Introduction to Catalyst Network

February 21st, 2024

Version 0.10.0

Abstract

Learning from blockchains and distributed ledgers as well as the wider IT industry, the Catalyst team has developed Catalyst, a full stack distributed network built to fulfil the real-world potential of Distributed Ledger Technology, enabling the next generation of distributed computing applications and business models. 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 and more broadly, Distributed Ledger Technology (DLT). 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 DLT. Distribution and collective consensus not only provide trust, but it also brings the benefit of resilience by removing any single point of failure. Blockchain and DLT 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 and DLT 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 and DLT, 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 and Ethereum has proven a market exists for a truly scalable and professionally engineered blockchain. Yet these blockchains have also demonstrated the challenges of scaling the benefits of blockchain to large public networks, or to support industrial use cases, as well as highlighting many other challenges including keeping running costs low and stable and supporting data types other than tabular data. For example, a smart utility system might entail millions of smart meters writing frequent records to a SQL Azure database at a cost of around 0.00059202 cents per record. At the other end of the scale, a media system might depend on the storage of large video assets, an oil exploration company might store very large field mapping data sets or an NFT business might depend on detailed jpg files.

The idea to develop a new distributed computing technology derived from the lessons, but not the code, of existing blockchain and distributed ledgers began in 2012 as part of the Smart Water Utility Project “UrbanWater” with the European Commission (EC) and multiple stakeholders across Europe. €4.8 million grant was awarded to develop a demonstrable platform for securely collecting and distributing data and services for future smart cities while being resilient to future threat actors. That project focused on data collection, storage and distribution using a range of technologies from cloud computing to homomorphic cryptography, but certain key challenges proved intractable using these approaches. Work also included looking at early blockchain code bases such as Bitcoin and Ethereum. While these code bases provided benefit around trust, they prove unsuitable for supporting millions of smart meters and other sensors. The project highlighted the need for a new network that could provide immutable data storage and consensus at scale without limitations of data types, choice of programming language for running decentralised business logic and applications (smart contracts) and enable seamless integration with industrial and other types of systems. This work sowed the seeds for engineering a new decentralised system and the eventual formation of the team behind Catalyst to focus on blockchain to see this vision through.

Catalyst is an original software engineering project that sets out to provide a stack of technologies on top of the Internet for the purpose of supporting all types of data storage and services. This paper presents the vision of Catalyst, providing a high-level look at the most unique and important technical elements of the network including its ledger architecture, file storage, compute and consensus mechanism, along with its economic and governance frameworks.

1. Summary

Blockchain has undoubtedly revealed the capability for distributed ledger technologies to disrupt our business models. 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, next generation blockchains such as Ethereum and Neo demonstrated the potential for blockchain platforms to provide decentralised computing services, enabling more complex applications and reaching more markets than straight forward storage of value. Subsequent blockchains and distributed ledgers established use-cases in many other areas notably through the use of IoT devices and machine learning techniques [5].

Building a distributed ledger 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 DLT. 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 project started from scratch by first surveying operational requirements and existing limitations to create a new distributed computer system capable to overcome these limitations and deliver the necessary requirements. The code base developed by Catalyst engineers, named Catalyst, is original - does not fork from any other code base - and will be made available as open-source software. Catalyst is a full stack distributed network written using the .NET Core framework.

Learning from popular and new blockchains and distributed ledgers as well as the wider IT industry, Catalyst outlines key objectives that it believes forms the set of requirements that must be met. The following list sets out the fundamental objectives for Catalyst which led to the design decisions and novel approach taken by the Catalyst team and described in this paper. 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. Be able to benefit from the investment in skills and technology already made by businesses, by allowing decentralised Applications (dApps) to be developed in popular industry programming languages and frameworks.

6. Have simple and recognizable pricing models for dApps, more in line with cloud computing.
7. Allow anyone to earn from the network, not just people who can afford expensive mining equipment or large stakes.
8. Allow rich file types such as documents and videos to be stored and shared efficiently.
9. 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 Distributed Ledger

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 structured tabular records through to large Binary Large Objects at low cost to users, as well as dApps written in any language. Broadly, this meant solving the blockchain trilemma to maintain decentralisation and support a high transaction throughput in a continuously growing network without compromising on security.

The Catalyst team addressed this challenge by building the components of Catalyst as independent modules that could be customised and utilised individually as required.

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.

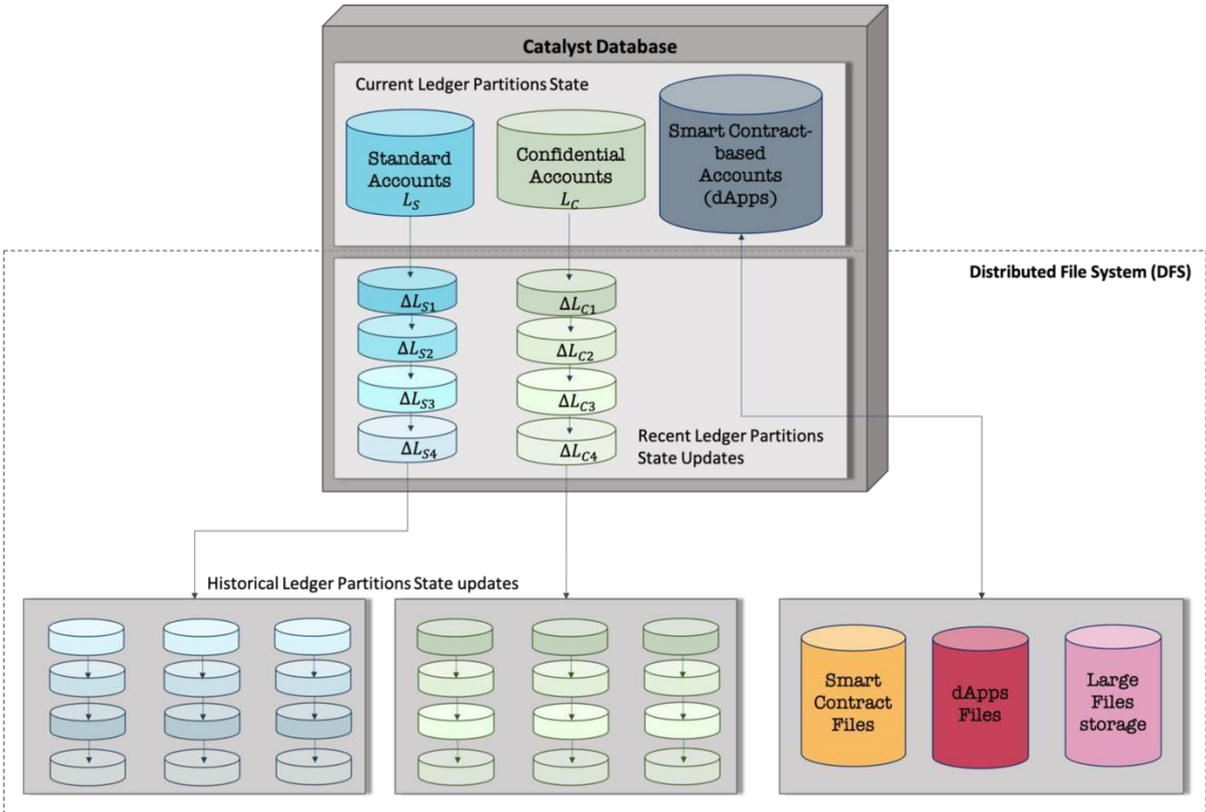

Figure 1: Illustration of Catalyst database architecture.

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 on the Catalyst team 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 Network is the ability to run feature rich dApps without restrictions around the programming languages employed [13] or the type of data stored on the ledger (structured versus unstructured data), therefore providing a similar experience to developers of applications and services running in the cloud.

Catalyst accomplishes this with a dual approach to running distributed processing services in 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].

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 was made for two main reasons:

1. It provides a way for businesses running projects on Ethereum to migrate these to Catalyst and benefit from some of the distinct features of Catalyst Network, including its DFS and Catalyst ability to achieve a high transaction throughput.

2. It removes the need for developers already working in the Ethereum space to learn other programming languages and provides a convenient opportunity to use developer tools created for Solidity.

KVM will thus be familiar to anybody who is used to working with Ethereum but is distinct to EVM to enable features specific to Catalyst.

2.2.2 Distributed Compute System

While the KVM module follows the tried and tested approach of other blockchains for handling transactions, it presents clear limitations:

1. Its limited bytecode sets, and domain specific programming languages exclude the world major developer communities from developing feature rich dApps in the programming languages and frameworks that they are familiar with.
2. The plethora of previously written software libraries, tools and design patterns cannot be reused within a decentralised network.

Decentralised networks must be able to support the standards, software and skillsets that already exist in the wider IT industry to play a significant role in the web 3.0 world and reach widespread adoption.

Catalyst addresses this challenge with its Distributed Compute System module (DCS) which enables rich software services to be developed in any language or framework and run in a decentralised fashion using containers.

DApps written for DCS can be written in any language or framework (such as Java, C++ and C#) and can take as long as necessary to complete. The only operational requirement is that it must be able to run within a locked down but otherwise standard virtual container and must support the Catalyst dApp messaging interface for connecting with the node process. A DCS dApp can interact with files stored on DFS and with oracles. It can also make calls to smart contracts running on KVM.

Updates to the ledger require calls to smart contracts on KVM, similarly to traditional native processes calling smart contracts in a database management system (DBMS). This thus allows for highly complex software systems to be built and run in a decentralised fashion without needing to complete within a single ledger cycle and without the bytecode limitations of ledger specific programming languages. It also allows for specialised node types (GPU, ASIC or even, in the future, quantum nodes) to be deployed for certain types of process.

2.2.3 dApps Running Cost

The approach to pricing dApps running costs is yet another innovation on Catalyst. In blockchains such as Ethereum, dApps must be developed before they can be fed into a price calculator that derives short-term running costs. This is impractical since it requires individuals or businesses to build products before they can get an estimate of the running costs. It is found that running costs can be over one million times [15] that of a cloud environment.

Catalyst uses an entirely different approach, derived from the world of cloud computing where running costs are calculated as a simple multiple of resource and time. Since dApps on Catalyst are run in a virtualised environment with memory, storage and compute then just like with cloud computing, the running cost is calculated as the function of the resource required for the virtualised environment. If a business can develop an application for a virtual machine environment in the cloud, they can develop a dApp on Catalyst, calculate a comparable running cost and easily deploy it.

2.3 User Interface

People and machines need to interface with Catalyst to benefit from the services supported by the network. Individuals need to be able to connect to Catalyst with their mobile phone and other devices to check their balances, securely store and decide who may access their personal data, and potentially perform unlimited kinds of other activities. Machine learning algorithms and initiatives need to be able to connect for the purpose of analytics as well as for providing new services to Catalyst users.

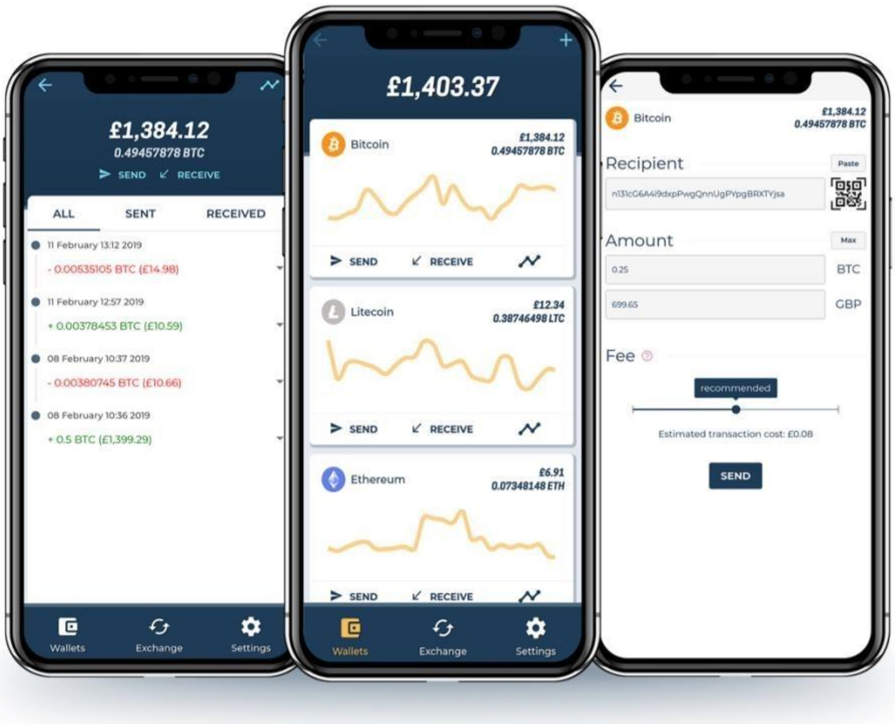

Figure 2: Screenshot of the Catalyst CryptoWallet UI.

The Catalyst mobile wallet application illustrated in Figure 2, CryptoWallet, is available for working with Catalyst tokens and common digital currencies.

Nodes on Catalyst Network can be integrated with the mobile wallet application allowing a rich set of services to be developed and run on it. It will interact with the user's mobile phone and other (IoT) devices, whether they are smart home devices or remote sensors in a logistics network. A powerful node (or hub) could also run machine learning algorithms in conjunction with a dApps store to provide a whole new services ecosystem and user experience unlike any which have existed in the digital world before.

3. Economy

Catalyst places equal significance on the need to innovate around governance and economics policy as it does on the technological aspects. Catalyst Network provides an environment that is stable and affordable for service providers and their customers as well as having the ability to adapt to changing real-world conditions.

3.1 Base Currency and Tokens

Most blockchains require a native base cryptocurrency on top of which all activities are derived. An Ethereum dApp may introduce its own ERC-20 token but this is still ultimately dependent on the native cryptocurrency, Ether. Catalyst Network takes an alternative approach by introducing the ability to add new base cryptocurrencies independent of dApps.

Catalyst Network 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.

A native cryptocurrency or token on Catalyst Network is an assembly, or binary, that implements an interface and runs alongside the Catalyst Network base currency. Such assembly is stored on DFS in a similar manner to dApps and is dynamically loaded and bound to a dApp. This allows for highly complex tokenisation models to be developed with fully independent dApps that use those tokens. The currency assembly is loaded and run inside a locked down container along with the calling dApp. It is therefore free to contain as much logic as it chooses with the outputs being sent as messages to the host nodes for feeding into the base consensus mechanism.

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 the individuals that participated to the different phases of TGE and as such purchased tokens (see Appendix for more detail). These accounts will hold KAT tokens, the sum of which will constitute the initial volume of tokens in circulation.

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 practical 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 creators and operators of services but must also consider the demand for such services. Services on a network are provided through dApps, which in turn require the ability to manage large flows of transactions, storage space and RAM for smart contracts execution. 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 are collected and distributed amongst the producers. In addition, new tokens are injected into the system and also 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 takes inspiration from modern democratic systems. The governance body, so-called Catalyst Council (or Council), will be comprised of representatives from the Catalyst team and a range of communities including developers, cryptographers, economists, legal experts and other representatives who specialise and contribute to the network evolution, in order to ensure a holistic view behind Catalyst.

It is the Catalyst teams view that the Catalyst governance body should be decoupled from the ledger activity. That is to say that a stakeholder holding many worker nodes, or a vast number of tokens will not have an inordinate or directly proportional impact on the governance decision-making process. As with many real-life institutions, the governance body will have a mandate set in advance and be required to carry out all responsibilities in accordance with said mandate [17].

4.1 Governance Committee

Under this governance body, three vertical areas of governance will be defined: Technology, Economy and Community. Each Committee will have a panel of experts appointed by the Council and tasked with day-to-day responsibilities to engage with Catalyst ecosystem stakeholders as well as outside experts and advisors. The expert committees will propose recommendations to the Council for changes or new features within their committee to ensure actions are taken to keep the network healthy and dynamic. The Catalyst Council will be the decision-making body of Catalyst Network.

An outline of responsibilities for each Committee is noted below:

- *Catalyst Technology Committee* - work related to building and releasing updates of the Catalyst Network, and other technical issues.
- *Catalyst Economy Committee* - work related to monetary policy around token supply and treasury, and other economic and commercial governance issues; and
- *Catalyst Community Committee* - work relating to marketing and promoting the Catalyst Network globally, and the appointment and management of Catalyst ambassadors for outreach and education.

Each expert Committee will have the ability to establish Sub-Committees, to address domain-specific topics and issues. These Sub-Committees may change from time-to-time based on the needs of the network and as approved by the Council.

The Catalyst team, as the originator of the network, will help initiate and coordinate the Council and these expert Committees in order to get them established and self-sufficient. It is intended that the Council will as soon as practically possible be independent from the Catalyst team and comprised of a majority of non- Catalyst core members. Any member of the Catalyst community (e.g. any Catalyst user node) can apply to join an expert Committee and the Catalyst Council, in conjunction with each panel, will decide who gets accepted to ensure best representation of our society experts.

4.2 Catalyst Council

The Catalyst Council shall include nine Representatives. The Representatives will consist of one selected from each Expert Committee (for a total of three appointees), plus six Elected Representatives elected by the Governance Stakeholders. The Chairperson will be selected from the six Elected Representatives by the Representatives.

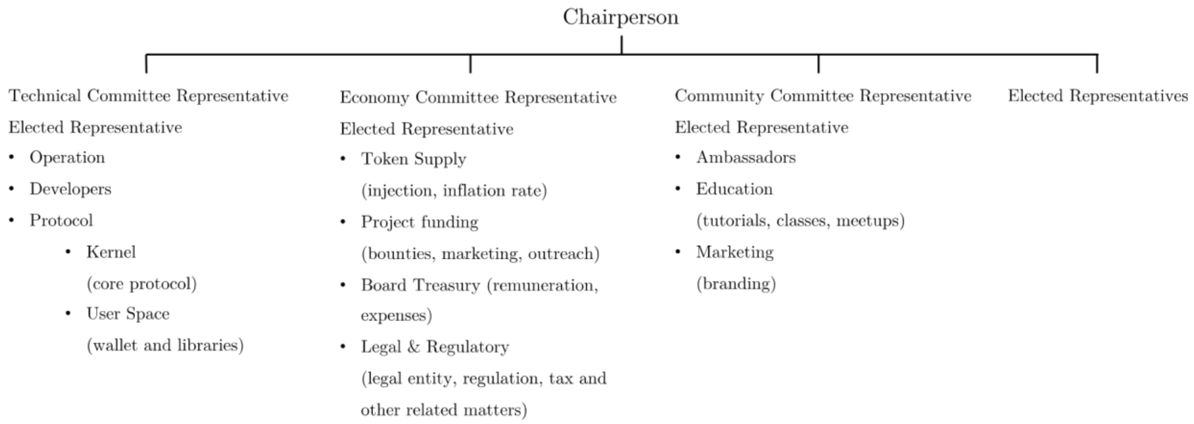

Figure 3: Organisation of the initial domains managed by Catalyst Council Committees.

One specific responsibility of the Elected Representatives is to represent the voice of individual contributors and worker nodes on Catalyst in the aim to avoid hard forks of the network.

Each Representative will also work on specific goals which he/she brings to the Council as highlighted during the election process.

The Council will determine the focus of its work and publish a limited number of primary objectives and key results (“OKRs”) decided by the Representatives. The OKRs will be decided and reported back to the Catalyst community on a periodic basis, such period to be not less than twelve months, and not more than eighteen months.

4.3 Decision Making Process

Engineering decisions about Catalyst base code maintenance will be made by the Technology Committee, and submitted to the Catalyst Council for approval, following their expertise and that of the actively engaged developer community (including the Catalyst engineering team). Similarly, issues that lie within the Economy Committee's and Community Committee's domain will be made by the respective Committee and recommended to the Catalyst Council for adoption.

Larger decisions that impact the Catalyst Network community on technological, economic and community areas (collectively "Significant Matters") will be put to the community for a vote. Significant Matters will be defined, analysed and communicated as Catalyst Improvement Proposals (CIPs), and will be developed and submitted for vote by the Catalyst Council.

As a result, decisions that impact dApp developers in a significant way such as changing the dApp implementation framework or fee structure will be made by the Catalyst community. This allows engineers to deploy quick optimisation of the Catalyst code base while giving the community control over major engineering, commercial or community decisions.

5. Conclusion

The individual technical components underpinning Distributed Ledger and Blockchain Technologies have existed for decades. As the 1st generation blockchain, Bitcoin managed to recombine these previously established elements in a unique fashion so as to instil and enable trust in a trust-less system, thus achieving decentralisation and eliminating the need for a centralised authority. Whilst completely revolutionary at the time, the implementation and expansion of this new approach uncovered limitations and hurdles to both expanded use and ultimately mainstream adoption. 2nd generation DLTs and blockchains built and improved upon this original foundation but fall short of resolving all associated issues.

The Catalyst team has developed a distributed network, Catalyst, to solve the issues of previous DLTs and blockchains, improving upon those which came before, resolving such challenges and enabling an equitable and proportionate compensation to participants on the network. Catalyst was designed around the notion that a democratic and ethical network can exist and be secure, decentralised, scalable and respect its users' privacy.

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 in the Catalyst TGE (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. The Tokens should not be used or purchased for speculative or investment purposes. By participating in the TGE, 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 the TGE, 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). The Catalyst team 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 the 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

The Catalyst team 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 Catalysts business and even limit or prevent it from developing its operations in the future. Any person undertaking to acquire the Tokens must be aware of Catalysts 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.

The Catalyst team 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 the Catalyst team 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.