm transactions and grow the chain – inevitably, multiple nodes will confirm transactions at approximately the same time and create disagreements that are eventually resolved with the losers (and their transactions) discarded.

[11] https://hedera.com/blog/finality-of-consensus-you-can-take-it-to-the-bank-or-maybe-you-are-the-bank

Consequently, users of PoW chains are typically recommended to wait for some number of block confirmations before believing the transaction is fully confirmed.

Deterministic operational finality means a transaction has not operationally settled until it is operationally irrevocable. As explained below in an excerpt from a Hedera blog post, deterministic operational finality, such as that found in hashgraph, reduces or eliminates such settlement risk:

> “In the hashgraph algorithm, the proposition under question that nodes must collectively establish agreement on is "is this particular witness famous?" The hashgraph data structure connects together groupings of transactions called "events". Certain events have a special place in that structure and are called "witnesses". Some witnesses are even more special – they are deemed "famous". You can think of famous witnesses as those that are deeply woven into the hashgraph – like human celebrities, everybody "knows" them. All nodes look at the same hashgraph, identify the same set of witnesses for a certain portion of the hashgraph, and use the same algorithm to determine the famous witnesses within that set. Once the famous witnesses are determined, then it’s a straightforward process to calculate timestamps for earlier events within the hashgraph. All nodes identify the famous witnesses and perform the timestamp calculation separately, without any additional confirmations or receipts beyond the gossiped events themselves – but nevertheless come to the same conclusion.
>
> “And critically, once a node determines which witnesses are famous in a given section of the hashgraph, they won’t change their mind. If a node determines that a particular witness is not famous, then there is no possibility that it will receive additional information that will cause the node to reevaluate and instead determine that the same witness is famous. Nodes make a choice, and then stick with it. Of course, nodes don’t decide lightly, a node won’t decide on the fame of a witness until it receives sufficient evidence to support the choice - famous or not. The algorithm requires that nodes see agreement from more than 2/3 of the network before making the decision. With such a hard threshold, once a node is able to count enough votes and decide on fame of a particular witness, then hearing from any more of the network, whether that additional information affirms the choice or otherwise, is pointless. In fact it’s more than pointless, it’s wasteful and inefficient. Once nodes reach the threshold, they move on to the next decision - determining the fame of more recent witnesses. Another voting system that has a similar threshold and so similar finality is the US electoral college - once a presidential candidate receives 270 electoral votes, they are the winner. The states keep counting beyond that, but technically they don’t need to.
>
> “The above stubborn certainty for hashgraph nodes on the fame of witnesses is called "finality" of consensus. And finality in determination of the fame of witnesses translates into finality of the consensus timestamps and order of all events within the hashgraph (not just witnesses or famous witnesses). Once an event is assigned a timestamp and place in the full order, it won’t change. It can’t change; that would require that a set of

famous witnesses changed and, as we saw above, nodes will not entertain that possibility."

Legal finality is the process by which a transaction reaches settlement as a matter of law. The moment of finality applied to any given transaction usually depends on the type of contract, the type of asset, and other factors such as the terms embedded in the contract. Critically, in the context of digital assets and distributed ledger networks, the application of existing legal finality structures is underdeveloped.

For example, the American Law Institute and the Uniform Law Commission recently approved amendments to the Uniform Commercial Code which included a new Article 12 to provide rules governing various commercial transactions in digital assets. Article 12 "governs transactions involving new types of digital assets (such as virtual currencies, electronic money, and non-fungible tokens), and corresponding changes to UCC Article 9 address security interests in digital assets. The 2022 amendments also update terminology to account for digital records, electronic signatures, and distributed ledger technology, provide rules for electronic negotiable instruments, and clarify the rules for UCC applicability to hybrid transactions involving both goods and services."[12] State legislatures have yet to adopt and provide effective dates for Article 12. Similar efforts may be required by commodities and securities regulators to account for the unique characteristics of, and risks presented by, digital assets and their underlying distributed ledger technologies.

Conclusion

We support the U.S. administration in their efforts to evaluate the benefits and risks of digital assets and DLT systems should there be the potential for 'mass adoption' of this new technology. Our observations regarding the distinctions between the original blockchain systems that rely on proof-of-work versus some of the newer conceptions such as Hedera are presented for the U.S. Department of the Treasury to understand implications particularly if stablecoins or central bank digital currencies are adopted so as to recognize where fairness fails and succeeds within DLT technology.

In this response, we shared with you our beliefs of how a public distributed ledger built on the open source hashgraph technology solves the issues of fairness of timestamping, fairness of ordering, and settlement finality. There may be other methods used by other DLT networks that also adequately address these risks, but what is important is that these be identified as risks and the protections each technology claims to have are analyzed and understood by those responsible for regulating the systemic risk of the entire financial system. We look forward to future opportunities to engage with the administration where our experience might be helpful to policymakers navigating the complexities of the impacts these innovations will have on the future state of the U.S. and global financial system.

[12] https://www.uniformlaws.org/discussion/ulc-wraps#bm612b6597-280a-4d9e-aa31-5fbb67f8e5ba