Introduction to Catalyst Network

January 28th, 2022

Version 1.0.0

Abstract

In 2018, the story of Catalyst began with the mission to build a modular blockchain framework that could support the complex processing of structured on-chain data and unstructured distributed data. The thesis for this was that many use cases would emerge that needed to store large datasets such as images, video and music in a way that was distributed and managed by smart contracts on a blockchain.

Millions of dollars went into R&D which culminated in the Catalyst blockchain framework covered by this document. At its heart, Catalyst is a collection of modules combined through an interface framework to allow the blending of distributed file storage services, blockchain, consensus mechanisms and third-party off-chain services. While this makes Catalyst a powerful framework for many use cases, we are focusing primarily on the NFT and emerging metaverse as industries which are ideally suited to the Catalyst framework.

Catalyst has been developed in .NET which allows it to be cross-platform and familiar to many developers as well easy to integrate into gaming, media and other such systems.

Background

Since the release of Bitcoin, an entire industry has sprung up, experiment and discovering just what new types of world models become possible through this new paradigm of decentralised ownership. Digital cash led to decentralised finance with new ways to invest, borrow and trade. Digitised non-fungible assets has led to new forms of artwork, new ways to own and share those assets and new ways to combine and protect those assets.

Today the story continues forward and fortuitously, it happens at a time when another field of technology is moving forward in a way that could cause the blockchain industry to have its biggest impact on the world to date.

The movie Ready Player One paints a picture of a world where people mix the real world with the virtual. People live and work in both worlds, they have identities in both, they have property and social lives in both. While this is just a movie it does provide a glimpse of where the world could be and highlights, they type of technology that would need to exist to truly blend the physical and digital world.

Facebook recently rebranded itself to Meta, setting out its belief that the future is a virtual online world where people come together. Today people do this through social media platforms such as Facebook but if the environment is just flat images on a screen, then people will never be fully emersed in the experience. Microsoft and other companies have set out their intentions to be a part of this new virtual world building, for Microsoft it would be through their consoles and gaming environments. Games companies, hardware companies, world builders are important players in this emerging space that is being called the Metaverse.

But what we see, and experience online is only part of the Ready Player One vision. A truly immersive experience requires much more

- People in this new metaverse need identity and from that identity they will develop a reputation, friendships, communities.
- People will need trade and money which can be taken with them wherever they travel in this new metaverse, safe that their money won't just disappear.
- People need to truly own what they take into the metaverse with them and what they buy in there. It needs to be as secure and dependable as the real world.

When people in the blockchain talk about the metaverse they are often talking about digital ownership more than the visual experience of the metaverse. For this industry, the metaverse is their digital identity and reputation, the assets attached to that identity and trade. Blockchain play an important role in the emerging metaverse but even blockchain has its limitation. Virtual worlds need large files such as 3D models, images, video and audio and this needs to be stored in a way that can't simply disappear when a server is shut down.

This brings in a third technology, distributed file storage to hold these large assets alongside on-chain data.

We exist at an exciting time in the IT industry, a time when advances in data storage, security, AI, blockchain, computing power, VR, Quantum Computing and more are advancing at such a pace that for the first time we can perceive a future where a Ready Player One experience could be a reality in our lifetime. This reality however will only exist if these technologies come together with minimal tribalism, with industries working together and recognising the valuable contribution that each has to offer.

People don't play games to make money, they play games to have fun, to develop characters, to follow a story, even to part of a community having shared adventures. The games industry has decades of experience for building game worlds that people want to visit time and time again as well as creating economies within games that don't get in the way but rather contribute towards the overall fun experience. But games companies don't necessarily know how to give their players true ownership within games and identities that follow the person wherever they go.

This is an emerging space. What exists in the decades to come will be different to anything we can imagine but for now we know what needs to be built, what experiments to run and so we need the tooling and environment to support this progress forward.

1. Summary

Catalyst was formed not to replace any blockchain or other technology but rather to create framework and networks that would assist with the creation of digital assets and in time, virtual worlds. Catalyst was started in 2018 before we were commonly using the term metaverse and the concept of the metaverse was not something the Catalyst team was thinking about at the beginning.

In those early days, the Catalyst team was meeting with construction companies, oil companies, transport companies. We started by asking businesses about what assets they own or support, how are they managed, what benefits could come from digitising them onto a blockchain. This line of questioning becomes a rabbit hole because while you start with the idea of creating a digital representation of the real world you quickly find yourself discovering that without the limitations of the physical world then entirely new universes become possible. Why limit what the world can be if we don’t have to?

But whether we’re building identical copies of the real world or entirely new imagined worlds, the fundamental technologies that need to exist are the same.

- The technology needs to be open source and decentralised without any single entity having absolute control. People share the world, and it needs to be the same for the digital world.
- People need identity, with an identity they can build a reputation. The field of blockchain has much to offer in this area.
- People need to be able to buy and sell. Cryptocurrency and stable coins provide true ownership of money.
- People need to be able to truly own property and have it held as securely as an object in the real world. NFT’s are a powerful example of this.
- People need more than just simple pieces of data, they need pictures, video, audio and more. Distributed file systems allow for files to be stored and shared securely.
- People need to benefit from all of this without knowing about it. They need to experience the benefits in the games they play, in their cars, in their homes, on their mobile devices. This means integration with the builders whether it’s game engines such as Unity or consoles or other software or hardware system.

To fulfil this, we realised that we couldn’t and shouldn’t build it all. What we could do is create a framework that allows modules to be created and added. Blockchain Lego is a popular term today and we set out with that in mind from the very first line of code in Catalyst.

We wanted to allow people to use as many programming languages as possible and we wanted to make it accessible to a large developer community across many operating systems as well as making it accessible to builders, particularly game makers and media producers.

With this in mind, we opted to build the framework in .NET for the following benefits.

- .NET allows for apps to be built and run-on Windows, MacOS, Linux and Android.
- .NET supports many programming languages including C#, Visual Basic and F#
- .NET supports many frameworks and technologies including WebAssembly
- .NET makes it easy to integrate with and use for games makers who target Windows or Xbox as well as popular games engines such as Unity

But Catalyst is also a protocol and so there's no reason why the community shouldn't develop the same framework and modules in other languages and frameworks. Indeed, this is encouraged to create the broadest possible user case while helping to protect networks that are running on Catalyst.

While Catalyst is the framework and modules, it is also a set of networks. Developers need networks to connect to and so there will be at least two public Catalyst networks. One network will be a test network for the Catalyst developer community to experiment with and the second will be a live main network with its own token economy to support the work underpinning the development and support of the Catalyst network and environment. It is expected that over time, other test and production networks would form to support specific markets and to run experiments with different consensus mechanisms and technologies.

While Catalyst will have a live production environment with its own consensus mechanism and token economy, it is not the intention of Catalyst to take value from other networks such as Ethereum. Indeed ultimately, we believe it's vital that Catalyst should become part of the wider blockchain ecosystem including Ethereum and so the intention is to move the main network in time to become a layer two network to Ethereum. This will allow assets and value created on Catalyst to move to Ethereum and back again as well as reassuring users that value on Catalyst once at scale is secured by the Ethereum network as well as its own consensus mechanism.

2. Technology

2.1 Catalyst Framework

The Catalyst framework consists of a set of interfaces and modules which can be combined in different configurations to create different types of nodes. For example, modules could be combined to create a node ideally suited to run as a cloud-based service using the PoRW consensus mechanism while a different configuration could combine different modules to create a desktop node running PoA on the test network.

This modular approach simplifies the process for blockchain developers to build and test new modules or even configure and deploy entirely new networks.

Modules exist spanning many areas including consensus, ledger, distributed file system, mempool, signature schemes, hashing modules, web3 services, networks, runtime environments including the EVM compatible KVM environment and more. Modules are combined using the Visual Studio solution (.sln) file. Presently there are two .sln files.

Catalyst.sln – Builds a node using the PoRW consensus mechanism to become the main network. This consensus mechanism is still in development and will provide a novel, resilient and efficient consensus mechanism that rewards anyone running a node. A separate detailed paper on this consensus mechanism is available through the Catalyst website.

Catalyst.Node.POA.CE.sln – Test network node running the POA consensus mechanism.

The main difference between the above two configurations is the consensus modules used while both provide a combined decentralised ledger and distributed file system experience. Working with the community we will continue to grow this collection of modules and new solution files.

The following figure shows a list of the modules presently available within the Catalyst framework although this list is likely to continue to grow over time. Following on from this are sections covering some of the modules presently included in the Catalyst module library that are combined to form the PoRW network.

..	
Catalyst.Abstractions	Merge dev into master (#1237)
Catalyst.Benchmark	Merge dev into master (#1237)
Catalyst.Cli.Tests	Merge dev into master (#1237)
Catalyst.Cli	Merge dev into master (#1237)
Catalyst.Core.Lib.Tests	Merge dev into master (#1237)
Catalyst.Core.Lib	Merge dev into master (#1237)
Catalyst.Core.Modules.Authentication.Tests	Merge dev into master (#1237)
Catalyst.Core.Modules.Authentication	Merge dev into master (#1237)
Catalyst.Core.Modules.Consensus.Tests	Merge dev into master (#1237)
Catalyst.Core.Modules.Consensus	Merge dev into master (#1237)
Catalyst.Core.Modules.Cryptography.BulletProofs.Tests	Merge dev into master (#1237)
Catalyst.Core.Modules.Cryptography.BulletProofs	Merge dev into master (#1237)
Catalyst.Core.Modules.Dfs.Tests	Skip tests which fail intermittently. (#1242)
Catalyst.Core.Modules.Dfs	Bump PeterO.Cbor from 4.0.0 to 4.5.1 in /src/Catalyst.Core.Modules.Dfs (
Catalyst.Core.Modules.Hashing.Tests	Merge dev into master (#1237)
Catalyst.Core.Modules.Hashing	Merge dev into master (#1237)
Catalyst.Core.Modules.KeySigner.Tests	Merge dev into master (#1237)
Catalyst.Core.Modules.KeySigner	Merge dev into master (#1237)
Catalyst.Core.Modules.Keystore.Tests	Merge dev into master (#1237)
Catalyst.Core.Modules.Keystore	Merge dev into master (#1237)
Catalyst.Core.Modules.Kvm.Tests	Merge dev into master (#1237)
Catalyst.Core.Modules.Kvm	Merge dev into master (#1237)
Catalyst.Core.Modules.Ledger.Tests	Merge dev into master (#1237)
Catalyst.Core.Modules.Ledger	Merge dev into master (#1237)
Catalyst.Core.Modules.Mempool.Tests	Merge dev into master (#1237)
Catalyst.Core.Modules.Mempool	Merge dev into master (#1237)
Catalyst.Core.Modules.P2P.Discovery.Hastings.Tests	Merge dev into master (#1237)
Catalyst.Core.Modules.P2P.Discovery.Hastings	Merge dev into master (#1237)
Catalyst.Core.Modules.Rpc.Client.Tests	Merge dev into master (#1237)
Catalyst.Core.Modules.Rpc.Client	Merge dev into master (#1237)
Catalyst.Core.Modules.Rpc.Server.Tests	Merge dev into master (#1237)
Catalyst.Core.Modules.Rpc.Server	Merge dev into master (#1237)
Catalyst.Core.Modules.Sync.Tests	Merge dev into master (#1237)
Catalyst.Core.Modules.Sync	Merge dev into master (#1237)
Catalyst.Core.Modules.Web3.Tests	Merge dev into master (#1237)
Catalyst.Core.Modules.Web3	Merge dev into master (#1237)
Catalyst.KBucket.Tests	Merge dev into master (#1237)
Catalyst.KBucket	Merge dev into master (#1237)
Catalyst.Modules.POA.Consensus.Tests	Merge dev into master (#1237)
Catalyst.Modules.POA.Consensus	Merge dev into master (#1237)
Catalyst.Modules.POA.P2P.Discovery.Consortium.Tests	Merge dev into master (#1237)
Catalyst.Modules.POA.P2P.Discovery.Consortium	Merge dev into master (#1237)
Catalyst.Modules.Repository.CosmosDb	Merge dev into master (#1237)
Catalyst.Modules.Repository.MongoDb	Merge dev into master (#1237)
Catalyst.Modules.Server.Blazor	Merge dev into master (#1237)
Catalyst.Node.POA.CE.Tests	Skip tests which fail intermittently. (#1242)
Catalyst.Node.POA.CE	Merge dev into master (#1237)
Catalyst.Protocol.Tests	Merge dev into master (#1237)
Catalyst.Protocol	Merge dev into master (#1237)
Catalyst.Simulator	Merge dev into master (#1237)
Catalyst.TestUtils	Merge dev into master (#1237)
Catalyst.Tools.KeyGenerator	Merge dev into master (#1237)
Lib.P2P.Tests	Merge dev into master (#1237)
Lib.P2P	Merge dev into master (#1237)
MultiFormats.Tests	Merge dev into master (#1237)
MultiFormats	Merge dev into master (#1237)

Figure 1: Catalyst module set

2.1.1 Catalyst Database Structure

By default, Catalyst has a multi-levelled data architecture, as illustrated in Figure 2.

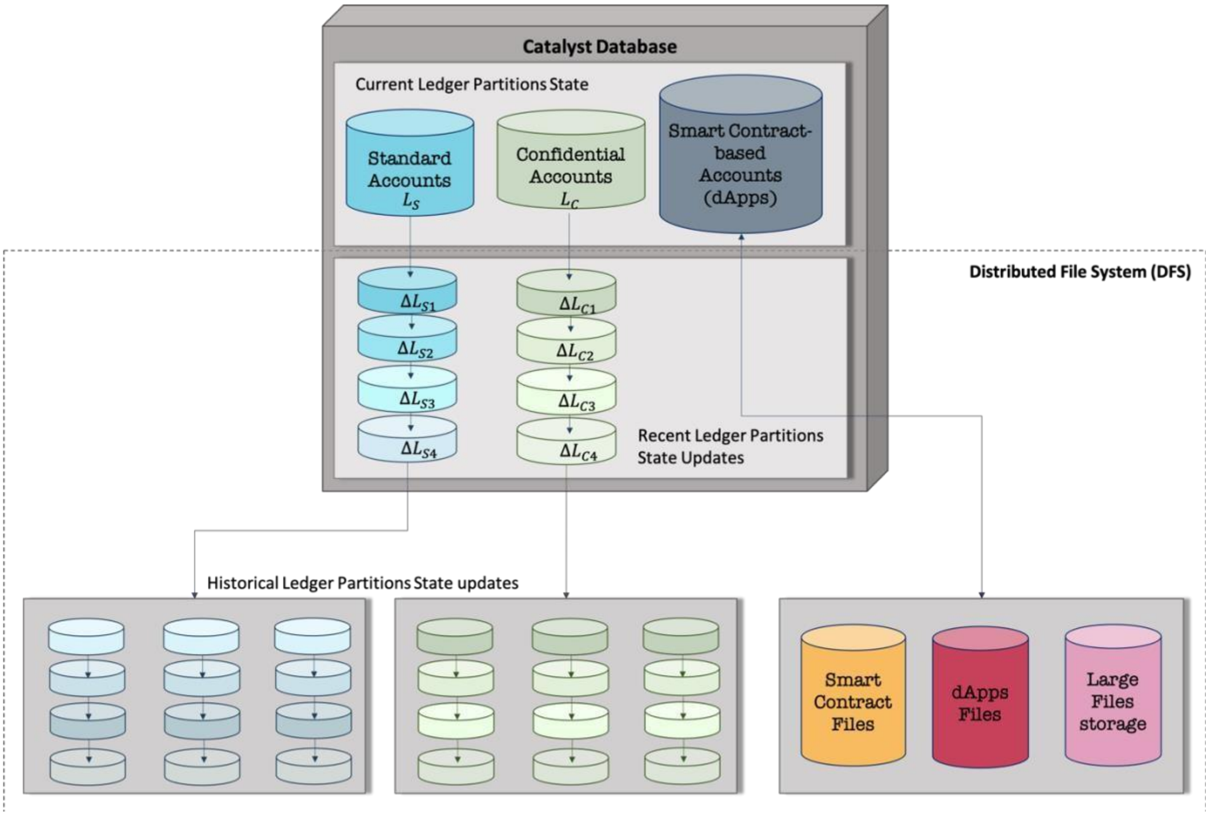

Figure 2: Illustration of Catalyst database architecture.

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 of time 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 of time. 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]. 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:

- In reality, 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 objective of Catalyst is to simplify the experience of writing smart contract logic for developers from backgrounds other than Solidity or Javascript. At the same time, Catalyst must support the broad Solidity developer community including following the latest EVM standards.

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)

KVM has been developed in partnership with Nethermind, the company behind the popular Nethereum node for Ethereum and is an extension of the runtime environment used in the Ethereum node. This means that Catalyst can and does merge the latest updates to EVM back into KVM and can and has merged Catalyst code in this module back into the Ethereum node. This helps to keep Catalyst's KVM aligned with EVM while also contributing back to EVM.

DCS is still in early development and provides a smart contract experience better suited to developers from a .NET or WebAssembly background. 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 [13].

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 and allow EVM dApps to be deployed straight 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. Communities of developers such as the .NET developer community are very large and influential within organisations, but they are largely excluded from the blockchain space due being unable to develop or deploy code in the languages and tools of choice.
2. The plethora of previously written software libraries, tools and design patterns cannot be reused within EVM
3. The metaverse is made up of many interconnected systems. Runtime environments such as EVM and KVM do not lend themselves to easily interact with off-chain services and technologies.

Catalyst addresses this challenge with its Distributed Compute System module (DCS) which enables developers to build and deploy .NET and WebAssembly components which in turn interact with the KVM runtime environment.

DApps written for DCS can be written in any .NET language 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.

DCS can't update the ledger directly and so ledger state is protected by requiring DCS to make calls to contracts within KVM. 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 Tooling

Since Catalyst is to act as a sandbox for developers then it's important to build tooling around Catalyst to assist both users and developers building on Catalyst or using dApps within the Catalyst ecosystem. Catalyst presently includes a number of tools including the following.

- Catalyst-js, a Javascript libraries for developers building on Catalyst
- Catalyst Dashboard, node explorer that displays a nodes peer list, pending transactions as well as network stats
- Catalyst Wallet, a web and mobile wallet for Catalyst. At least one commercial wallet is based on this code base and so there will be commercial wallets support as well
- Catalyst Explorer, a block explorer for Catalyst
- Two Visual Studio extension toolkits to assist with writing smart contracts
- Transactions, a simple tool to broadcast transactions to the network
- Benchmarking projects – Several crypto related benchmarking toolkits
- Various libraries, SDK's, smart contracts and demo's
- A faucet has been developed for the test network

More toolkits and projects are planned, particularly to better support the NFT and Metaverse space such as toolkits to more tightly integrate Catalyst with gaming and media systems.

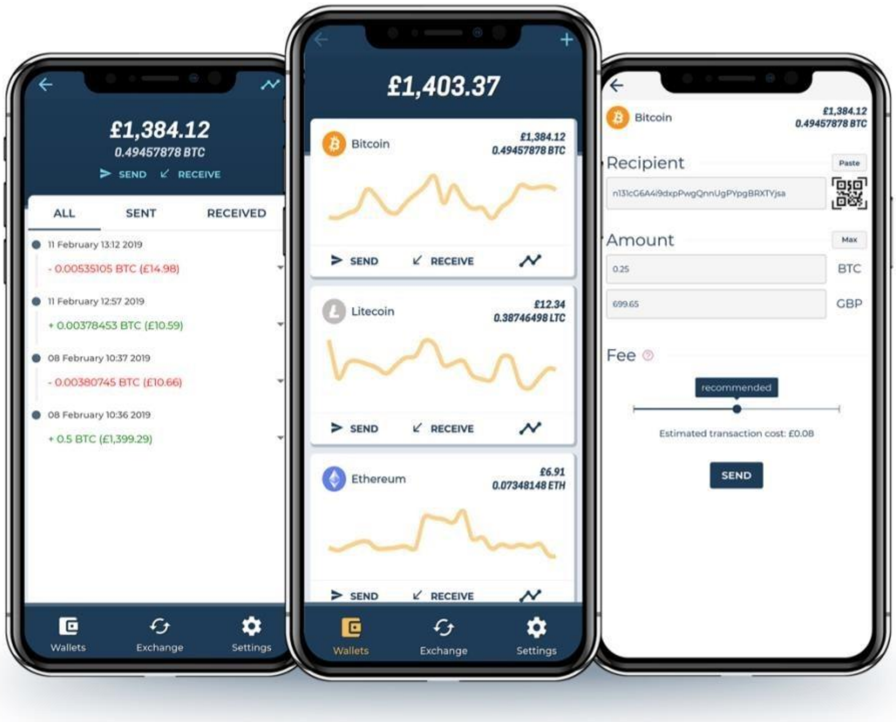

Figure 3: User Interface of the Catalyst *CryptoWallet*

3. Tokenomics

The Catalyst main network must become as decentralised as possible to best support the emerging NFT and Metaverse space. From a technology perspective, we deliver this through a combination of an open and modular code base combined with a scalable and fair consensus mechanism.

Tokenomics also has an important role to play in this area and so in this section we set out how tokenomics will work on the Catalyst main network.

3.1 Base Currency and Tokens

Most blockchains start with a base currency that's baked into the code base of the nodes rather than as something existing on the blockchain itself. This allows a network to get going quickly but has several impacts that need to be considered.

1. An off-chain code base is mutable. If a single node code base accounts for a majority of nodes on the network, then the code base could be changed in a way that changes the very tokenomics itself. This opens the network up to malicious economic attacks as well as accidental impacts from code updates.

2. The tokenomics implementation is embedded in a complex code base and so it isn't as simple or accessible for users to read than a token on a blockchain.

To improve in this space, Catalyst creates the base token in the genesis block which ensures the base tokenomics exists from the beginning of the network while ensuring the tokenomics are transparent and immutable. This also ensures that the base token can be an ERC20 token and treated no differently to any other token.

It also opens areas of research around alternative tokenomics models such as introducing new base currencies to sit alongside the genesis base currency or even currencies used for specific types of application or situation, channelling rewards to nodes that are focused on specific types of dApp.

The 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.

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. These tokens are a 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 to 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].

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 for the first two years. 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.

One thing that has been learned over the past decade is that the economics of any network are difficult to predict as markets and regulations change. Therefore, through the governance layer we recommend that a review of the economy is performed every two years and adjustments made to keep the economy healthy. This is like how governments set budgets every few years to encourage a healthy economy but, in this case, the government is replaced by token holders taking part in Catalyst governance.

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 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 broken down into three tiers covering different types of governance decision.

Rapid governance (operations)
For any type of organisation there exists a need to be able to make rapid decisions and take rapid actions for the good of the organisation. Within the context of Catalyst, examples would include critical bug fixes, continuous partnership building, marketing and general engineering and business operations.

A core team titled Operations will perform these actions on behalf of Catalyst. This group can be considered the equivalent of a C-Suite in a traditional business, reporting to token holders and the DAO. Their role is to implement the will of the community while working to grow and develop the Catlayst ecosystem.

Members of the operations team may change over time. Operations receives a budget to conduct its work.

Mid-level governance (DAO)
The Catalyst DAO allows community members to come together and buy voting shares at a price of 1 KAT per share. People need just 1 KAT to be able to raise proposals in the DAO, sponsor proposals and vote on proposals.

The reason for a DAO is that it provides a simple mechanism for community members to raise proposals while allowing community members with a real interest in governance to have an active impact on the direction of Catalyst.

Since voting shares are purchased with KAT tokens then it's expected that voting share holders will be those people with the most interest in governance.

The DAO is open to debate and raise proposals on any type of issue from partnerships to community funding. It is the intention of Catalyst to create a fund to support projects built on Catalyst and so the DAO would become the primary way for teams to apply for funding and for the community to vote on whether funding should be awarded.

High level governance

A subset of issues is so important that they should go out to the entire community to vote on. Examples of such issues would be fundamental changes to tokenomics. If the DAO feels that a proposal has a significant impact on the wider community then they can run an on-chain token vote where any KAT token holder can cast their vote on the subject.

It's expected that this type of vote will be few and far between and it's up to the DAO to decide if such a vote is necessary. As we've seen with token voting in other projects, most token holders do not take part in these types of votes and so it's debatable whether such broad votes offer improvement above and beyond DAO voting but this option remains available to the DAO for such wide impacting decisions.

Future

As with tokenomics, the issue of governance is free to evolve over time.
Initially it will be the founders and early contributors that make up operations and will have most voting shares in the DAO. This allows founders and early users to focus on building, testing and rolling out a stable network and community. Over time, the DAO will grow and that control will naturally decentralise.

5. Conclusion

The blockchain space is filled with many exciting and innovative networks and projects. Catalyst sets out to be a bridge between the blockchain space and the wider metaverse industry by providing a network, tools and technologies that open this emerging industry to the wider world. This is not to replace networks such as Ethereum but is to augment such networks, helping to bring in more users in a way that grows all networks and the industry.

This means building out the Catalyst network, tools, integration as well as tokenomics and governance. For example, we hope to see the DAO become populated not only by people in the blockchain space but by people in the gaming, media, hardware and other technology spaces. This allows these industries to express what they need to see happen and to help guide the roadmap of Catalyst to meet the needs of these industries.

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., *"E fficiency of delayed-acceptance random walk Metropolis algorithms",* arXiv:1506.08155v1

9. S. Gal-On et al. "*Exploring CoreMarkTM – A Benchmark Maximizing Simplicity and E fficacy*", 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. 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

Appendix

Risk Warnings and Key Legal Information

General Information

The KAT tokens and related convertible ERC-20 tokens launched as part of a planned token event (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 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 the 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 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

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 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 Catalyst 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 the 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.