Security Coefficient — a measure of short term attack possibilities in PoW and PoS networks

Why economic incentives, not just the node count in the network, dictate security

Rag Bhagavatha
Storecoin.com
San Francisco CA
rag@storecoin.com

Chris McCoy
Storecoin.com
San Francisco CA
chris@storecoin.com

Abstract

In this paper, we show that security in any decentralized network is determined by economic incentives built into the protocol of the network. We also show that a popular indicator of decentralization — the number of nodes in the network — doesn't guarantee network security unless aided by in-protocol economic incentives. We examine the security properties of a few popular blockchain projects and showcase the differences between the perceived and the actual security. Specifically, we conclude the following.

1. A Network should have a *security budget*, which determines the cost of attack on the network.
2. If the network has economic incentives defined, the incentives must be much smaller than the security budget to ensure real security.
3. All other indicators, including the degree of decentralization, give a false sense of security. A network will be under imminent threat, if it relies solely on such indicators.

We introduce a measure called the *security coefficient*, which can be used to compare the security characteristics of both Proof-of-Work (PoW) and Proof-of-Stake (PoS) networks. In this paper, we describe the methodology to calculate the security coefficient for any blockchain protocol.

What is decentralized network security?

A decentralized network, such as a public blockchain, is used as a systematic approach to replace *trust*. More precisely, the participating nodes who may not trust each other, can reach consensus and cooperate without a third party or a central authority. A lack of a single authority makes the system fairer and considerably more secure. However, trust demands decentralization, which typically requires the participation of a large number of diverse participants. So it is theorized that greater decentralization results in greater trust, which in turn results in higher security.

As for the security itself, it is often defined with a very narrow scope, such as double-spending attack[1] or cost of attack on the network[2] over a long horizon of time, such as one year. Such indicators usually appear very expensive in terms of the cost of attack or seem impossible. While these threats must be defended against, security also covers short term incentives to attack and profit from it. When conditions are right, such short term attacks can be launched fairly cheaply. We analyze a few examples of such attacks in this paper.

In all of the examples discussed in this paper, we show that networks are secure if and only if proper economic incentives are built into the protocol.

Definitions

Security budget

This is the **cost of a short term attack** on the network such that the underlying security assumptions are breached. For PoW blockchains, this is the cost of a 51% attack[2] for 1 hour. For example, it costs approximately $950,000 per hour[1] to launch a 51% attack on Bitcoin. This security budget doesn't include or address other types of attacks such as defending against spam or DDoS. While such attacks may affect liveness, they don't undermine the security assumptions of the network and hence they are not considered for the security budget.

We want to emphasize that the source [2] used for determining the security budget for PoW networks doesn't imply that short term attacks can be launched by renting hashpower. We only imply the approximate hashpower (and the resulting cost) required to launch a short term attack. The hashpower itself can be acquired or produced in many different ways.

[1] All numbers are as of the time of writing this paper. These numbers change often. Please consult the references provided for up to date information.

Economic incentive

This is the incentive built into the protocol to pay for different actors who help with securing the network. In Bitcoin, miners are compensated with block rewards in BTC and transaction fees for securing the network. The more deterministic this reward is, the more likely a network is to incentivize miners to help secure the network.

In the classic literature of Bitcoin, the security budget is same as the economic incentive defined in this paper. Specifically, the security budget is defined as:

(Block rewards x number of blocks per hour x price per BTC) + Transaction fees earned per hour

However, we differentiate between the security budget and the economic incentive because:

- in Proof-of-Work networks, the cost of producing/renting the hash power required for 51% attack is different from the potential miner rewards. This difference can be taken advantage of under certain circumstances to attack the network successfully. We discuss examples of such attacks in this paper.
- in Proof-of-Stake networks, the loss of staked tokens due to slashing is different from the potential Validator rewards.

Security coefficient

This is the ratio of the economic incentive to the security budget. For example, the security coefficient for Bitcoin is (excluding transaction fees) approximately:

(block reward x blocks per hour x price per BTC) / security budget per hour

=

(12.5 x 6 x $10,200) / $950,000 [see note [2] below] = **0.8052**.

This coefficient must be less than 1. **The smaller this coefficient, the more secure the network from short term attacks** because, if the economic incentive is larger than the security budget, a short term attack may become attractive. Transaction fees however, alter this coefficient and it is possible that the security coefficient becomes large enough to make the attack economically attractive.

[2] The "one hour cost of attack" values used in this paper are as of this writing.

If a network does not have a clearly defined security budget or economic incentive, the security coefficient becomes undefined. This makes the security characterization of such networks impossible to determine.

Security coefficient vs security factor

There have been previous attempts to characterize the security of blockchain networks. For example, [4] defines "security factor" as shown in fig. 1.

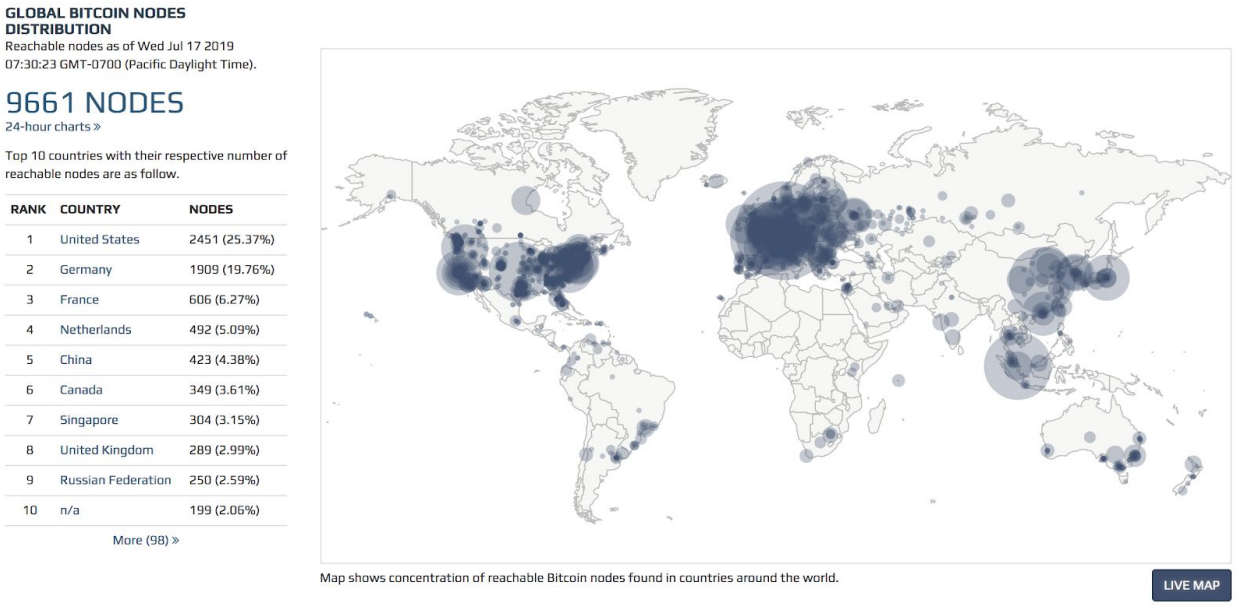
```
SF = attack_cost/network_value
SF = SB/network_value
SF = SB/market_cap
SF = (block_rewards_usd + tx_fees_usd) / market_cap
SF = (block_rewards_btc * price + tx_fees_btc * price) / market_cap
SF = (block_rewards_btc + tx_fees_btc) * price / market_cap
SF = (block_rewards_btc + tx_fees_btc) * price / supply * price
SF = (block_rewards_btc + tx_fees_btc) / supply
SF = block_rewards_btc / supply + tx_fees_btc / supply
SF = block_reward_security_factor + tx_fees_sec
```

Fig. 1 — Security Factor (SF) definitions

The security factor looks at the security of the network over a long horizon — for example, the cost to attack the network over 1 year. Security coefficient, on the other hand, looks at short term incentives to mount an attack. We show later in this paper the incidents where short term incentives became attractive enough to launch 51% attacks.

Security in Bitcoin (BTC)

Bitcoin is often hailed as the most decentralized public blockchain. According to Bitnodes, there are 9,661 reachable full nodes at the time of this writing. Fig. 2 shows the distribution of reachable nodes around the world.



GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Wed Jul 17 2019 07:30:23 GMT-0700 (Pacific Daylight Time).

9661 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2451 (25.37%)
2	Germany	1909 (19.76%)
3	France	606 (6.27%)
4	Netherlands	492 (5.09%)
5	China	423 (4.38%)
6	Canada	349 (3.61%)
7	Singapore	304 (3.15%)
8	United Kingdom	289 (2.99%)
9	Russian Federation	250 (2.59%)
10	n/a	199 (2.06%)

More (98) »

Fig. 2 — Bitcoin network of reachable full nodes around the world

We ask the following question.

> Is Bitcoin network's security derived from the large number of full nodes or incentives built into the Bitcoin protocol that pays its miners?

To answer this question, we will take a look at Bitcoin Cash (BCH), a hard fork of Bitcoin, which was in the news[3] recently for a 51% attack by two mining pools in an apparent effort to reverse another miner's transactions. Bitcoin Cash currently has 1,441 public nodes running. While this number is much lower than Bitcoin's, it is sufficiently decentralized. We will not discuss the legality of this 51% attack, but the attack successfully reorganized and removed transactions from the third miner, in favor of transactions from the two mining pools. All the full nodes running on the Bitcoin Cash network accepted the reversal of transactions because the chain contained the *most cumulative proof of work*. The full nodes would have accepted the block(s) with reversed transactions, even if this attack were purported to harm the Bitcoin Cash network. The security coefficient of Bitcoin Cash is:

$$(12.5 \times 6 \times \$308) / \$21{,}316 \text{ [2]} = \mathbf{1.0837}.$$

The security coefficient is greater than one without including transaction fees and other incentives, which makes a short term attack worthwhile. In this case, 25 transactions worth 3,391.7 BCH[3] ($1,044,643.6 at $308 per BCH) are reversed by the two mining pools to ensure that the other miner doesn't get these coins transferred. So, the actual security coefficient is:

$$(12.5 \times 6 \times \$308) + \$1{,}044{,}643.6 / \$21{,}316 = \mathbf{50.0911}.$$

This security coefficient demonstrates that the attack was indeed attractive, despite its cost. We can extend this illustration for Bitcoin and conclude that if the benefit of a 51% attack is more than $950,000 (security coefficient is greater than 1) and the attack can be successfully completed within an hour, such an attack is technically possible.

Observations

1. Steady state security coefficient of the network can be computed easily and dynamically because the economic incentives and the security budget are well published.
2. While the steady state security coefficient can be fairly low indicating that the network is very secure, under certain circumstances, transaction fees and other incentives may result in a security coefficient with a value greater than 1. In such circumstances, a 51% attack may be attractive despite the cost.
3. A large number of reachable full nodes don't deter or undo such attacks because there is no economic incentive defined for full nodes. Moreover, the resulting chain will likely contain the *most cumulative proof of work*, so all protocol rules will fully validate.
4. The 51% attack can be launched for a short duration of time, such as 1 hour, for relatively low cost (approximately $950,000 for Bitcoin) to reverse transactions selectively, if such attacks are deemed profitable. The recent attack on Bitcoin Cash proves that such short-term attacks are possible.

Security in Ethereum (ETH1)

Ethereum follows a similar model as Bitcoin. It uses PoW, has a block duration of approximately 15 seconds, and pays about 2.16 ETH per block. Ethereum's security coefficient can be computed as (at $213.85 per ETH):

(2.16 x $213.85) x (4 blocks per minute) x 60 / $116,614[2] = **0.9506**.

Notice that the steady state security coefficient is approaching 1 and depending on ETH's price fluctuation and transaction fees included, it can go over 1 at any time. This shows that Ethereum is vulnerable to 51% attacks from the economic point of view. The degree of decentralization — Ethereum has over 7,800+ clients running around the world — is not a deterrent against 51% attacks as in Bitcoin.

Short term incentives for attacks, when attractive, will more likely to be carried out. As a second example, we'll look at the deep chain reorganization attempt[7] on Ethereum Classic (ETC). We'll start with ETC's security coefficient at steady state, which is computed as follows.

(Price of ETC x rewards per block x number of blocks per hour) / Security budget per hour

=

($6.01 x 4.009 x 257) / $5,961 [2] = **1.0387**.

Notice that the security coefficient hovers around 1 as in ETH. The deep chain reorganization resulted in the double-spending of 219,000 ETC worth nearly $1.1M at the time of the attack. The attack is spread over 3 days, but the attack duration in terms of reorganized blocks (start ancestor block — 7,249,343, end ancestor block — 7,261,676) lasted for 2 days. The security budget for 2 days would be ($5,961 x 48) = $286,128, making it worthwhile to carry out the attack.

($6.01 x 4.009 x 257) x 48 + $1.1M / $286,128 = **4.883**

This attack also highlights the fact that the attack doesn't necessarily have to be swift, lasting a few blocks, to prevent detection. The attack demonstrates the imminent threat of short term incentives, when the conditions are right.

Observations

1. Steady state security coefficient of the network can be computed easily and dynamically because the economic incentives and the security budget are well published.
2. The steady state security coefficient is already near or above 1, making Ethereum vulnerable to short term 51% attacks.
3. A large number of reachable full nodes don't deter or undo such attacks because there is no economic incentive defined for full nodes. Moreover, no protocol rules would actually be broken, so full nodes accept reverted blocks.
4. Short term incentives may become attractive to carry out 51% attacks.

It is worth noting that there are no penalties for malicious behaviors in PoW networks. This is because all the miners, including the malicious ones, would spend their resources up front to generate the proof of work. So, if their work is accepted by the network (as evident from Bitcoin Cash and Ethereum Classic examples above), miners don't have to worry about any penalties for malicious behaviors.

Security in Polkadot (DOT)

Polkadot is a *global network of blockchains* and empowers them to work together under the protection of a shared security. In Polkadot any DOT-holder can become a Nominator when they nominate one or more Validators with their DOTs. The elected Validators secure the Relay Chain, which maintains the global state of the Polkadot Network. The Parachains are networks of their own and maintain their local states independent of the global state secured by the Relay Chain. The Collators in Parachains post their local states to the Relay Chain for updating the global state. A subset of Validators is assigned to each Parachain to verify proofs of state transitions. Fig. 3 illustrates the relationships between all the parties in the Polkadot network.

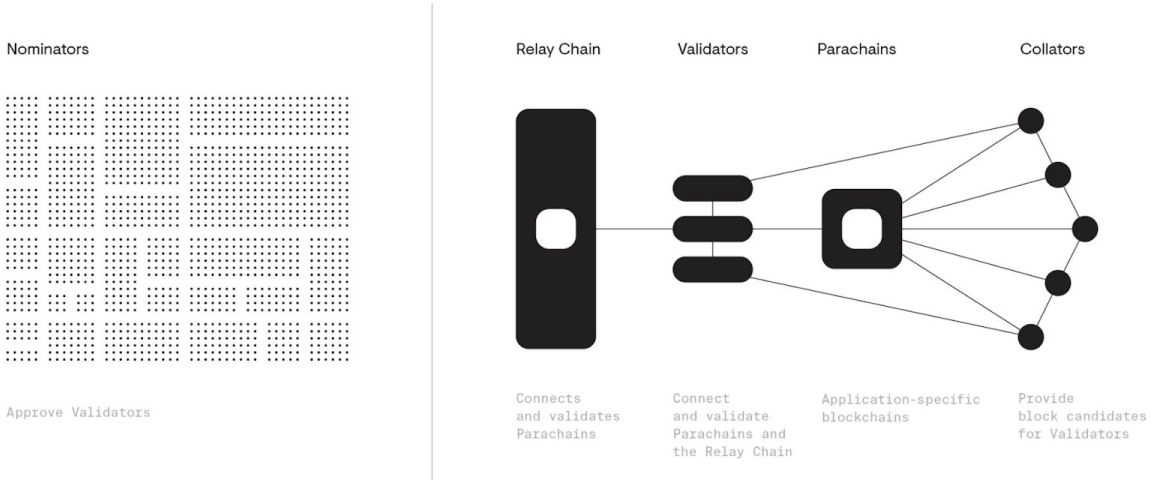


Fig. 3 — Relationship between Nominators, Validators, Collators, Relay Chain, and Parachains in Polkadot [4]

Polkadot allows developers to launch chains and applications (as Parachains) leveraging its shared security model, without having to worry about attracting enough miners or validators to secure their own chains. Since all state transitions in Parachains are verified by the Validators in the central Relay Chain, a Parachain with a weak security model can still be secure. For the purpose of this paper, we will analyze Polkadot's shared security model [5] and compute the security coefficient for it.

The Polkadot network is not live yet, so the economic model described in this paper is derived from [this and this]. For this model, we assume the following:

- Validators didn't stake their personal DOTs, but were staked only by Nominators.
- Validators are equally staked since Polkadot encourages *fair representation* of Nominators.

- When a Validator is penalized for not keeping the uptime or for malicious behaviors, the entire pool gets slashed.
- According to [5], collusion among Validators results in 100% of the stake slashed.

Parameters	At launch	At maturity (Numbers marked with * are estimates)
Total DOT supply (T)	**10,000,000**	**10,000,000**
Staking rate (sr)	50%	75%*
Total DOTs staked (S) = T * sr	**5,000,000**	**7,500,000***
inflation rate % (i)	10%	2.75%
Number of Validators (N)	60* (from "Each validator will get 1,000 - 2,000 DOTs per month)	500*
Validator pool size in DOTs (Pv) = S / N	83,333	15,000
Annual Validator pool reward (R) = (T x i) / N	**16,667**	**550**
Commission fees charged by Validators (c)	5%*	5%*
Annual Validator net reward (R * c)	833	27.5
Penalty[3] for collusion among Validators	100%	100%
Number of Validators elected for verifying state transitions in a Parachain (Vs)	22*	55*
Number of Validators colluding to pose security risks (Vc) = ⅔ Vs +1	15	37
Economic incentives for good behavior (I) = R x Vs	**366,666**	**30,250**
Security deposit (Sd) = Vc x Pv	**1,250,000** **$211,687,500** at $169.35 per DOT (IOU)	**555,000** **$93,989,250** at $169.35 per DOT (IOU)
Security coefficient (**Sc**) = I / Sd	**0.2933**	**0.0545**

Table 1 — Polkadot security coefficient computation

Observations

1. The security coefficient at launch is fairly high, although in absolute costs, the cost of attack is also high. At maturity, the network's security improves significantly.
2. The security coefficient works differently in PoS networks compared to their PoW counterparts. The penalty for misbehavior, if sufficiently large and properly enforced, can greatly improve the security of the network.
3. In PoW networks the security deposit is dependent on the hashrate and difficulty. In PoS network the security deposit is proportional to the total size of the tokens staked. If a PoS network launches with a lower percentage of the total token supply, the security at launch will be lower too. For example, if Polkadot launches with a staking rate of 30%, the security coefficient will raise to **0.600**.
4. In PoW networks the security coefficient represents short term attack possibilities when the conditions are right. In PoS networks, since a single critical attack can result in slashing, there is no lower threshold for short term attacks.
5. A smaller PoS network has similar vulnerabilities as a smaller PoW network because of a smaller security deposit.

Security in Cosmos Hub (ATOM)

The Cosmos Network is a PoS-based *internet of blockchains*. It uses Tendermint[8] Byzantine Fault Tolerant (BFT) consensus algorithm, which tolerates up to 1/3 of machines fail in arbitrary ways. The Cosmos Network supports interoperability of blockchains using the Inter Blockchain Communication (IBC) protocol, which allows blockchains to interact with other blockchains. The blockchains are connected in a hub and spoke model to the Cosmos Hub. The spokes of the network — the independent blockchains — are called Zones, as illustrated in fig. 4 below. The Cosmos Hub is secured by Validators, similar to Validators in the Polkadot Network. The Validators are delegated by ATOM holders, similar to Nominators in the Polkadot Network. The Cosmos Network was launched with 100 Validators and at maturity, it is expected to run 300 Validators.

In this paper, we analyze the security coefficient for the Cosmos Hub.

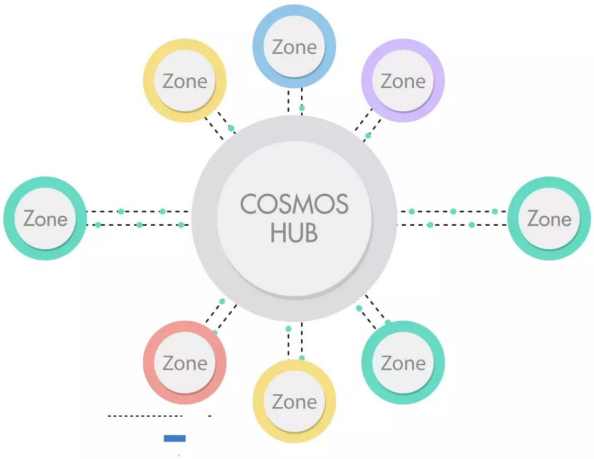


Fig. 4 — Cosmos network consisting of Zones and Hubs [9]

An attack on the Cosmos Hub requires more than ⅔ of Validators to collude. The path to recovery is to slash those who are responsible for equivocation via a chain reorganization. So, the cost of attack on the Cosmos Hub is the ATOMs slashed for the colluding Validators. Table 2 illustrates the economic incentive and the security budget data[10] to calculate the security coefficient for the Cosmos Hub.

Parameters	Now	At maturity (On 10th year. All numbers are estimates)
Rate of inflation [10] — 7% - 20%	7.2%	7.0%
Total circulating supply (Tc)	193,611,046	329,138,778
Number of elected Validators (N)	**100**	**300**
Engaged balance of elected Validators [from this] (Tb) and % engagement of elected Validators	**170,766,033** and **88.2%**	**290,300,402** (same % engagement assumed)
Estimated annual blocks at average block time of **6.892 seconds** [from this and this] (B)	4,575,740	4,575,740
Estimated annual block reward at **3.81 ATOMs** per block (R) = B x 3.81	**17,433,569**	**17,433,569**
Penalty for collusion among Validators	100%	100%
% of Validators colluding to pose security risks (Vc) = (⅔ N +1) / N	67%	67%
Security deposit (Sd) = Vc x Tb	170,766,033 x 67% = **114,413,242** ATOMs (**$655,587,877** at average	290,300,402 x 67% = **194,501,269** ATOMs

	price of $5.73 per ATOM)	
Security coefficient **(Sc)** = R / Sd	**0.1523**	**0.0896**

Table 2 — Security coefficient computation for the Cosmos Hub

The security coefficient of the Cosmos Network at the time of this writing is much superior to the security coefficient of the Polkadot Network at launch. As in the Polkadot Network, the security coefficient at maturity is superior, assuming the conditions illustrated in table 2.

Observations

1. The security coefficient at launch is higher than the long term value, although in absolute costs, the cost of attack is also high. At maturity, the network's security improves significantly.
2. When a Validator is slashed for misbehavior, the delegators who voted for the Validator lose their stakes proportionally. This behavior is similar to Nominators losing their stakes in the Polkadot Network.

Security in EOS

EOS is a Delegated Proof-of-Stake (DPoS) network with 21 top block producers responsible for creating blocks on the EOS.IO blockchain. EOS token holders delegate their votes to elect the block producers. Transactions are considered *finalized*, if 15 of the 21 block producers confirm the transactions. We are unable to find any information on slashing or other punitive measures when block producers engage in malicious activities, such as collusion. For that reason, we are unable to calculate the security coefficient for EOS and hence its security characteristics are undefined.

Security in Storecoin (STORE)

Storecoin [11] is a zero-fee payments and p2p cloud computing public blockchain that will transform data into money (into *datacoins*). The project is still in research and development. Storecoin is a PoS network with a two-tier network architecture — a compute and validation tier and a storage and consensus tier. The nodes on the compute tier are called Validators and the nodes on the consensus tier are called Messagenodes. Fig. 5 illustrates the Storecoin network.

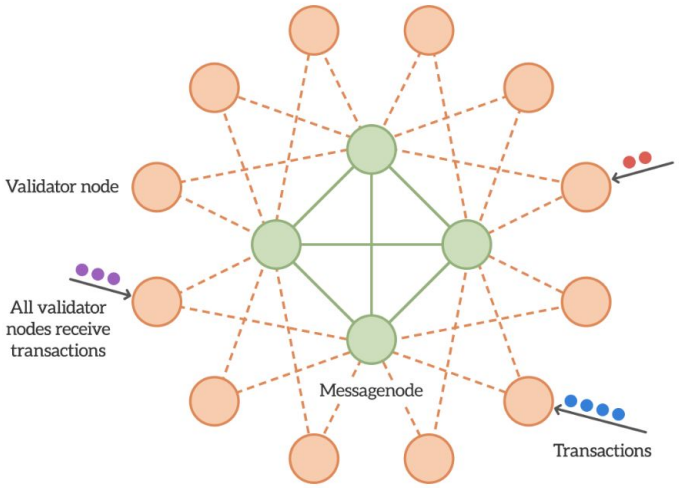


Fig. 5 — Storecoin's two-tier network of Validators and Messagenodes

The Storecoin network is divided into a set of *Cloud Markets*, where each market hosts one or more tokenized apps — apps that structure, label, and tokenize their data for better discoverability and trading, while preserving data privacy and security. The cloud markets also provide specialized services catering to the needs of the apps. Each market consists of a subset of Validators and Messagenodes from the Storecoin network. This is in contrast to the Polkadot network discussed above, where Parachains and the Relay Chain are independent of each other, except for the shared security responsibilities. In addition, settlement transactions, such as the base layer payment transactions are validated and secured by all the Validators and the Messagenodes in the Storecoin network. So, the security budget and the security coefficient are computed on the whole network instead of scoping to the cloud markets.

Table 3 illustrates the economic incentive and the security budget data for the Storecoin network.

Parameters	At launch (Q2 2020) (2-3 cloud markets)	At maturity (Q1 2022) (10-15 cloud markets)
Number of Validators (Nv)	70	253
Number of Messagenodes (Nm)	22	82
Total STORE supply (T)	1,000,000,000	1,000,000,000
Estimated circulating supply of STORE (Ts)	560,000,000	730,000,000
% of total STORE supply emitted as annual inflation towards the block reward (i)	2.00%	2.00%

Inflationary block reward (# of STORE) R = T x i	**20,000,000**	**20,000,000**
% of the block reward earned by Validators and Messagenodes (rp)	93%	93%
Annual block reward earned by Validators and Messagenodes (Re) = R x rp	**18,600,000**	**18,600,000**
Expected average stake per Validator (Vs)	750,000	750,000
Expected average stake per Messagenode (Ms)	2,000,000	2,000,000
Total STORE tokens staked (S)	70 x 750,000 + 22 x 2,000,000 = **96,500,000**	253 x 750,000 + 82 x 2,000,000 = **353,750,000**
Penalty for collusion to attack the network (% of the tokens staked)	100%	100%
Minimum nodes required to collude to attack Storecoin = 67% of Validators + 67% Messagenodes	47 Validators 15 Messagenodes	170 Validators 55 Messagenodes
Penalty for collusion (Pc)	47 x 750,000 + 15 x 2,000,000 = 65,250,000	170 x 750,000 + 55 x 2,000,000 = 237,500,000
Security coefficient computed based on slashing. Sc' = Re/ Pc	**0.2850**	**0.0783**

Table 3 — Storecoin's security coefficient calculated based on the cost of attack

The security coefficient is higher at launch than at maturity. This pattern is common across many PoS networks. Storecoin doesn't allow nomination or delegation as in Polkadot and Cosmos networks. So, when Validators and Messagenodes are slashed for misbehavior, only the entities behind them lose their staking.

Observations

1. The security coefficient at launch and maturity follows similar pattern of Polkadot and Cosmos networks — high at launch and goes low at maturity.
2. The security coefficient is calculated for the whole network. This means, the whole network must be attacked. This is in contrast to the attack on the Hub in the Cosmos Network or the Relay Chain in the Polkadot Network.

Conclusions

In this paper, we introduced security coefficient, which is the ratio of incentives in the network and the security budget. The lower this ratio, the more secure the network at steady state from short term attacks. Table 4 summarizes the security coefficients for various networks discussed in this paper.

Network	Security coefficient now or at launch	Security coefficient at maturity
Bitcoin	**0.8052**	N/A
Bitcoin Cash	**1.0837** **50.0911** (when the chain was reorganized recently [3])	N/A
Ethereum	**0.9506**	N/A
Ethereum Classic	**1.0387** **4.883** (when the chain was reorganized recently [7])	N/A
Polkadot (Relay Chain)	**0.2933**	**0.0545**
Cosmos (Hub)	**0.1523**	**0.0896**
EOS	**Undefined**	**Undefined**
Storecoin	**0.2850**	**0.0783**

Table 4 — Security coefficient comparison

Assigning a numeric score on the security helps with comparing various networks, each of which has different economic incentives and security budgets. For example, PoW networks use hashrate and difficulty as the security budget whereas PoS networks have the security budget calculated based on how nodes are penalized for attempting to attack the network. However, a numeric score, by itself, will not be sufficient to model short term threats. We can observe the following in the above models.

1. In PoW networks, short term incentives exist where a 51% attack is profitable despite high long term cost of attacks. We demonstrated this possibility with recent attacks on Bitcoin Cash and Ethereum Classic networks.
2. When a Validator in Polkadot pool gets slashed, all Nominators, who backed that Validator will also be punished. So, there is a *social effect* to slashing, which tends to increase the overall security of the network. The same is true with the Cosmos Network.
3. When a Validator or a Messagenode in Storecoin gets slashed, the tokenized apps and its users hosted on the cloud market get affected. This is a different kind of social effect, but its effect on improving the overall security of the network is the same.
4. PoS networks don't differentiate between short term and long term incentives to attack the network. The cost of both types of attacks are the same.

References

1. Double spending — https://en.wikipedia.org/wiki/Double-spending
2. Cost of PoW 51% attack — https://www.crypto51.app/
3. BCH 51% attack — https://www.coindesk.com/bitcoin-cash-miners-undo-attackers-transactions-with-51-attack and https://blog.bitmex.com/the-bitcoin-cash-hardfork-three-interrelated-incidents/
4. Polkadot Nominated Proof-of-Stake — https://medium.com/web3foundation/how-nominated-proof-of-stake-will-work-in-polkadot-377d70c6bd43
5. Polkadot shared security model — https://wiki.polkadot.network/en/latest/polkadot/learn/security/ and https://docs.google.com/spreadsheets/d/1-9Hc3kZ23EhZC3X6feRUKSTv6gj4xR7cvUbJD2zUEZk/edit#gid=0
6. Bitcoin security in one chart — https://medium.com/coinmonks/bitcoin-security-in-one-chart-694ee3ed8c2d
7. Deep chain reorganization in Ethereum Classic — https://blog.coinbase.com/ethereum-classic-etc-is-currently-being-51-attacked-33be13ce32de
8. Tendermint consensus algorithm — https://tendermint.com/docs/introduction/introduction.html
9. Blockchain Interoperability: Cosmos vs. Polkadot — https://medium.com/@davekaj/blockchain-interoperability-cosmos-vs-polkadot-48097d54d2e2
10. Cosmos statistics — https://stakingrewards.com/asset/atom
11. Storecoin p2p cloud computing platform — https://storecoin.com/cloud