Introduction to Catalyst Network

February 25th, 2024

Version 0.12.0

Abstract

At the heart of the Catalyst Network lies a bold vision: to redefine blockchain by championing true decentralization and seamless integration with the wider IT industry. From Bitcoin's inception, the blockchain industry has strived for innovation, yet faced challenges, particularly the trend towards centralization in some of the most successful blockchains. These have necessitated either costly mining hardware or substantial staking investments, diverging from the foundational principle of decentralization in control and benefits.

Catalyst Network emerges as a beacon of innovation, addressing these challenges by emphasizing the core tenets of decentralized control and wealth distribution. It stands out by empowering developers as a central pillar, ensuring blockchain technology's accessibility beyond the confines of niche applications, and fostering integration within the broader IT landscape.

This paper unveils the technological innovations and economic considerations underpinning the Catalyst Network. It outlines our commitment to a decentralized, developer-focused ecosystem that makes blockchain accessible and beneficial across the IT industry, thereby contributing to the blockchain domain's evolution and addressing its prevailing challenges.

Background

The inception of blockchain, symbolized by the launch of Bitcoin in 2009, marked the beginning of a new digital era [3]. It promised a future where financial transactions and data exchanges could occur without central authority, fostering an environment of trust, transparency, and security. This revolutionary concept laid the groundwork for the development of numerous blockchain platforms, each aiming to expand upon Bitcoin's original premise by introducing functionalities that cater to various industries beyond finance.

As the blockchain landscape evolved, it became evident that while innovation flourished, so did the complexity and, paradoxically, centralization. Many advanced blockchain projects, in their quest for efficiency and scalability, inadvertently embraced mechanisms that favoured concentration of power and wealth—moving away from the decentralized ethos that had been their cornerstone. This shift not only raised questions about the true nature of decentralization in blockchain but also highlighted barriers to entry for developers and users alike, stifling innovation and accessibility.

Enter Catalyst, born from the desire to realign blockchain technology with its foundational principles of decentralization, inclusivity, and open collaboration. Recognizing the challenges of centralization and accessibility, Catalyst positions itself as a bridge between the pioneering spirit of early blockchains and the practical needs of the modern digital world. Our mission is to empower developers with a modular, intuitive framework that brings the benefits of blockchain to a wider audience, fostering innovation and participation across the IT industry.

At Catalyst, we believe in the power of blockchain to transform not just financial systems but also the way we share information, build communities, and innovate for the future. Our approach combines the robustness and security of blockchain with the benefits of distributed file storage and off-chain event and messaging systems, ensuring that developers have the tools they need to create groundbreaking applications. By prioritizing decentralization in both control and wealth distribution, we aim to create a more equitable digital landscape where opportunities for innovation and growth are accessible to all.

As we look to the future, Catalyst stands as a testament to the enduring relevance of blockchain's core principles. We are committed to advancing these ideals through our technology, governance, and community engagement, paving the way for a new generation of blockchain applications that are truly decentralized, user-friendly, and integral to the broader IT ecosystem.

1. Summary

In January 2009, Bitcoin introduced the world to a revolutionary concept: a decentralized and trustable store of value, setting the stage for the blockchain era. Building upon Bitcoin's success, subsequent blockchains like Ethereum and Solana expanded the technology's horizon, enabling decentralized computing services that cater to a wider array of applications beyond mere value storage. These developments highlighted blockchain's potential to decentralize various sectors, including financial markets and industrial systems, even collaborative environments for AIs [5].

However, the journey of blockchain innovation is marred by significant challenges, notably in scalability, privacy, speed, and interoperability. The majority of existing blockchain projects are derivatives or forks of a few original blockchains, limiting fresh perspectives on overcoming these fundamental issues [6]. This forking practice has constrained the industry's ability to address core technological limitations, leaving scalability, privacy, speed, and interoperability as persistent challenges.

Catalyst Network emerges from a ground-up approach, starting with a thorough examination of operational requirements and existing limitations. Our team, leveraging extensive research and development, has created a new, original codebase that eschews forking in favour of innovation. Catalyst is designed to be modular, incorporating third-party modules like Nethermind's EVM for computational environments and distributed file storage built on IPFS. This modularity and originality position Catalyst as potentially the first truly modular blockchain, designed from the outset to accommodate independent module development by partners.

Our key objectives underscore the fundamental requirements Catalyst aims to fulfil decentralization at scale, scalability to meet future demands, operability on devices with varying resources, a dynamic economy to foster engagement, and inclusivity allowing broad participation. Catalyst supports the integration with wider IT industry standards, enabling a new generation of web services that prioritize user privacy and data control.

The Catalyst blockchain is engineered to address the blockchain trilemma, balancing decentralization, scalability, and security. Our consensus mechanism, alongside a suite of modular components, forms a comprehensive framework. This framework supports a wide array of functionalities, from smart contract execution to efficient peer-to-peer communication, poised to redefine blockchain utility and adoption.

2. Technology

2.1 Catalyst blockchain

The Catalyst Blockchain represents a bold approach in the development of decentralized networks, embodying a balanced approach to the long-standing blockchain trilemma of achieving scalability, security, and decentralization. Designed by a team of seasoned engineers and researchers, Catalyst is poised to redefine the landscape of blockchain by offering an infrastructure that can store a diverse range of data types—from simple tabular records to large files—efficiently, cost-effectively, and in a manner that perpetually encourages the decentralization of control and benefits.

At its core, the Catalyst Blockchain is a modular framework, akin to a highly adaptable structure where various modules can be seamlessly replaced via a framework of interfaces or “sockets”. This modularity is central to Catalyst's philosophy, allowing for the agile evolution of the network to meet emerging needs and technologies. Initially, the blockchain encompasses several key modules:

Database Module: Manages the ledger's structure, ensuring secure and orderly storage of digital account information.
Network Module: Facilitates robust peer-to-peer communication and efficiently allocates node responsibilities.
Consensus Module: Implements a novel mechanism for achieving agreement across the network, underpinning the ledger's integrity and the secure validation of transactions.
Distributed File System Module: Provides a scalable solution for storing diverse data types, underpinning the network's capacity to handle extensive files and historical data.
KAT Virtual Machine (KVM) Module: Enables the execution of smart contracts on the Catalyst network, ensuring compatibility and extending functionality.

The Catalyst Blockchain's architecture is designed to balance the blockchain trilemma:

Decentralization: Through its modular design and consensus mechanism, Catalyst ensures that control and benefits are equitably distributed across the network, resisting centralization even as the network scales.
Scalability: Catalyst's innovative approach to data storage and transaction processing allows it to accommodate the growing demands of modern applications and services without sacrificing performance or security.
Security: Leveraging advanced cryptographic techniques and a robust consensus model, Catalyst maintains a secure and immutable ledger, protecting against fraud and ensuring the integrity of transactions.

Furthermore, the introduction of a new consensus mechanism marks a significant departure from energy-intensive processes like Proof of Work (PoW) or costly staking limitations of Proof

of Stake (PoS). This mechanism prioritizes efficiency and environmental sustainability, allowing for a collaborative, rather than competitive, validation process that rewards participation proportionally and keeps transaction fees low.

Catalyst Blockchain is not merely a technological infrastructure; it is a visionary project aimed at democratizing access to decentralized technologies, fostering innovation, and empowering communities. Through its unique combination of modularity, security, and scalability, Catalyst is poised to become an important addition to the next generation of decentralized applications and services, truly embodying the ethos of an open, accessible, and equitable digital future.

2.1.1 Catalyst Database Structure

Catalyst has a multi-levelled data architecture, as illustrated in Figure 1.

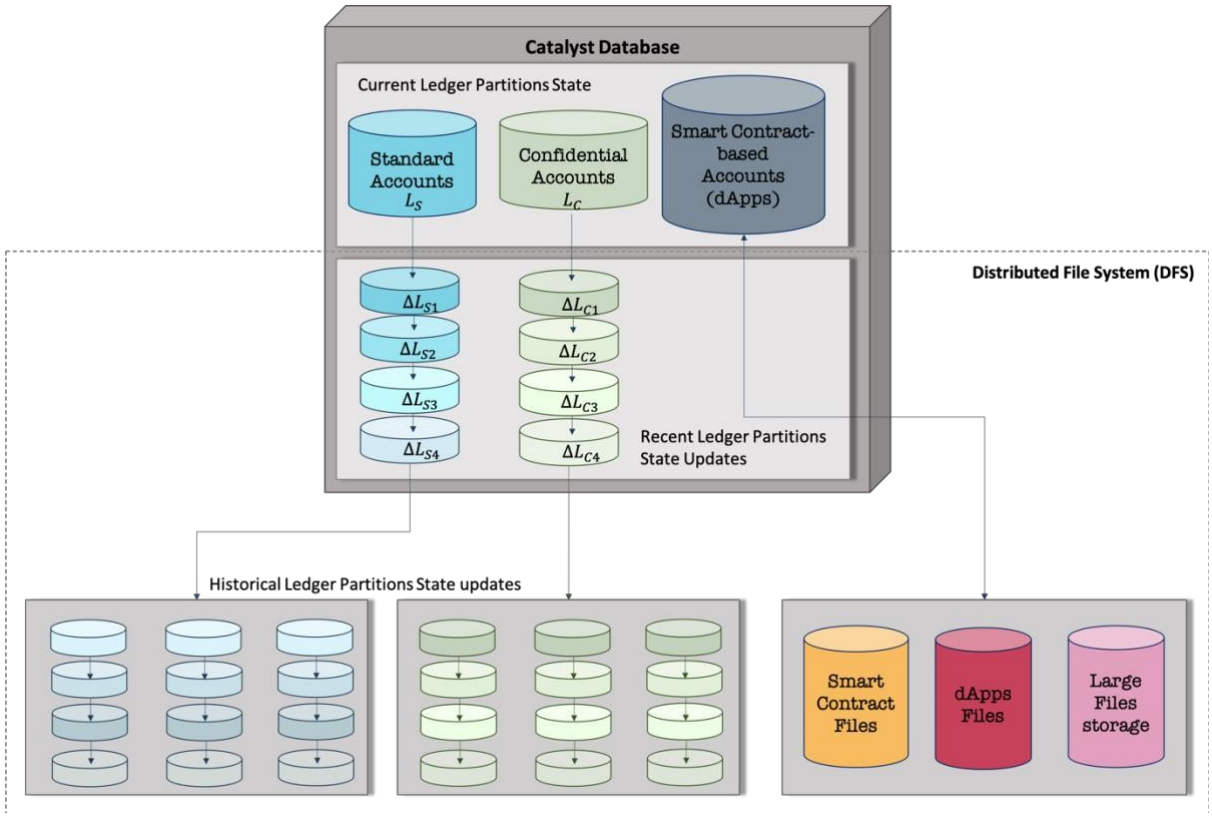

Figure 1: Illustration of Catalyst database architecture.

At the top level lies the current state of the global ledger, i.e. the database containing the current balance of digital accounts recorded on the ledger. The current ledger state represents a snapshot of the ledger state, at the present time. It is periodically updated. At the end of a ledger cycle, that lasts for a fixed period between 30 seconds and 1 minute, a ledger state update is generated by a pool of nodes selected to manage the ledger database, and distributed to the network users who can then update their local copy of the ledger state. The process followed by these nodes to generate a ledger update, i.e. the consensus-based protocol, is described in section 2.1.4.

The middle level comprises the recent ledger state updates, that is a set of the last recent ledger state updates accepted by and broadcast across the network. Historical data, or old ledger state updates, represent the bottom level. Both middle and bottom levels are maintained by the Catalyst Distributed File System (DFS) module. The top and middle levels reside on every node on the network and are thus immediately accessible. On the other hand, the bottom level is maintained by some but not necessarily all nodes in the network. Long term data is thus available with a short delay which constitutes a small trade-off for a compact ledger database maintained by every node.

Different types of accounts are stored on Catalyst ledger. Namely:

- Non-confidential user-based accounts, with a balance in tokens that is updated via the validation of non-confidential transactions. The account balance is visible to all.
- Confidential user-based accounts, with a balance in tokens that is updated through the validation of confidential transactions. The account balance is hidden, only known to the account holder(s).
- Smart contract-based accounts. A smart contract-based account has an associated code that can be triggered by transactions or messages generated by other codes.

As such, Catalyst database is naturally split into partitions where each partition stores accounts of a given type. A node on Catalyst Network may not maintain a copy of all partitions but must remain aware of the possible dependencies among partitions. Figure 1 also shows the ledger partition dedicated to smart contracts and dApps which communicates with DFS for the access, production and storage of files.

2.1.2 Catalyst Peer-to-Peer Network

Anyone can create a node and join the Catalyst network. A node's default status on joining is user node. As such, it can create and relay valid transactions. This default status allows nodes to join the network without committing any storage or computing resources and will be of particular interest to very small devices such as smart watches, sensors and other low resource devices.

Catalyst Network implements a peer identification protocol. Each node that joins the network must have a unique peer identifier that describes the node's identity. This allows users to track their connected peers and associate a reputation to each node, which promotes nodes' good behaviour and helps preventing Sybil attacks on the network [7].

Peer discovery on Catalyst Network is performed using a Metropolis-Hastings Random Walk with Delayed Acceptance (MHRWDA) [8]. The random walk reduces any communication bias towards nodes which have many peers. Indeed, it is designed to cause a high cost to eclipse attacks from malicious nodes.

The management of the ledger database is handled by worker nodes. These nodes are member of a worker pool (one pool per ledger partition) and are granted a worker pass, valid for a limited period. Users willing to contribute to the management of the ledger database can apply to become worker nodes. By providing proofs of their available computing resource [9], they register their node(s) in the work queue associated to a specific ledger partition. As worker nodes leave the worker pool, nodes waiting in a queue join the associated worker pool.

During a ledger cycle, a subset of nodes from the worker pool is randomly selected to generate the state update of a ledger partition, these are called producer nodes. The producers follow a consensus-based protocol in order to reach consensus on the state update produced at the end of the ledger cycle and used by all nodes to synchronise their local copy of the ledger partition database.

2.1.3 Catalyst Distributed File System

Once a ledger partition state update is generated by a pool of producers, it is stored on DFS and can be accessed by any node to update their local copy of the ledger partition. DFS is built upon the IPFS protocol [10] and is used to store files as well as historical ledger state updates. This removes the burden on user nodes to maintain the full history of the ledger database while allowing for fast retrieval of files as well as old ledger state updates. DFS is maintained by all nodes on the network. However, DFS is made of a multitude of compartments and each node needn't hold all compartments. The design of a ledger compartment dedicated to the storage of files and historical ledger state updates is an approach taken to prevent the bloating of the ledger and allow the network to support services at scale. Indeed, this approach allows Catalyst ledger to remain both lean and cryptographically secure.

2.1.4 Catalyst Consensus Protocol

Proof-of-Work (PoW) and derivate algorithms are commonly used to manage blockchains and DLT in a distributed manner. Consensus protocols based on such algorithms rely on a plurality of nodes, called miners, that compete to generate at regular interval of time a valid block of transactions to append to the blockchain. Part of the competition consists in solving a cryptographic puzzle that ensures the validity of the content of a block.

This competition amongst nodes wastes a tremendous amount of energy as all miner nodes expend computational power to solve the same problem, yet only the work performed by one node is used to update the blockchain. The energy consumption per year for Ethereum and Bitcoin combined is roughly 67 TWh which is comparable to the yearly energy consumption of Switzerland (around 62 TWh) [11]. It is clear that this is not sustainable nor environmentally friendly. Moreover, as the difficulty associated with the cryptographic puzzle increases over time, miners are forced to invest in more computing resources to have a chance of earning miner rewards. Such consensus protocols have a clear negative environmental impact and counteractive economic implications with high risk of mining centralisation.

The consensus algorithm designed by the engineers and researchers at Catalyst [12] rests on the principle that every node participating in the network can contribute to maintain the ledger database. Indeed, Catalyst consensus protocol was conceived based on the observations that:

- Not every node needs to validate every transaction for a network to be secure and a ledger fully decentralised.
- Collectively across a network of nodes there is significant distributed computer resources to securely maintain a ledger. Network performance should as a result improve as the network scales up.

Catalyst consensus protocol is not based on a competitive process. Instead, nodes on the Catalyst network collaborate to build the state update of the ledger partitions and get rewarded proportionally to the amount of work they performed, by collecting new tokens injected at the end of every ledger cycle as well as fees paid by the users issuing transactions. Fees are kept low and estimated based on the amount of work required to process transactions.

Catalyst consensus protocol, described in [12], is a decentralised voting protocol that eliminates the execution of computationally expensive tasks, thus allowing nodes with limited resources to contribute. It is designed to scale while continuously pushing towards network decentralisation.

2.2 Smart Contracts and dApps

Catalyst Network introduces a paradigm shift in the deployment and execution of smart contracts and decentralized applications (dApps), fostering an environment where developers are not constrained by the limitations of any one runtime environment. At the heart of this innovation is Catalyst's commitment to versatility and developer empowerment, ensuring that the network remains at the forefront of decentralized technology. The ledger contains data, the compute environment that updates that data does not need to be constrained to one language or runtime environment but should be extendable over time through the protocol's interfaces.

2.2.1 Flexible Smart Contract Execution

Catalyst distinguishes itself through its support for smart contracts in a manner that does not confine developers to a single programming language or runtime environment. This openness is achieved through a modular framework that can be extended and adapted over time, accommodating various runtime environments as they evolve.

Initially, Catalyst will feature the Katalyst Virtual Machine (KVM), a variant of the Ethereum Virtual Machine (EVM) that is extended to leverage distributed file storage capabilities. This design choice ensures EVM compatibility, allowing for the straightforward deployment of existing Ethereum smart contracts on Catalyst. Moreover, KVM's extension to integrate with Catalyst's distributed file system opens new possibilities for smart contracts to interact with a wider range of data types, facilitating more complex and feature-rich dApps.

Later, additional runtime environments such as SVM will be integrated to allow the ledger to be updated using Rust and allowing dApps written for Solana to be deployed to Catalyst.

2.2.2 Roadmap for Enhanced Compute Capabilities

The Catalyst roadmap envisions the introduction of a novel messaging layer to allow Smart Contracts to generate events and messages to be broadcast across the Catalyst network. Off-chain applications register to receive events and messages much like they would for a service bus. For example, a desktop or web application could monitor for balance transfer events in a smart contract and be immediately notified when event is settled by the consensus mechanism, immediately displaying the balance update on screen. This enables remote systems to integrate with Catalyst in real-time without needing to develop any new blockchain specific technology, instead treating Catalyst the same as any other service bus.

2.2.3 Empowering Developers

Catalyst's approach to smart contracts and dApps is characterized by its emphasis on developer freedom and innovation. By providing a flexible, expandable platform, Catalyst aims to attract a vibrant community of developers interested in pushing the boundaries of what's possible with blockchain technology. This developer-centric ecosystem is supported by comprehensive documentation, development tools, and a supportive community, ensuring that developers have everything they need to succeed.

2.2.4 Global State Machine

The Catalyst Network's Global State Machine is underpinned by the Catalyst Virtual Machine (KVM), a sophisticated runtime environment designed for the execution of smart contracts. KVM embodies a strategic enhancement of the Ethereum Virtual Machine (EVM), incorporating a bytecode superset that maintains full compatibility with Ethereum's existing smart contracts while extending functionality to leverage Catalyst's unique features, such as distributed file storage and advanced event handling mechanisms.

2.2.5 Bridging Traditional and Decentralized Computing

KVM's design philosophy is rooted in providing seamless interoperability with Ethereum, thereby enabling businesses and developers already operating in EVM-compatible networks to transition or extend their projects onto Catalyst with minimal friction. This compatibility ensures that the wealth of existing smart contracts, tools, and developer expertise can be directly applied within the Catalyst ecosystem, accelerating innovation and adoption.

2.2.6 Enhanced Smart Contract Capabilities

Beyond basic EVM compatibility, KVM is engineered to exploit Catalyst's distributed file storage, enabling smart contracts to interact with a broader range of data types and structures. This capability significantly expands the potential use cases for smart contracts on Catalyst, from simple token transfers to complex decentralized applications that require access to large-scale data or off-chain resources. Smart contracts on Catalyst can, therefore, go beyond traditional financial applications, opening new avenues for decentralized applications in fields such as decentralized finance (DeFi), supply chain management, and decentralized autonomous organizations (DAOs).

2.2.7 Distributed File Storage Access and Events

The integration of distributed file storage with smart contract execution is a hallmark of Catalyst's Global State Machine. KVM facilitates both read and write operations to the distributed file system as atomic actions, ensuring deterministic outcomes across the network. This deterministic nature is crucial for maintaining the integrity and consistency of smart contract executions, even when interacting with external data stored on the Catalyst network.

Files stored on this file system are named as a hash of the file, meaning that each node can be certain that the file being accessed will be the same on every node, thus protecting the principle of being deterministic. If a file is changed then it will have a new hash.

For reads, all nodes reading a file by its hash name will retrieve the same file and give a deterministic result.

For a write, if different nodes generate a different result, then they will create different files. If different nodes generate the same result, then the hashes will match meaning a single file instance is created. Files can be stored on DFS in numerous ways, not just by smart contracts and so a common pattern will be to load data into a low cost or free file on DFS and have the smart contract read that data when it runs, much like it would read data from the ledger.

Moreover, KVM's architecture is designed to emit and handle events in a manner that aligns with traditional service-oriented architectures. This design enables smart contracts to broadcast information about their execution states, such as transaction outcomes or specific state changes, which external applications can listen to and act upon. This event-driven approach simplifies the development of responsive and dynamic dApps that can react in real-time to changes on the blockchain.

2.2.8 Empowering the Catalyst Ecosystem

By establishing a Global State Machine that is both backward-compatible with Ethereum and forward-looking in its integration with distributed data storage and event handling, Catalyst lays the groundwork for a rich ecosystem of dApps. This ecosystem is poised to benefit from the robustness and security of blockchain technology while offering the flexibility and scalability demanded by modern applications. Through KVM and the broader Catalyst framework, developers are equipped with the tools and capabilities to push the boundaries of what's possible in decentralized computing, heralding a new era of blockchain utility and innovation.

2.3 Tools and Extensions

The Catalyst Network is not only a testament to blockchain innovation but also a hub for development efficiency and creativity. Recognizing the importance of accessible, powerful tools for developers, Catalyst has curated a suite of tools and extensions designed to streamline the development process, foster innovation, and facilitate the seamless integration of blockchain technology into a wide array of applications.

2.3.1 Comprehensive Developer Toolkit

Catalyst Web Wallet: A pivotal tool for both developers and users, the Catalyst Web Wallet offers a secure, intuitive interface for managing digital assets on the Catalyst Network. Its integration capabilities with other networks underscore Catalyst's commitment to interoperability and ease of use.

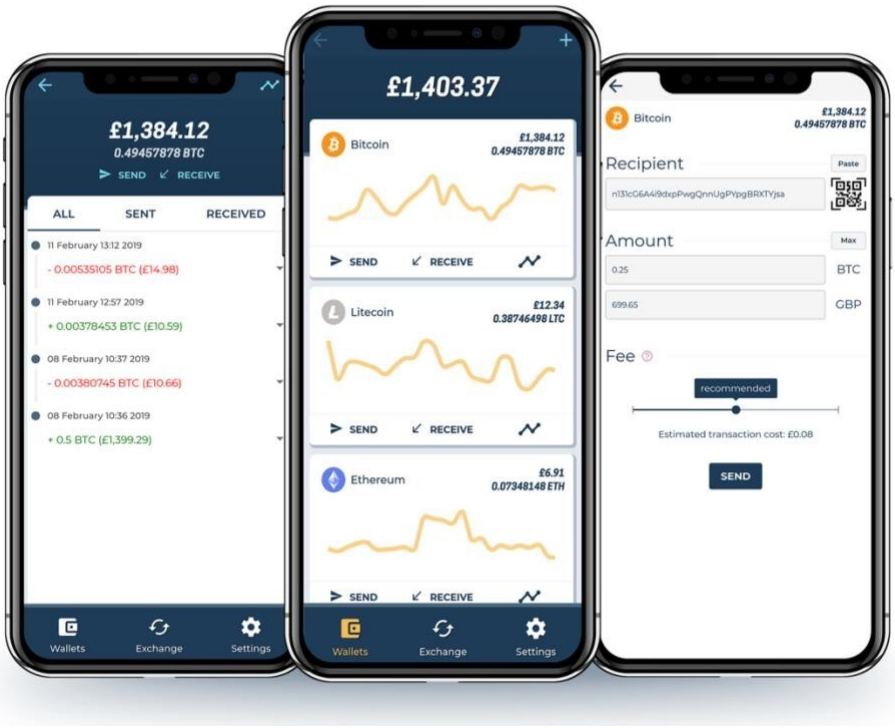

Figure 2: Screenshot of Catalyst CryptoWallet UI.

Block Explorer: This tool provides transparency and insight into the network's activity, including transaction history, block details, and network statistics, enabling developers and users to track the network's health and activity in real-time.

Network Monitor: A web portal that offers a comprehensive overview of the network's status, including node distribution, transaction volume, and network health, assisting developers in optimizing their applications.

Simulator for Network Performance: A testing tool that simulates network conditions and performance at scale, allowing developers to assess the resilience and scalability of their applications under various scenarios.

Development Plugins for Visual Studio Code: These plugins streamline the smart contract development process, offering syntax highlighting, code snippets, and debugging tools tailored for Catalyst development.

Software Development Kits (SDKs): Catalyst provides SDKs for various programming languages and frameworks, ensuring developers can easily integrate Catalyst's blockchain capabilities into their applications, regardless of their technology stack.

2.3.2 Expanding the Ecosystem

The Catalyst team is actively working on expanding this toolkit, with plans to introduce more SDKs and tools tailored for popular programming languages and frameworks. This initiative aims to lower the barrier to entry for blockchain application development, making it accessible to a broader range of developers, from those specializing in systems programming with Rust and C/C++, to those working with high-level languages such as Java, .NET, Python, and Go.

2.3.3 Facilitating Cross-Network Interoperability

With an eye towards fostering a connected and interoperable blockchain ecosystem, Catalyst is also exploring tools and extensions that facilitate bridging to other networks. This not only enhances the utility and reach of the Catalyst Network but also supports the broader vision of a decentralized web where applications and assets can seamlessly interact across blockchain boundaries.

2.3.4 Conclusion

The Catalyst Network's tools and extensions are foundational to its mission of empowering developers and advancing blockchain technology. By providing a robust, developer-friendly ecosystem, Catalyst is paving the way for the next generation of blockchain applications, characterized by their innovation, efficiency, and interoperability.

3. Economy

A founding principle of Catalyst is decentralising control and value and so the whole economy is designed to enable anybody to earn from the running of the network. Users don't need expensive hardware or large cash stakes to benefit. Bitcoin was created to replace a financial system that benefitted privileged groups of people and so Catalyst measures its success by how it measures up to this vision.

3.1 Base Currency and Tokens

Catalyst Networks native network token (coin) is called KAT (in reference to Katal, the unit of catalytic activity). KATs provide the network with the functionality to pay for network services or receive value for the provision of network services. It derives its intrinsic value from the development and use of the network and hence provides utility for the use of the network as well as the work undertaken by producer nodes which maintain the ledger.

A Fulhame (FUL) is the smallest unit of a KAT token, representing 0.0000000000001 KAT (a thousand-billionth of a KAT token), named in homage to the chemist who invented the concept of catalysis. The economic consideration defining the token supply model of KAT are described later and are particular to this currency.

Catalyst Network's base currency KAT is a utility token and as such aims at providing Catalyst users with access to services supported by dApps and smart contracts. The tokens are not designed as an investment although the value of the tokens can vary according to the demands for services on the network. These tokens are considered medium of exchange as these can be used to facilitate the sale, purchase or trade of services on the network. Such trades take place via the use of transactions created by users and broadcast on the network.

The ledger database needs to be frequently and securely updated to account for these token transfers. A healthy network thus relies on a robust mechanism to manage the ledger database in a decentralised manner. Consensus-based protocols are implemented to incentivise users on the network to contribute to the ledger database management, often offering them tokens as reward for their work. Such reward typically comprises of two components: a) tokens paid by the users issuing transactions and directly debited from the user accounts, in the form of transaction fees; b) new tokens injected (or released) into the system.

3.2 Token Supply Model

Some requirements that must be met by Catalyst and mentioned in the introduction of this paper shaped the design of the token supply model for KAT tokens. Namely:

- Ensuring that the network scales and remains secure.
- Incentivising users to join the network and uses practical services available on it.

- Having simple and recognizable pricing models for dApps, in line with cloud computing.
- Allowing anyone to earn from the network, not just people who can afford expensive mining equipment or large stakes.
- Allowing rich file types such as documents and video to be stored and shared efficiently.

The token supply model adopted for Catalyst base currency (KAT tokens) is a dynamically adjusted inflation model [16]: when the genesis ledger state is created the ledger will come into existence with a set of accounts held by founders, investors and community members (see Appendix for more detail). These accounts will hold KAT tokens, the sum of which will constitute the initial volume of tokens in circulation. They will also have the prestige of being genesis accounts for all time.

New tokens will be injected into the ledger as a reward, distributed to the worker nodes who contribute to the ledger database management. Further to this, nodes will be rewarded for providing DFS storage space or smart contract execution RAM. The number of new tokens per unit of time will be capped between 1 and 2% (annually) of the total amount of circulating tokens. The exact token injection factor will be driven by economic and technological factors such as the demand and supply for work as well as demand and supply for services deployed on the network.

3.3 Token Distribution

Users of the network need services accessible at costs that are stable for short periods of time and comparable to currently existing services, notably provided by cloud-based platforms. A healthy economy should therefore reward the builders and operators of services but must also consider the demand for such services. Services are paid for by users via transactions that transfer tokens from and to accounts stored on the ledger.

Transactions are made of transaction entries (spending or receiving tokens). Each transaction entry is typically defined by the address to an account stored on the ledger and the number of tokens debited from or credited to that account, that is the number of tokens paid or received for accessing a service. There are different types of transaction entries, namely:

- Confidential transaction entry
- Non-confidential transaction entry
- Storage transaction entry
- Smart contract transaction entry

Some transaction types can affect the update of multiple ledger partitions. Any transaction includes (small) transaction fees paid to the producers who work to create ledger partition state updates.

During a ledger cycle, a pool of producers creates a ledger state update for a specific partition. The different pools of producers reach consensus on the global ledger state update. At the end of cycle, each ledger partition state is updated. The transfers of tokens embedded in the transactions included in that update reflect the payment for services provided to users on the network. The sum of all the transaction fees is collected and distributed amongst the producers. In addition, new tokens are injected into the system and allocated to the producers for their effort toward maintaining the ledger state up to date.

3.4 Aligning Incentives with Network Goals

The economic model of Catalyst is intricately linked to its overarching goals of decentralization, scalability, and innovation. By aligning incentives with contributions to the network, Catalyst ensures that its economy not only supports the network's technical infrastructure but also fosters a vibrant, engaged community. This approach encourages a wide range of participants, from individual users to large organizations, to contribute to and benefit from the network, driving forward the vision of a decentralized, accessible, and equitable digital future.

4. Governance

The governance refers to any actions carried out by the network that change the rules of the decentralised system. These can be taken out at the protocol-layer (for example, changing the consensus algorithm) as well as at the application-layer (typically impacting the services supported on the ledger). The governance model adopted for Catalyst is built on the principles of decentralising control and decision making while guarding against anyone from buying disproportionate amounts of control over decisions. Therefore, decisions are managed through a mix of strategies that are discussed in this section.

1. Informal discussions through platforms including Discord and Telegram. The team encourages free and open discussion of any and all subjects relating to Catalyst to ensure that as many voices are heard before any kind of formal votes take place.
2. A Decentralised Autonomous Organisation (DAO) that requires users to stake a small quantity of KAT tokens in order to take part in votes. Note: The system works on a one account, one vote system and so no one account holder can disproportionately affect a vote.
3. On-chain votes via smart contracts that weight votes by accounts according to the amount of KAT tokens held in that account.
4. Core team actions that do not require a vote or permission from the community.

4.1 Informal Discussions

Catalyst recognizes the value of open dialogue and community input. Platforms such as Discord and Telegram serve as the foundation for informal discussions, where community members can freely exchange ideas, propose enhancements, and voice concerns. This grassroots level of engagement is crucial for fostering a sense of ownership among participants and for surfacing diverse perspectives that might not emerge through formal channels alone.

4.2 Decentralised Autonomous Organisation (DAO)

At the heart of Catalyst's governance model is its DAO, a decentralized entity that embodies the network's commitment to democratic decision-making. The DAO operates on a principle of one member, one vote, ensuring equitable participation regardless of token holdings. This structure prevents wealth concentration from dictating network evolution, aligning decision-making with the interests of the broader community.

Membership in the DAO requires a nominal stake of KAT tokens, a mechanism designed to prevent spam and ensure participants have a vested interest in the network's success. The DAO oversees significant decisions such as protocol upgrades, tokenomics adjustments, and community initiatives, with proposals subjected to community vote.

4.3 On-chain votes by KAT per account total

Complementing the DAO, Catalyst employs on-chain voting mechanisms to facilitate decision-making for specific technical and economic adjustments. Votes are weighted by KAT token holdings, allowing for a proportional representation of investment in the network. This method ensures that those who contribute more significantly to the network's security and operation have a commensurate influence on its direction, while still maintaining a balance with the egalitarian approach of the DAO.

For a change to tokenomics or consensus to pass, it must therefore pass a DAO vote and an on-chain contract vote. The DAO may also vote to hold this type of vote for other actions.

4.4 Core Team Actions

Acknowledging the need for agility in certain scenarios, the Catalyst governance model empowers the core development team to make unilateral decisions in cases of urgent security or operational issues. This capability is strictly limited to circumstances where delay could compromise the network's integrity or user safety, ensuring that the core team's autonomy does not undermine the network's decentralized governance principles.

4.5 Decision Making Process

The governance framework is designed to be transparent and inclusive, with clear processes for proposal submission, discussion, and voting. Any community member can propose changes, which are then debated within the community and subjected to DAO and/or on-chain voting, depending on the nature of the proposal. This inclusive approach ensures that Catalyst remains adaptable and responsive to the needs of its users, developers, and stakeholders.

5. Conclusion

As the blockchain landscape continues to evolve, the Catalyst Network stands at the leading edge of this technological revolution, embodying a commitment to decentralization, innovation, and accessibility. Through its advanced architecture, including a modular framework and a robust economic model, Catalyst has laid a solid foundation for a new generation of blockchain applications. Our governance model further ensures that this growth is guided by the collective wisdom and participation of our community, maintaining Catalyst's ethos of openness and democracy.

The journey of Catalyst Network is more than just the introduction of another blockchain platform; it represents a leap forward in addressing the persistent challenges of scalability, interoperability, and user accessibility that have hindered blockchain technology's broader adoption. By prioritizing these elements, alongside a steadfast commitment to decentralization and security, Catalyst is well-positioned to drive innovation across various sectors.

Looking ahead, the Catalyst Network is not merely aspiring to be a part of the blockchain ecosystem but to lead its evolution by holding onto the core principles of this industry. We envision a future where blockchain technology becomes seamlessly integrated into everyday life, offering solutions that are not only secure and decentralized but also intuitive and accessible to everyone. This future is not a distant dream but an imminent reality, as we continue to expand our toolkit, foster our community, and welcome new partners and developers to join us in this journey.

The Catalyst Network invites you to be part of this exciting journey as we explore the limitless possibilities of blockchain technology together. With each step, we move closer to a more decentralized, efficient, and inclusive digital world. Thank you for your interest in Catalyst, where innovation meets opportunity, and every voice has the power to shape the future

References

1. V. Tabora, *"The Evolution of the internet, From Decentralised to Centralised"*, https://hackernoon.com/the-evolution-of-the-internet-fromdecentralized-to-centralized-3e2fa65898f5, March 2018

2. D. McCann, *"Data Oligarchs: Power and Accountability in the Digital Economy"*, https://neweconomics.org/uploads/files/Rise-of-the-dataoligarchs.pdf, May 2018

3. T. Berners-Lee, *"30 Years on, What Next For The Web?"*, https://webfoundation.org/2019/03/web-birthday-30/, March 2019

4. IBM, *"What's the potential ROI of IBM Blockchain?"*, https://www.ibm.com/uk-en/blockchain, July 2018

5. M. Walport et al., *"Distributed Ledger Technology: beyond block chain"*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, 2016

6. D. Roe, *"10 Obstacles to Enterprise Blockchain Adoption"*, https://www.cmswire.com/information-management/10-obstacles-toenterprise-blockchain-adoption/, June 2018

7. Ameya, "Sybil Attack and Byzantine Generals Problem", https://medium.com/coinmonks/sybil-attack-and-byzantine-generals- problem-2b2366b7146b, July 2018.

8. C. Sherlock et al., *"Efficiency of delayed-acceptance random walk Metropolis algorithms",* arXiv:1506.08155v1

9. S. Gal-On et al. "*Exploring CoreMark – A Benchmark Maximizing Simplicity and Efficacy*", https://www.eembc.org/techlit/articles/coremarkwhitepaper.pdf

10. IPFS, "*IPFS is the distributed web*", https://ipfs.io/

11. Digiconomist, "*Ethereum Energy Consumption Index (beta)",* https://digiconomist.net/ethereum-energy-consumption, 2019

12. P. Bernat et al, "*Catalyst Network: the Consensus Protocol*". Available under NDA.

13. Hibryda, *"Why Solidity isn't Solid"*, https://medium.com/@Hibryda/whysolidity-isnt-solid-3341af77fc1c, June 2016

14. "Catalyst Network: *Smart Contracts and dApps"*. Report soon available.

15. B. Wang, *"Ethereum is About 1 Million Times Less Efficient for Storage, Network and Computation"*, https://www.nextbigcoins.io/ethereum-isabout-1-million-times-less-efficient-for-storage-network-and-computation/, August 2018

16. "Catalyst Network: *Tokenomics"*. Report soon available.

17. "Catalyst Network: *Catalyst Council Chart"*. Available upon request.