



First Published: - December 21, 2021

(Cheetah Protocol – The fastest smart contracts platform)

Cheetah Litepaper, Version 1.0

Overview

Since the debut of Bitcoin in 2008, the blockchain sector has seen numerous important developments emerge that have affected the path of the whole ecosystem as well as the larger financial market. One of these developments is Decentralized Finance (De-Fi). De-Fi refers to a wide range of financial products and services that are built on blockchain technology and regulated by decentralized communities. The exponential growth of the De-Fi market reflects the potential of digital currencies and decentralized platforms to provide an alternative to the traditional finance paradigm, which has been steadily consolidating for decades, suffocating innovation and reducing the importance of financial inclusion. Within the growing digital economy, De-Fi is laying the groundwork for permissionless, blockchain-based financial services. Decentralized finance (De-Fi) promises to improve the financial world by empowering communities while delivering alternative financial solutions. Almost all decentralized finance transactions are now conducted on Ethereum network, but high users traffic and rising "gas fees" are stifling activity on the network. While other blockchains are attempting to capitalize on the surge in De-Fi demand, none come close to the volumes carried by Ethereum — a protocol that has exploded in popularity thanks to its first-mover advantage and "composability," which allows less-experienced developers to contribute to the ecosystem's development. The popularity of De-Fi is also clogging the already-bustling Ethereum network, raising transaction costs known as gas and transaction settlement time.



Problem Statement

Because of Bitcoin, blockchains have grown in an unusual way. Because Bitcoin was the original blockchain, it inspired the architecture of all future networks, including Ethereum. This is currently problematic for a number of reasons: Bitcoin's Proof of Work consensus causes transactions to be delayed and expensive. Decentralization is hampered by the time and resources required to validate Proof of work(POW) chains. The usage of blockchain is accelerating, necessitating scalable solutions. Because there were so few people using Bitcoin when it first began in 2009, the technological restrictions were less of a concern. However, decentralized finance and the adoption of NFTs have drastically altered the blockchain scene today. Around 100 million individuals were utilizing cryptocurrencies by the start of 2021, according to some estimates. Similarly, the value of De-Fi apps has risen to well over \$100 billion. Smart contract-enabled blockchains like Ethereum and Bitcoin are experiencing network congestion and outages as a result of their exponential growth. To fix the challenge, the majority of today's De-Fi value is implementing layer 2 scaling solutions. Layer 2 separates transactions from the main Ethereum chain, bundles them, and returns the bundles to Ethereum. This relieves demand on Ethereum while also adding levels of complexity that may jeopardize security. The most elegant option is to maintain everything on a scalable, secure, and decentralized layer 1 protocol. So, what does any of this have to do with Cheetah?

Cheetah proposed solution

As blockchain technology advances, it offers new answers to scalability, interoperability, and usability issues. With the usage of four different blockchains on our platform, Cheetah protocol has adopted a unique approach. At Cheetah protocol, we promise to be "the quickest smart contracts platform in the blockchain industry, as measured by transaction completion time," thanks to our native coin CTH and numerous consensus processes.

What issues does Cheetah address?

There are three key issues that Cheetah is trying to address. Scalability, transaction costs, and interoperability are all three major factors to consider.

Decentralization vs. scalability - Traditional blockchains have failed to strike a balance between scalability and decentralization. With more users and activity, a network may struggle to reach agreement on legitimate transactions rapidly. Bitcoin (BTC) is an excellent example of the problem, with transactions taking hours or even days to complete during periods of network congestion. Making the network more centralized and giving fewer individuals more authority to authenticate network activities is one strategy to prevent this. Transactions may be confirmed considerably more rapidly if fewer persons have to review and validate them. Decentralization, on the other hand, is a crucial and desirable feature of blockchain technology. With technical improvements, new blockchains are continually

attempting to overcome this problem, and Cheetah has developed a unique method, which we'll discuss later on this paper.

Fees that are too high- Gas costs are another major issue with bigger blockchains such as Ethereum. The problem is exacerbated by increased traffic and user numbers. This deters people from using these blockchains, yet the competitors has fewer well-established ecosystems. The popularity of Ethereum, for example, along with a lack of alternatives, has resulted in near-constantly high traffic and costs with no way to get rid of such high costs. Simple transfers might cost more over \$10 at times, and complicated smart contract exchanges are considerably more costly. Cheetah is building a fastest blockchain platform with low fees even when traffic is high and congested.

Interoperability- When it comes to blockchains, different projects and enterprises have different requirements. Previously, projects had to choose between using Ethereum, another blockchain that wasn't adapted to their needs, or a private blockchain. Finding a balance between customizability and collaboration amongst various blockchains is a challenging issue. Subchilds and specialized custom blockchains, which share the network's security, speed, and compatibility, are Cheetah's answer to the problem.

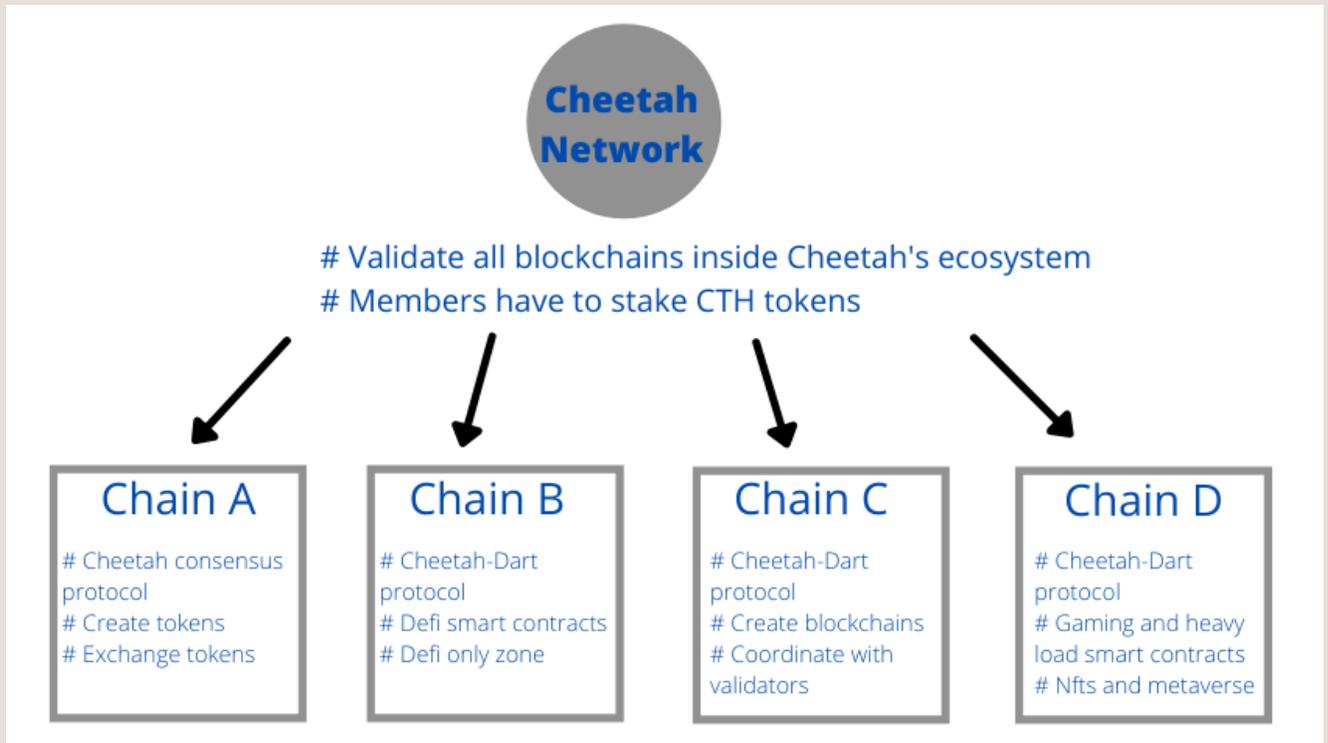
What is Cheetah?

Cheetah is a flexible smart contract platform for creating custom blockchain networks and decentralized applications especially for those focused on Decentralized finance, Non fungible tokens, web 3.0 and metaverse. Cheetah is a blockchain platform with smart contracts that focuses on faster transaction speed, cheapest costs, and environmental friendliness. Cheetah's ultimate goal is to create a highly scalable blockchain that doesn't compromise decentralization or security. The Cheetah crypto platform, is one of several initiatives vying to dethrone Ethereum as the most frequently used smart contract platform in the blockchain ecosystem. With a transaction throughput of 110,000+ transactions per second, Cheetah promises to be more scalable than Ethereum. Cheetah's native CTH token, which has a restricted supply of 220 million, is used to pay network transaction fees as well as part of the Cheetah consensus process. Cheetah is building its own decentralized finance (De-Fi) ecosystem to compete with Ethereum. Cheetah is also working on a bridge to the Ethereum network, which will allow users to transfer assets effortlessly between the two networks.

Cheetah Protocol, the company behind Cheetah, believes we've created the world's quickest and scalable smart contract blockchain platform. Cheetah operates at internet-scale for a future when crypto is a global backbone technology, thanks to the use of four separate blockchains beneath the hood. The time it takes for a crypto transaction to process and be regarded permanent and irreversible is known as the time to finality. Once a transaction has reached finality, it cannot be reversed or changed. Clearly, finality is an important blockchain characteristic particularly for financial applications, but the time it takes for a blockchain to reach finality varies. Ethereum, for example, reaches finality in under a minute. Cheetah reaches finality in a fraction of a second, which is near-instantaneous in real-world applications and this matters the most in today's world of Defi.

CHEETAH CONSENSUS MECHANISM

The main novelty of Cheetah is that it is made up of four blockchains rather than the traditional one. The reasoning behind this architectural decision is brilliant: rather than having one chain handle everything, each blockchain focuses on a certain purpose inside the Cheetah ecosystem. The Cheetah platform can fulfill the golden trinity of blockchain qualities — decentralization, security, and scalability — by distributing jobs over many chains.



Chain of Exchange (Cheetah A) - The Exchange Chain (A Chain) is the blockchain that allows Cheetah assets to be created and traded. Fees are paid in CTH for transactions on the A-Chain. This is comparable to how Ethereum gas costs are paid in ETH. Fees are always settled in CTH, even if you're dealing with other tokens issued on the Cheetah blockchain.

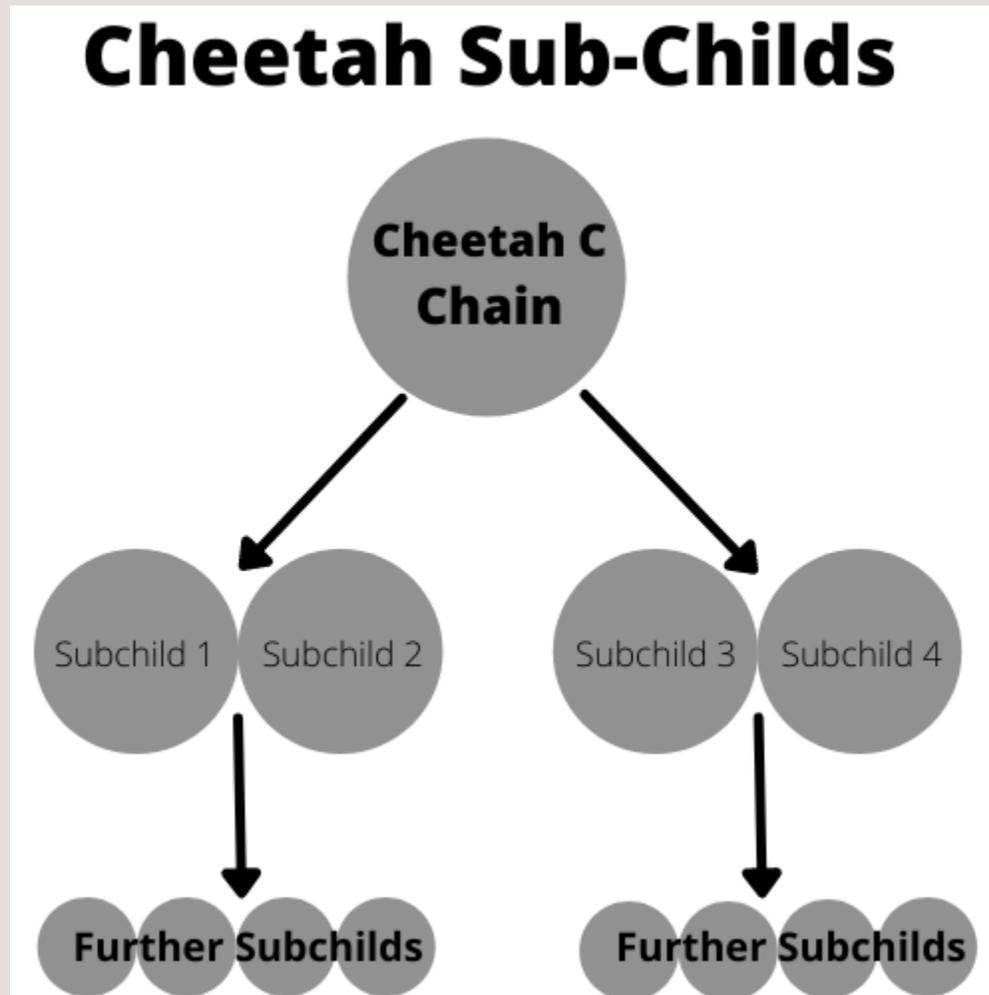
Chain of financial Contracts (Cheetah B) - Cheetah's main feature is smart contracts for De-Fi. Developers may use this capability to create decentralized financial apps on Cheetah while taking advantage of the platform's security and scalability. Users and developers are able to create new decentralized financial apps and execute smart transactions on this chain. The B-Chain is an Ethereum Virtual Machine (EVM) compliant smart contract platform for the Cheetah platform. Because Cheetah is EVM compatible, anybody may use it to deploy Ethereum smart contracts. What's the big deal about that? Existing Ethereum programs, such as De-Fi giants Aave, may quickly release an Cheetah version of their product.

Import solidity smart contracts and execute on Cheetah

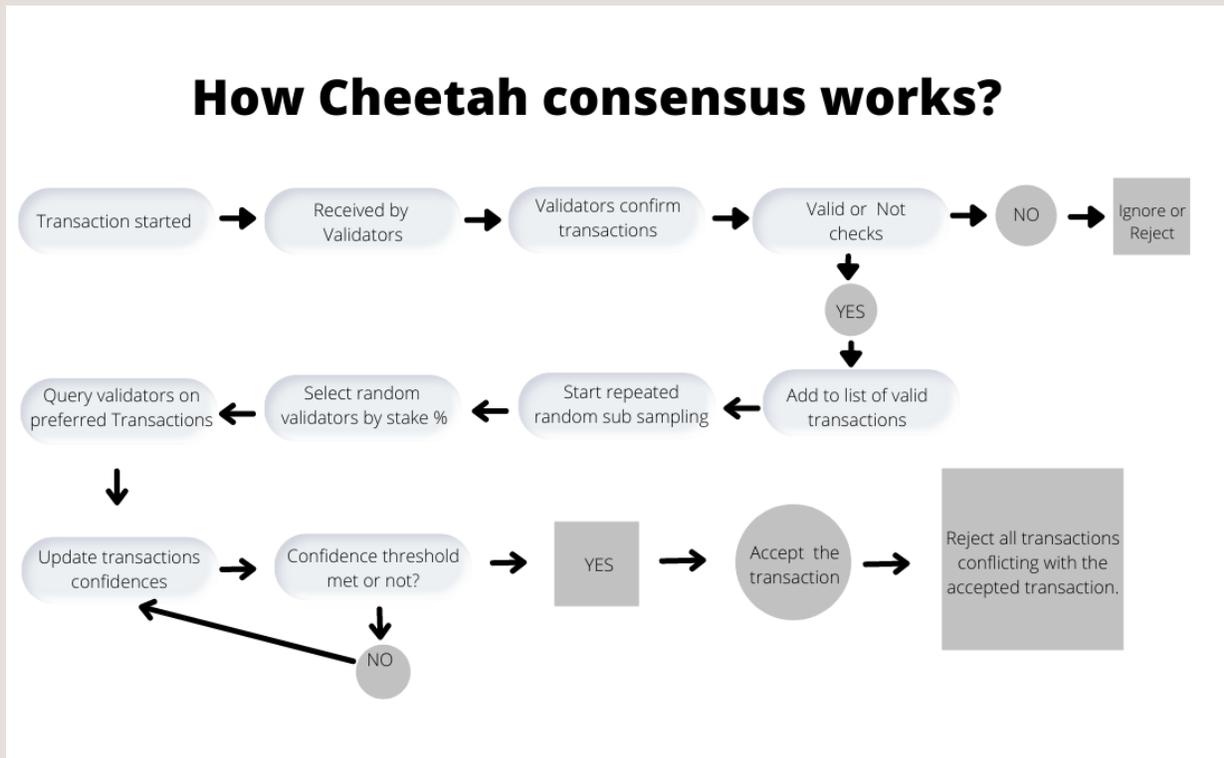


Chain of Platforms (Cheetah C)- Anyone can create an Layer 1(L1) or Layer 2(L2) blockchain with Cheetah's C-Chain. You could even put together a group of them. These blockchains are known as subchilds in Cheetah, with the C-Chain serving as the default subchild for everybody. The C-Chain keeps track of validators to manage the landscape of Cheetah subchilds, but subchilds are also responsible for verifying the C-Chain.

Chain of Gaming, Nfts and Metaverse (Cheetah D) – Users can execute gaming, nfts and metaverse specific smart contracts on this chain. This highly reduce the load on Chain B thus allowing more flexibility to the Decentralized finance chain.

Cheetah Scaling Requires Subchilds-

Cheetah subchilds were briefly mentioned in the C-Chain section above. Their significance, though, is worth elaborating on. Subchilds in Cheetah perform similarly to sharding in Ethereum 2.0. A subchild is a clone of the default blockchain (in the case of Cheetah, this is the Primary Network) that is connected to the platform at startup. More significantly, users can build subchilds on their own time and as needed. In reality, this implies that a subchild can establish another subchild to meet or surpass network traffic needs and free up transactions once its scaling restrictions are temporarily reached. In a word, the number of subchilds you can construct is limitless (subchilds can infinitely create subchilds). Cheetah's B-Chain will have a transaction capacity of around 110000+ transactions per second. Cheetah platform, on the other hand, has no real Transaction per second limit due to its limitless capacity for producing subchilds. Despite the fact that subchilds can develop their own rules for how their blockchain runs, all subchilds must validate their own blockchain as well as the Primary Network chain. To validate the Primary Network, each subchild must be a Primary Network member, which is granted to those who stake 1,000 or more CTH tokens.

Cheetah Crypto Consensus

The Cheetah Virtual Machine is a proprietary Virtual Machine (VM) that powers Cheetah's architecture (CVM). Subchilids built on the Cheetah platform can use the CVM to reach consensus using "traditional" blockchain databases like Bitcoin, Ethereum, or Cardano, but they can also use other database structures like the "block lattice" database structure pioneered by crypto networks like IOTA, Fantom, or Nano. Such adaptability ensures that projects using Cheetah may achieve a high level of customization while maintaining compatibility with a variety of platforms. Cheetah makes use of Cheetah-Dart an Cheetah protocol -designed Proof-of-Stake (PoS) consensus mechanism that requires users to stake CTH in order to become transaction validators. To participate in consensus, validators must stake at least 1,000 CTH tokens. By delegating your CTH to a validator, you may also participate in consensus. To participate, you must assign at least 70 CTH.

Validator nodes in a subchild continually query each other to evaluate the validity of the network's transactions until they achieve a common judgment — and so build network-wide agreement — using the Cheetah-Dart consensus mechanism. The higher a node's stake in CTH currencies, the more frequently it is queried. The Primary Network is required for all validator nodes, while involvement in other subchilids is optional. Validators are compensated based on their uptime and reaction latency, with payouts proportionate to their overall investment. Validators will earn more if they keep their investment for a longer length of time. You will also earn a reward if you delegate your CTH coins to a validator and that validator obtains a reward. Finally, unlike previous PoS systems, Cheetah does not penalize rogue nodes by lowering their stakes; instead, they are simply not rewarded.

Cheetah aims to stand out in a crowded market of Ethereum competitors by focusing on De-Fi and offering a three-pronged offering of customizability, scalability, and interoperability. Though it is unclear if Cheetah will offer a long-term competitive threat to Ethereum, the platform is well on its way to building its own ecosystem, with a focus on De-Fi applications, lower transaction fees and faster transactions.

CTH Tokenomics

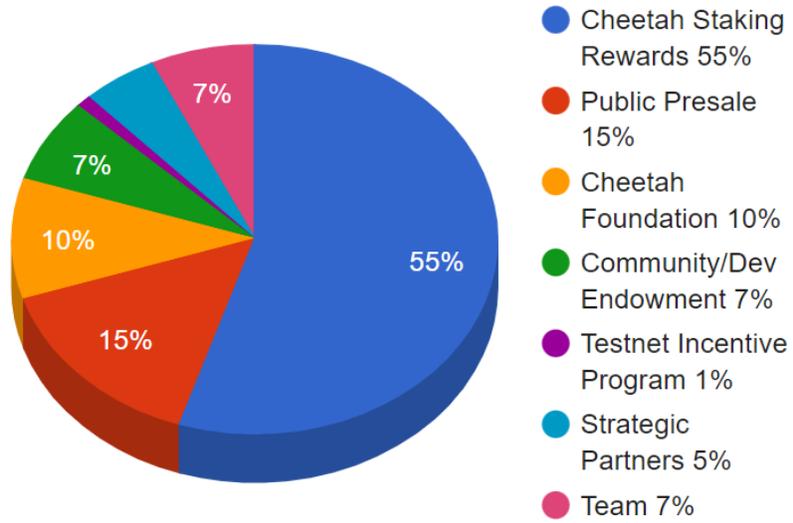
The Cheetah token, abbreviated as CTH, is a utility token that acts as the ecosystem's primary medium of exchange. CTH staking protects the network and pays stakers with extra CTH, in addition to its usage as currency in the Cheetah platform. The CTH is a deflationary token and the main objective of a deflationary token is to compound the currency value derived from staking. CTH tokens used to pay transaction fees are destroyed, reducing the quantity of CTH in circulation forever. Validators must possess and stake CTH tokens as collateral in all subchilds, including the Primary Network.

CTH allows you to pay transaction fees. The Cheetah currency CTH is referred to as the ecosystem's common unit of account. In layman's terms, this means CTH is the default money on the network. CTH is the common currency between subchilds and is used to pay all transaction costs. It's crucial to utilize CTH between subchilds because it aids interoperability between subchilds that would otherwise use their own internal coins.

Tokens and Subchilds can be created-

Creating new custom coins/tokens and blockchain networks(subchilds) are two of CTH Cheetah's main use cases. Additionally, Developers can use the platform to create NFTs, De-Fi protocols, games, metaverses, and many other internet of things, the possibility is limitless. CTH payments are required for creating custom tokens, subchilds, games, Nfts, De-Fi applications on the Cheetah platform.

Cheetah Protocol (CTH) Tokenomics



CTH Token Metrics

Total Coins: 220,000,000

Public Sale: 15%

How Cheetah maintains faster transaction settlement?**Consensus comparison: Classical vs Nakamoto vs Cheetah**

	Classical	Nakamoto	Cheetah
Robust	-	+	+
Scalable	-	+	+
Decentralized	-	+	+
Low latency	+	-	+
Lightweight blockchain	+	-	+
Eco friendly	+	-	+
High throughput	+	-	+
Resilient to 85% attacks	-	-	+

The Cheetah network aims to increase scalability while maintaining decentralization. The Cheetah consensus protocol is used to manage/exchange assets on the A-Chain. The D-Chain is used for heavy loads i.e. gaming, NFTs and metaverse projects. The B-Chain is used to create smart contracts, whereas the C-Chain is used to coordinate validators. The Cheetah-Dart consensus protocol is used by these two blockchains i.e. B and C chains. All nodes in the Cheetah consensus mechanism operate in parallel to examine the transaction confirmations of other validators at random. A transaction is probabilistically proven to be true after sufficiently repeated random subsampling. This increases transaction throughput to 110000+ TPS and delivers a transaction completion time of less than two second. Cheetah-Dart is similar, except it uses blocks in a linear method. Cheetah also enables the building of interoperable, customizable blockchains called subchilds. There is no limit on the quantity of subchilds that can be built on the platform. Unlike Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake, the Cheetah consensus process does not require a leader to obtain consensus. This factor boosts the Cheetah network's decentralization without losing scalability. PoW, PoS, and DPoS, on the other hand, have one actor execute transactions, which is subsequently confirmed or validated by others. Cheetah implements a directed acyclic graph (DAG) efficient consensus system that leverages all nodes to process and validate transactions. The network can process transactions in parallel with the help of a DAG. Validators poll other validators at random to see if a new transaction is legitimate. It is statistically shown that a transaction would be almost difficult to be fake after a given amount of this repeated random subsampling. All transactions are completed instantly, with no additional confirmations required. This implies that instead of blocks, like in typical blockchains, vertices, or parented

transactions, are used. The hardware requirements for running a validator node and validating transactions are minimal and accessible, which aids performance and decentralization.

Cheetah-Dart Consensus-

The Cheetah-Dart consensus system is based on the Cheetah consensus algorithm, however transactions are ordered in a linear fashion. When working with smart contracts like the B-Chain and D-Chain, this trait comes in handy. Cheetah-Dart, unlike the Cheetah consensus protocol, makes blocks.

(Comparing to other blockchain platforms)

Metrics/Platforms	Ethereum	Polkadot	Cheetah
Transactional outturn	14 transactions per second	1500 transactions per second	110000+ transactions per second
Transaction finalization time	Up to 6 minutes	Up to 60 seconds	Less than 2 seconds
Eco friendly?	No(PoW)	Yes(PoS)	Yes(PoS)
No. of validators	2 pools > 51% hash rate	<200 nodes relay chain	More than 2000 nodes
Validating mechanism	Proof of work	Proof of stake	Proof of stake
Safety threshold	51%	33%	85%

References:

DAG: https://en.wikipedia.org/wiki/Directed_acyclic_graph

Bitcoin scalability problem

https://en.wikipedia.org/wiki/Bitcoin_scalability_problem#:~:text=The%20Bitcoin%20scalability%20problem%20refers,limited%20in%20size%20and%20frequency.

<https://www.diva-portal.org/smash/get/diva2:1111497/FULLTEXT01.pdf.10>

<https://101blockchains.com/blockchain-scalability-challenges/>