

Finality: Unpacking Blockchain Settlement

Commissioned By





Finality: Unpacking Blockchain Settlement

Commissioned By



Flexa provides merchants and developers with simple integrations for digital currency acceptance that are fast, affordable, and completely fraud-proof. Founded in 2018, Flexa's mission is to make payments more efficient and accessible for people all over the world. More information about Flexa can be found [here](#).

Researched By



The Block is an information services company founded in 2018. Its research arm, The Block Research, produces research content that covers the digital asset, fintech, and financial services industries.

Contact

Email: research@theblockcrypto.com

Twitter: @theblockres

Authors

Carlos Reyes - Research Analyst

Twitter: @Crypt0Carlos

Andrew Cahill - Research Director, Reports

Twitter: @Andrew_Cahill_



Finality: Unpacking Blockchain Settlement

Table of Contents

Introduction	4
Blockchain Basics	4
Block Times and Block Confirmations	4
Proof-of-Work vs. Proof-of-Stake	7
Probabilistic vs Deterministic Finality	7
Evaluating Finality on Layer-1 Networks.....	10
Finality on Proof-of-Work Blockchains	10
Finality on Proof-of-Stake Blockchains	13
Chain Reorganizations	15
Network Performance: Downtime & Congestion	17
Evaluating Finality on Layer-2 Networks.....	18
What are Layer-2 Scaling Solutions?	18
Bitcoin's Payment Channels	18
Ethereum's Rollups	19
Conclusion	21
Disclosures	22



Finality: Unpacking Blockchain Settlement

Introduction

Blockchains are often touted for facilitating near instant transactions on a global basis. Where an international bank transfer may take days or weeks to settle, a blockchain transaction typically takes seconds or minutes. While this is a true benefit of blockchain transactions, there is more to it than meets the eye.

In traditional finance, settlement is understood to be the transfer of a security or cash in order to complete a transaction. In practical terms, it is measured in time to settlement. In other words, how long does it take for a transaction to complete?

When it comes to blockchains, there are additional considerations. In particular, how blockchains reach consensus (i.e, come to agreement) impacts how transactions are finalized or, more precisely, when transactions can be considered irreversible.

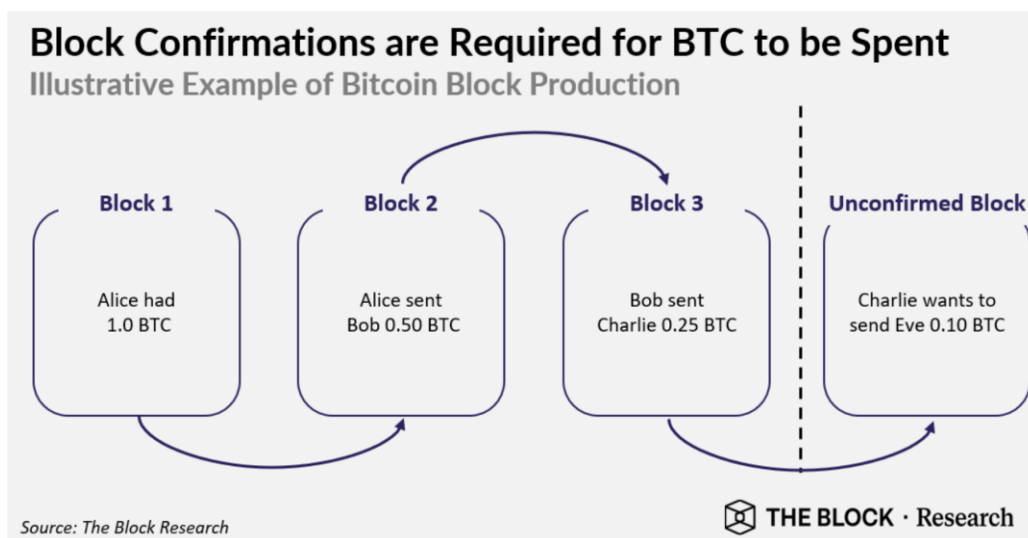
This research report analyzes these different consensus mechanisms, how they impact blockchain settlement, and their related implications for users.

Blockchain Basics

Block Times and Block Confirmations

A blockchain is essentially a public ledger that tracks transactions, balances, and interactions. When a new transaction is broadcast to the blockchain's network, it is revised and, if accepted by the network, included in the next block of transactions to be added to that blockchain's history.

In the figure below, we can see a series of example Bitcoin transactions. Alice already owns 1 bitcoin (BTC) and from that sends 0.50 BTC to Bob who later sends 0.25 BTC to Charlie. We can also see in the figure that there is one unconfirmed block. Once this block is verified, it will be added to the chain (hence blockchain) and its resulting balance (0.10 BTC) can be spent from Eve's wallet in future transactions.





Finality: Unpacking Blockchain Settlement

When it comes to breaking down how transactions are finalized, there are two primary components:

Block time is the average amount of time a blockchain takes to create the next block. Bitcoin's block time is approximately 10 minutes.

Block confirmations represent how many blocks have been mined after a transaction has been added to the chain. For example, Alice's original transfer of 0.50 BTC to Bob has two confirmations - the block which included her 0.50 BTC transfer to Bob (block #2) and the block where Bob made his 0.25 BTC transfer to Charlie (block #3). Once the unconfirmed block is added to the chain, Alice's original 0.50 BTC transfer transaction will have three confirmations.

Block times can be altered depending on the trade-offs that a blockchain wishes to make. For example, Bitcoin's 10-minute average block time was devised to ensure that nodes have ample time to reach agreement on the state of the Bitcoin ledger before the network progresses. Some networks which were forked from the Bitcoin protocol reduce block time as one of their differentiating features. For example, Litecoin's average block time is 2.5 minutes.

Block confirmations are an important measure of settlement assurance. The more confirmations a block has, the further back in the chain it is. The further back in the chain a block is, the lower the probability that any of its contents could ever be altered (when it comes to proof-of-work blockchains). This is due to the fact that in proof-of-work, the longest blockchain is the de-facto chain of record. To change the contents of a block which has been added to the chain would require re-performing all of the computational work which had been expended since this block was originally added to construct a longer chain. Hence, transactions with more confirmations on proof-of-work chains have stronger settlement assurances.

Block confirmations are also an important consideration for businesses that operate in the digital assets industry. While blockchain reorganizations (which result in transaction reversals) are typically thought of in terms of attacks on networks, they can also occur naturally during normal network conditions.

The most common type of these reorganizations are caused by temporary forks in networks. During these forks, competing blocks are added to the chain at the same time causing uncertainty over which chain is the longest and hence which set of transactions will be finalized. As nodes communicate, they eventually converge on the one chain with the most cumulative work performed. Accordingly, only one of the competing blocks is accepted and transactions which were included in the other "dropped block" would be invalidated.

Confirmation requirements serve to mitigate these settlement risks which can be caused by forks.



Finality: Unpacking Blockchain Settlement










How do confirmation requirements impact users?

Individual users and digital asset businesses must find a balance between a desired level of security and practicality when it comes to setting their minimum confirmation requirements.


If a time sensitive business, such as a digital asset exchange, were to optimize for security across all proof-of-work chains (that is, require a large number of confirmations before considering deposits final) customers would likely complain or turn to other exchanges as this could prevent them from trading and being able to withdraw assets on a timely basis.

On the other hand, a less time sensitive business, such as an online retailer, can allow for more confirmations to occur before shipping a product without creating a negative customer experience. Businesses may also find ways of implementing policies that improve customer experience without reducing security. For example, an exchange may allow a customer to trade as soon as the first confirmation is received, but it may disable withdrawals for that asset until a higher confirmation threshold is met.

Deposit time requirements on centralized digital asset exchanges provide concrete examples of controls that businesses employ to mitigate this settlement risk. Based on US-based exchange Kraken's deposit requirements in the chart below, confirmation times range from "near-instant" on certain blockchains to ~1 week on others. For example, a Bitcoin transaction requires ~40 minutes to reach finality and be eligible for withdrawal while an Ethereum transaction requires ~5 minutes based on Kraken's policy.

Kraken's "Rule of Thumb" Deposit Requirements			
Blockchain	Consensus Mechanism	Confirmations required	Estimated Time for Confirmations
 Avalanche	PoS	20	1 Minute
 bitcoin	PoW	4	40 Minutes
 BitcoinCash	PoW	15	2.5 Hours
 CARDANO	PoS	15	10 Minutes
 ethereum	PoW	20	5 Minutes
 ethereum classic	PoW	40,000	6.5 Days
 Polkadot	PoS	25	2 Minutes
 SOLANA	PoS	N/A	Near-instant
 Terra	PoS	N/A	Near-instant

Source: Kraken

 **THE BLOCK** · Research



Finality: Unpacking Blockchain Settlement

Furthermore, these deposit requirements showcase an important distinction across blockchains when it comes to finality - different chains that have the same block time have different confirmation requirements.

For example, Bitcoin and Bitcoin Cash have the same block time (~10 minutes), but Bitcoin Cash deposits require nearly four times as many confirmations as Bitcoin deposits. An even more dramatic divergence can be seen between Ethereum and Ethereum Classic. Both blockchains have the same block time (10 to 15 seconds), but have confirmation requirements that differ by a factor of 2,000. Ethereum transactions only require 20 confirmations while Ethereum Classic transactions require 40,000 confirmations.

Clearly, not all block confirmations are equivalent from a settlement assurances perspective; especially in the case of proof-of-work blockchains. This concept will be explored in depth in the “Evaluating Finality on Layer-1 Networks” section of this report.

Proof-of-Work vs. Proof-of-Stake

Thus far, finality has primarily discussed in the context of proof-of-work blockchains. But layer-1 networks employing an alternative consensus mechanism, proof-of-stake, have gained significant adoption over the past two years.

What is proof-of-stake?

Proof-of-stake blockchains perform similar functions to proof-of-work blockchains. They are publicly available ledgers that track transactions, balances, and interactions. However, while proof-of-work blockchains are extended when a miner successfully completes a proof-of-work hashing algorithm and proposes a new block, proof-of-stake blockchains are extended when the majority of financial stake (i.e., native blockchain tokens being used to secure the network) affirms the validity of blocks. Due to this difference, analyzing the security and by extension the weight and reliability of settlement guarantees, provided by proof-of-work and proof-of-stake blockchains requires different approaches.

Probabilistic vs Deterministic Finality

Proof-of-work blockchains function with probabilistic finality. With each block that is added to a proof-of-work blockchain, the probability of a chain reorganization (i.e., transaction reversal) decreases and approaches but never reaches zero. This is due to the fact that the cost of building a longer competing chain increases with each additional block that is added after the block in question. Eventually, it becomes prohibitively costly (though not theoretically impossible) for one or few entities to try to construct a longer chain containing a different set of transactions.

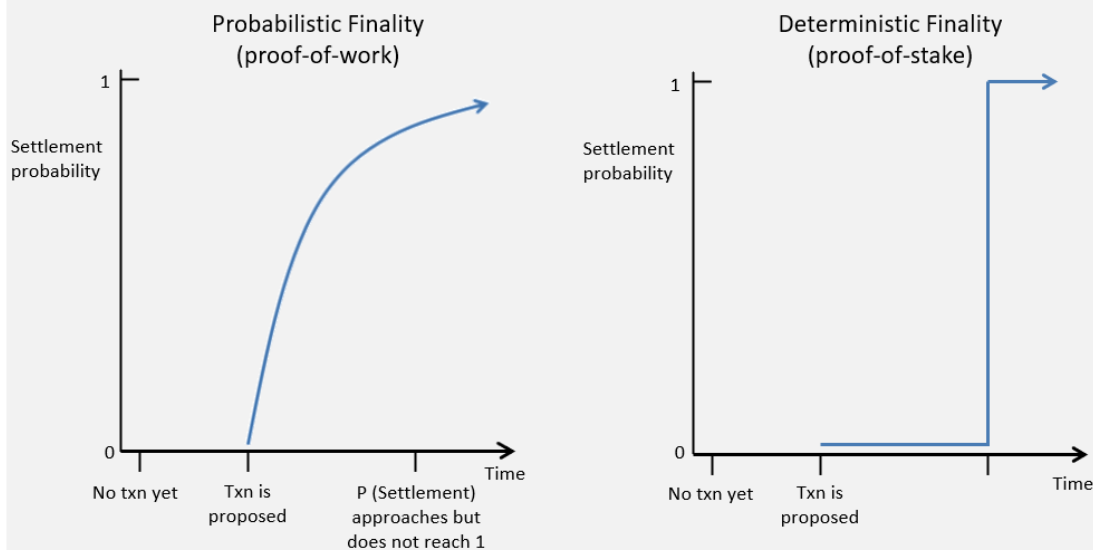


Finality: Unpacking Blockchain Settlement

Proof-of-stake blockchains operate with deterministic finality. As opposed to how proof-of-work blockchains extend as miners solve cryptographic hashing puzzles and add blocks to the blockchain, proof-of-stake networks require a set threshold of the financial stake on the network (typically 67%) to agree in order for transactions to be finalized and for their blockchains to progress. Given that the aggregate amount of financial stake securing the network is known in a proof-of-stake framework, there is a definitive point in time at which this 67% threshold is reached. And once this threshold is reached, the new block is added to the chain and all of its contents are deemed final and irreversible; irrespective of the number of confirmations it has.

Finality Comes in Different Flavors

Probabilistic vs Deterministic Finality



Source: "It's the settlement assurances, stupid" by Nic Carter, The Block Research

 THE BLOCK · Research

Are transactions ever fully irreversible?

While many proof-of-stake based networks will often tout having “immediate finality” and “immutable transactions”, reality can be quite different. Even networks which have deterministic finality can tolerate temporary forks and undergo small reorganizations which result in transaction reversals.

Additionally, the state of any blockchain network is ultimately determined by the consensus of the majority of its participants; irrespective of what protocol documentation may state. As illustrated in the upcoming “Evaluating Finality on Layer-1 Networks” section of this report, there have been several instances where previously finalized transactions were reversed when a sufficiently large share of the community decided that reversing them was in its collective best interest.



Finality: Unpacking Blockchain Settlement

The Different Types of Proof-of-Stake Consensus

While Bitcoin (BTC) and Ethereum (ETH) remain the largest digital assets by market cap, several competing blockchains with material levels of adoption have emerged. In the layer-1 blockchain sphere, Solana and Cardano are the top two proof-of-stake blockchains by market cap¹ that provide examples of the nuances associated with deterministic finality.

Solana

Like many proof-of-stake blockchains Solana has its own variation of proof-of-stake consensus. Specifically, Solana uses a technique called proof-of-history to allow for validators to rapidly propagate blocks and then later finalize them with its proof-of-stake consensus algorithm, Tower BFT. By decoupling the execution and finalization of transactions, Solana operates with extremely fast block times that typically range around ~400 milliseconds.

On Solana, once a transaction has received 31 block confirmations (which typically takes ~12 seconds), it is considered final per the protocol defined definition of finality. However, unlike most other blockchains where blocks equal confirmations, a Solana transaction with less than 31 confirmations is still technically considered pending. Accordingly, it is not uncommon for the 31 block confirmations to be treated as a single confirmation, after which the transaction is considered final.

Due to Solana's rapid block propagation mechanism, exchanges like Kraken can decide to credit Solana transactions on a "near instant" basis rather than wait for the protocol-defined 31 confirmations. However, other exchanges like Coinbase do specify a requirement for 31 network transactions to credit a user deposit.

Cardano

Similar to how Solana transactions technically have a window of probabilistic finality, Cardano's proof-of-stake mechanism, Ouroboros, showcases the nuances associated with deterministic finality. In strict terms, transactions reach finality after 129,600 slots² on its current mainnet, or after approximately 36 hours. The official Cardano documentation also [states](#), "[129,600 slots] normally exceed the requirements in most situations, so a more practical approach is to consider the probability for a transaction to become immutable...we consider that a transaction is confirmed if the probability for it to become immutable is *high enough*."

¹ Though BNB Chain's native token (BNB) has a higher market cap than Solana's (SOL) and Cardano's (ADA), its consensus mechanism contains elements of proof-of-stake and proof-of-authority and hence, it is excluded for the sake of simplicity.

²A slot is a one second window in which zero or more block-producing nodes might be nominated to be the slot leader that creates a block within the current slot.



Finality: Unpacking Blockchain Settlement

Hence, even though Ouroboros is a deterministic consensus protocol, Cardano transactions have a window of probabilistic finality in which end users must determine the balance between security and practicality. Kraken's deposit confirmation requirements call for 15 confirmations (~10 minutes) for transactions on Cardano; a massive differential when compared to the ~36 hour time to finality based on strict protocol definitions.

Solana and Cardano are just two examples of proof-of-stake blockchains. Dozens of other layer-1 blockchains with their own variations of proof-of-stake consensus, and by extension distinct finality frameworks, have emerged. And notably, Ethereum is currently undergoing a network overhaul from proof-of-work to proof-of-stake which will impact how its network reaches finality.

Evaluating Finality on Layer-1 Networks

Finality on Proof-of-Work Blockchains

While block confirmations are a starting point for assessing finality, the aggregate computational work required to add blocks to proof-of-work blockchains impacts the settlement assurances that they provide. It is the driving factor behind the differences in confirmation requirements put in place by digital asset exchanges like Kraken amongst blockchains with the same block time. As a reminder, Kraken's deposit requirements call for 4 confirmations for Bitcoin deposits vs. 15 confirmations for Bitcoin Cash deposits and 20 confirmations for Ethereum deposits vs. 40,000 confirmations for Ethereum Classic deposits.

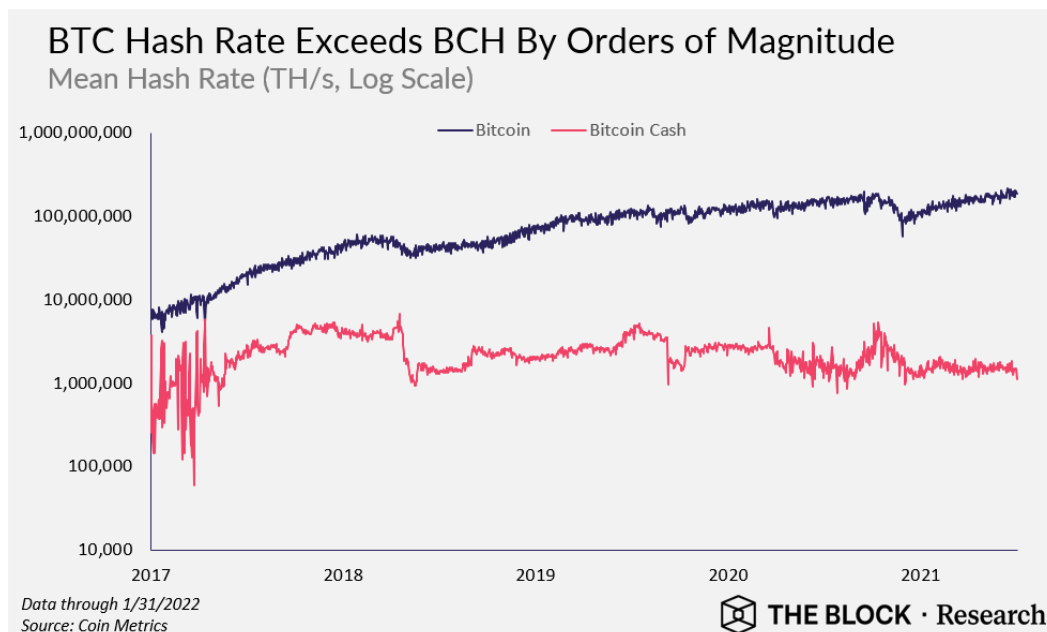
Quantifying computational work

Hash rates, which measure the quantity of calculations performed to mine new blocks on proof-of-work blockchains, approximate the cost of creating new blocks and, by extension, the settlement assurances that each additional confirmation provides.

As displayed in the chart below, Bitcoin's current hash rate stands at ~204.3 million TH/s (terahashes per second) while Bitcoin Cash's stands at ~1.4 million TH/s. In other words, mining one Bitcoin block requires ~150x the amount of computational work that it takes to mine one Bitcoin Cash block. Accordingly, the economic weight and therefore the settlement assurances provided by one Bitcoin confirmation are orders of magnitude higher than those of one Bitcoin Cash confirmation.

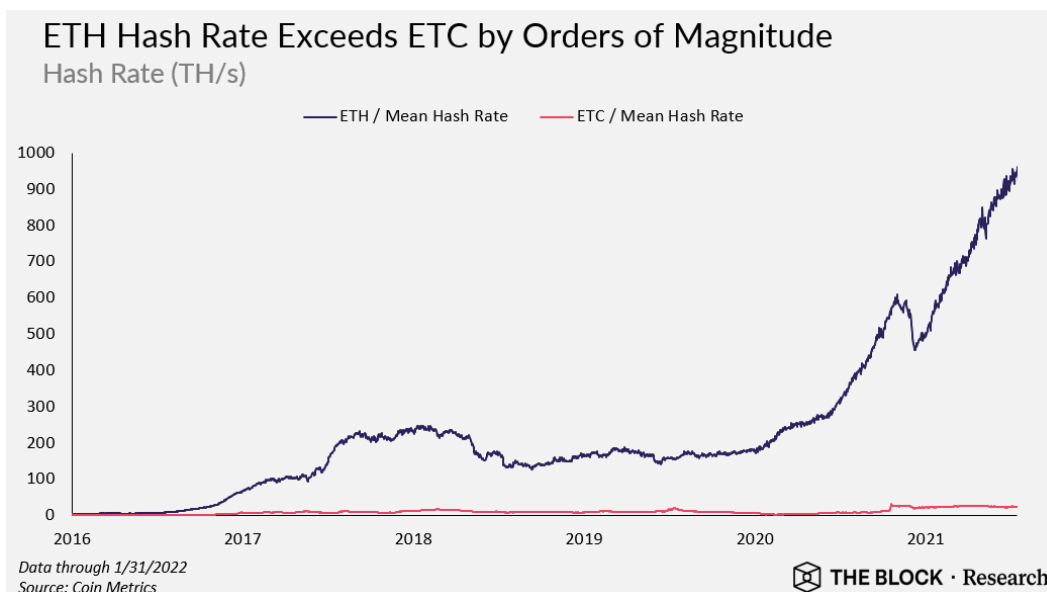


Finality: Unpacking Blockchain Settlement



Additionally, given that Bitcoin and Bitcoin Cash employ the same hashing algorithm (SHA-256), both networks can be mined using the same computer hardware which poses risks for the network with the smaller share of the total hashing power. Should several major entities that mine the Bitcoin network decide to employ their hardware to instead mine Bitcoin Cash, they could easily assume the majority (51%) of Bitcoin Cash hash power and carry out [double spending attacks](#) on the network which would result in transaction reversals.

Likewise, a similar dynamic exists between Ethereum and Ethereum Classic. Ethereum's current hash rate stands at ~940 TH/s while Ethereum Classic's stands at ~24 TH/s. In other words, mining one Ethereum block requires ~40x the amount of computational work that it takes to mine one Ethereum Classic block. Notably, Ethereum and Ethereum Classic use a different hash function (Ethash) than Bitcoin and Bitcoin Cash (SHA-256) and hence Bitcoin's and Ethereum's hash rates are not comparable on a 1:1 basis.





Finality: Unpacking Blockchain Settlement

Ethereum Classic's low hash rate showcases the low quality of settlement assurances that its confirmations provide. Its network hash rate has routinely been monopolized in 51% attacks which have resulted in multiple chain [reorganizations](#) that span thousands of blocks and modify transactions that were executed days prior.

Hence, Kraken's exceptionally high confirmation requirements for Ethereum Classic (40,000 confirmations which take ~6.5 days) are designed to reduce the likelihood that it would be impacted by one of these reorganizations.

While exchange confirmation requirements are examples of the "rule of thumb" number of confirmations that a business deems acceptable, they are ultimately subjective. For example, based on the ~150x hash rate differential between Bitcoin and Bitcoin Cash, Kraken's 15 confirmation requirement for Bitcoin Cash seems relatively low when compared to Bitcoin's 4 confirmation requirement.

More theoretical approaches to assessing settlement assurances, which directly account for the quantity of computational work expended on proof-of-work blockchains have also emerged. According to analysis conducted by blockchain researcher Luke Childs, the confirmation requirements for Bitcoin and Ethereum should in reality be far different from what exchanges such as Kraken typically require. According to his [research](#), which estimates the total electricity costs incurred to mine blocks, it would take ~669 Ethereum confirmations (~2h27m) to equal the computational work (and hence the security) of 6 Bitcoin confirmations (~59m).

Finally, other methods for assessing and mitigating settlement risk suggest different times to finality based on the size of the transactions in question.

Transaction Value and Mining Value Equilibrium

Former University of Sydney Computer Engineering Lecturer Elaine Ou proposed an alternative method for analyzing finality on proof-of-work blockchains. She states that recipients of blockchain transactions should wait until the value of a transaction matches the cost of creating a proof-of-work block which can be approximated by average miner revenues. For example, a \$5 million BTC transaction should wait for 18-19 block confirmations to be considered secure. This is calculated by taking the average daily mining revenue of the past month ~\$39 million, dividing it by 144 (the number of 10-minute periods in 24 hours) resulting in an average block revenue of \$271,872. When the \$5 million BTC transaction is divided by this \$271,872 worth of revenue per block, it yields a suggested ~18 block confirmations wait time for finality.

Why Decentralization Matters

While settlement assurances can be approximated by gross hash rate, the degree of concentration of this hash rate is another important consideration. If hashing power on a blockchain is highly concentrated amongst few entities, then the blockchain can be susceptible to 51% attacks, regardless of raw hash rate levels.



Finality: Unpacking Blockchain Settlement

Accordingly, an in-depth assessment of attack difficulty and, by extension, the quality of settlement assurances provided by proof-of-work blockchains would require pinpointing the distribution of hashing power amongst independent entities.

Finality on Proof-of-Stake Blockchains

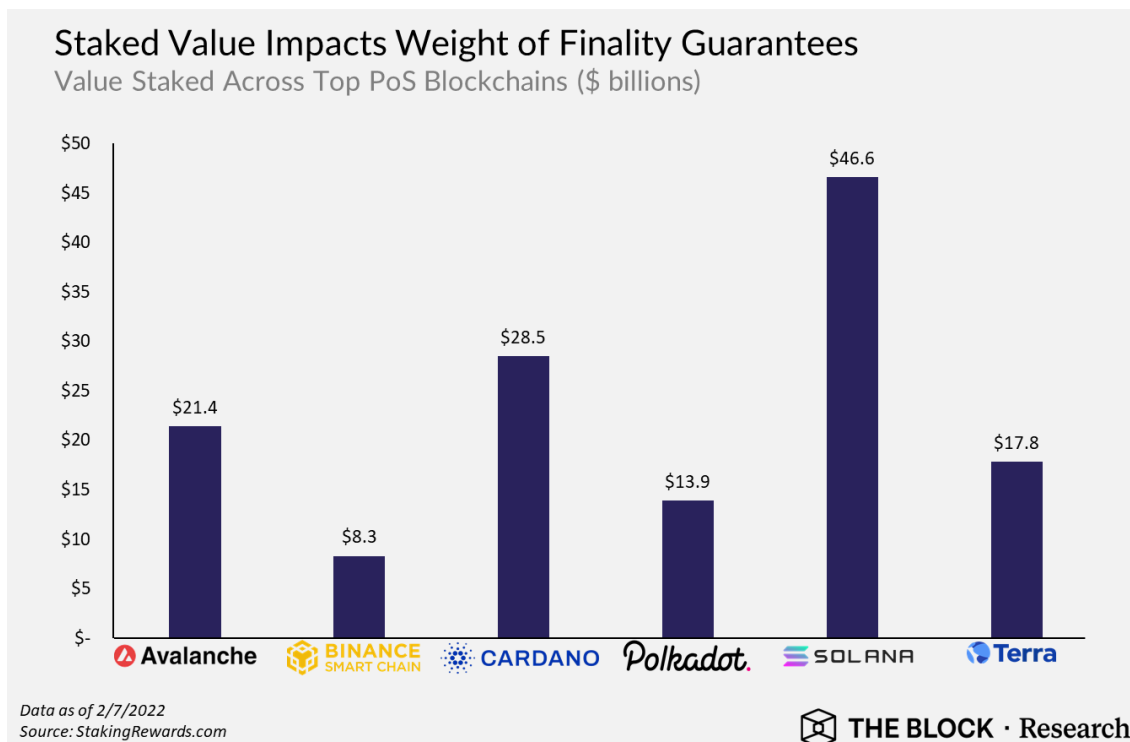
Despite proof-of-stake blockchains operating with deterministic finality, their security and, by extension, the quality of the settlement assurances, can still be analyzed.

Total Value Staked

Similar to how examining gross hash rate provides insight into the economic weight of block confirmations on proof-of-work blockchains, examining the total value staked on proof-of-stake blockchains provides insight into the weight of their settlement assurances.

Abstracting from the actual ownership distribution of the stake being used to secure a proof-of-stake blockchain, the more financial stake that is put at risk (i.e. susceptible to being [slashed](#)) to validate a proof-of-stake blockchain, the more costly it would be for a malicious actor to procure the requisite amount of financial stake (34%) to temporarily halt the network and prevent it from finalizing transactions.

As displayed in the chart below, the aggregate value staked, and by extension, the estimated cost of accumulating 34% of this financial stake differ substantially across top proof-of-stake networks. For example, on the Solana network as much as ~\$16 billion worth of SOL tokens would be required to account for 34% of its ~\$47 billion worth of total voting power. In contrast, on the BNB Chain network only ~\$2.8 billion would be required to account for 34% of its ~\$8.3 billion of total voting power.





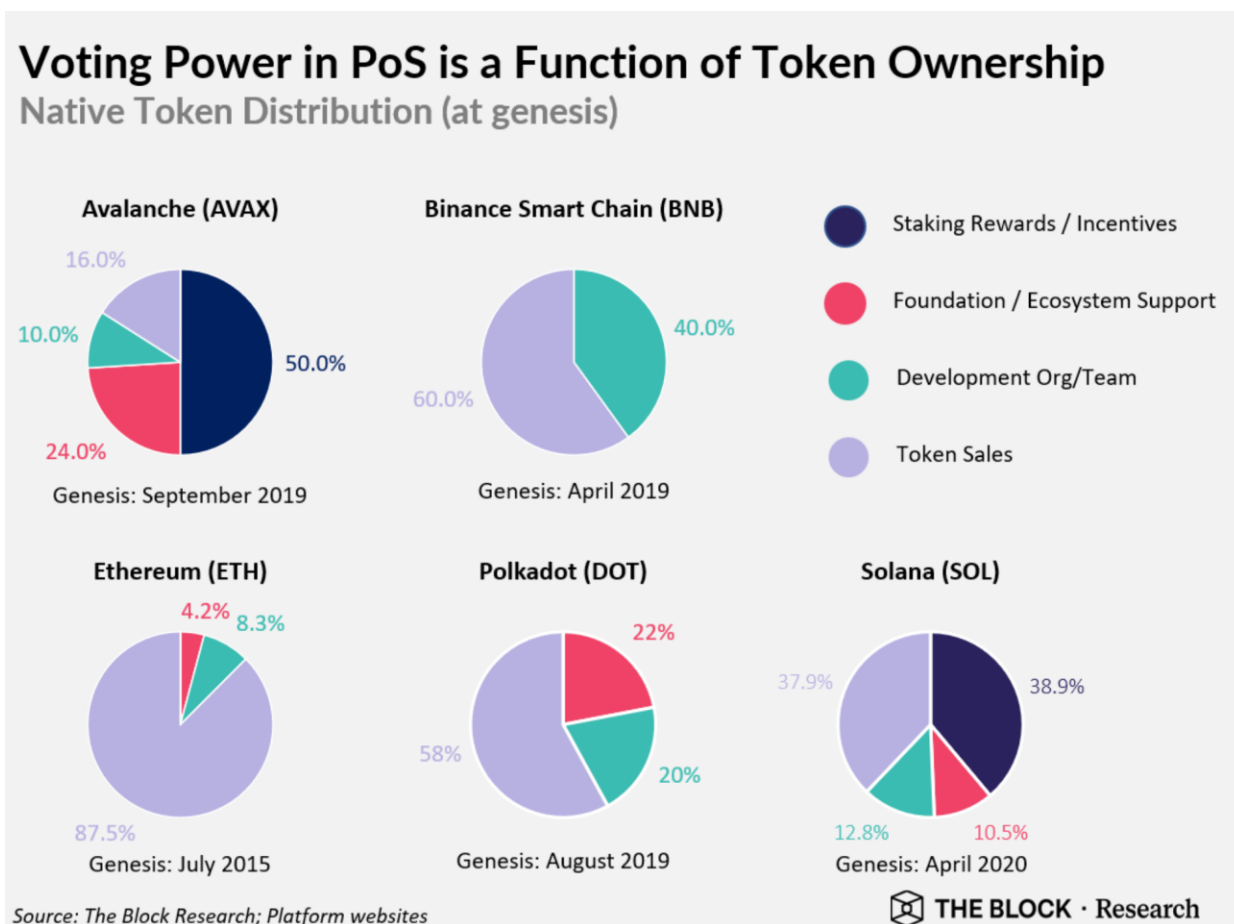
Finality: Unpacking Blockchain Settlement

However, there are several nuances as it relates to this high-level analysis. Firstly, attempting to acquire such a high share of coins would likely result in a high degree of slippage and further increase the cost of acquisition. Secondly, procuring the requisite computer hardware to run validators that stake these 34% of tokens is an additional financial consideration which would significantly increase the all-in cost of attacking one of these networks.

Native Token Distribution

Taking this analysis one step further, the actual distribution of token ownership within these respective networks provides insight into the reliability of their finality guarantees. Ultimately, an attacker would need to find a way to source this 34% of active stake from current token holders. And all else equal, the more distributed the ownership of the stake is, the harder it would be in theory for one entity to amass 34% of the financial stake.

While pinpointing ownership of native tokens is more of an art than a science, the chart below, which shows token distribution at the genesis of several proof-of-stake blockchains, provides a useful starting point for assessing who holds how many tokens.





Finality: Unpacking Blockchain Settlement

As can be seen in the chart above, layer-1 development teams and/or foundations typically retain a considerable share of token distributions - in many cases 34% or more. This means that, if they wished to, these entities could censor their networks and prevent users from being able to finalize transactions.

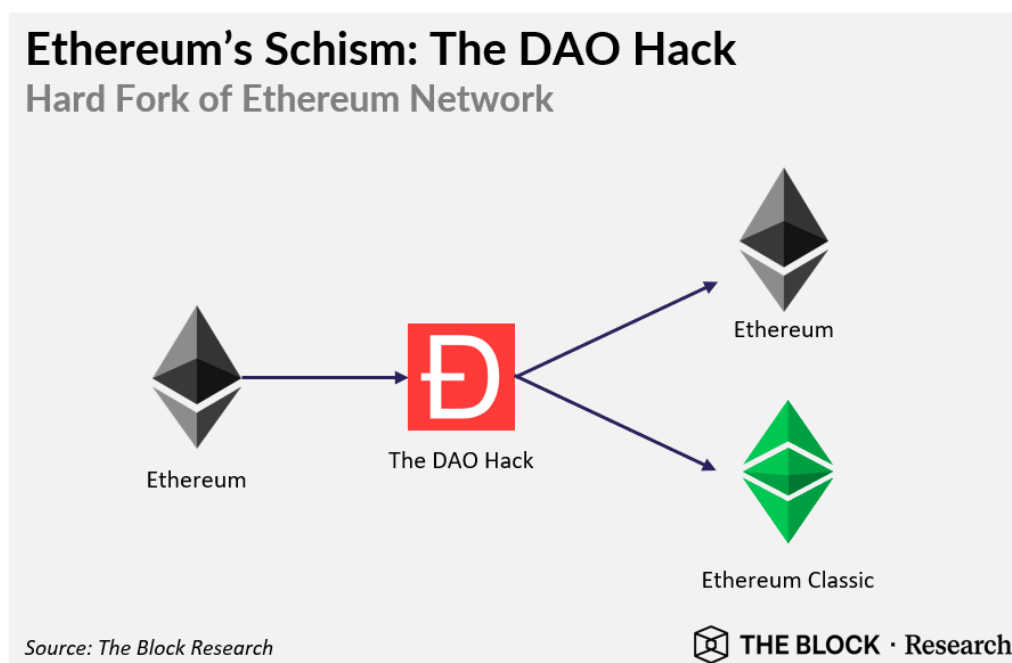
In summary, the quality of settlement assurances provided by both proof-of-work and proof-of-stake blockchains can be quantitatively analyzed. While these theoretical approaches provide valuable insights, complications can and do happen in live production environments which impact settlement. Two such types of complications are chain reorganizations and degraded network performance and/or downtime.

Chain Reorganizations

Ethereum's Schism: The DAO Hack

One of the most noteworthy chain reorganizations to have taken place is related to The DAO hack. Created in 2016, The DAO was among the earliest examples of a Decentralized Autonomous Organization (DAO). It was meant to serve as a participant-led venture capital firm and raised over \$150 million (approximately 14% of all ETH in circulation at the time) from ~11,000 investors. However, vulnerabilities in The DAO's smart contract code were exploited by attackers who were able to siphon upwards of \$50 million worth of ETH (as valued at the time of the attack) from The DAO.

After much debate on potential solutions to this misappropriation of funds, the Ethereum blockchain was eventually hard forked to modify transactions related to The DAO hack to return the funds to investors. While the modification to the blockchain was proposed by the Ethereum developers, for it to succeed, miners, node operators, and exchanges all had to update their software. Hence, there was broad community support for this action beyond just the DAO investors and Ethereum developers.





Finality: Unpacking Blockchain Settlement

However, some in the community believed that the decision to modify these transactions represented a breach in the ethos and functionality of the network since blockchains are meant to be immutable and all of their transactions irreversible. Those who were opposed to the modification instead supported the un-modified version of the chain which is now referred to as Ethereum Classic (ETC).

Though quite an exceptional example, The DAO hack illustrates how previously finalized transactions have been modified in extreme circumstances. In this case, the hack occurred on June 17th, 2016, and the hard fork occurred on July 20th, 2016. Hence, The DAO hack related transactions were undone approximately month after they would have typically been considered irreversible.

EOS Core Arbitration Forum Orders a Reversal

Like The DAO hack, other blockchains have undergone transactions reversals. The EOS blockchain operates on what is known as a delegated proof-of-stake consensus model, meaning that EOS token holders vote for nodes to be selected as block producers with only 21 block producer positions available. According to EOS developer documentation, an [irreversible block](#) is a block confirmed by 2/3 + 1 of the current block producers.

The EOS Core Arbitration Forum (ECAF), a now discontinued dispute resolution body, had historically directed chain modifications on behalf of its community, even for transactions that were previously confirmed by 2/3+1 of block producers. ECAF rulings in 2018 included an order for block producers to [return ownership](#) of stolen funds to a claimant that was the victim of a phishing attack. EOS block producers approved the ECAF's request and the transaction reversals were effected on [November 11th, 2018](#).

Polygon PoS Chain Reorganizations

Similar to how a proof-of-work chain can organically produce a temporary fork, some proof-of-stake protocols can experience reorganizations during normal operations.

One such protocol is Polygon's PoS chain, which operates as a proof-of-stake Ethereum sidechain. The Polygon sidechain experiences non-adversarial reorganizations on a normal basis. These reorganizations can occur for multiple reasons, with communication issues between validator nodes and backup nodes being identified as a leading cause.

Polygon's block explorer even features a [page](#) that tracks when reorganizations have happened and how deep they are. While these reorganizations typically range from single blocks to low double digits, they routinely reach 100+ blocks.



Finality: Unpacking Blockchain Settlement

Network Performance: Downtime & Congestion

In addition to these instances of transaction reversals, whether a blockchain is live and actually capable of finalizing transactions is an important settlement consideration.

Both [Bitcoin](#) and [Ethereum](#) experienced spam attacks early in their history in which a large series of transactions attempted to disrupt the network by either making transactions more expensive or slowing down transaction processing. Development communities of both networks have taken specific actions taken to address spam attacks such as implementing targeted [fees](#) or [penalties](#). Along with these improvements, Bitcoin and Ethereum's price appreciation have increased the cost of carrying out a spam attack on their networks. Spam attacks are now more commonly seen in proof-of-stake blockchains as they typically have much lower transaction costs.

Solana has experienced [degraded performance](#) in the face of high network usage which has led to large numbers of failed transactions. The most significant of these incidents occurred in September 2021 when the network experienced approximately [17 hours of downtime](#). Accordingly, for transactions that were submitted during this period, time to finality spiked as high as 17 hours; a far cry from the "near instant" finality that its transactions typically have.

Likewise, Cardano experienced network congestion in conjunction with the launch of its network's first decentralized exchange, SundaeSwap. Leading up to SundaeSwap's mainnet release, its development team [warned](#) users that because of high levels of demand and congestion, swaps "may take days to process". And unsurprisingly, users experienced failed transactions and were unable to submit orders for ~4 hours on SundaeSwap once it launched on the Cardano mainnet.

As was the case with Bitcoin and Ethereum, development teams of these layer-1 proof-of-stake networks are actively refining their network technology to minimize these disruptions. For example, Solana developers identified duplicate transactions as the source of heightened network load (similar to previously mentioned spam attacks), and later released a new version of its mainnet, Solana v1.8.14, to mitigate their effects. Likewise, on Cardano, several improvement proposals have been proposed to address the congestion issues that occurred during the SundaeSwap launch.



Finality: Unpacking Blockchain Settlement

Evaluating Finality on Layer-2 Networks

Thus far, this report has discussed finality in the context of layer-1 networks. But pinpointing one definitive time to finality is slated to become even more challenging with the increased usage of layer-2 scaling solutions.

What are Layer-2 Scaling Solutions?

Layer-2 scaling solutions refer to a variety of complementary protocols aimed at enhancing the capacity of layer 1 networks to increase transaction throughput and drive down transaction fees.

Layer-2 networks achieve these scalability gains by offloading the actual execution of transactions from layer-1 networks to their own respective blockchains. However, they still rely on layer-1 networks as a settlement layer to finalize transactions. Accordingly, how transactions are finalized on layer-2 networks is a function of how they operationalize settlement on their respective layer-1 platforms.

Layer-2s Decouple Transaction Execution & Settlement Layer-1 Networks and Layer-2 Scaling Solutions



Source: The Block Research

THE BLOCK · Research

Scaling solutions come in different shapes and sizes and can ultimately be used in conjunction with a number of layer-1 platforms. This report focuses on the most popular scaling solutions employed on Bitcoin (payment channels) and Ethereum (rollups).

Bitcoin's Payment Channels

Bitcoin's main layer 2 technology, the Lightning Network, is based on the concept of payment channels. With payment channels, two or more parties that often transact with each other create a multisignature (multisig) wallet and deposit an agreed amount of BTC into the wallet. The Lightning Network then facilitates value transfers between these parties by recording transfers of ownership of the pooled deposited funds rather than transferring the BTC itself.



Finality: Unpacking Blockchain Settlement

Accordingly, transactions conducted on the Lightning Network are not subject to Bitcoin's block time and can be confirmed much faster and at a lower cost. The state of a payment channel can be updated as quickly as parties are able to create, sign, and transmit transactions. Each new transaction in a payment channel encodes the new balance of the channel and invalidates the previous transaction's encoded balance. This ensures no participant can return to a state before the most recent transaction.

A properly created payment channel allows for participants to independently close the channel at any time and have their balances settled by submitting the latest state to the Bitcoin blockchain. Once a closing transaction is processed by the Bitcoin blockchain, users will receive their share of BTC from the multisig wallet based on the state of the latest transaction. Accordingly, pinpointing one single time to finality for transactions executed on payment channels is challenging. While users can transact within these channels on a frequent basis, their transactions only receive the full settlement assurances of Bitcoin once funds are withdrawn from multisig wallets.

Ethereum's Rollups

On Ethereum, multiple layer-2 protocols have gained adoption due to the sustained high transaction fees seen on its network throughout 2020 and 2021. While these layer-2 technologies could eventually leverage any layer-1 platform for settlement, they are currently settling transactions on Ethereum.

Layer-2 rollups work by executing transactions on their own respective blockchains (as opposed to layer-1 networks), aggregating the data from these transactions, and posting a summarized version of this transaction data on their respective layer-1. They rely on a series of layer-1 smart contracts which process deposits and withdrawals of assets on and off layer-2 networks and, importantly, verify the validity of the transactions that occurred on the layer-2 blockchains.

Rollups come in two main forms: optimistic rollups which employ fraud proofs to finalize transactions and ZK-Rollups which employ validity proofs to finalize transactions.

Optimistic Rollups

After transactions are executed on optimistic rollups, batches of their compressed transaction data are posted to a layer-1 platform. These rollups are "optimistic" in the sense that when transaction data is posted, it is assumed to be valid. But ultimately any participant in the network can challenge the validity of these transactions by submitting what is called a fraud proof.

In order to determine whether a fraud proof is correct, transaction data posted to the Ethereum blockchain can be used to replay the history of transactions and determine if transactions were indeed fraudulently executed. To allow participants sufficient time to monitor transactions and submit fraud proofs, optimistic rollup solutions have protocol defined dispute periods (which typically last 7 days). Hence, while transaction data batches are periodically posted to the layer-1 network every couple of minutes or hours, transactions do not achieve finality on layer-1 platforms until the expiration of this



Finality: Unpacking Blockchain Settlement

dispute period (at which point users can withdraw assets from the layer-2 network).

Like payment channels, when users transact within a particular layer-2 network, they do not need to wait for the expiration of the 7-day dispute period in order for their transactions to be considered final within their respective layer-2 networks. Notably, several liquidity bridging protocols have emerged that give layer-2 users the ability to withdraw assets prior to the expiration of the 7-day dispute period in exchange for a fee. Thus, time to finality on layer-1 can also be drastically reduced by employing these bridges.

ZK-Rollups

After transactions are executed on a ZK-Rollup, the batches of transactions data as well as cryptographic [validity proofs](#) are posted to the layer-1 blockchain. In contrast to how optimistic rollups rely on fraud proofs, ZK rollups rely on these validity proofs to mathematically verify that the layer-2 transactions were indeed executed correctly.

Accordingly, finality on layer-1 can occur as soon as transaction batches are posted to the layer-1 (typically once every several hours) and the validity proofs are verified.



Finality: Unpacking Blockchain Settlement

Conclusion

While finality is rarely mentioned in the mainstream discourse of blockchain and digital asset development, it is clearly a crucial consideration for blockchain users.

From a straightforward measurement of block confirmations to examining network hash rates to analyzing the distribution of stake in proof-of-stake networks, there are several ways to evaluate the security profiles of blockchains, and by extension the quality of settlement assurances that they provide.

Nonetheless, assessing blockchain settlement requires an adaptive approach. Layer-1 development teams are continually fine tuning their existing protocol technology and consensus algorithms which impacts their finality. Ethereum is fully transitioning from proof-of-work to proof-of-stake which will fundamentally alter how it settles transactions. Layer-2 scaling solutions are decoupling transaction execution from settlement and introducing new complexities when it comes to understanding finality. Finally, new blockchains with novel different consensus models will continue to emerge and require new models for assessing finality altogether.



Finality: Unpacking Blockchain Settlement

Disclosures

This report is commissioned by Flexa Network Inc. The content of this report contains views and opinions expressed by The Block's analysts which are solely their own opinions, and do not necessarily reflect the opinions of The Block or the organization that commissioned the report. The Block's analysts may have taken positions in the assets discussed in this report and this statement is to disclose any perceived conflict of interest. Please refer to The Block's Financial Disclosures page for author holdings. This report is for informational purposes only and should not be relied upon as a basis for investment decisions, nor is it offered or intended to be used as legal, tax, investment, financial or other advice. You should conduct your own research and consult independent counsel on the matters discussed within this report. Past performance of any asset is not indicative of future results.

© 2022 The Block Crypto, Inc. All Rights Reserved.