Introduction to Catalyst Network

February 24th, 2024

Version 0.11.0

Abstract

Since the creation of Bitcoin, the blockchain industry has continuously innovated and made strides towards ever faster, more Turing complete, more creative blockchains. But the journey is far from over and there have been stumbles along the way.

Some of the most innovative blockchains have fallen for the alluring benefits of centralisation, requiring either costly mining hardware or high staking buy-ins to benefit from the operation of the network. The foundation of this very industry is decentralisation of control and benefit and so a core tenet of Catalyst is a renewed focus on decentralisation of control and wealth.

But in equal measure, Catalyst is about empowering developers and making blockchain accessible to an industry built on the convenience of cloud computing and APIs. Catalyst is a modular framework seeking to bring the quality and convenience of the wider IT industry to blockchain while bringing the benefits of blockchain and decentralised file systems to the wider IT industry.

This paper gives an overview of the technology innovations and economic considerations behind Catalyst Network.

Background

The 20th century saw the emergence of the Internet, a network technology that has transformed our world, connecting people around the globe in a fair and unbiased fashion while opening new growth of world economies for all. Decentralised and empowering, the Internet has been an enabler of digital services without any native care of fairness. Indeed, fairness was just a by-product of the original decentralised nature of the Internet. As it grew in popularity and saw an explosion of valuable new content, business began to capitalise on and ultimately consolidate that value. Recent decades have seen a small number of businesses disproportionately grow their ownership of and influence on the Internet, effectively re-centralising control and the very nature of the Internet itself [1,2]. Misuse of this centralised power has seen the erosion of trust in those services, but not in the dream of a truly decentralised and honest global network of services that can empower people to work together. As Sir Tim Berners-Lee, the father of the Internet, wrote: "*The web is for everyone and collectively we hold the power to change it. It won't be easy. But if we dream a little and work a lot, we can get the web we want.*" [3].

Following the rumblings of discontent at how the centralised Internet led to an excess of control and value accruing to the largest participants, and concurrent abuses of trust in the use of individuals' personal data together with a resulting increase in bad actors seeking to steal, or ransom, data from the vast centralised data stores, new data storage and processing technology came into sight: the Blockchain. While the Internet is a stack of networking technologies for routing packets of data in decentralised way for the purpose of connecting remote devices, blockchain is a technology that adds the concept of consensus among distributed devices for the purpose of ensuring data is valid, trusted and immutable. Consensus-based protocols require multiple participants across the network to agree on the correct state of the ledger. In the purest implementation of a distributed ledger with decentralised consensus, no single participant is trusted to govern; the network is neutral and enacts the collective agreement of the network users. All nodes on the network are considered equal.

This need for unbiased trust in the data stored and shared, as well as the services hosted on the Internet is factored into the rapid growth of interest in blockchain networks. Distribution and collective consensus not only provide trust, but it also brings the benefit of resilience by removing any single point of failure. Blockchain can provide the ability for users to take back ownership and control of personal data. Decentralised systems tied to business logic and payment mechanisms, makes it possible for individuals to be compensated and rewarded for the use of their data in a consensual and transparent way. The absence of centralised data stores and services leads to an increase in productivity and reductions in cost, while offering more secure and controlled ways for businesses and individuals to share data. IBM reports that for accounting services alone businesses can expect cost reductions as large as 80% [4].

However, the much-anticipated adoption of decentralised computing using blockchain is yet to happen. Indeed, the technology is still new and not yet developed to match today's commercial expectations. The Internet evolved gradually, with a user base and set of services growing over

time, providing time for the technology to mature. Blockchain by contrast, has been launched into a world of billions of users running millions of services, and as such faces a vastly more complex environment with varied and competing requirements. The enthusiasm for blockchains such as Bitcoin, Ethereum and Solana have proven that the market exists for decentralised blockchain networks that decentralise benefit and control. Yet these blockchains have also demonstrated the challenges of scaling the benefits of blockchain to large public networks and have often fallen back to centralising approaches to deliver scale, a compromise that undermines the core purpose for the technology.

Catalyst is a project that has its roots going all the way back to 2012 when a Smart Water Utility Project called “UrbanWater” run with the European Commission (EC) and multiple stakeholders across Europe looked at how to decentralise new smart utility meter data and control. This project was funded by a €4.8 million grant and while predominantly looking at mainstream approaches such as cloud computing and different network topologies, the project also looked at a newly emerging technology called blockchain. After the conclusion of the project in 2018, a new R&D company was formed in London called Atlas City with $5 million of private funding to develop a new open source blockchain that could be used for industrial systems and national scales without compromising on the principles of decentralisation. Working with contributors to established networks such as Ethereum, along with UK universities and commercial organisations, Atlas City developed the open-source Catalyst network technology stack and published research developed over several years. With the conclusion of this R&D project, Atlas City was wound down and the Catalyst technology stack made public, with some code making its way into other projects such as Ethereum.

In 2024, some members of the original Catalyst project have decided that the need is greater than ever to protect the principles of decentralisation and quality developer support and so we are renewing work on the Catalyst blockchain. Our mission is to complete the work that was started and to bring Catalyst to market as a new layer 1 blockchain. This isn’t to compete with existing networks such as Ethereum, but to create a network based on the founding principles of this industry and to grow a community that as well as supporting Catalyst, go on to influence the wider industry and protect the importance of decentralisation.

.

1. Summary

Bitcoin, the first successful public blockchain that came to existence in January 2009 demonstrated the potential for this new technology to be used as a decentralised yet trusted store of value. Building on this early success, new blockchains such as Ethereum and Solana demonstrated the potential for blockchains to provide decentralised computing services, enabling more complex applications and reaching more markets than straight forward storage of value. Bitcoin decentralised money, Ethereum decentralises financial markets. Other blockchains established use-cases in many other areas notably using IoT devices and machine learning techniques [5].

Building a blockchain is a tedious task and for that reason most existing projects are clones, also known as forks, made from a small number of original blockchains. This allows organisations to benefit from already developed blockchains while modifying the elements relevant to their field. The problem with such an approach is that it restricts truly original thinking about wider technological issues such as how a network can scale or operate in environments not designed for a blockchain. As a result of forking from the past, the fundamental issues restricting present blockchain technologies such as scale, privacy, speed and interoperability remain as much of a challenge today as when these early blockchains were first developed [6].

The Catalyst team started from scratch by first surveying operational requirements and existing limitations to create a new design and code base capable to overcome these limitations and to deliver on requirements. The core code base, named Catalyst, is original - does not fork from any other code base - and is made available as open-source software. From its first inception, Catalyst was designed to be modular and so does include some third-party modules such as Netherminds EVM as a compute environment. Indeed, Catalyst could be the earliest example of a modular blockchain since a founding requirement was to start from a set of interfaces to allow partners to build modules independently.

Learning from popular and new blockchains and distributed ledgers as well as the wider IT industry, the team outlined key objectives that it believes forms core requirements that must be met by Catalyst. The following list sets out the fundamental objectives for Catalyst which led to the design decisions and novel approach taken by the Catalyst team. Catalyst must:

1. Become increasingly decentralised at scale.
2. Be capable of scaling to meet future data and distributed service demands.
3. Be able to run nodes on limited resource devices, such as IoT devices, as well as those with larger computing power.
4. Have a flexible and dynamic economy that encourages activity and good behaviour.
5. Allow anyone to earn from the network, not just people who can afford expensive mining equipment or large stakes.

6. Support wider IT industry paradigms such as broadcasting events, integration with service buses and queues, API access and integrate with other emerging technologies such as AI.
7. Allow rich file types such as documents and videos to be stored and shared efficiently.
8. Enable web3.0 and a new generation of online services, that respect the privacy and confidentiality of users: decentralised messaging, email and web applications which give the user control of their data while creating new markets for online services.

2. Technology

2.1 Catalyst blockchain

Catalyst was designed by an experienced team of engineers and researchers who were presented with a difficult challenge: build a large, decentralised network capable of storing all types of data ranging from tabular records through to large files at low cost, in a way that encourages continuous decentralisation of control and benefits. Broadly, this meant solving the blockchain trilemma to maintain decentralisation of control and benefits while supporting a high transaction throughput in a continuously growing network without compromising on security.

The Catalyst team addressed this challenge through a combination of a new consensus mechanism on top of a collection of modules, held together within a modular framework. One way to think of Catalyst is as a framework made up of sockets (interfaces), that modules can be plugged into. Consensus for example exists as a simple Proof of Authority (PoA) module, but the team is working on the primary new consensus mechanism that can be swapped in once complete by unplugging the PoA module and plugging in the new consensus module.

At the core level, the modules that compose the public instance of Catalyst are:

- The *Database* module which is responsible for the structure of the ledger database where digital accounts are stored.
- The *Network* module which handles peer-to-peer communication and different node assignments.
- The *Consensus* module which defines the mechanism used to manage the ledger database (and encapsulates the encryption techniques used for the signature of transactions and generation of private keys and addresses).
- The *Distributed File System* module which manages the storage of all data and old updates of the ledger database.
- The *KAT Virtual Machine* (*KVM*) module integrated into Catalyst which allows previously written smart contracts to be used on Catalyst.
- The *Distributed Compute System* module which, using binaries running inside virtual containers, allows the creation of fully-fledged applications to be run on Catalyst.

The functionalities and specificities of these modules are presented in the following sections.

2.1.1 Catalyst Database Structure

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

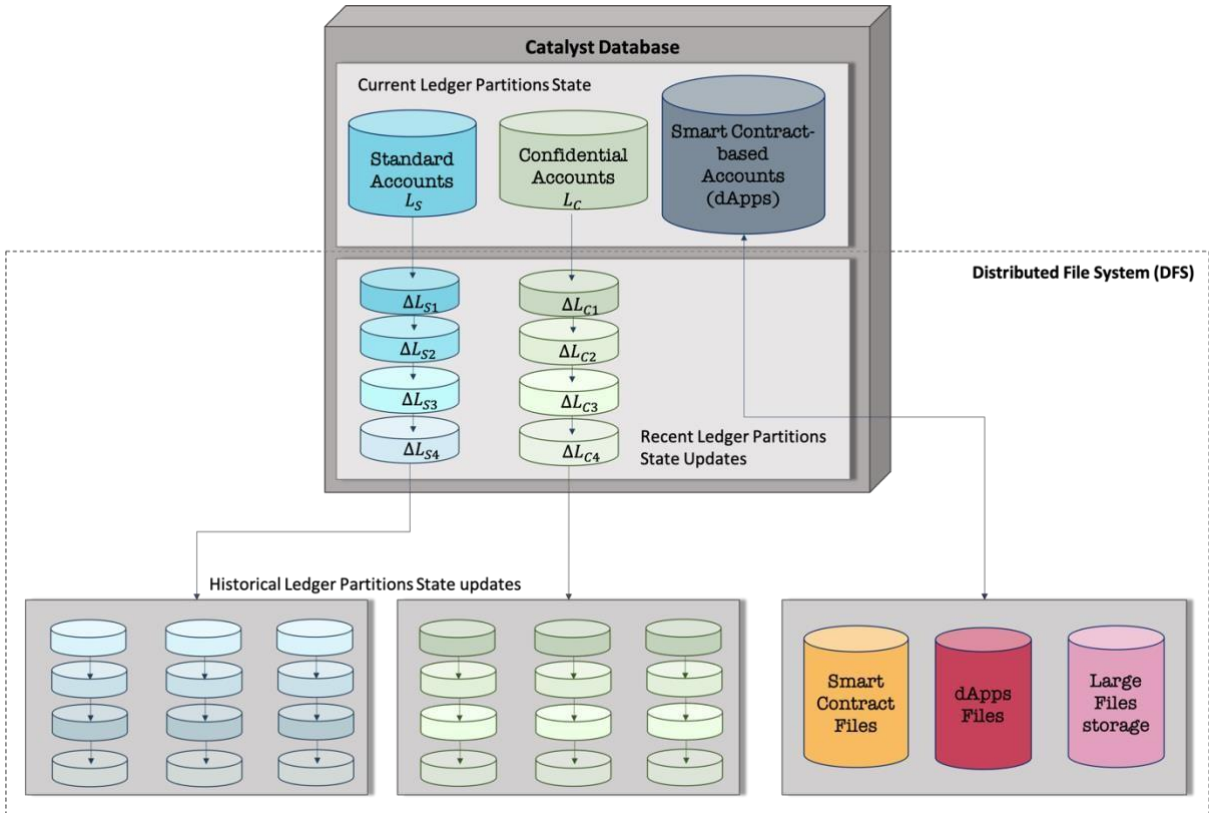

Figure 1: Illustration of Catalyst database architecture.

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

An important feature of Catalyst is the ability to run smart contacts, without unnecessarily restricting the languages that can be used by developers [13]. Since Catalyst is modular then it is possible to extend and switch in different runtime environments over time.

Initially, Catalyst will support KVM, a variant of EVM extended to benefit from distributed file storage. The initial version of KVM will be fully EVM compliant to enable any smart contracts written for EVM to be deployed to Catalyst. KVM will then be extended to incorporate access to data stored within Catalysts distributed file system, allowing smart contracts to process much more than structured ledger data.

Therefore, the computer layer consists of two modules.

1. The Global State Machine Smart Contract System (KVM)
2. The Distributed Compute System (DCS)

This dual approach enables rich distributed applications to be developed by today's industrial developer communities without compromising on the need to maintain a consistent ledger state [14].

The Catalyst roadmap also includes more features to extend the Catalyst compute capabilities.

1. Add additional virtual runtime environments such as SVM which can be targeted by transactions.

2. A new messaging layer added to act as a service bus, allowing contracts to post events and messages that subscribers can register to receive. This removes the need for third party event systems such as Subgraph.

2.2.1 Global State Machine

The KVM module is a runtime environment for updating ledger records using the bytecode superset defined in the Ethereum Virtual Machine (EVM). The decision to create a variant of the EVM for Catalyst as the first runtime environment was made for two main reasons:

1. It provides a way for businesses running projects on EVM networks to easily cross-deploy to Catalyst.
2. Developers already working on EVM networks can develop for Catalyst without learning a new language while continuing to use the developer tools they're familiar with.

2.2.2 Distributed File Storage access and events

While the KVM starts as a pure EVM compatible runtime environment, it will be extended to support access to file objects stored on the distributed compute layer. 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.

KVM will therefore provide read and write access as atomic actions.

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.

To go along with the addition of file access for KVM, KVM as part of the consensus mechanism update will also be extended to generate events that are broadcast on the network and which clients can register with. This means that smart contracts can broadcast messages relating to the result, such as logging information or events that a client can use to build up an event history. This is much like how Subgraph works but would be baked into the framework itself. Subgraph however allows a history of events to be run while the Catalyst node would be running in real time.

2.3 Tools and Extensions

Catalyst already has numerous tools developed by both the Catalyst team and third parties. Some useful tools include:

- Catalyst web wallet (Figure 2). Note: Cent Finance has deployed a rebranded version of this wallet as an iOS and Android wallet for Ethereum, Celo and Gnosis networks. We plan to update the Cent Finance web wallet to be a commercial wallet for Catalyst since the Cent Finance wallet has onramp from two payment providers added. This wallet could also assist with bridging to other networks and provide a nice mobile experience. But even without that, the Catalyst web wallet is a reliable web wallet for Catalyst.
- Block explorer for Catalyst.
- Network monitor as a web portal.
- Simulator, for testing network performance at scale.
- Two plugins for Visual Studio Code for developing smart contracts.
- SDK for wallet and app builders

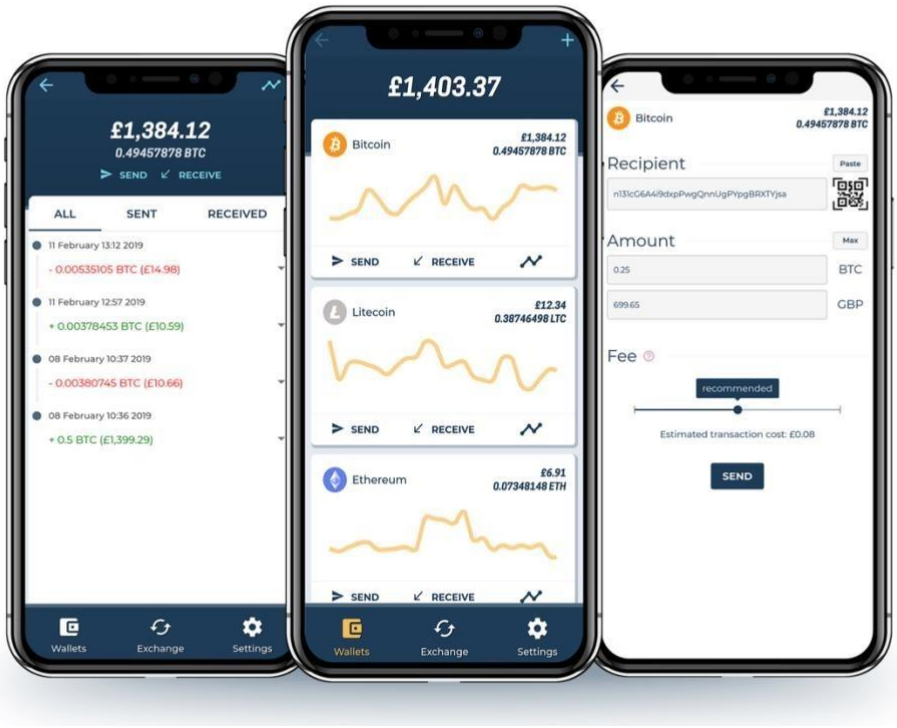

Figure 2: Screenshot of Catalyst CryptoWallet UI.

The team will be building many more tools and SDK's for popular languages and frameworks to assist with integrating systems written in Rust, C/C++, Java, .NET, Python, Go and other popular languages and frameworks.

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.

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

As much as possible, the community in the broadest sense must be given adequate information and time to consider proposals and to debate the merit of proposals. Community members should therefore set out proposals clearly and encourage broad debate through Discord, Telegram and other channels, as well as communicating any dates and mediums of voting to be applied.

This process is an important part of governance even though it doesn't directly involve the vote activity itself.

4.2 Decentralised Autonomous Organisation (DAO)

Initially, Catalyst will employ a DAO running on an Ethereum layer 2 network. This is to ensure that the community is involved and empowered before the main Catalyst network is complete and live. Once the Catalyst main network is live, the DAO will transfer to Catalyst.

To join the DAO, users will be required to stake a small number of KAT tokens into the DAO. This ensures there is a low bar to entry while still guarding against bots spamming the DAO with no cost.

Votes through the DAO are applied as 1 vote per account, regardless of the number of KAT tokens held in the account or staked into the DAO. This ensures that everyone gets an equal

voice at the table, much like one person gets one vote in an election or referendum, regardless of wealth or status.

Any vote impacting consensus or tokenomics MUST have a majority vote through the DAO, to ensure that no one person or small group can impacts the economy that everybody is part of.

4.3 On-chain votes by KAT per account total

A second form of voting is via a smart contract that measures the balance of accounts casting votes, giving accounts with the largest balance a larger impact on the vote. An account with 1000 KAT tokens will have 10 times the impact on a vote to an account containing 100 KAT tokens.

Any vote impacting tokenomics or consensus MUST also include an on-chain vote of this type, since changes of this type directly impact the wealth of token holders.

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

The core team on occasion MUST be able to take actions without the delays associated with a vote. These actions are strictly restricted to matters of security or legal actions. An example of such an event would be the discovery of a zero-day exploit that must be fixed quickly and before public disclosure of the security vulnerability.

4.5 Decision Making Process

The core team working on the Catalyst code base and other features managed under source control will continuously make decisions relating to code and day to day running of the network. The community accepts that the core team is permitted to do this to allow the network to run safely and reliably.

Anybody can raise discussions in Discord and other channels on any subject.

Any DAO members can raise votes for other DAO members to vote on.

If a vote is to enact an on-chain contract vote or if a DAO vote impacts tokenomics or consensus and passes a DAO vote, then a smart contract vote is triggered immediately after.

After all votes are completed, the action goes to the core team to enact.

5. Conclusion

The individual technical components underpinning Blockchain have existed for decades. As the 1st blockchain to find product market fit, Bitcoin managed to recombine these previously established elements in a unique fashion to instil and enable trust in a trust-less system, thus achieving decentralisation and eliminating the need for a centralised authority. Whilst revolutionary, the implementation and expansion of this new approach uncovered limitations that restricted Bitcoin from moving beyond large payments and acting as a store of value. Following blockchains such as Ethereum and Solana built and improved upon Bitcoins approach to open new markets such as DeFi and NFTs, but without finding sufficient market fit to take blockchain mainstream to the same extent as other technologies such as cloud and mobile.

Catalyst sets out to focus on builders to assist with market fit while incorporating crucial supporting technologies such as distributed file storage and integration with APIs and Service Bus. Of equal importance is work on designing a consensus mechanism that supports privacy and decentralisation of control and wealth, the founding drivers that started this entire industry.

The Catalyst code base does not fork from a previously existing projects and includes original and innovating work, including a new collaborative and environment-friendly consensus-based protocol, the possibility to process both confidential and non-confidential transactions as well as smart contracts, an efficient peer-to-peer communication layer and a multi-levelled data architecture for a lean ledger database storing a multitude of data.

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

Appendix

Risk Warnings and Key Legal Information

General Information

The KAT tokens and related convertible ERC-20 tokens launched as part of the Catalyst project (together the "Tokens") do not have the legal qualification of a security. The sale of the Tokens is final and non-refundable. The tokens are not shares and do not give any right to participate to the general operations or management of Catalyst beyond the designated community activities set out in this document. The Tokens should not be used or purchased for speculative or investment purposes. By participating in any token sale, the purchaser of the Tokens is agreeing that they are aware that national securities laws, which ensure that purchasers are sold purchases that include all the proper disclosures and are subject to regulatory scrutiny for the purchasers' protection, are not applicable. Anyone purchasing the Tokens expressly acknowledges and represents that she/he has carefully reviewed this document and fully understands the risks, costs and benefits associated with the purchase of the Tokens.

Knowledge Required

By participating in any token sale, the purchaser of the Tokens undertakes that she/he understands and has significant experience in cryptocurrencies, blockchain/DLT systems and services, and that she/he fully understands the risks associated with the crowd sale as well as the mechanism related to the use of cryptocurrencies (incl. storage). Catalyst shall not be responsible for any loss of the Tokens or situations making it impossible to access the Tokens, which may result from any actions or omissions of the user or any person undertaking to acquire the Tokens, as well as in case of hacker attacks.

Risks

Acquiring the Tokens and storing them involves various risks, in particular the risk that Catalyst Network may not be able to launch its operations and develop its blockchain and provide the services promised. Therefore, and prior to acquiring the Tokens, any user should carefully consider the risks, costs and benefits of acquiring the Tokens in the context of the crowd sale and, if necessary, obtain any independent advice in this regard. Any interested person who is not in the position to accept or to understand the risks associated with the activity (incl. the risks related to the non-development of Catalyst) or any other risks as indicated in this Appendix should not acquire any Tokens.

Important Disclaimer

This document shall not and cannot be considered as an invitation to enter into an investment. It does not constitute or relate in any way, nor should it be considered as an offering of securities in any jurisdiction. This document does not include or contain any information or indication that might be considered as a recommendation or that might be used as a basis for any investment decision. The Tokens are utility tokens which can be used only on Catalyst Network and are not intended to be used as an investment. The offering of the Tokens on a trading platform is done in order to allow the use of Catalyst Network and not for speculative purposes. The offering of the Tokens on a trading platform does not change the legal qualification of the Tokens, which remain a simple means for the use of Catalyst Network and are not a security.

Legal

Catalyst is not to be considered as an advisor in any legal, tax or, financial matters, or a provider of investment advice. Any information in the document is provided for general information purposes only, and Catalyst does not provide any warranty as to the accuracy and completeness of this information.

Regulatory authorities are carefully scrutinising businesses and operations associated to cryptocurrencies across the world. In that respect, regulatory measures, investigations or actions may impact Catalyst's team and even limit or prevent it from developing its operations in the future. Any person undertaking to acquire the Tokens must be aware of Catalyst's business model, the document or terms and conditions may change or need to be modified because of new regulatory and compliance requirements from any applicable laws in any jurisdictions. In such a case, purchasers and anyone undertaking to acquire the Tokens acknowledge and understand that neither Catalyst nor any of its affiliates shall be held liable for any direct or indirect loss or damage caused by such changes.

Catalyst will do its utmost to launch its operations and develop Catalyst Network. Anyone undertaking to acquire the Tokens acknowledges and understands that Catalyst does not provide any guarantee that it will manage to achieve it.

Representation & Warranties

By participating in the crowd sale, the purchaser agrees to the above and in particular, they represent and warrant that they:

- have read carefully the document and this Appendix, and agree to their full contents and accept to be legally bound by them

- are authorised and have full power to purchase the Tokens according to the laws that apply in their jurisdiction of domicile

- are not a US citizen or resident

- live in a jurisdiction which allows Catalyst to sell the Tokens through a crowd sale without requiring any local authorisation

- are familiar with all related regulations in the specific jurisdiction in which they are based and that purchasing cryptographic tokens in that jurisdiction is not prohibited, restricted or subject to additional conditions of any kind

- will not use the crowd sale for any illegal activity, including but not limited to money laundering and the financing of terrorism

- have sufficient knowledge about the nature of the cryptographic tokens and have significant experience with, and functional understanding of, the usage and intricacies of dealing with cryptographic tokens and currencies and blockchain based systems and services

- purchase the Tokens because they wish to have access to Catalyst Network; and

- are not purchasing the Tokens for the purpose of speculative investment or usage.

Governing Law & Arbitration

Any dispute or controversy arising from or under the crowd sale shall be resolved by arbitration in accordance with the UK Rules of International Arbitration in force on the date when the Notice of Arbitration is submitted in accordance with these Rules. The arbitration panel shall consist of one arbitrator only. The place of the arbitration shall be London, UK. The arbitral proceedings shall be conducted in English.