phemex
Student Papers

Avalanche: A Novel Solution To The Blockchain Trilema

Shubh Patni
Northeastern University

Introduction

The advent and growth of smart contract platforms have transformed the cryptocurrency industry. The conversation has shifted from crypto as just a monetary system to it being the next Internet. Even Bitcoin, which was originally supposed to facilitate transactions can now run smart contracts on layer-2 using technologies like Stacks and Sovryn. Despite the unprecedented growth of the whole market from a few billion dollars to a peak of about $2.8 trillion, we're far from the future CryptoPunks envisioned – a future where all applications are decentralized, fair, and accessible to everyone. To get there, developers and crypto entrepreneurs need to solve the blockchain trilemma.

The blockchain trilemma is a set of problems that all blockchain networks face i.e., scalability, security, and decentralization. All networks that exist today are forced to make a trade-off between these three factors and thus cannot create a true trustless and open-source network that can reach the mainstream without compromising on decentralization.

But there's one network that's seeking to solve these issues – Avalanche. Avalanche boasts of a very simplified and unique consensus mechanism (the Snowman Protocol) that claims to have figured out the blockchain trilemma. In addition, Avalanche has three main chains to distribute the workload and make the network more efficient.

In 2021, Avalanche came into the spotlight when it outperformed almost all major cryptocurrencies and grew by over 1,500% in just four months. This price boom was in tandem with a growth in development. According to Electric Capital, the number of developers in the Avalanche ecosystem grew 3x. So with this amazing performance, a new question has arisen – can Avalanche be a potential "Ethereum killer?"

To answer this question, this research will analyze the Snowman consensus protocol and evaluate the questions around Avalanche's decentralization, scalability, ecosystem growth, tokenomics, and many sub-categories within each of these fields. The goal of this paper is to provide as much data as possible to users, developers, researchers, and investors interested in Avalanche, to summarize the project's value thesis, and to make predictions on its future.

The Blockchain Trilemma

Scalability

Scalability is the key necessity any public blockchain network needs to gain mainstream adoption. It's an umbrella term used to evaluate a blockchain's performance as it scales to more users and use cases, as well as provides support for more applications to be built on top of it. An ideal network should become more scalable as more users adopt it. This is because more users mean more computers, which translates to more network resources.

However, in Proof-of-Work (PoW) systems such as Bitcoin, there are two categories of nodes: miners and validators. The PoW consensus protocol used by Bitcoin makes it very easy to validate transactions but very hard to create new transactions. Thus, miners are rewarded to run the system but validators do not get any incentive other than a sense of security and assurance. This is a scalability issue because not everyone is willing to store over 300GB of data (which would only grow over time) for no monetary incentive. This is the reason why people reference block size battles and talk about the Bitcoin network as a layer-1 that's only used for transactions.

More or less, the same problem exists with the current version of Ethereum, except it's Turing Complete with different tokenomics and a much wider ecosystem. Other networks like Solana, Polkadot, and Cosmos, currently make a tradeoff in terms of the blockchain trilemma. Let's see how Avalanche handles this problem.

TPS: TPS is used as the most common indicator of scalability (but it's not the only or most essential one). Visa's transaction speed is often used as a benchmark to compare these networks, but this comparison isn't perfect nor fully relevant since most blockchains these days handle more complicated data.

Avalanche claims to have infinite transactions per second since there are many subnets and each can process 4,500 transactions. So if an individual needs more TPS, they can spin up another subnet and achieve higher throughput.

At this point, no other blockchain claims to scale to infinite transactions per second. The only network that comes close to it with a comparable market cap is Cardano's Ouroboros Hydra with one million TPS.

Finality: Finality is the time it takes to confirm a transaction. The Bitcoin network can do around seven transactions per second but it takes anywhere from 30 to 60 minutes for a transaction to be confirmed. For Ethereum it's six minutes, for Polkadot it's 60 seconds, for Solana it's around 13 seconds, for Cosmos it's seven seconds, and a few days for traditional finance. Technically, finality is probabilistic and never certain i.e., a transaction can always be reverted, but the probability of such an event occurring reduces with increasing block confirmation. Avalanche provides sub-two second finality which is unheard of in the industry.

Interoperability: Interoperability is often overlooked when talking about scalability, but it's a key component since there wouldn't be a single blockchain network that would rule and it's important to communicate with other blockchains as well as off-chain sources.

Ethereum being the most used smart contract platform has become a hub for developers and most projects and large protocols on the blockchain. Projects can communicate with this huge ecosystem if they make their application EVM-compatible. Unfortunately, Solana is not yet EVM compatible whereas Avalanche can have many subnets with Ethereum compatibility.

Pruning: Early blockchain platforms like Bitcoin and Ethereum require nodes to store the entire history of the blockchain, all the way back to genesis. For slow and only transaction-based systems like Bitcoin, this is somewhat manageable because of the improvements in storage hardware technology. But such a design simply won't suffice for a decentralized world computer like Avalanche, which it aspires to become.

Avalanche has three types of node clients: Archival, Full, and Light. Archival nodes store the whole history of the blockchain and they're incentivized by other nodes which may wish to download the old state. Full nodes store the current UTXO set and light nodes just perform repeated sampling of the protocol.

Sharding: Sharding is the process of partitioning a database into many chunks to improve the retrieval and storage of a huge dataset. In decentralized networks, this will improve the scalability by magnitudes since more nodes will be able to participate with low storage requirements. Many blockchain networks have tried to achieve some form of sharding – Polkadot, Cosmos, and Avalanche currently perform this through specialized subnetworks.

Storage: For a network that's trying to be a decentralized computer, it's essential to be able to store a limitless amount of data securely and efficiently. Ethereum struggles with storage because of limited block space and high demand, leading to gas wars. At its limit, Solana can generate 4PB data/year and it uses Arweave to archive petabytes of data.

Avalanche uses Bundlr and Arweave both to improve the retrievability of limitless data stored on Arweave. However, the storage is expensive at around $5 to $8/GB. This is definitely a limitation that hinders the development of huge applications. But compared to other decentralized networks, this is the best option out there (at the moment). Developers need to be smart about what data they want to store in decentralized networks since not everything has to be decentralized. In fact, most users wouldn't mind having certain data on centralized sources.

Security

Security is an essential part of a decentralized network, especially a network trying to be the world's next application platform with trillions of dollars invested in the protocol.

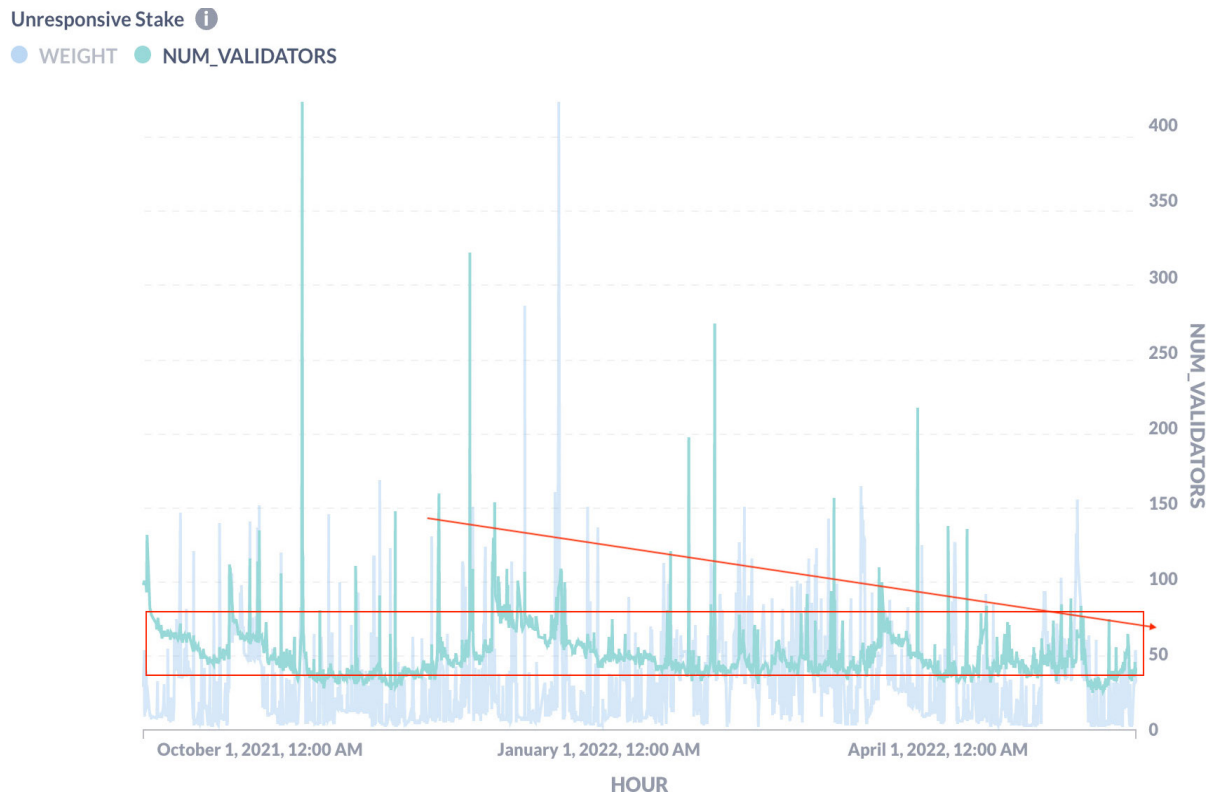
51% attack: The classical consensus model fails when there are f+1 attackers in the network and the Nakamoto consensus breaks down if 51% of the network hash power is controlled by an adversary. In contrast to both these primitive consensus mechanisms, Avalanche provides certain security variables that can be tweaked to handle a network with up to 80% adversaries, this would however compromise the liveness of the network.

Sybil Resistance: A Sybil attack occurs when a validator attains an unsafe amount of influence over the decentralized network. In PoW-based systems like Bitcoin, this is tackled through computing power. As the network grows, the required computing power to hack the system grows exponentially. For PoS-based systems, this is handled through native tokens on the network. In Avalanche, users must stake AVAX to validate the chain – the stake is locked for at least two weeks.

Unlike most other PoS systems like Ethereum 2.0, Polkadot, or Cosmos where validators are slashed for malicious or non-malicious downtime, Avalanche doesn't slash any stake, thus making it a safer and deterministic alternative.

Quantum Cryptography: Quantum computers can break some cryptography algorithms with ease which makes these systems a great adversary to a decentralized network. All blockchain platforms are working on quantum-resistant algorithms to be safe from quantum adversaries. Since Avalanche can handle any number of VMs, it can support a quantum-resistant VM with a suitable digital signature scheme.

Node Participation: Node participation is the number of live nodes at any given time. A high node participation makes the network less vulnerable to attacks. This metric can also be used to analyze the network's decentralization.



The graph above shows the number of inactive nodes since January 2021. For most of the time, this number seems to be range-bound between 30 to 70 nodes, and the peaks declining with time are visible, thus showing healthy growth in node participation. The decline can be due to the heavy development of subnets on Avalanche which is a good sign for network security.

Stake: The security of PoS systems like Avalanche is determined by the stake of the native token, in this case, AVAX. According to Staking Rewards, Avalanche is the

fourth highest staked cryptocurrency in terms of staked value in dollars with around 60% of its eligible tokens being staked. Ethereum sits in the first position with 10.2%, Solana is second with 73.3%, and Cardano is third with 71.6%.

Despite the constant downward movement in AVAX's price (similar to the whole market), the number of stakers is increasing. This is not the case with Ethereum, Solana, or Cardano. Growth in the number of stakers is a very good sign for Avalanche's security.

Decentralization

Decentralization is the process of transferring control/influence of a protocol, organization, or initiative from a few selected/special individuals or a group to everyone. Decentralization doesn't mean giving equal power to everyone, but rather creating a fair system anyone can use to gain more influence or power.

Decentralization and security, which often go hand in hand, should take more precedence over other factors – because, without decentralization, all of these ledger technologies are simply a very slow database on the Internet with 100x better-centralized alternatives.

Validators: Validators are the nodes that verify each transaction and update the state of the blockchain. The number of validators is correlated with the security and decentralization of the network since a larger number of validators means that a large portion of them have to be corrupt or vulnerable to attacks for the network to go down.

To maintain a high number of nodes or validators in the network, the requirements to become a validator need to be as low as possible. In PoW systems, the requirements are hardware-based, which is much harder to acquire now because of the semiconductor shortages worldwide. For PoS systems such as Ethereum 2.0 (the Beacon Chain at the moment), it's 32 ETH, and for Avalanche it's 2,000 AVAX.

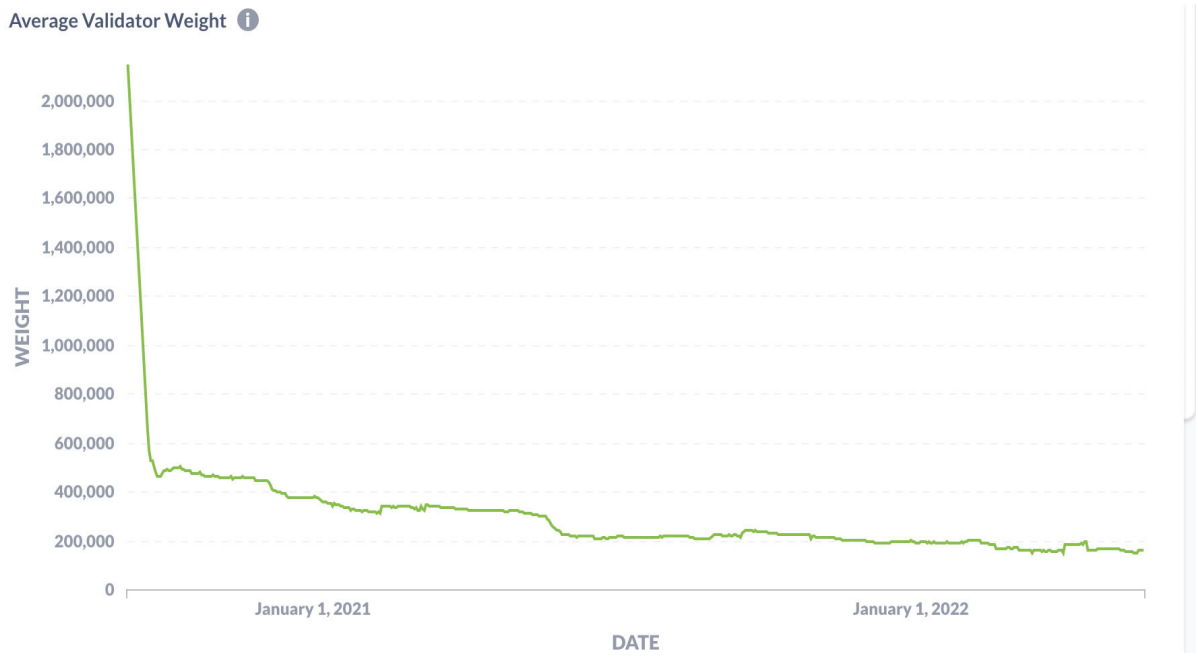
The current incentive to be a validator is 9.4%, which is higher than Ethereum, Solana, or Cardano. There are over 1,457 validators in the network.

In terms of hardware requirements for Avalanche, they vary based on the subnet a user wants to validate.

The number of validators on the Avalanche network has consistently grown. The downward price movement might affect the validator count, but the subnet incentive programs like Multiverse can be expected to offset the downward pressure. This is a

big positive for decentralization.

Average Validator Weight: Average Validator Weight is the average amount of AVAX staked by a validator. This number indicates how much money a validator is willing to lock to secure the network.



The average validator weight has been going down since the Avalanche network's inception. The growing number of validators is a good sign because it means more validators are joining the network and any individual node will not have a lot of power.

Delegators: Delegators provide their stake to the validators they trust to secure the network. The minimum delegation requirement is 25 AVAX with a 14-day lockup and participants don't need to run a node or need much technical know-how. This significantly lowers the barrier to securing the network. The current incentive to be a delegator is 8.95%.

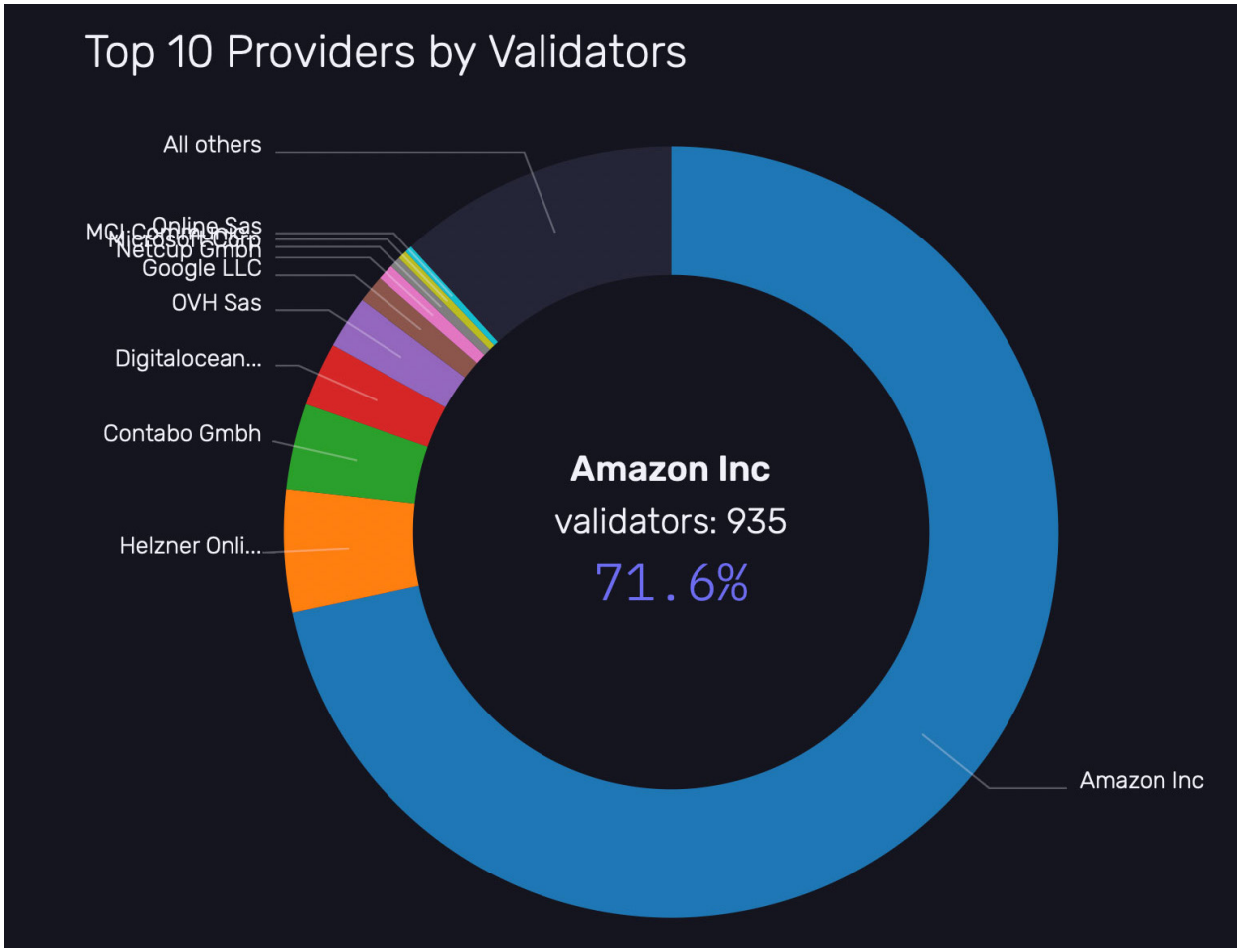
Despite the correction in price, the number of delegators has been increasing, which shows a healthy indication of the network's growth. There are over 21,800 delegators.

Nakamoto Coefficient: Nakamoto Coefficient is a concept that was introduced by Balaji Srinivasan. It essentially speaks to the number of nodes that can collude to compromise the network. Amongst the cryptocurrencies with over a $1 billion dollar market cap, Avalanche has the highest Nakamoto Coefficient of 27 – Solana has 19, Cosmos has 6, Ethereum has 3, while Polygon has just 2.

This makes Avalanche the most robust decentralized PoS system. With the launch of Ethereum v2, Ethereum will likely outperform this number since it'll have 150x more validators than Avalanche.

Cloud Centralization: Cloud services like AWS and Microsoft Azure are a huge point of failure for PoS systems. Many validators in all PoS systems, including AVAX and Ethereum rely on cloud services to properly function. These servers may shut down and authoritarian regimes can require them to stop providing services for DLT solutions. Thus, centralized servers can be a huge attack vector for Avalanche, hence, the team needs to work on creating incentives to mitigate this risk.

The graph below shows the distribution of nodes – over 71% nodes are in AWS.



The Team Behind Avalanche

Avalanche's fundamental protocols like its consensus mechanism were created by pseudonymous groups of cyberpunks called the "Team Rocket." Then, a group of professors and researchers from Cornell University took over the project and it's currently led by Emin Gun Sirer, a computer scientist and researcher. The project now comes under AVA labs and all of the code became open source in 2020.

Given the team's experience and the amount of in-depth research put into the whitepapers and code, Avalanche is likely to pass the test of time and be a serious contender in the layer-1 race.

How Does Avalanche Achieve Ground-Breaking Performance?

Avalanche's fundamental protocols like its consensus mechanism were created by So far this paper's analysis shows that Avalanche is very good at handling the blockchain trilemma. Next, the research will dive into the network's architecture to better understand how it achieves this performance.

The Consensus Protocol

At the core of any decentralized ledger technology is the consensus protocol. Consensus protocols are the set of rules that all nodes in the network follow to achieve agreement over the state of the network. This is necessary because millions of users are constantly sending data to the network and it's important for the network to know the succession of this data and whether such data or transactions are valid.

A few consensus protocols have existed throughout computing history like Classical consensus protocols and Nakamoto consensus in Bitcoin. Classical consensus like Tendermint and Practical Byzantine Fault Tolerance (PBFT) are very fast but require all nodes to vote for every state transition. This means that as the network grows in size, the communication overload explodes exponentially and there's a huge tradeoff between decentralization and scalability.

This problem was addressed by the Nakamoto consensus in the Bitcoin network. Any number of participants can join the network and the PoW works as a Sybil resistant mechanism, and combined with the longest chain rule, provides security. However, in this setting, the consensus is probabilistic and requires unnecessary mathematical computations. This means to be certain a transaction occurred, one must wait around 60 minutes. This isn't scalable for many applications.

Team Rocket introduced a new family of consensus protocols called Avalanche consensus protocols that try to solve this problem. The current implementation of consensus in the Avalanche network is called the Snowball++ consensus protocol.

Snowball Consensus

The Snowball consensus protocol is probably the most straightforward protocol to understand. For example, say there are n nodes in the network, and out of these n nodes, f of them are attackers. For each transaction, the network needs to reach a consensus, and f nodes may try to tamper with these transactions. For simplicity, let's assume there are only two possible states for the network – Black or Blue and the network must decide which one is correct.

Each node in the network talks to the k number of nodes randomly and asks them for their state. If the majority of them say they believe the Blue transaction is correct, the node gains more confidence in Blue, and if this confidence value exceeds some number A, the node changes its state. This process is repeated until the whole network agrees on a state which takes less than two seconds.

Subnets

Avalanche allows anyone to create their own blockchain with their own rules on top of the Avalanche network. These customizable, application-specific blockchains are called subnetworks. Subnetworks are a dynamic set of validators that work together to arrive at a consensus on the state of the blockchain. A validator can be a member of many subnets and any number of subnets can be created. A subnet can process thousands of transactions per second and can communicate with the main Avalanche network or other subnets if it wishes to. To do so, the user can connect with the Avalanche P chain and communicate with the rest of the network.

Why Create A Subnet?

The problem with existing blockchain networks is that they assume that their architecture is sufficient to support all kinds of applications, which is not true. Some applications require more speed, some need more storage, some need to be private, and much more. The system requirements of validators and other parameters in existing blockchain networks make it impossible to address all possible applications. For example, a game on top of Ethereum is very expensive and slow, but if we had a subnetwork where system requirements of validators were set in a way to support the game, this wouldn't be a problem.

Creating Modular Blockchains With Subnets

- Anyone can create a subnetwork by staking AVAX

- This blockchain can have its own token with its own tokenomics and fees
- It can have its own consensus mechanism
- System requirements of validators can differ from the main network to support specific applications
- Reduces network traffic since only validators that are interested in running that application would choose to be the member or validator
- Allows the creation of private blockchains
- Can add regulatory requirements or KYC for validators to join a subnet

A subnet can process thousands of transactions per second and can communicate with the main Avalanche network or other subnets if it wishes to. To do so, you can connect with the Avalanche P chain and communicate with the rest of the network.

Subnet Use Cases

- Application-specific subnets, for example - a subnet for DeFi, NFTs, Gaming, etc.
- Handle IoT operations over smart contracts, for example - a parking meter or washing machine that has smart contracts so you can pay for the service in real-time and everything is handled on-chain.
- Subnets that specialize in handling legal contracts for lands, apartments, nations, etc. A landlord can create a subnet and store all the transactions/smart contracts for the residents. So if a tenant doesn't pay the rent over the smart contract, electricity or water automatically stops for that resident.

Three Chains To Break The Trilemma

Avalanche is built with scalability and interoperability in mind. To achieve groundbreaking speed, everything in Avalanche is based on subnetworks and its primary network has three chains called Platform Chain (P-chain), Contract chain (C-Chain), and Exchange Chain (X-Chain)

P Chain

Platform chain is used to create subsets or add validators to subnets. It's the metadata blockchain on Avalanche that keeps track of all the active subnets. Existing subnets use P Chain to communicate with other subnets in the network or the main Avalanche network. It uses the Snowman consensus protocol.

Contract Chain

The Contract chain is the smart contract chain on Avalanche. On this chain, developers can create and deploy their EVM-compatible smart contracts and run DApps.

Exchange Chain

The Exchange chain is used to create and transfer assets or tokens. This chain uses Avalanche consensus protocol with PoS to create AVAX tokens. This chain is an instance of Avalanche Virtual Machine (AVM) and uses DAG architecture.

Virtual Machine

Each blockchain on Avalanche is an instance of AVM, which is similar to an object of a class in an object-oriented programming language. The virtual machine comes with some predefined properties such as:

- The contents of a block
- The state transition that occurs when a block is accepted
- The APIs exposed by the blockchain and their endpoints
- The data that is persisted on the disk

DAG

Unlike most decentralized networks where the primary layer is a blockchain, in the case of Avalanche, the X Chain is a DAG. DAG stands for directed acyclic graphs that have a tree-like branched unidirectional structure. This is similar to the blockchain which also goes from one block to another, but the key difference is that a vertex can have multiple children. In a blockchain, a block only has a child i.e., the next block.

This design choice allows for the parallel processing of transactions since validators are not competing for the next block, as in the case of blockchain. This architecture works best with the Snowball consensus protocol to validate transactions.

Avalanche's Tokenomics

Tokenomics is one of the most crucial metrics to evaluate the fairness and value of a cryptocurrency. The supply of the token and how it's to be distributed amongst various stakeholders, to some extent, writes the faith of how successful the project will be. Even if a project has cutting-edge technology and is very useful, if its token distribution seems centralized, people won't buy the token and use it. Let's explore a few key tokenomics of Avalanche.

- The rewards given to validators are proportional to their stake and staking period
- Validators are incentivized for correct behavior and more uptime
- AVAX has a maximum capped supply of 720 Million tokens
- Unlike most networks, all transaction fees on Avalanche are burned
- Avalanche's circulating supply is around 270 Million AVAX
- There's no slashing of staked AVAX
- The current ROI for staking is 9.4%
- The minimum amount that a validator must stake is 2,000 AVAX
- The minimum amount that a delegator must delegate is 25 AVAX
- The minimum amount of time one can stake funds for validation is 2 weeks
- The maximum amount of time one can stake funds for validation is 1 year
- The minimum amount of time one can stake funds for delegation is 2 weeks
- The maximum amount of time one can stake funds for delegation is 1 year
- The minimum delegation fee rate is 2%
- The maximum weight of a validator (their own stake + stake delegated to them) is the minimum of 3 million AVAX and five times the amount the validator staked. For example, if one staked 2,000 AVAX to become a validator, only 8,000 AVAX can be delegated to the node in total.

The purpose of a token in a decentralized system is to create an economic incentive wheel to make the system run on its own through decentralized governance. The governance in Avalanche can change the tokenomics with time to address economic challenges that might arise in the future or to create a better economic system. The reward rate however has boundaries to make sure that governance doesn't choose parameters that benefit certain groups of people more than others.

Tokenomic governance has a cool feature to prevent drastic economic changes. There are time and range limits associated with each governable parameter. So

a certain time must pass to pass any change for that parameter and it cannot be outside of certain bounds. This is done to make the system more predictable.

The minting mechanism in Avalanche prevents the “rich from getting richer,” which is the case with most existing PoS blockchain networks. Each node in the network stores the proof of uptime and responsiveness as a tuple of nodes it has interacted with. These two values are used to calculate the reward for that validator.

Transaction fees in Avalanche vary based on the type of transaction or network activity. Below is a table that represents this information.

Chain	Transaction Type	Transaction Fee (AVAX)
P	Create Subnet	1
P	Create Blockchain	1
P	Add Validator	0
P	Add Delegator	0
P	Import AVAX	0.001
P	Export AVAX	0.001
X	Send	0.001
X	Create Asset	0.01
X	Mint Asset	0.001
X	Import AVAX	0.001
X	Export AVAX	0.001
C	Simple send	>= 0.001575*

(*) C-Chain gas price varies. See below.

Transaction Tiers

Unlike most networks where all transactions are made possible through a fee

incentive structure, Avalanche provides a novel transaction tiers approach where an address receives certain free transactions which they can choose to use. After this tier runs out, they need to pay the transaction fee. In the future implementation of the protocol, users may be able to pay in the form of computational resources through PoW for the transaction, instead of paying in coins.

Spam Management

Fees in Avalanche for transactions are virtually negligible. This can lead to spammers trying to congest the network. To prevent such a scenario, in the future, the Avalanche network will also implement a PoW mechanism which won't be very difficult. However, if a certain address creates a lot of transactions, each consecutive transaction may require a more difficult PoW, thus preventing network congestion.

Token Distribution

The total supply of AVAX is fixed at 720 million tokens. 50%, or 360 million tokens were initially minted at the genesis and sold to private and public investors. The other 50% will be rewarded over time to the stakers through staking.

No matter how good the technology is, if the tokenomics are not set right, the token won't retain value. Chainlink is a prime example. It's the backbone of most blockchain solutions, yet not performing well in terms of price action because it's a utility token and tokenomics are not designed to make it a good store of value.

There are a few key ingredients to make a token retain value over time, which will be discussed below.

Supply

To evaluate the supply side of the equation, a few questions must be asked:

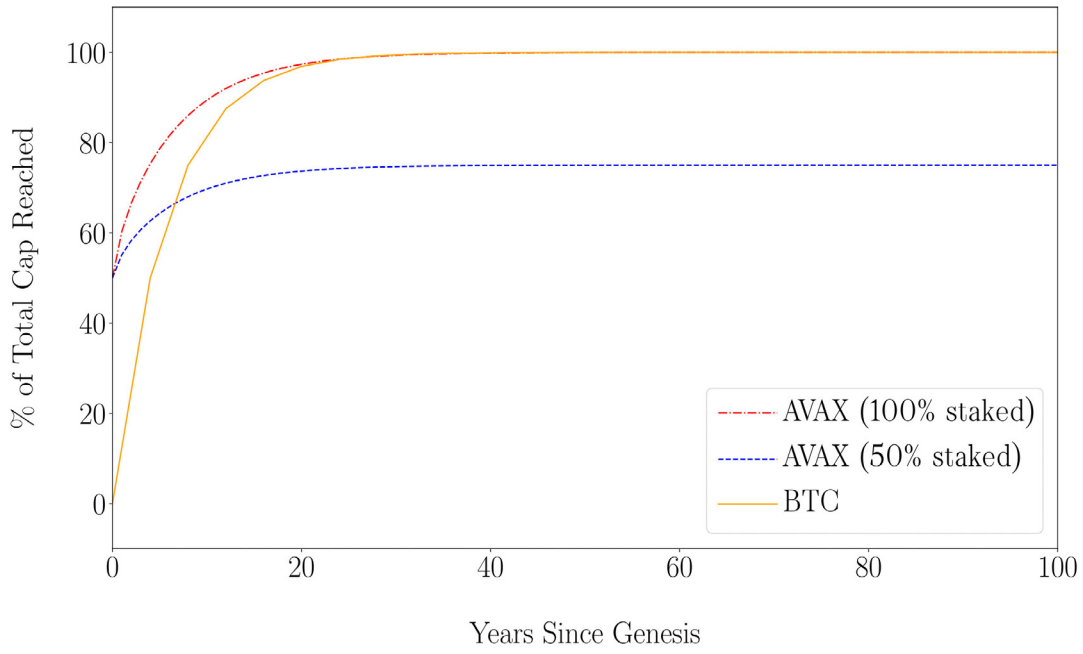
- How many tokens exist right now?
- How many will ever exist?
- How will it get there?

For Avalanche, there are 592 million tokens in circulation (counting the staked tokens). There will be 720 million tokens in total and these will come into circulation through staking rewards. According to the rewards schedule, if 100% of the tokens are staked

for a whole year, most of the supply will be minted in around 25 years, which is by around 2046. However, this will not be the case since Avalanche is a utility token and thus not all of it will be staked.

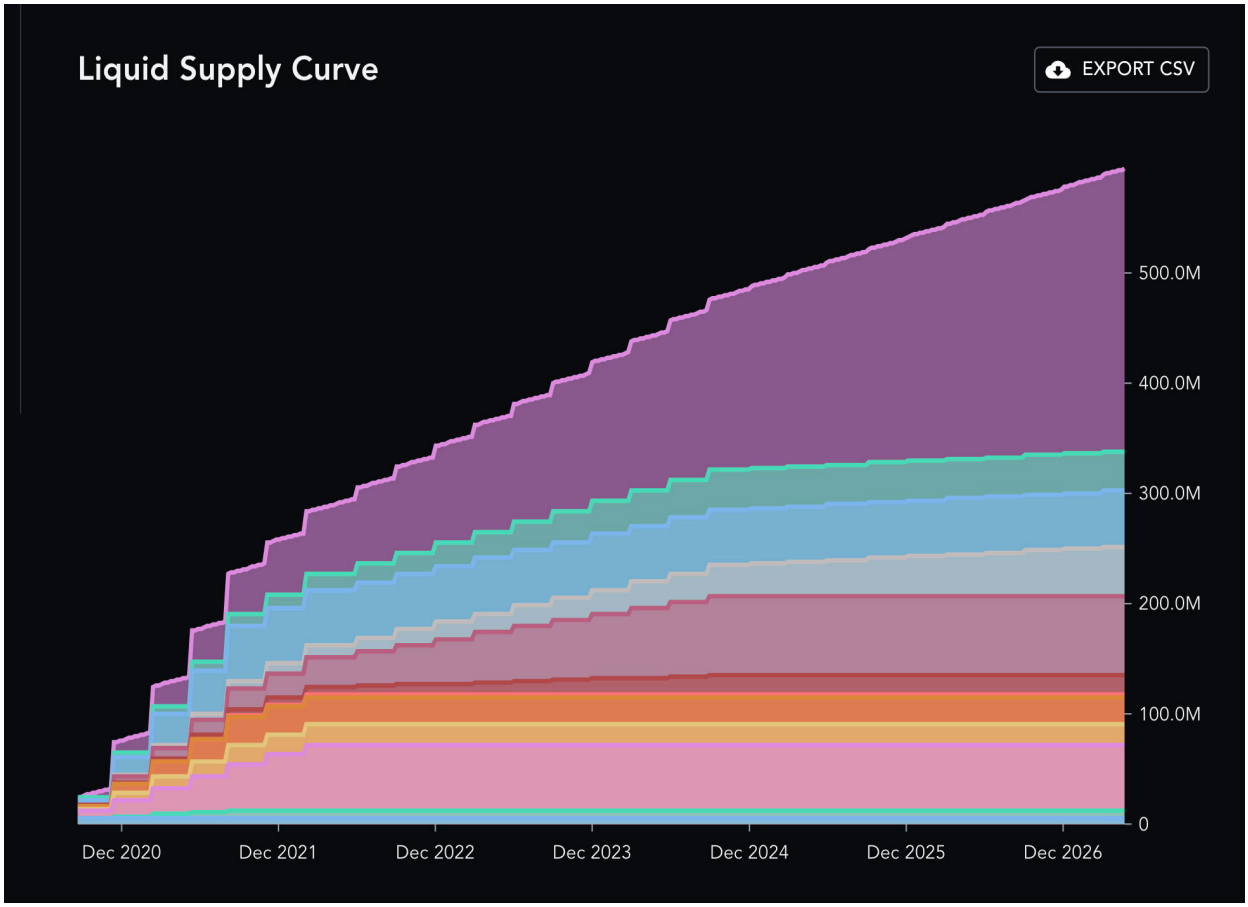
There are two other governable parameters in the network to tweak the staking rewards and influence the supply of tokens. Assuming that these parameters stay constant, and given the average engaged staking of around 60% of tokens, the supply schedule will be closer to the blue line in the graph below.

This is a good sign because it makes AVAX less inflationary than Bitcoin over the medium and long term. Moreover, the deflationary mechanism of burning fees will benefit all holders.



Vesting Schedule: 360 million AVAX tokens were minted at launch and sold through public and private sales. These early investors got AVAX for much cheaper than the rest of the market and thus are much more likely to sell and reap the rewards when their vesting period ends.

According to the vesting schedule below, in the near future, around 6.5% of existing tokens will be released every quarter. So to sustain the value of AVAX, Avalanche must grow by 6.5% every quarter.



Demand

AVAX has three main use cases that make up its total market demand: staking, subnets, and transaction fees.

Staking: Avalanche offers one of the best staking rates among the high market cap coins and there's no slashing, which makes it a much safer investment than its alternatives like Polkadot, which has brutal slashing.

Subnets: Subnets allow anyone to spin up their own blockchain with minimal effort and use the security of Avalanche in the base layer. Popular applications like DeFi Kingdoms and Crabada have launched their own subnets and reduced the load on the C Chain. Spinning up a subnetwork requires a set of validators and these validators need 2,000 AVAX. Subnets will increase the demand for AVAX

Transactions: Avalanche provides a much cheaper and more decentralized alternative (compared to Solana, BSC) to Ethereum. There are many popular games building on it and its $1 billion dollar ecosystem development fund should increase

the number of applications and demand for AVAX, all of which will be burned and thus good for the price of AVAX.

An Evaluation Of The Avalanche Ecosystem

The Avalanche ecosystem is rich with hundreds of applications. The sub-second finality, infinite transaction per second capacity, and compatibility with EVM and WASM make it a golden hub for developers. Avalanche allows anyone to create an application-specific blockchain written in Go, rather than Solidity, which has a much smaller developer base and a longer learning curve.

Ecosystem Growth Programs

Avalanche has many incentive programs to accelerate the growth of solutions on top of its chain. Over $770 million dollars is distributed into four different programs to target different markets that DLTs can disrupt.

Avalanche Multiverse

Avalanche Foundation recently launched its $290 million dollar incentive program called Avalanche Multiverse to boost the growth of its subnets. The program will springboard the development of new DeFi, GameFi, NFT, legal, private, and institutional platforms. DeFi Kingdoms, a very famous blockchain-based game along with Aave and Securitize are already part of this program.

Avalanche Rush

Avalanche Rush was launched in August 2020. It's a $180 million dollar liquidity mining incentive program to bring more DeFi projects into Avalanche. The blue-chip protocols of this program were Aave and Curve. For a period of three months, Aave and Curve users could farm AVAX as an LP token and the foundation plans to release more phases of this program to reach wider adoption.

Culture Catalyst Initiative

Culture Catalyst is a $100 million dollar incentive program that Avalanche launched with OP3N and Grimes. The project aims to fund growing NFT projects in music, gaming, and many other creative industries. Grimes will launch an "intergalactic children metaverse book" through this program and later Ava Max will release her music video.

Blizzard Fund

Blizzard is a venture capital and incubation fund worth $200 million dollars that will fund any early-stage application building on top of Avalanche. It can be DeFi, NFTs, social media apps, music platforms, games, or any new solution.

Notable Projects In The Avalanche Ecosystem

Securitize

Securitize is a leading digital asset securities firm and the first SEC-registered transfer agent. They've partnered with Avalanche to use the network and provide blockchain-based financial services. The long-term vision of Securitize is to digitize all the financial markets under legal compliance with SEC. With Avalanche, as of now, they're targeting the private capital market which raised over $2.9 trillion dollars in 2019. By 2023, this market is estimated to be worth around $14 trillion dollars.

Initial Litigation Offerings

ILO (or Initial Litigation Offerings) is a new $10 billion dollar asset class founded by Avalanche, Roche Cyrulnik Freedman LLP, and Republic Advisory Services. ILO is a blockchain-enabled litigation financing product open to anyone. It provides individuals, who may not have the means, with a financing option to fight for their case. Investors can invest in ILOs with an expectation of making a profit if the party they're supporting wins the case. Each ILO token represents a legal claim of winnings converted into a digital asset.

This industry was just recently created, therefore there is not enough data to

speculate how this may impact legal battles or who will invest in ILOs. However, it's exciting to see that Avalanche's technology enables the creation of such an industry that was never thought of or possible.

Pangolin

Pangolin is a UniSwap-like DEX built on top of Avalanche. Given Avalanche's groundbreaking performance, using Pangolin provides a similar experience to using a centralized exchange. Currently, Pangolin has $140 million dollars locked in its protocol and provides 114% APR for farming its LP token. However, the most unique thing about Pangolin is not its APR, but its tokenomics.

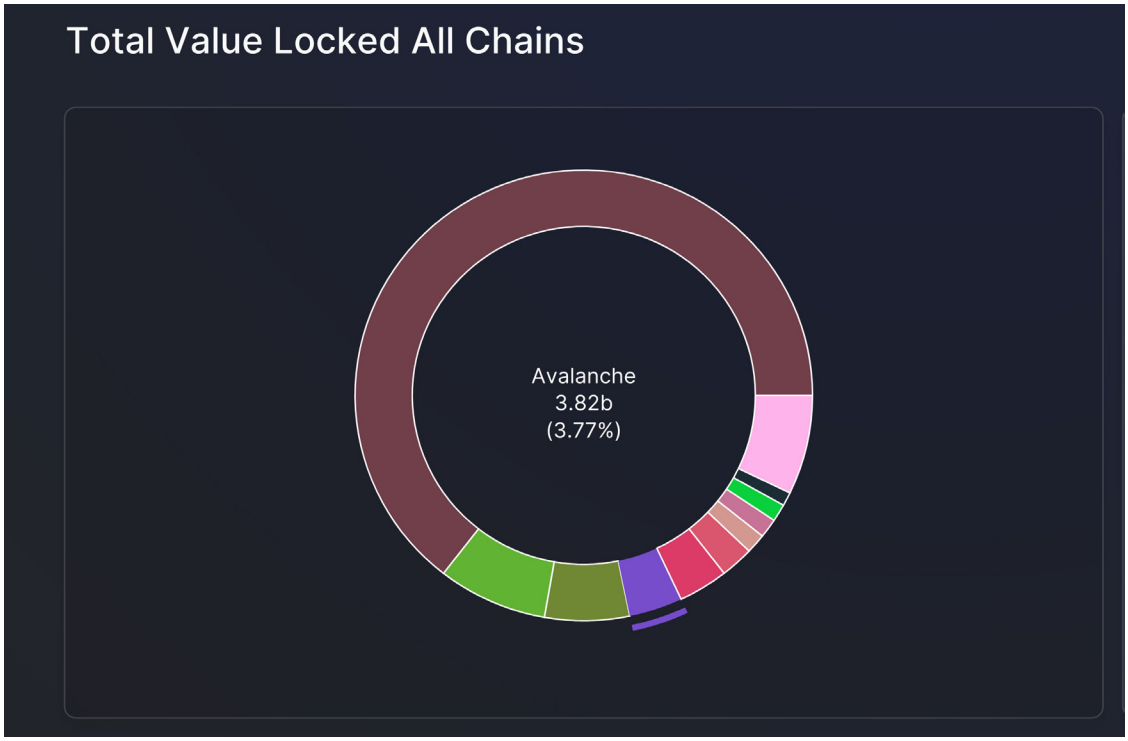
Unlike most other Defi projects, Pangolin's total supply is for the community. No tokens were allocated to the team, advisors, marketing, or anything. 5% of the supply was airdropped to the users and the rest 95% will eventually be minted through liquidity mining.

Gaming: DeFi Kingdoms & Crabada

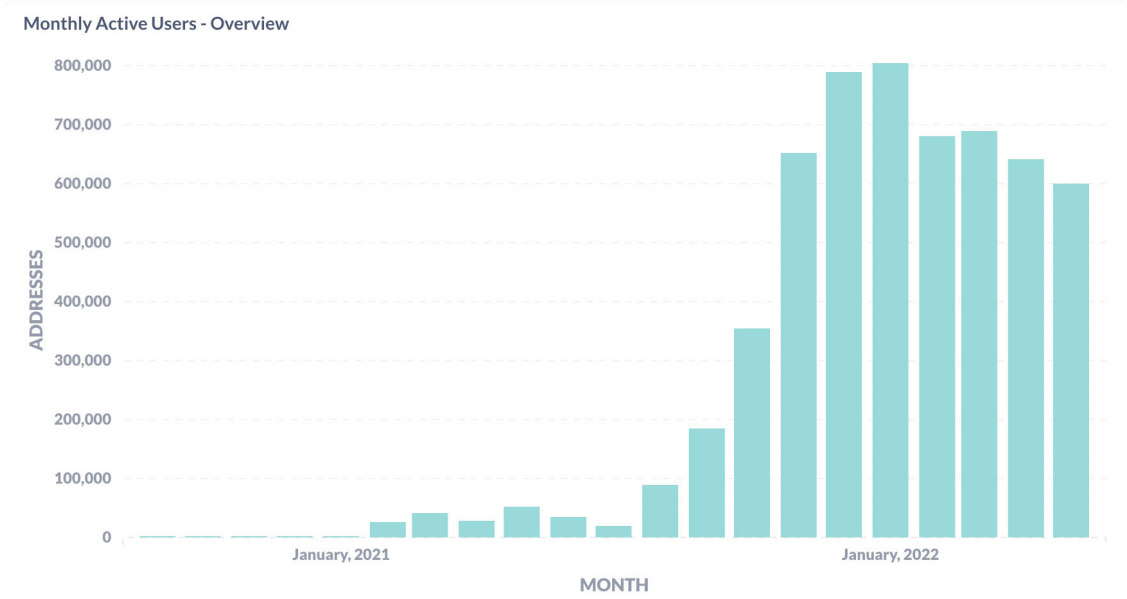
DeFi Kingdoms is one of the most popular games on Web3 which originally launched on Harmony. The game recently launched its subnet on Avalanche and it's called Crystalvale (with its own new token called Crystal). The launch of this subnet broke bridge volume records on Avalanche and set a new record of $330 million dollars. Crabada is another popular Web3 game that recently launched its Swimmer subnet on Avalanche. Both of these significant subnet launches have reduced the load on C Chain on Avalanche.

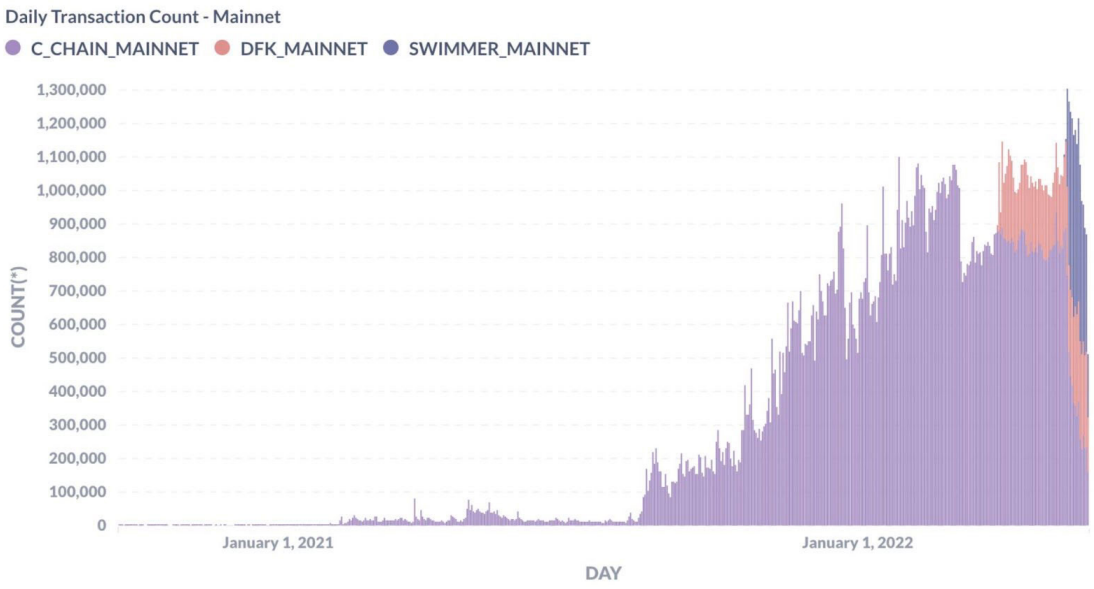
Stats

In terms of TVL, Avalanche is #4 with $4.08 billion dollars locked in its DeFi protocols. Tron, BSC, and Ethereum have $5.75 billion, $8.64 billion, and $67.63 billion respectively.



Despite the recent markevt downturn and Luna hit to Avalanche, monthly active users have held up really well, only decreasing by 25% from around 800,000 to 600,000. In fact, the daily transaction count reached an all-time high of 1.3 million thanks to the launch of the Swimmer subnet. Beyond the DeFi activity, the 24-hour NFT volume reached an all-time high beyond $1 million and the NFT market cap surpassed $110 million.





Developer Activity

According to a report by Electric Capital, released in January before the markets crashed,
developers in Avalanche grew 3x in 2021, compared to 2020. There are at least 300 active developers in the ecosystem. Avalanche is sixth on the list of fastest-growing ecosystems in terms of full-time monthly developers. Unlike Solana, Avalanche is EVM compatible and can have application-specific subnets which give it an advantage over the available talent pool. So these developers can develop on Avalanche or port their application running on Ethereum to Avalanche.

Analyst Commentary

Avalanche is one of the most innovative layer-1 solutions on the market. It's the only project to create a whole new consensus mechanism other than Bitcoin, which really says something about the team behind the project and the strength of the project. However, since it was launched much later than popular layer-1 solutions like Cardano, Ethereum, and Polkadot, it does not have the first-mover advantage and must work harder to create a community of active developers.

Avalanche has shown a commitment to grow the community by deploying over a

billion dollars towards the ecosystem. It's one of the few projects with a heavy focus on connecting traditional institutions to the blockchain. For example, it has partnered with Mastercard and is launching a whole new asset class called ILO. These partnerships give a real and measurable competitive advantage to Avalanche.

The network burns all the transaction fees, and eventually, all the tokens will be minted and the validators will not have any incentive to work. This is a common concern in the community and it's believed that the validators will drive the demand for AVAX since subnets need to create validators and validators must stake 2,000 AVAX. Moreover, a subnet can choose to take transaction fees in its own token. This is a good design for projects looking for customizable and scalable blockchain solutions.

Since Avalanche is EVM compatible and projects can create their own subnets, Avalanche can be treated as an Ethereum layer-2 as well as a layer-1 for projects that want to build their own blockchain on it.

Final Concerns

The initial mint was available to a few individuals who invested in the project with an expectation of profit and there was clearly a US-based entity promoting the project, AVA labs, thus there's a possibility that AVAX might be considered a security and face legal scrutiny.

Ethereum has the most engaged platform and is considered the most decentralized and fair network after Bitcoin. It has a flourishing L2 ecosystem and DeFi TVL in the L2 alone that surpasses Avalanche. However, even after the launch of Ethereum v2, it won't be able to kill Avalanche because of its flexible blockchain solution – but, Ethereum's L2 solutions can capture most on-chain activity and users. Thus, Ethereum's L2 solutions are a threat to Avalanche's growth in terms of users and value aggregation.

References

https://www.stakingrewards.com/?sort=totalValueLocked_DESC

https://medium.com/avalancheavax/arweave-broadens-decentralized-data-storage-capabilities-on-avalanche-898607e50e02

https://www.youtube.com/watch?v=AXrrqtFlGow
https://www.avalabs.org/whitepapers

https://cryptoseq.medium.com/the-avalanche-ecosystem-is-rapidly-expanding-private-securities-ilos-dexs-synthetics-ce480387a111

https://docs.avax.network/nodes/validate/staking-avax-by-validating-or-delegating-with-the-avalanche-wallet/

https://messari.io/article/state-of-avalanche-q1-2022-analyst-call-transcript?referrer=asset:avalanche

https://www.stakingrewards.com/

https://crosstower.com/resources/education/nakamoto-coefficient/
https://avascan.info/stats/staking

Electric Capital Developer Report (2021) | by Maria Shen

