
THE FINNEY RATIO AND THE SZABO SCORE

QUANTIFYING BLOCKCHAIN IMMUTABILITY OVER TIME

A PREPRINT

Yaz Khoury

Director of Developer Relations
Ethereum Classic Cooperative
yaz@etccooperative.org

November 25, 2019

ABSTRACT

Immutability is a term used a lot in blockchain and cryptocurrency development when attempting to analyze the economic interpretation of a network. Designs like the 21 million Bitcoin supply in BTC or incidents like the DAO fork bailout that split the Ethereum community into ETH and ETC are major examples of immutability values determining the ethos of a chain. This research sets out to categorize different features of blockchain immutability and analyze them in three different networks: Bitcoin (BTC), Ethereum (ETH), and Ethereum Classic (ETC). Further in the paper, the Finney Ratio is introduced to help understand how blockchain immutability can be measured over time. The paper then visualizes overall blockchain immutability over time using radar charts as an immutability map. The Szabo Score is then introduced as a tool to score overall mutability over time for each blockchain.

Keywords Immutability · Blockchain · Finney Ratio · Szabo Score · Bitcoin · Ethereum

1 Introduction

Cryptocurrency network communities like Bitcoin (BTC), Ethereum (ETH) and Ethereum Classic (ETC) often debate about the concept of immutability and what it means in the context of a blockchain. Bitcoin's white paper[1], proposed by Satoshi Nakamoto, introduces a major innovation in Byzantine Fault Tolerance (BFT) problem: It achieves 51% fault tolerance in what is called Nakamoto Consensus, which is an improvement over other BFT systems. This protects data and ledger immutability up to 51% of honest nodes on a technical level. However, this paper will show that there are various features of immutability in blockchain networks that still can be broken on the social level. Even if Nakamoto Consensus is still valid, certain social coordination by network participants can break aspects of blockchain immutability. Another example is the 21 million[2] Bitcoin supply cap being cited as a source of immutability for the network when it first came online. The adherence to a supply cap is in itself a social level immutability. On a technical level, it is easy to modify the supply cap in Bitcoin, but what protects its value is the adherence to the social contract given in the software origin and the white paper.

Ethereum[3] and Ethereum Classic[4] were one chain at a point in time before a hack[5] of a famous smart contract known as the DAO (Decentralized Autonomous Organization) allowed the hacker to steal \$50 million dollars at the time. A debate within the Ethereum community turned contentious over whether the community should hard fork to bailout the victims of the DAO hack or preserve ledger immutability. The resulting DAO hardfork[6] split the Ethereum community in two with ETH forking to return back the money to those that lost it while Ethereum Classic chose to run the original chain that resisted the fork. This major event is one of many examples of immutability debates that have occurred in the blockchain space.

Currently, immutability is often quantified in the binary sense: is blockchain X immutable or not? However, it's very hard to understand what this binary classification is referring to. Is it referring to a monetary policy, social contracts in a network, or perhaps any changes in the transactions written to a ledger? The applications here are endless and it often confuses stakeholders when trying to properly analyze what it means that a blockchain is immutable.

Table 1: Immutability Subsystems

Number	Subsystem Name
1	Monetary Policy
2	Consensus Mechanism
3	Hashing Algorithm
4	Chain State
5	Reserved State Space
6	Transaction History
7	Transaction Finality
8	Social Contracts

This paper will attempt to analyze multiple properties common in all blockchain networks and attempt to quantify the immutability of each property. This paper will present ways to do an overall quantification and scoring of each network based on its immutability properties. This research will also visualize the immutability properties of each blockchains so stakeholders can easily understand. This will help network participants understand how each network differs based on its immutability properties and then understand which network is more immutable than the other. It will also help stakeholders understand how blockchain immutability changes over time.

2 Immutability Subsystems

While measuring blockchain decentralization[7] through the minimum Nakamoto Coefficient and Gini Coefficient can be quantified more in percentages, immutability on the other hand must be a binary measurement. In other words, a subsystem can either be mutable or immutable. Therefore, this paper will define immutability more as a vector with multiple scalar features in it, each scalar feature with its own value measuring one subsystem.

The immutability variable is defined as the following in Theorem 1.

Theorem 1 *Let $i_{subsystem}$ be a variable for immutability,*

Where i is the immutability variable and subsystem is the sector of the blockchain whose immutability is being quantified.

Then,

$$i_{subsystem} \begin{cases} 0 & mutated \\ 1 & immutable \end{cases} \quad (1)$$

Here, the i variable represents a variable being classified as immutable or mutable, where it refers to a specific subsystem of the blockchain being measured. Various features of the immutability vector can be proposed. This paper aims to focus on eight subsystems of immutability as can be seen in Table 1. All eight of those subsystems will be analyzed and discussed in Section 2. The design of those methods of quantification for immutability allow for further extendability and addition of more subsystems in the future. The eight subsystems will focus on three blockchain networks:

- Bitcoin
- Ethereum
- Ethereum Classic

The blockchain subsystems in Table 1 can be grouped into an immutability vector as defined in Theorem 2.

Theorem 2 *Let \mathbf{I} be the immutability vector,*

Where the features of the immutability vector are specified as the following:

$$\mathbf{I} = [i_0, i_1, \dots, i_n] \quad (2)$$

Where n is the length of the \mathbf{I} immutability vector.

Then, each $i_{subsystem}$ variable inside vector \mathbf{I} represents a unique subsystem of immutability.

In the following subsections, each subsystem in Table 1 will be gone over and analyzed for immutability.

2.1 Monetary Policy

Immutability of the Monetary Policy is a measure of the change in the Monetary Policy of the blockchain historically. Examples of monetary policies in blockchains include the 21 million bitcoin supply cap or Ethereum’s infinite supply of Ether. Here, the paper will look at the moment a monetary policy was first described or mentioned and if changes were made to it after. For example, a change in the block issuance number from constant supply to a lower number or a supply cap on the total issued currency units constitutes a change in the monetary policy.

2.1.1 Bitcoin Monetary Policy

The question for Bitcoin has always been when was the monetary policy first introduced. The original whitepaper for Bitcoin and the code published by Satoshi Nakamoto (pre-release version) contain no mention of the 21 million supply cap, around November 2008. It was only in the first-version release in January 2009, a few months later, did Satoshi first mention the 21 million supply cap and references to it in the code.

The question for this research then becomes: which is the right Bitcoin canon, when it was first published in the white paper with the pre-release code or when it first went online in early January 2009? There is a 2 months gap in between where Satoshi Nakamoto first released the Bitcoin white paper and pre-release code and when Satoshi and Hal Finney and others worked on the first version release software, where the supply cap was introduced. A sample of the code written in the first version release[8] of the software is shown in the following code block.

```
int64 CBlock::GetBlockValue(int64 nFees) const
{
    int64 nSubsidy = 50 * COIN;

    // Subsidy is cut in half every 4 years
    nSubsidy >>= (nBestHeight / 210000);

    return nSubsidy + nFees;
}
```

In this code block, the block reward is halved approximately every 4 years, or every 210000 blocks. In the pre-release version, the code is not there. The Bitcoin first-version software release in January 2009 contains the following quote by Satoshi, the first ever mention of the 21 million supply cap[2]:

"Total circulation will be 21,000,000 coins. It'll be distributed to network nodes when they make blocks, with the amount cut in half every 4 years." - *Satoshi Nakamoto*

So, this paper will consider the first time the Bitcoin network went online to be on the first version release of the Bitcoin client software. Therefore, Bitcoin’s immutability value for monetary policy is 1, denoted as $i_{monetarypolicy} = 1$.

However, it is important to note here that Satoshi was not the best programmer and even though he intended there to only be 21 million bitcoins, it actually would continue over 21 million supply due the way C++ language is designed. BIP-42[9] intends to set the supply cap to strictly 21 million bitcoins in the year 2214, which by then will violate immutability of monetary policy. So although currently, Bitcoin has a monetary policy value of 1, it will violate it in the year 2214 due to BIP-42.

2.1.2 Ethereum and Ethereum Classic Monetary Policy

In the case of Ethereum’s white paper[3], the monetary policy was an infinite supply with a fixed block reward issuance of 5 ETH for the rest of the chain’s life cycle. However, in Byzantium and Constantinople hard forks, there was a decrease in issuance from 5 to 3 ETH and from 3 to 2 ETH respectively, specifically described in EIP-649[10] and EIP-1234[11]. This is clearly a violation of the immutability of monetary policy. While one can argue that Ethereum does not have a monetary policy due to having an infinite supply, the constant issuance of ETH per block for its infinite supply is still a monetary policy. Therefore, Ethereum’s monetary policy scores a 0 on immutability, denoted as $i_{monetarypolicy} = 0$.

Ethereum Classic (ETC) follows the same story due to the application of a supply cap on circulating ETC as can be seen in ECIP-1017[12]. Because Ethereum Classic continues the original chain from the white paper with a resistance to the DAO fork, a change in its monetary policy by issuing a supply cap is a violation of immutability of the monetary policy. Therefore, ETC also scores a 0 on monetary policy, denoted as $i_{monetarypolicy} = 0$.

2.2 Consensus Mechanism

Consensus deals with the mechanism of decision-making on the blockchain. The most popular type of consensus is Proof-of-Work[13], which is currently found in Bitcoin, Ethereum and Ethereum Classic. Immutability of the consensus mechanism is an important measure of understanding whether a blockchain is modifying its mechanism in the future.

For example, if Ethereum moves from Proof-of-Work to Programmatic Proof-of-Work (ProgPoW)[14] or to Proof-of-Stake, it breaks the immutability value for consensus mechanism. What's more interesting about Ethereum is ETH 2.0 plans. If the plan for ETH 2.0 is to not share state with ETH1X (current chain), then technically ETH 2.0 becomes its own network with own state and monetary policy and consensus mechanism, starting fresh from scratch. If however it shares the state with current ETH1X, then it will be violating immutability of the consensus mechanism by moving directly to Proof-of-Stake. Analysis of ETH1X to ETH 2.0 is outside the scope of this research paper.

Currently, all three coins (ETC, BTC, and ETH) have always been on Proof-of-Work consensus, so the value for each of them is denoted as: $i_{consensusmechanism} = 1$.

2.3 Hashing Algorithm

Hashing algorithms refer to the tools used to measure consensus mechanism. For example, most Proof-of-Work chains like BTC use Hashcash[15] based on SHA256 algorithm while ETH/ETC use Ethash[16] that is based on Keccak256. If at any time in the future, any of those chains switch the hashing algorithm to be SHA3 or some other algorithm, then it violates immutability of the hashing algorithm.

This can be useful to do if for instance SHA256 is broken in the future and the security of all those chains relies on having a harder to break hashing algorithm. By then, despite breaking immutability in that category by moving to a new hashing algorithm, it actually improves security. It is a trade-off of security vs. maximum immutability.

For now, though, all three chains will receive a score of 1, denoted as: $i_{hashingalgorithm} = 1$.

2.4 Chain State

The immutability of the state set is the assumption that the state never gets irregularly modified outside of its regular change. In other words, if we assume the state of the blockchain is \mathbf{S} , where \mathbf{S} is constantly being updated and modified regularly with each block, any irregular modification of \mathbf{S} would denote a value \mathbf{S}' such as \mathbf{S}' is an irregular state set. What is defined as irregular state change is anything that affects the transaction history and finality of the ledger in a way specified outside of the network protocol. For instance, adding a function to a protocol that stops the protocol at a specific block time when it is syncing and having the protocol move funds to hardcoded addresses is an example of irregular state change. This is due to this function operating outside the original design specifications of the protocol and affecting transaction history and finality. This has only happened in Ethereum's main net, where in every client[17] that runs ETH, they will have to come across the DAO Fork[6] code which literally stops the chain sync momentarily at block 1.92 million, and returns stolen funds back to the victim addresses which are hardcoded into the client. The irregular state change allowed for a bailout of stolen money from the DAO hacker, which has modified the state to result in \mathbf{S}' .

Bitcoin experienced a fork split between v0.7 and v0.8 over database issues for several hours. The stakeholders of the network coordinated to support the lower version 0.7 on the social layer, and the chain on v0.8 was abandoned. This incident still doesn't imply irregular state change because it followed the rules of the network without modifying the protocol.

Chain State can be written in the following Theorem:

Theorem 3 Let S_t denote a blockchain state,

Where the state S being regularly changed through time t is S_t

Then,

$$S_{t-1} \Rightarrow S_t \tag{3}$$

$$S_{t-1} \Rightarrow S'_t \tag{4}$$

Where (3) is a regular state change denoted with S_t and (4) is an irregular state change denoted with S'_t .

Using this definition, the immutability values for ETC and BTC are 1, denoted as $i_{chainstate} = 1$ while ETH is 0, denoted as $i_{chainstate} = 0$.

2.5 Reserved State Space

Reserved State Space is a measure of empty addresses that are reserved for future modifications on the blockchain to allow for the addition of new features. For example, when one adds in op-codes for Solidity like REVERT on Byzantium Hardfork[18] for Ethereum or the Atlantis Hardfork[19] for Ethereum Classic, they are modifying the reserved state space which was initially empty.

This category is important to note that the modification of empty reserved state space follows its intended design and even if there has been a new addition of op-codes that break immutability here, it is acceptable because that is the whole point of using reserved state space. Currently, Bitcoin has a 0 for no modification of reserved state space because Bitcoin added its first new op-code in December 2015 with BIP-65[20]. Ethereum, having implemented Byzantium and Constantinople hardforks which added several new op-codes, breaks immutability in this category. Ethereum Classic having implemented the Atlantis Hardfork, also violates immutability in the reserved state space category.

So, here, ETC, ETH and BTC all get a value of 0, denoted as $i_{reservedstatespace} = 0$.

2.6 Transaction History

Ethereum's bailout of the DAO token holders who lost their ETH during the DAO hack isn't a violation of transaction history on the ledger because the original transaction by the DAO hacker to steal the ETH was not modified in the future by the DAO fork. Instead, what the DAO fork introduced was an irregular state change, as discussed in the previous Section 2.4.

Therefore, in this category, historically, neither of the three chains ever experienced a violation of transaction history immutability. So, each chain gets a score of 1, denoted as $i_{transactionhistory} = 1$.

2.7 Transaction Finality

In transaction finality, this paper looks at whether a transaction that enters the blockchain after some confirmations is final. Since blockchains are probabilistic and the more confirmations a transaction has, the more it is final, the measure becomes one of what constitutes a good amount of confirmations.

If one decides a confirmation of 1 block for each chain, we are in trouble because sometimes 51% attacks and blockchain reorganizations[21] happen. Reorganizations or reorgs can happen if say there is a delay in network propagation from miners in China, which means a transaction that is added to a block mined by someone in America might not be final if for example a miner in China has mined a longer chain but has a delay in communicating with the rest of the network. By the time they do, their chain becomes the longer chain and the other transactions will have to be re-added to the network. Therefore, transaction finality on one block confirmation would result in a 0 for all chains and is an unrealistic way of looking at immutability of transaction finality.

It is important to understand that due to 51% weakness of Proof-of-Work chains, waiting for longer confirmations is the only way to probabilistically reach transaction finality. In the events of the 51% attack on Ethereum Classic[22] with a double-spend attack on two exchanges, exchanges were waiting for shorter block confirmations than the economic security of 6 bitcoin blocks[23]. No other transaction was lost in the process, but the finality at the moment was threatened on the exchange side.

The solution was longer confirmation times. This paper will use the Coinbase metric for confirmation times[24] that are fit for each chain, which then results in BTC, ETH, and ETC all having a score of 1, denoted as $i_{transactionfinality} = 1$. To further illustrate the point of how longer confirmation times improve transaction finality, observe the early interactions between Satoshi Nakamoto and Hal Finney[25] on the following quote.

The transaction in whichever branch ends up getting ahead becomes the valid one, the other is invalid. If someone tries to double spend like that, one and only one spend will always become valid, the others invalid. Receivers of transactions will normally need to hold transactions for perhaps an hour or more to allow time for this kind of possibility to be resolved. They can still re-spend the coins immediately, but they should wait before taking an action such as shipping goods. — *Satoshi Nakamoto*

2.8 Social Contracts

Social Contracts relates to any rules that a user acknowledges before using the blockchain. A violation of social contracts is a change in immutability. Many examples of social contracts exist, such as "Code is Law", "21 million",

Table 2: Immutability Vectors Table

Immutability Features	Bitcoin	Ethereum	Ethereum Classic
Monetary Policy	1	0	0
Consensus Mechanism	1	1	1
Hashing Algorithm	1	1	1
Chain State	1	0	1
Reserved State Space	0	0	0
Transaction History	1	1	1
Transaction Finality	1	1	1
Social Contract	1	0	0

or "No Dev Block Rewards", but here, the paper will use the example of private and public key rules. The rule of blockchains is that only the owners of the private keys can transact from the address and the account. So, if a user does not own the private key of an account on the blockchain with say 1 million ETH, they can't move those ETH around.

This is why it is important that Satoshi's address on Bitcoin has 1 million BTC that has not been moved. It's also why Craig Wright can't prove he is Satoshi because he does not own the private key for the address that is known to belong to Satoshi. In the case of the DAO hard fork, a violation of social contract has taken place with the bailout of stolen funds on a new forked network by Ethereum, which makes ETH mutable in this category and is therefore assigned a value of 0, denoted as $i_{socialcontract} = 0$.

Ethereum Classic was a rejection of the DAO hard fork and therefore still maintains on the social layer the social contract, making it still a 1. However, ECIP-1015[26] which modified the gas costs on Ethereum Classic did violate the Social Contract on block 2,463,000, since a modification gas costs violate the immutability of the network promised to network participants to deploy their contracts or to transact on the chain. Therefore, ETC has a value of 0 in this category. There has never been historically a bailout in the history of Bitcoin, even during the Mt. Gox Hack, so it retains a value of 1, denoted as $i_{socialcontract} = 1$.

3 The Finney Ratio and Immutability Maps

This paper has done the preliminary analysis of the immutability features in Section 2. They are summarized in Table 2. Binary values for each immutability variable gives an immediate picture of whether or not there is a mutation in one of the features. While Table 2 provides a quick way to measure blockchain immutability, this paper is also interested in measuring blockchain immutability over.

The benefit of using time is that stakeholders can actually see how long each feature of a blockchain stays immutable before there is a violation in immutability. This paper will measure time passing in blockchain via block numbers. This paper proposes the Finney Ratio, denoted as R_{finney} , for measuring time passage in blockchain with mutated features, as defined in Theorem 4

Theorem 4 *Let B_{mutate} equal the block number where the violation in immutability occurs,*

Let B_{height} equal the block number of the height or latest block in the blockchain.

Then, the Finney Ratio is:

$$R_{finney} = \frac{B_{mutate}}{B_{height}} \quad (5)$$

Which is the ratio between the mutated block number and the latest block number.

Here, the Finney Ratio applies to any of the immutability variables that have a 0 value. So, for all variables in immutability vector \mathbf{I} , the 0 is replaced with the correct Finney Ratio R_{finney} . This gives the ratio of when the mutation occurs (as measured by block number it occurs on) by the latest block value. For the calculations for this paper, the following latest block numbers B_{height} (latest) will be used in the calculations for each chain:

- **Bitcoin:** Block 600762
- **Ethereum:** Block 8798811
- **Ethereum Classic:** Block 9044480

Table 3: Ethereum Finney Ratio

Immutability Features	Ethereum
Monetary Policy	0.4966
Consensus Mechanism	1
Hashing Algorithm	1
Chain State	0.2182
Reserved State Space	0.4966
Transaction History	1
Transaction Finality	1
Social Contract	0.2182

Table 4: Ethereum Classic Finney Ratio

Immutability Features	Ethereum Classic
Monetary Policy	0.5528
Consensus Mechanism	1
Hashing Algorithm	1
Chain State	1
Reserved State Space	0.96987
Transaction History	1
Transaction Finality	1
Social Contract	0.27232

3.1 Ethereum Finney Ratio

Ethereum’s violation of Monetary Policy immutability happens around the Byzantium Hard Fork where there was a reduction in reward at block number 4,370,000[10]. It is also the same block where the new op-codes were added[18], violating Reserved State Space category of immutability. So, the Finney Ratio for those two categories is $R_{finney} = 4.37/8.798811 = 0.4966$.

In regards to the other violations, both the violation in Social Contract and Chain State happen on the DAO Fork at block number 1,920,000[6]. So, the Finney Ratio for those two categories is $R_{finney} = 1.92/8.798811 = 0.2182$. Table 3 groups the Finney Ratios back into the immutability vector for Ethereum.

Table 3 can now be plotted as radar chart that will be called an immutability map for this paper where immutability over time can be visualized, as can be seen in Figure 1. Here, the effects of the DAO in early penalization of Ethereum can be observed, with the larger growth in the chain pushing the Chain State and Social Contract closer to 0 as time passes on. One can also observe the effects of Byzantium Hard Fork on the network.

3.2 Ethereum Classic Finney Ratio

In Ethereum Classic, three violations happened, the Monetary Policy breaking in immutability which happens at block 5,000,000, the Social Contract violation back at block 2,463,000 for ECIP-1015, and the Atlantis Hardfork at block 8,772,000 which is a violation of Reserved State Space immutability. This will result in a Finney Ratio of $R_{finney} = 0.5528$ for Monetary Policy, a Finney Ratio of $R_{finney} = 0.27232$ for Social Contract, and one of $R_{finney} = 0.96987$ for Reserved State Space. Table 4 highlights the values calculated for Ethereum Classic’s Finney ratios. An immutability map of the Finney Ratios is plotted in Figure 2.

The violation in Monetary policy for ETC has a Finney ratio of 0.5528, which is close to the Finney ratio of 0.4966 for ETH’s violation in monetary policy immutability, indicating the periods where both network’s violations have occurred are close to one another.

3.3 Bitcoin Finney Ratio

For Bitcoin, the violation of Reserved State Space happens around December 2015 with the implementation of BIP-65 for adding a new op-code. No information about when in December 2015 has BIP-65 been activated, or rather at which specific block, due to it being a User Activated Soft Fork (UASF). This paper instead takes an estimate based on the

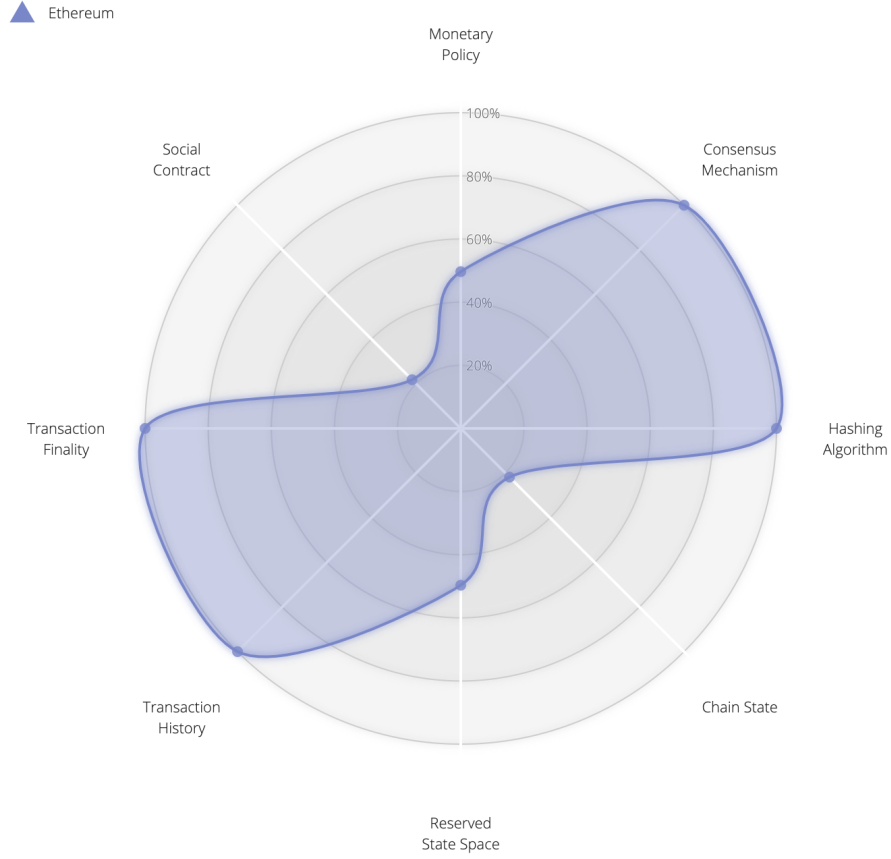


Figure 1: Ethereum Immutability Map

Table 5: Bitcoin Finney Ratio

Immutability Features	Bitcoin
Monetary Policy	1
Consensus Mechanism	1
Hashing Algorithm	1
Chain State	1
Reserved State Space	0.647
Transaction History	1
Transaction Finality	1
Social Contract	1

minimum and maximum block number for December 2015 via the timestamp of the block being included in the ledger. Then, the average of both minimum and maximum blocks give the approximate block number.

- 386,270 is Minimum Block number on December 2015
- 391,150 is Maximum Block number on December 2015

Average Block Number for BIP-65 is 388,710. So, the Finney Ratio for Reserved State Space is $R_{finney} = 0.647$. Table 5 shows the updated immutability vector values with the Finney ratio. A plot of the Bitcoin immutability map is shown on Figure 3.

What's the benefit of calculating the Finney ratio for each violation in immutability in the Immutability vector? It helps stakeholders understand the timelines of blockchain immutability better when they can see how long a blockchain's features preserve immutability through time. One property of Finney Ratio given a long enough timeline, the Finney

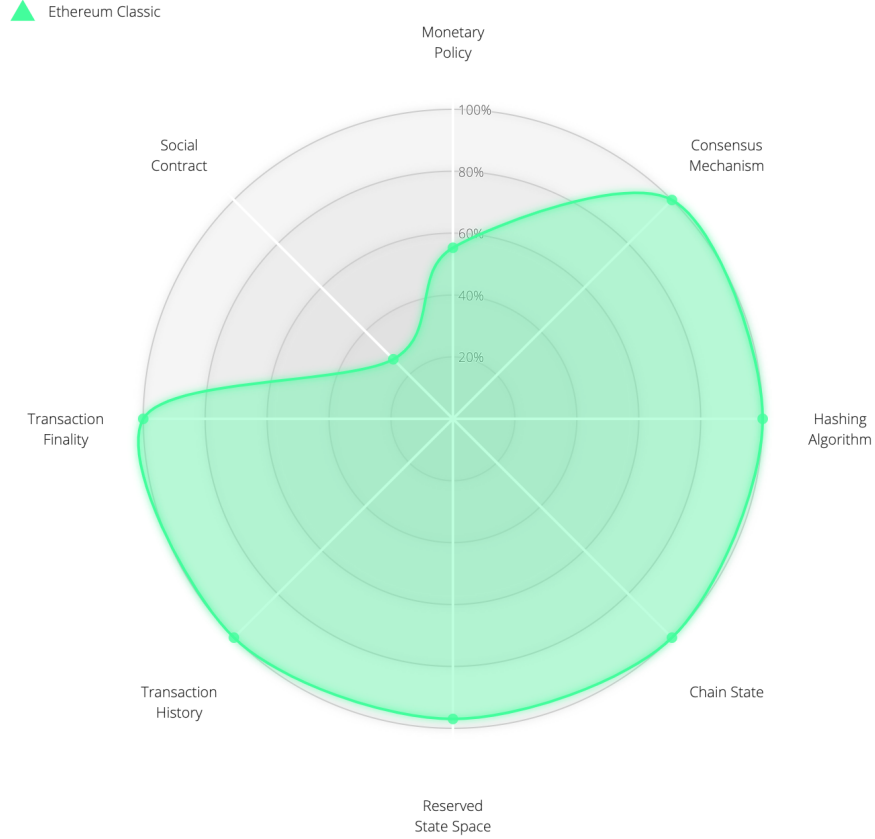


Figure 2: Ethereum Classic Immutability Map

Ratio R_{Finney} approaches zero. The longer a blockchain preserves immutability in each of its features, the larger the immutability map.

In the case of Bitcoin, it is going to maintain a great area of immutability until BIP-42 is implemented around the year 2214 whereafter, the violation in Monetary Policy value happens, as covered in Section 2.1.1. In the following section, the paper will provide a score of immutability for each blockchain network.

4 The Szabo Score

In order to quantify the immutability maps plotted to a score number, this paper proposes using the Szabo Score. The Szabo Score is simply using the entropy formula to quantify a blockchain's immutability. It is specified in Theorem 5. Why use entropy here to measure mutations in blockchain over time? In information theory, entropy measures the unpredictability of the state.

If a highly probable event happens, it gives no new information about it since it's expected to happen. Also, if a lower probable event happens, it gives a lot of more information of when it occurs. So, in entropy, flipping a dice has a higher value because of the low probability of each dice value than say flipping a coin.

This paper replaces probability with immutability as measured via the Finney Ratio. Here, if a Finney Ratio is 1 for each value of the immutability variables, it gives no new information as it will always be a 1, and thus, fully immutable. The entropy value of a fully immutable vector (all values are 1) is 0. The interest lies in variables where there is a violation of immutability, or a mutation, and pushing the Finney Ratio towards 0 over time. Here, over time, the dropping in Finney Ratio for one of the variables does increase the mutability or Szabo Score. It allows stakeholders to gauge how a violation in immutability in a blockchain leads to more uncertainty over time.

The Shannon Entropy[27] formula can be rewritten in terms of the Szabo Score as follows:

Theorem 5 Let S_{szabo} denote the Szabo score,

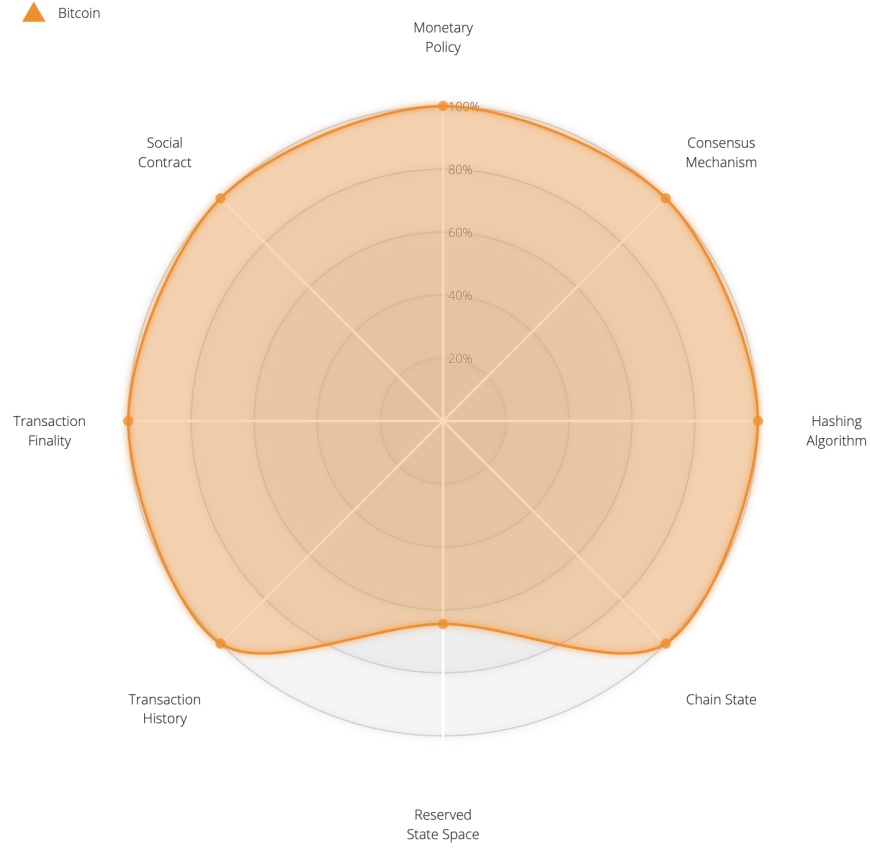


Figure 3: Bitcoin Immutability Map

Table 6: Szabo Score Table

Blockchain	Szabo Score
Bitcoin	0.1223
Ethereum	0.5904
Ethereum Classic	0.3090

Let R_{finney} denote the Finney ratio,

Where I_i denotes all Finney ratios i in the Immutability Vector I .

Then,

Szabo score can be written as follows:

$$S_{szabo} = - \sum_i I_i \log_{10} I_i \quad (6)$$

Szabo Score is measuring on a base of 10 of the logarithm because it is concerned with decimals and not binary points. Given the vector values of each chain in the previous tables where the 0s are replaced with their Finney Ratios, the Szabo Scores of each chain can be calculated as shown in Table 6.

Here, it can be seen that the higher the Szabo Score, the less immutable a blockchain is over time, and therefore the more mutation is in a blockchain. The more time passes after a blockchain violates one of its immutability variables, the higher the Szabo score climbs, decreasing its immutability. Bitcoin in Table 6 above has the lowest Szabo Score, therefore the highest immutability. Ethereum Classic has a higher immutability than Ethereum due to its lower Szabo Score.

A good way to measure the immutability of blockchains is to take the Szabo Score (entropy of the immutability vector with mutable values of 0 replaced by their Finney Ratio) and the minimum Finney Ratio (ratio of the first break in the immutability of a blockchain feature) to be able to understand blockchain immutability and their timelines better.

5 Conclusions

One of the most important aims of this research was to allow stakeholders to visualize immutability in blockchains over times. Having tools like the Finney Ratio, Immutability Maps and the Szabo Score help quantify and analyze blockchain immutability at a deeper level. Being able to do quantify immutability in a coherent manner that helps stakeholders understand the implications of blockchain immutability allows for decision making on what aspects of immutability are important to a community's values.

For example, a break in SHA256 algorithms and an network upgrade to SHA3 algorithm violates the Hashing Algorithm category of immutability but improves security. This an important trade-off a blockchain community must make to preserve immutability of its social contract but sacrifice immutability of hashing algorithm. Moving from Proof-of-Work to Proof-of-Stake violates Consensus Mechanism of immutability but improves scalability in the long term. In the case of ETH 2.0, that is an acceptable goal, the trading of immutability and higher security for scalability and speed.

Adding new op-codes violates Reserved State Space but extends blockchain functionality over the long term by improving the Turing-completeness properties of blockchains. The aim of this paper was to not be subjective to which features of immutability were more important than others since that was political and local to the network's underlying social layer. What can be done in future research is categorizing immutability features based on technical maintenance vs. socio-economic immutability properties. In this research, eight subsystems or features of immutability were considered and analyzed.

However, the immutability vector is not limited to just eight. More properties and features can be considered and added to the vector for analysis. For example, one can add backward-compatibility as a feature of immutability. If new changes added to blockchains in a hardfork break backward-compatibility of existing contracts, that violates this immutability.

While technical immutability of transactions is preserved via Nakamoto Consensus of following the longest chain in Proof-of-Work networks, it is important to consider that all those different subsystems that affect a blockchain's immutability happen on the social layer. On the social layer, stakeholders can propose a hard fork to add a supply cap or remove restrictions and caps. Stakeholders can implement an irregular state change to return back people's money or they can add new op-codes.

They can break agreed-upon social contracts or add new ones. The technical probabilistic immutability of Nakamoto Consensus that protects networks up to 51% fault tolerance is not enough. Social layer quantification of immutability is important to ensure stakeholders understand the risks in modifying immutability properties of a blockchain and adding more complexity instead of minimizing trust.

In Sections 3 and Section 4 of quantifying and visualizing the immutability of the different blockchain networks, Bitcoin scores the highest on immutability. It has the lowest Szabo Score on mutability, making it the most resilient of all networks to changes. What is also interesting about Bitcoin is that it has the longest timeline of the three networks analyzed yet its still the most resilient to change.

One aspect of Bitcoin's immutability was not categorized for this research: the inflation bug. The categorization of this bug might fall under "Transaction Malleability" or potentially some other feature if a pattern is found for this bug in other networks.

Another interesting property to highlight is the delta block time and its relation to immutability over time. The higher the delta block time between two blocks, the more immutable it is over time according to the model proposed in this paper due to the fact that the Finney Ratio for such a network slowly decreases vs. a network with faster delta block time. There are plenty of arguments to support longer block time vs shorter block time in Proof-of-Work networks. A relationship to immutability can potentially add an extra signal to stakeholders considering delta block time design. Bitcoin scoring the highest in immutability due to its low Szabo Score has block times that average around 10 minutes, while Ethereum and Ethereum Classic have block times that average around 15 seconds.

One final remark on the methodology used in this research paper is the ability to predict future immutability. If a stakeholder knows what new changes will occur on a blockchain at a specific hardfork in the future, they can plot a future immutability map and quantify immutability at a block height far in the future while accounting for any violations that will occur on a specific hard fork block. This allows one to understand how future hard forks can change the immutability and behavior of blockchain networks. The important thing to note, however, is that immutability is about

trade-offs in the end and each blockchain community would then need to decide which trade-offs and features of immutability are worth preserving.

References

- [1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *metzdowd.com*, 2008.
- [2] Satoshi Nakamoto. Bitcoin v0.1 released, January 2009.
- [3] Vitalik Buterin. Ethereum white paper: A next generation smart contract & decentralized application platform. *Ethereum Github Wiki*, 2014.
- [4] The Ethereum Classic Community. The ethereum classic declaration of independence, July 2016.
- [5] Klint Finley. A \$50 million hack just showed that the dao was all too human. *Wired*, 2016.
- [6] Casey Detrio. Eip 779: Dao fork, November 2017. [Online; posted 26-November-2017].
- [7] Balaji S. Srinivasan and Leland Lee. Quantifying decentralization, July 2017. [Online; posted 27-July-2017].
- [8] Satoshi Nakamoto and Hal Finney. Bitcoin code, January 2009.
- [9] Pieter Wuille. Bip 42: A finite monetary supply for bitcoin, April 2014.
- [10] Afri Schoedon and Vitalik Buterin. Eip 649: Metropolis difficulty bomb delay and block reward reduction, June 2017.
- [11] Afri Schoedon. Eip 1234: Constantinople difficulty bomb delay and block reward adjustment, July 2018.
- [12] Matthew Mazur. Ecip 1017: Monetary policy and final modification to the ethereum classic emission schedule, November 2016.
- [13] Ari Jakobsson, Markus Juels. Proofs of work and bread pudding protocols. *Secure Information Networks: Communications and Multimedia Security, IFIP — The International Federation for Information Processing*, 23, 1999.
- [14] Eip-1057: Progpow, a programmatic proof-of-work, may 2018.
- [15] Adam Back. Hashcash - a denial of service counter-measure. *Tech Report*, August 2002.
- [16] Ethereum Community. Ethash, January 2015.
- [17] Péter Szilágyi. Geth source code, July 2016.
- [18] Alex Beregszaszi. Eip 609: Hardfork meta: Byzantium, April 2017.
- [19] Isaac Ardis. Atlantis evm and protocol upgrades, February 2019.
- [20] Peter Todd. Bip 65: Op checklocktimeverify, October 2014.
- [21] Bitcoin Wiki. Chain reorganization, May 2019.
- [22] Mark Nesbitt. Deep chain reorganization detected on ethereum classic (etc), January 2019.
- [23] Anthony Lusardi. Your exchange needs more confirmations: The bitconf measure, December 2018.
- [24] Coinbase. Why is my transaction pending, 2019.
- [25] Cryptography Mailing List. Bitcoin p2p e-cash paper, November 2008.
- [26] Cody Burns. Ecip 1015: Long-term gas cost changes for io-heavy operations to mitigate transaction spam attacks, October 2016.
- [27] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27, October 1948.