Centrifuge

CENTRIFUGE OS

A Decentralized Operating System For The Financial Supply Chain

www.centrifuge.io

WHITE PAPER DRAFT

V20180625

hello@centrifuge.io

TABLE OF CONTENTS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Centrifuge Operating System (Centrifuge OS) is a decentralized platform to support a new generation of applications for the financial supply chain. It enables businesses to exchange financial documents such as invoices, purchase orders, company data, etc. while providing an unalterable and single source of truth for all involved parties. A decentralized data layer paired with public verifiability and provable business relationships form the foundation for decentralized applications (DApps) for the financial supply chain.

Centrifuge OS is proposing a peer-to-peer network (P2P network) for decentralized data exchange in combination with the use of a public blockchain for document notarization, maintenance of corporate identity, and the ability for DApps to interact with documents in the form of non-fungible tokens (NFTs). All users retain full sovereignty over their data, being able to share information with specific business partners or applications of their choosing. Centrifuge OS is proposing the idea of "unstoppable business documents" which are business documents that have long-term verifiability, are censorship resistant, and stored and processed in a decentralized fashion.

The data exchange layer promotes standards for financial supply chain documents while abstracting consensus algorithm complexities and conflict resolution for the end user. Centrifuge OS can be used to upgrade existing financial systems and legacy processes to operate on a global single source of truth. This reduces reconciliation efforts and improves interoperability of existing systems. More importantly, Centrifuge OS introduces the ability to link documents across company boundaries, supply chains, networks, and traditionally siloed accounting systems. It presents a new way to interact with globally interconnected financial systems to create the financial supply chain of the future. This document describes the philosophical underpinnings, technical foundations, and economic mechanisms of Centrifuge OS.

THE PROBLEM WE SEE

How businesses transact and exchange business documents has not changed substantially since medieval times. Double entry bookkeeping was first used in the 1300s, and the concept of agreeing on orders and sending invoices with negotiated payment terms has existed for at least as long. In the quest for optimizing systems and improving existing methods, the so-called financial supply chain world has become increasingly automated and streamlined. The advent of software applications in the 1970s and '80s brought the creation of the digital twins of those centuries-old processes and documents. This digitization further optimized existing flows but generally fell short of fundamentally rethinking those archaic, established flows.

The decades that followed brought further improvements and faster processing times. Today, it is possible for a large organization to receive paper invoices, scan them, feed the data into their financial systems, and approve a document within a few days. Business networks for e-invoicing or procurement connect their customers with each other to eliminate paper-based exchanges altogether. These centralized networks produce large sets of data that are then used to analyze the network participants and offer additional products which, again, is used to further optimize existing processes or offer additional products that are tightly coupled to the respective closed network.

Financial systems rarely connect to one another directly across company boundaries. Business networks are in competition for market share; thus, they do not have incentives to share user profiles, build a robust and shareable reputation system within a network, or to open their data silos to others, and developing innovative products and services via collaboration.

We believe that the time of incremental optimization has to come to an end. Only by collectively shaping an entirely new system for the global financial supply chain can we foster widespread economic opportunity. This new system can only be established by dismantling the existing financial supply chain infrastructure, stripping it down to its essential components, and reassembling it for the 21st century. From that point, we can create the foundation for an era of financial applications, processes, and paradigms that will serve businesses well into the future.

The Financial Supply Chain

When we talk about the financial supply chain, we refer to actions and communications that are part of the procure-to-pay process as well as the order-to-cash cycle: the flow of information, data, and eventually money between companies doing business with each other: The suppliers and buyers - often also referred to as sellers and customers.

Some examples of areas of the financial supply chain that will be touched by the systems described in this paper are services like e-invoicing (a multi-billion dollar market[1]), decentralized digital identities of businesses (by some estimates a USD 20B market[2]), supply chain finance in its various forms (a multi-trillion dollar market[3]), and others.

We aim to build a platform that substantially improves access to affordable financing and liquidity for any business worldwide. According to an annual research conducted by Visa, at any given time, approximately USD 20 Trillion of payments owed are locked up due to lengthy and often unfair payment terms[4]. In other words, businesses frequently wait months on end to receive payments from their larger clients, which creates a scenario where they must seek additional financing to fill in those cash flow gaps themselves; an option that is both expensive and not consistently available. Our proposed approach, building on the decentralized identity and the improved ability to exchange data within the financial supply chain, will provide the needed opportunity for businesses of all sizes to finance themselves and on their terms.

Closed Systems and Moats vs. Connection and Collaboration

The motivation behind the software and consulting service providers within the financial supply chain field is to continuously optimize business practices, lock existing customers into their solutions for future upsell opportunities, and build “competitive moats” around their networks and user base. This makes switching to another service provider a costly proposition. Currently, when using business software, companies commit not only their data to a specific platform, but also create representations of their corporate identity,

1 https://ctmfile.com/story/e-invoice-market-to-grow-5-fold-by-2024

2https://www.forbes.com/sites/rogeraitken/2018/01/07/blockchain-to-the-rescue-creating-a-new-future-for-digital-identities/#2b5400675492

3 https://www.economist.com/finance-and-economics/2017/10/12/technology-is-revolutionising-supply-chain-finance

4 http://www.commercialpaymentsinternational.com/sites/default/files/Amit-Sethi.pdf, assuming average payment terms of 59 days in the US and Europe.

transaction history, and business relationships repeatedly in each network and software package.

A shift of the global mindset from “closed systems” to a more connected world emerged over the last decade but stops short of truly opening the playing field. APIs expose parts of those siloed invoices, orders, master data, and business relationships but all players involved continue guarding data as “their assets,” holding end-users captive to a single platform instead of truly opening a new way of cooperation.

We are proposing a network that allows data sharing for the financial supply chain where the owner of the information - the business - has the power to decide which applications can use their information and for what purpose. It becomes possible to prove the authenticity of information to anyone and allow all applications to operate on a single source of truth. Anyone can join the network, with no centralized authority that will grant or restrict access or hold data captive.

This open network, built explicitly for the financial supply chain, enables participants to trade freely with each other while trusting the validity of information and business partner identity. The Centrifuge OS participants have access to the global graph of business relationships, reputation, and global trade in a secure way. Service providers can deploy value-added applications that operate on top of the network to enrich existing applications or fundamentally rethink what it means to offer services for the financial supply chain.

THE CENTRIFUGE OPERATING SYSTEM

Centrifuge OS provides a way to create, exchange, and utilize the data that is used throughout the financial supply chain. The OS codifies organizations and business entities as well as business objects like orders, shipment details, invoices, and remittance information. Centrifuge OS creates transparent and shareable relationships between interacting companies. Data owners can selectively share their information with their business partners or other users of the OS. This creates the foundation for data ownership, privacy, and transparency throughout the financial supply chain. It also allows 3rd parties to offer additional services based on the information shared with them. The data owners have the power to decide whether or not to take advantage of those services.

Beyond the codification and share-ability of data, Centrifuge OS provides a censorship-resistant way to verify the authenticity of data that is transacted through and stored in it. It

does not aim to provide management of identity per se but creates a way for corporates to own the identity that is directly connected to their business transactions and relationships with other corporates. Centrifuge OS also enables the public verification of the company's business relationships and data on a granular level. The selective granularity of information sharing is required to prevent laying all details of a supply chain open to unauthorized parties while sharing relevant data with authorized participants within the network. Users of Centrifuge OS feed their information into the OS only once. From there they can re-use this data as a single source of truth for further processing and share it with (decentralized) applications that require financial supply chain data.

For example, a supplier who is using Centrifuge OS to submit invoices to their customers can seek financing for those invoices on a decentralized funding marketplace built on top of the Centrifuge OS network without re-submitting information or duplicating any data. At the same time, the supplier can use the underlying data to build a reputation within the network. The supplier shares all of the invoice details with their customers, a limited set of invoice details on the marketplace, and only some metadata about transactions for reputation scoring within the network. The same principle of data sharing and privacy applies to corporate information like bank accounts or tax details and all other private data that exists throughout the financial supply chain.

In the past, true data sovereignty only occurred when holding data in private data silos. The silos might be technical, by hosting walled-off applications, or legal, when hosting a service with a provider who is not able to easily offer value-added services beyond their core competencies.

Today, business networks act as multipliers to transmit data more efficiently and with less integration effort but result in yet another data silo, hosted by the network provider itself. Even if data ownership is legally tied to the user of the business network, the lack of open access and ways to share and verify this valuable information locks the information within the centralized network. Data is disjointed, hard to control, difficult to share, and only kept in sync with tremendous efforts – assuming that true synchronization is at all possible.

By providing a codification of what it means "to be a business entity," "to have business relationships," and "grant data access to third-parties" and making this codification available on a decentralized network, Centrifuge OS creates a fundamentally new way of doing business. With this in mind, Centrifuge OS promotes a re-thinking in the following goal areas.

Goal Area	Current State	Solution within Centrifuge OS
Document data	Each party stores and validates data independently according to their own rules.	Global, reliable, single source of truth that guarantees consensus on document data.
Document state	Documents are stored in disconnected, siloed off systems and networks with different data and status.	Shared, single source of truth assures common agreement of document state.
Data sovereignty	Data is locked in single purpose business networks or private deployments. Users might "own" their data but cannot easily use it for purposes of their choosing or make it available to other applications and 3rd parties.	Data is stored and processed in a decentralized way while users can grant granular access to others. No single application provider can withhold document information or censor transactions.
New generation of applications	Network effects reach a local maximum within any closed off business network or application provider. New applications (outside of the existing application provider) require re-building the business graph or re-launching multi-party marketplaces to kick-start novel apps.	Users can choose whom to grant access to their information. Applications can receive access to current transactions and history and document relationships. This enables a new generation of applications for the financial supply chain.
Relationships between businesses and their data	It is impossible to link business relationships, reputation, or supply chain connections freely due to siloed deployments.	It becomes possible to map relationships (with granular access) to enable new ways of paying, financing, and supply chain management.

DECENTRALIZING DOCUMENTS AND BUSINESS RELATIONSHIPS

A few of the results of codifying and transacting business data on a decentralized network include:

- Business documents, business identity, and its reputation become first-class citizens on decentralized networks. Similar to defining standards like the ERC-20 standard for Tokens on Ethereum, it becomes possible to operate with standard definitions of business objects like Business Entities, Order Agreements, or Invoices in a decentralized fashion.

- Given these standards, it is possible to easily interact with business partners, service providers or any other entity connected via Centrifuge OS., e.g., corporates can share new orders with their suppliers and accept orders from clients, regardless of their internal financial systems. Standards for business objects are nothing new. However, it has not been easily possible to truly transact on these standards without middlemen while operating on a shared state and a single source of truth for all involved parties.

- Corporates can integrate their traditionally siloed data with others who are connected to the OS, understanding the same data exchange and sharing mechanisms without giving up control over their information, e.g., corporates can now work with any 3rd party funding provider who is interested in funding their business based on the corporate data. Funders can gain access to many different funding opportunities by using Centrifuge OS.

- When business objects are stored and anchored on a public and permission-less blockchain, they become tamper-proof and censorship-resistant. Any party with access to an object can verify the authenticity of the data provided, the timestamp of the object, and that they are operating on the most up-to-date version of the object.

- Business objects can interact with each other directly through the OS., e.g., a payment can be triggered automatically after an order has been fulfilled. No rent-seeking middlemen are required.

- Completely new ways of accounting and novel interactions between business objects become possible, e.g., it provides businesses with the opportunity to traverse circular graphs of business relationships, creating a global netting of outstanding transactions or payments. This allows moving only the money that genuinely needs to be moved, at precisely the time that was agreed upon. The automatic rerouting of payments to the right place in case of defaults of payment in one part of the supply chain becomes possible.

- Given the decentralized and public availability of the codified business documents, trustworthy and transparent reputation scores based on real and transparent business interactions can be created. When operating on a public blockchain, the underlying algorithms for the calculation of the scores can be reviewed and audited. This allows each network participant to not only know their score and control their data but also transparently know why they carry a specific score. Being a good business partner pays off: conducting business transactions that positively impacts the overall network, environment, or society does accrue an ROI as long as the network values these contributions. Different ways of measurement can be quickly and easily built on top of the shareable data.

In short, Centrifuge provides the operating system, protocols, and tools to fuse the silos of business data and business logic on a public and decentralized network. This process allows public verifiability of the data while allowing the owners of each object to control access according to their needs.

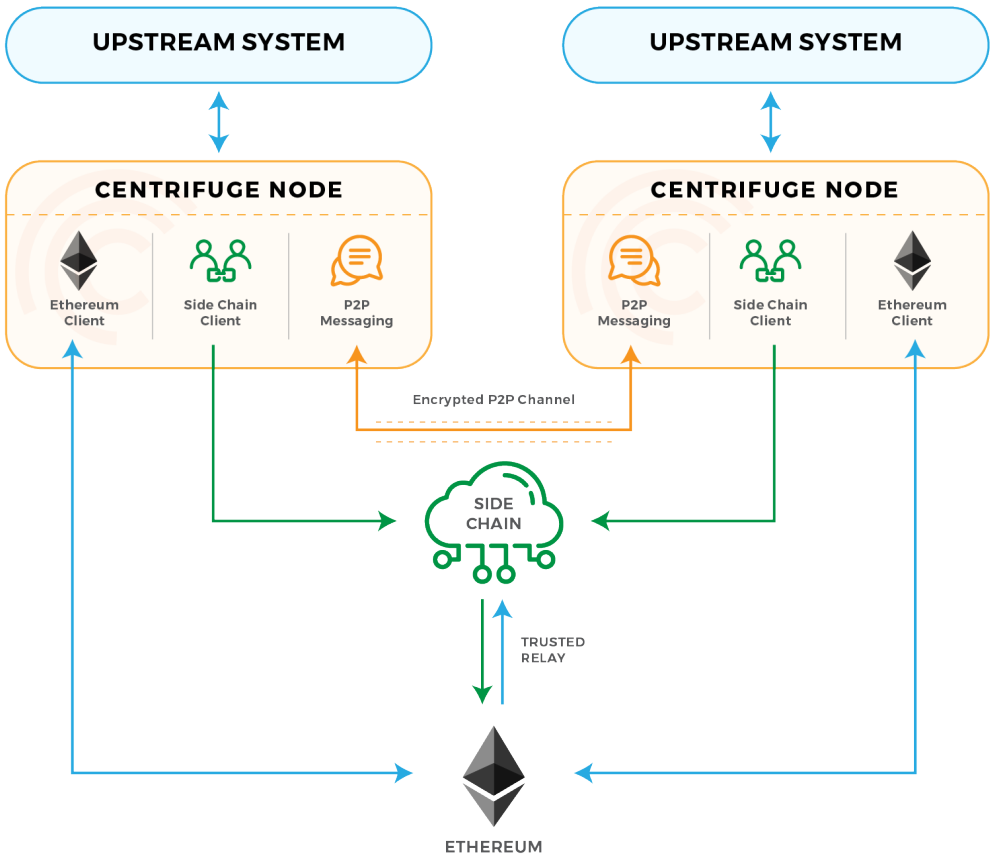
TECHNICAL OVERVIEW

The building blocks of Centrifuge OS are:

- Contracts that are deployed on Ethereum;
- Centrifuge Nodes that facilitate data exchange on a peer-to-peer layer;
- An Ethereum-based sidechain with Centrifuge OS-specific contracts and data.

Core components of Centrifuge OS will operate on a decentralized, public blockchain application platform. Initially, this platform will be Ethereum. Support for other decentralized application platforms will be evaluated; but for illustration purposes, and as a matter of focus, the initial launch of Centrifuge OS leverages Ethereum as the platform of

choice. In this document, we use the terms “public blockchain” or “decentralized application platform” to refer to the Ethereum blockchain and its decentralized computing capabilities. In addition to the essential components that operate on the public blockchain, Centrifuge OS consists of a peer-to-peer network that exchanges private data directly between OS participants. We call this part of the network the “peer-to-peer data exchange/layer/network” (P2P data exchange/layer/network). This communication is based on P2P messaging with anchoring data in the public blockchain. The third major component of Centrifuge OS is an Ethereum-based sidechain (“sidechain”) that is implemented within an open and decentralized setup and anchored back to Ethereum mainnet.



High-Level Overview of Centrifuge OS Components

TECHNOLOGY AND ARCHITECTURE

The State of Decentralized Systems

Currently, Ethereum provides a secure, public, decentralized platform for the execution of applications. The possibilities to keep specific contract information and data private are not yet sufficient for all Centrifuge OS use cases. The cost, transaction throughput, and transaction speed of Ethereum are not currently suited to power the types of transactions that Centrifuge will need to process. The team behind Centrifuge believes in Ethereum's current proposals for improving transaction throughput via sharding[5] or Plasma[6] as well as bringing zkSNARKs to a level of general usability (e.g. via ZoKrates).[7] The lack of transaction privacy is one of the reasons the Centrifuge OS private data only exists on the P2P Layer, while the Centrifuge sidechain supports shielding transactions and higher transactional throughput at a low cost.

Projects like IPFS,[8] BigchainDB,[9] or Ocean Protocol[10] are promising methods for solving distributed public storage of large files, distributed storage of data as assets, and creating marketplaces for data streams that allow data owners to monetize their information. Projects such as Keep[11] and NuCypher[12] are on their way to innovating decentralized encryption, storage, and retrieval of private data. The Centrifuge team will continuously evaluate both established and emerging technologies that support distributed, decentralized, public computation and data storage in a secure and scalable environment.

One can separate core enabling technologies from the Centrifuge OS-specific logic. Applications that will be built on top of the OS will then provide value to end-users as well as deliver value through the network at large. These value propositions are achieved while supporting the vision of a public, decentralized network to power global trade. To develop the core components of the OS which support the vision of becoming the Operating System for the global financial supply chain, we will make measured concessions regarding the architecture of the first version.

[5] https://github.com/ethereum/wiki/wiki/Sharding-FAQ
[6] https://plasma.io
[7] https://github.com/JacobEberhardt/ZoKrates
[8] https://en.wikipedia.org/wiki/InterPlanetary_File_System
[9] https://www.bigchaindb.com
[10] https://oceanprotocol.com
[11] https://keep.network
[12] https://www.nucypher.com

Ethereum

Functionality deployed on Ethereum acts as the primary and trusted entry point and anchor for the other Centrifuge OS components. The censorship-resistance and decentralized nature of the platform provide trustless lookups for Centrifuge OS users. Ethereum also allows users to publish identity, reputation management, and document information through Centrifuge OS Smart Contracts without relying on any 3rd-party. Furthermore, Ethereum's architecture provides a well-tested system for the issuance of tokens to incentivize honest participation within the OS, issuance of tokens directly related to business documents, as well as decentralized governance layers of the OS at large.

The Centrifuge Sidechain

The Centrifuge sidechain is a public Ethereum--based blockchain that deploys a proof-of-authority consensus algorithm ("PoA" or "PoA Consensus"). The parties operating the sidechain are voted "in" or "out" based on a token curated registry ("TCR") that resides on Ethereum mainnet. The sidechain operates without a central governing entity but still allows for a relatively controlled setup. The sidechain will be anchored back to Ethereum mainnet at set intervals through a mechanism similar to trusted relays[13] and the Kaleido relay.[14] The Centrifuge team is working towards a PoA sidechain that is anchored back to the Ethereum mainnet as described. However, we will continuously evaluate projects that provide similar constructs using standard public utilities such as Cosmos/Tendermint[15], Plasma, and Polkadot.[16]

The Centrifuge Peer-to-Peer Network

Private Components & P2P Layer

Private data elements are stored on the OS participant's P2P node. Some of this information might, in fact, never be stored on the public blockchain itself but rather be held on the local node or on other 'trusted nodes' for replication, backup, and long-term data availability. Private data, exchanged between business partners, is anchored in the public chain to prove the validity of the data as well as the associated timestamps for creation and modification. Examples of data that is transacted only on the P2P layer:

[13] https://blog.gridplus.io/efficiently-bridging-evm-blockchains-8421504e9ced?gi=c89e56327f15
[14] http://console.kaleido.io/docs/docs/kaleido_relay/
[15] https://cosmos.network/
[16] https://polkadot.network/

- Detailed company master information such as bank account information, tax IDs, detailed address information, etc.;
- Full details of order agreements, invoices, or business relationship logic;
- Binary file attachments that belong to specific transactions.

Interacting with P2P Nodes

Upstream systems that use Centrifuge nodes, as well as specific DApps, will require special handling of incoming and outgoing data and the interpretation thereof on the client side. The P2P node, developed by the Centrifuge team, supports this by operating on a "service bus" principal where plugins and outside systems can subscribe to messages about specific objects (e.g., a procurement application can subscribe to changes of order objects). The P2P Node abstracts the events that occur on the public blockchain, sidechain, and P2P Layer and translates them into messages on this internal bus for other applications to consume. The same is true for incoming/outgoing changes to objects. Subscribed applications can interact with those messages while the core P2P Node handles all the signing, anchoring, and communication.

The P2P Node also offers the connectivity to Ethereum and the Centrifuge sidechain for applications that build on top of the P2P Node such that the higher-level applications do not have to concern themselves with key management or corporate identity management but simply utilize the APIs that the P2P Node offers.

IDENTITY ON CENTRIFUGE OS

Identity Management

Any participant of Centrifuge OS is identified by a unique identifier ("CentrifugeID") within the network. A CentrifugeID can be created by calling the Centrifuge OS identity management contract on Ethereum. When a new CentrifugeID is generated, a unique public representation of the identity is generated for the public blockchain. The data associated with a CentrifugeID is only modifiable by the creator and/or a delegate chosen by the creator.

Every CentrifugeID has three sets of associated data that are relevant for using the OS. This data is submitted when creating a CentrifugeID or added later by the owner or a delegate.

1. Peer to Peer Messaging Encryption Keys: The public keys that correspond to private keys which are used to encrypt/decrypt messages sent via the P2P protocol. These public keys are also used to resolve participants' P2P Layer addresses within the network.
2. Signing Keys: Public keys that correspond to private keys that are used to sign documents that are transacted within Centrifuge OS.
3. Ethereum Accounts: When interacting with a smart contract on Ethereum, an account needs to be linked to the identity to act on its behalf. The linked Ethereum accounts are the accounts that are allowed to interact with DApps utilizing Centrifuge OS.

Using Identities for Peer-to-Peer Data Exchange

Centrifuge OS participants register their identity on the public Ethereum network and maintain a set of public keys as part of their identity. These identities and their keys are then used to resolve nodes on the P2P layer when one node wants to transmit data to another Centrifuge Participant. This means that nodes on the P2P Layer find others by looking up their public keys from the public identity register based on CentrifugeID. The resolution of lower network level addresses (IP address, Ports, etc) are then handled by the P2P Layer. The P2P layer uses libp2p[17] for the node resolution and internode communication.

PEER-TO-PEER DOCUMENT EXCHANGE

The following dimensions need to be considered to transact business objects on a global, enterprise scale:

- **Cost-effectiveness:** A single transmission of a business object between companies shouldn't cost more than a tiny fraction of USD cents.
- **Scalability:** A solution needs to handle many thousands of message transmissions per day for each business partner with most transactions occurring during peak times.

[17] https://github.com/libp2p

- **Privacy:** A business needs to be able to conduct business on the platform without divulging unwanted data to others.
- **Auditability:** Any party with appropriate access to document data should be able to verify the authenticity of the document and its history.

One part of the solution for the requirements for all dimensions is a network that allows direct, verifiable communication between business partners at rapid speeds without waiting for commits and transactions being propagated through the public blockchain. For this purpose, Centrifuge leverages nodes that communicate in a peer-to-peer fashion to exchange cryptographically signed messages between OS participants.

To create an immutable record of those messages, their signatures, and the hashes of the messages are published to the public blockchain as an "anchor." This anchor is created when either a use-case benefits from immediate anchoring or if disagreement between two nodes on data consistency occurs that needs to be resolved. In the latter case, the disputing node can publish the previously agreed upon hash of a document as the last "known state."
This allows for consistent private, verifiable exchange of data and publishing new anchor versions on demand, e.g., when agreement was achieved between two or more nodes on the content of a specific document.

One can compare this chaining of document changes and periodic anchoring with how a sidechain would anchor its status back to a main chain. In essence, Centrifuge OS creates the "document sidechains" where the state of this "document chain" is known to all the involved P2P Layer participants with a public anchoring back to the main chain.

Walkthrough of a Simple P2P Document Exchange

Let's assume the scenario where Alice (Node A) wants to send a document to Bob (Node B). Before sending the document, Node A calculates a Merkle root that uniquely identifies this document via precise proofs[18] and signs the document with its private key. Node A has two options at this point:

1. Submit the signed root hash to the public blockchain before sending the document to Node B in order to anchor the document.
2. Submit the signed root hash together with the document to Node B.

[18] https://github.com/centrifuge/precise-proofs

Node A finds Node B through a search via the CentrifugeID associated with its "owner" (Bob). The upstream system that is instructing Node A to send the document also provides the recipient's CentrifugeID. Node A finds the public keys attached to the receiving CentrifugeID on Ethereum. After retrieving the public keys from Ethereum, Node A resolves Node B's address within the network with the help of lip2p and a distributed hash table that holds the mapping between the public key and Node B's address. From there, Node A is able to transmit the document data to Node B.

Node B processes the document, calculates the Merkle root according to the same rules as Node A, and signs this root with its own private key. Depending on the specific use case, Node B now has three options:

1. Respond with the signed root hash which is the signaling agreement for document validity;
2. End the communication at this point, simply storing the calculated document plus hash locally;
3. Submit its own signed hash to the public blockchain to anchor the document or append the signature chain if the sending node had initially anchored the document.

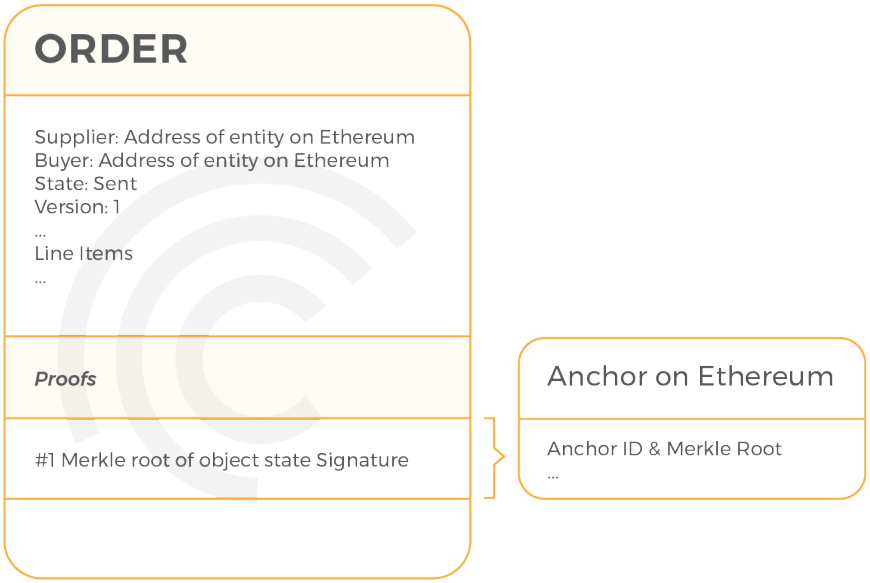
Any upstream systems that are connected to Node A or Node B are notified of the document transfer status and can then process this information accordingly on either side.

This is a simplistic walkthrough of the document exchange, signature, and anchoring process. The detailed consensus algorithm is in peer-review and will be published in a separate document.

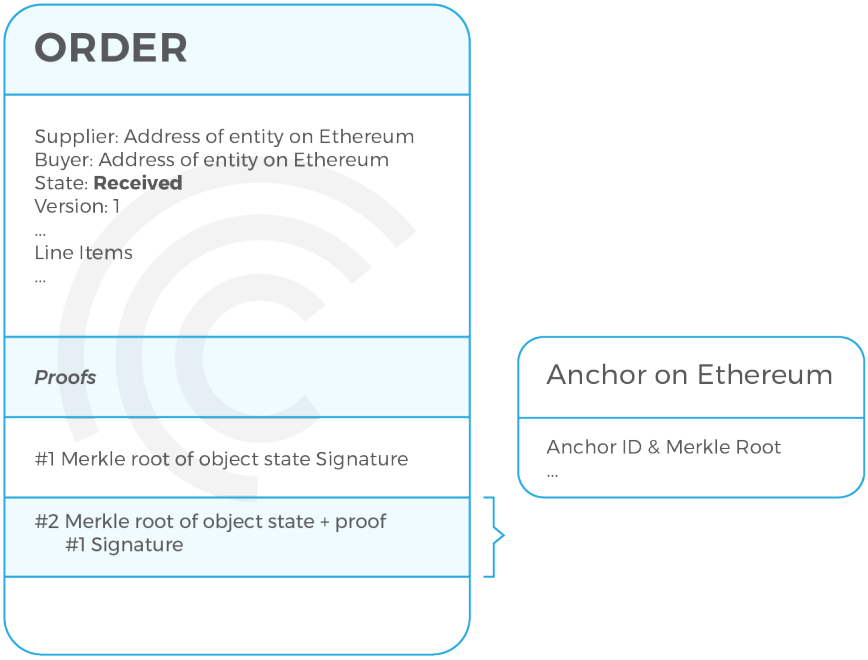
Changes to Documents

In addition to the initial transmission and anchoring of documents, an important feature of Centrifuge OS is the consistent and authentic proveability of these documents throughout their lifecycle. This means when a document changes (e.g., the quantity of an order is adjusted) it needs to be retroactively possible to prove that the involved business partners agreed on such a change.

We will assume any transmitted and anchored object is a combination of sorted mapping of attributes. It is important that mappings are sorted because the calculation of the Merkle root relies on a field order; a different order of fields would result in a different hash of the Merkle Tree. The ordering for fields follows a standardized set of rules.



When a document is updated and sent to a business partner, the new document undergoes the same sorting and hashing process but includes the previous document hash plus the signature. The single document changes get chained together, and each new document version contains the hashes of the previous documents and their signatures. Below is an example of changing the state of the above object.



This generates a tamper-proof history of an object that can be exchanged between the involved business partners indefinitely up to the point where one of them chooses to publicize the new hash-plus-signature to the public anchor.

While it would be possible to attach all document changes on a field level, recording all document changes and versions within each message would lead to a bloated message format. Validating all changes in the document's history would require requesting past document versions based on the previous hashes and anchors. Any client can then validate document history version by version.

Anonymity of Public Anchors

The anchoring operates in such a way that the anchor repository does not contain links between single object updates but rather only a mapping of anchor ID to the Merkle root of the document and the CentrifugeID which can be used to find the respective P2P node to request details of the document at a later point.

Taking the example below, the CentrifugeID starting with *ed844555f60186f...* published two anchors with different root hashes. The public ledger only contains the information that the anchor was published, but there is no way to associate the anchor with a specific document when viewing the data on Ethereum alone.

Anchor ID (byte32)	Merkle Tree Root Hash (byte 32)	CentrifugeID (byte 32)
9c20aa75d8e19da...	2260c23bba33bbd...	ed844555f60186f...
0c31d2ab200f086...	39f65e8af3fefd1...	ed844555f60186f...
...	...	...

When published to other P2P nodes, each document contains the next anchor ID as part of the document structure such that a trading partner can publish an updated version of the document while nobody else knows that this newly published anchor is actually the new

version of the prior document. However, anybody with the original and valid document can check if a new version has been published in the meantime. Subsequently, they can request the new version from the respective network participant.

ASSETS OF THE FINANCIAL SUPPLY CHAIN AS NON-FUNGIBLE TOKENS

Any document that is exchanged and anchored in Centrifuge OS can be registered on an OS-level as a transferable and ownable asset. The term "Non--fungible Token" (NFT) has been gaining wide acceptance for assets of this type via Ethereum's ERC-721 standard.[19] Following ERC-721, Centrifuge OS supports this asset creation and transfer.

Due to the private nature of the data that is exchanged with Centrifuge OS, an NFT, registered on Ethereum, contains only a few data points about the actual asset that is transacted within the OS. The NFT metadata contains a link to the private data that can be requested on the P2P Layer. The P2P nodes are operating in such a way that the current owner of an NFT can request the NFT details at any time. To initially register a document as an NFT on Centrifuge OS, the following conditions must be met:

- The registrar needs to have a valid identity on Centrifuge with a registered, active node;
- A valid document anchor needs to be provided during registration, i.e., the document needs to have been anchored before;
- The registrar needs to be the original creator of the anchor as identified by the CentrifugeID on the anchor.

Data Privacy and NFTs

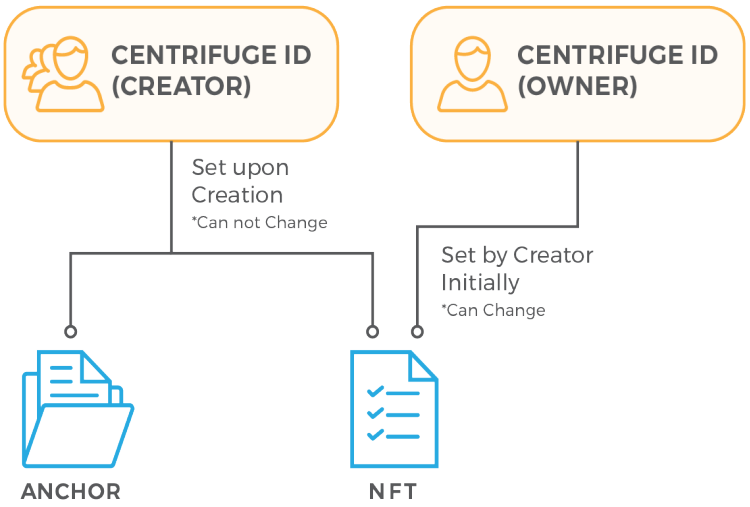
A simple document anchor does not reveal any information about the underlying document other than who created an anchor. NFTs within Centrifuge OS remove one layer of privacy from a specific document by revealing the current owner of an asset. To enable a truly decentralized platform where any asset can be used for any purpose within the ecosystem and enable creation of DApps, this is a conscious tradeoff between adequate levels of privacy, censorship resistance, and decentralization. The private data of the

[19] https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md

document is untouched and only communicated on the P2P layer and never revealed by simply registering an NFT.

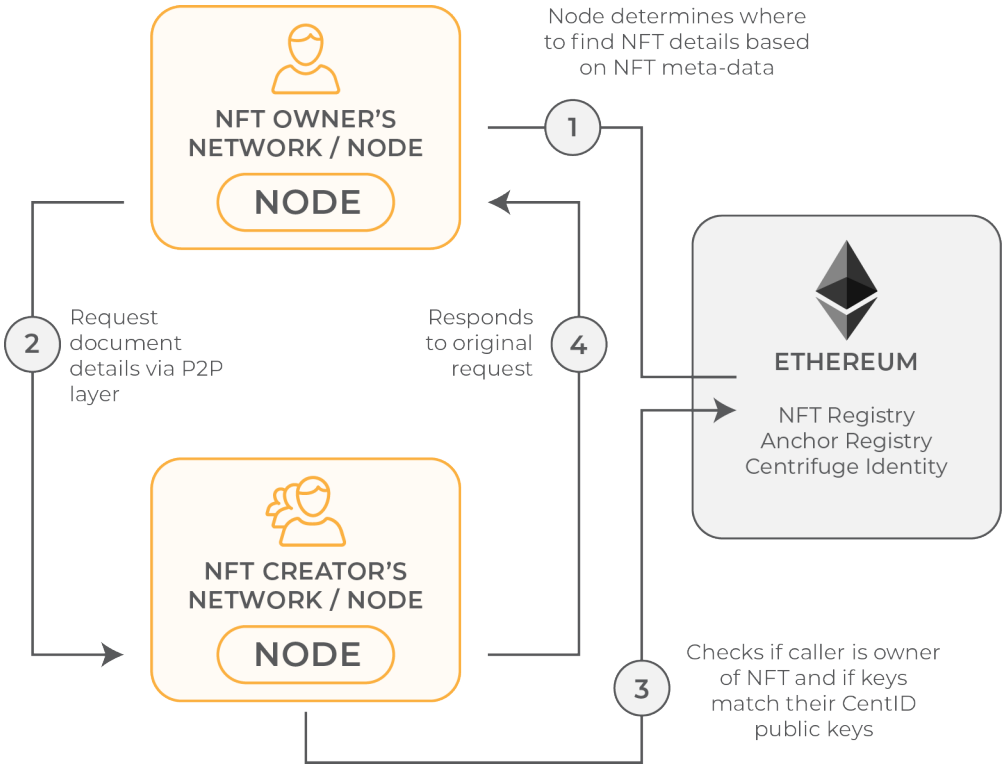
Access to Private Data of NFTs

Each NFT on Centrifuge OS is linked to a document anchor. This allows for anyone with access to the underlying document to prove the authenticity of data and document changes over time.



NFT Data Structure

When a P2P node receives a request to share information about a specific document, the node checks the NFT register to validate if the caller is currently registered as an owner or an authorized handler of said NFT. If this check validates, the node returns the adequate information to the caller.



Document detail retrieval based on NFT ownership

This means the owner of an asset on Centrifuge can register their asset as an NFT and register this asset on an exchange, marketplace, or any other DApp by giving the exchange provider access to their NFT. The operator of said exchange, marketplace, or DApp can then call the respective P2P node to retrieve the information about the asset and further process the data.

CENTRIFUGE OS NATIVE TOKENS

Centrifuge OS has two native tokens: Medallion and Cent. Medallion is a fixed supply token used for governance, staking and reputation seeding; Cent is a variable supply token used for transaction processing, metering, and value transfer within the Centrifuge OS economy.

The Medallion Token

The Medallion token is an ERC-20 token and is used for the following functions within Centrifuge OS:

- Holders are able to participate in the governance of Centrifuge OS at large and voting on specific changes to protocol parameters;
- Staking Medallions opens functionality to seed one's reputation within the network and participating in the Centrifuge sidechain validation.

As decentralized on-chain governance is in an early stage of its evolution, we see it as important to gradually introduce governance concepts as they become necessary and feasible for implementation. It might be tempting to commit to a specific scheme of governance at this point. However, the reality is that governance mechanisms need to be flexible enough to evolve over time and support the growth of the network as well as the needs of its participants. Centrifuge OS treats governance as an emerging property of the network, guided by the participants. To support this emergence, the network contains upgradeable governance contracts as well as a minimum set of governance layers and features. As such, network participants can steward the network over time.

Centrifuge, the Company, will hold a majority of Medallions to support a controlled evolution of the network in partnership with its users. The ultimate goal is to distribute Medallions to the network participants until Centrifuge, the Company, is merely a small contributor to the governance of the network at large.

Voting and Governance with Medallion Tokens

Medallions can be used to vote on changes to the OS, core logic, or pricing of transactions within Centrifuge OS. Voting is only possible by staking Medallions for a period of time and then participating in proposing changes and/or voting for proposed changes. The exact governance and voting mechanics will be developed together with the community during the first phase of the public network launch but will likely adhere to the following parameters:

- Medallion has to be staked for different periods, depending on the type of vote;
- Price adjustments for OS-level transactions are possible in shorter intervals and require a shorter staking time;
- Voting on upgrades of core components or core OS logic, on the other hand, require a longer staking time;

- Voting on changes to TCRs used for the sidechain operation will likely require longer staking time.

Where possible, features, libraries, and learnings from systems like Aragon[20] or DAOstack[21] will be used to develop the governance and voting layers.

Staking Medallion

Beyond staking Medallion to participate in governance, Medallion can be staked to seed one's reputation as a participant in the network. Similarly, validators of the Centrifuge sidechain are required to hold and stake Medallions in order to participate in the validation. Exact staking conditions are being researched.

The Cent Token

The Cent token is used by participants and users of Centrifuge OS to exchange value and pay for OS-level transactions and services. It is a utility token that is used by users to reward each other for their services within Centrifuge OS.

Even though Centrifuge OS participants use the Cent token to pay each other for services within the Centrifuge OS economy, the Cent token is neither a stable coin[22] nor a general-purpose currency. This also means that the Cent token does not aim to be used for payments in the sense of "paying an invoice." It is used for rewards within the Centrifuge OS economy. Centrifuge OS will, at a later stage, evaluate core-level support for integration with stablecoin projects like Maker[23] and others for general purpose payments tied to the financial supply chain.

Cent is issued by algorithmic agreements, based on the current circulation and usage of Cent to achieve relative stability of the relation of velocity and price of the token. Cent tokens exist in two separate realms: The Centrifuge sidechain and Ethereum mainnet. Users can "transfer" Cent from mainnet to the sidechain and back. The contract that governs Cent on Ethereum mainnet follows the standard ERC-20 token specifications. Once Cent tokens are transferred onto mainnet the user can trade them freely and transfer them back to the sidechain for use within the OS.

[20] https://aragon.one
[21] https://daostack.io
[22] https://medium.com/@argongroup/stablecoins-explained-206466da5e61
[23] https://makerdao.com

Pricing of Transactions Within Centrifuge OS

To provide stable and predictable transaction costs and rewards within Centrifuge, the OS contracts on Ethereum have a register of the current price of OS-level transactions. OS-level transactions are defined as “all exchanges of data on the P2P Layer”.

As the price of the freely tradeable Cent token can fluctuate, but the cost/reward for transactions and services is desired to be stable within the OS, Centrifuge OS utilizes the proxy of a “stable currency” for pricing of transactions. Conceptually, it doesn’t have to be a “currency” but for the sake of simplicity the US Dollar (USD) is used as the “stable currency.” In the beginning, all transaction costs within the OS are expressed in a fraction/multiple of USD. For the sake of illustration in this document, transaction costs and rewards are expressed in USD while the actual transaction occurs with Cent tokens.

Concretely, this means that a specific transaction within the OS will have the reliability of costing a specific amount of USD. For example, one document transfer between two P2P Nodes will be charged at the same USD cost while the actual charge in Cent might differ due to exchange rates between USD and Cent. The value of Cent itself is not pegged to USD, but the cost of each transaction within the OS is tied to USD. In turn, this valuation system will likely lead to less speculation on the price of Cent overall as the possible use of the token is limited and has a transparent price per transaction with a restriction on the actual volatility of cost.

One or multiple trusted oracles will provide the current exchange rate of Cent to USD. This exchange rate is retrieved and made available for all Centrifuge participants and the OS itself.

P2P Layer Charges

Data exchange between P2P network participants on Centrifuge incurs a charge paid in Cent on the transaction level - with the Cent amount being based on the USD price as outlined in the previous chapter. The amount of the charge is document agnostic, meaning it is the same charge for any document that is transferred between P2P nodes.

One can compare this charge to the stamp on a standard sized mail envelope: it has the same price regardless of the value of the contained sheet of paper. This charge serves as a metered and baseline reward model for providing and consuming data at the OS level. This baseline charge also acts as a building block for applications that incorporate value-added services on the Centrifuge OS. These applications can add their additional charge to the

baseline charge for their specific document lookups or transfers. In keeping with the stamp analogy, the additional charge can be compared to the additional charges to 2-day delivery, signature upon delivery, insurance of the letter, a fancier envelope, international stamps, etc.

Application Specific Charges

Whenever an application requests an additional amount to be added to a P2P Layer charge, the payer of said charge pays the baseline P2P Layer charge plus the added amount. The payer then specifies in the payment transaction which portions are awarded to the respective recipients. This allows the application provider to react to incoming payment notifications and correlate payments with specific P2P Layer communications that they were involved in. Centrifuge OS does not charge additional Cent for interacting with core components on the Ethereum blockchain, e.g., Centrifuge OS does not require Cent payments to create a new identity within the core contracts of Centrifuge OS.

Use of The Sidechain for Cent Transactions

To allow for more flexible governance and to support a high amount of tiny P2P Layer charges, the transactions of Cent related to P2P Layer charges will solely occur on the Centrifuge sidechain. Support for payment channels on the sidechain also increase throughput and offer a layer of anonymity for payments at high speed with low computational cost.

Participants of Centrifuge OS can send their ERC-20 based Cent tokens on Ethereum to a holding contract that transfers the Cent on the Centrifuge sidechain. The Centrifuge sidechain supports the ongoing Cent payments and rewards while allowing holders to “withdraw” their Cent from the Centrifuge sidechain and transfer them to Ethereum mainnet at any time. The deposit to and withdrawal from the Centrifuge sidechain does not incur additional Cent charges.

Who Pays the P2P Document Charges?

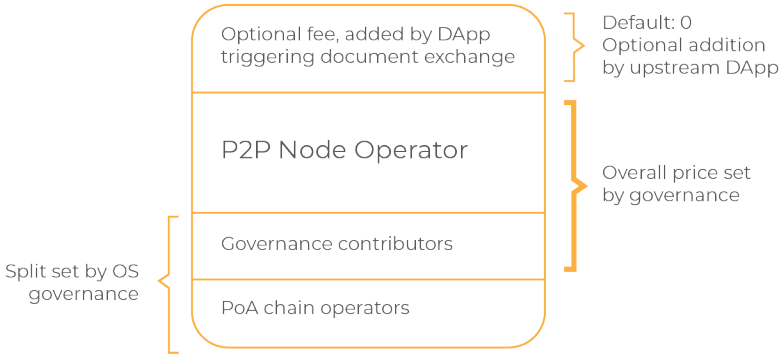
The P2P Layer supports pre-payment of transactions by any Centrifuge OS participant. This method allows for a variety of cost models where either the originating node includes the required proof of fee payment or the receiving node of data can be required to provide proof of payment before the document details are transferred. It also allows for a third-

party (a custodian, financier, service provider, etc.) to pay for document transfer between two participants.

Paying and Receiving Cent When Using The OS

Data exchange within Centrifuge OS is aimed to be as affordable as possible while at the same time including a reward system for data providers on a core level. When data is used to create value or make valuable decisions, the owner of the data -- not an intermediary, controlling the data -- should be rewarded. Applications built on top of Centrifuge OS can implement additional pricing strategies by including an added charge for transfer and/or request of documents of higher value which could then generate financial benefits (e.g., funding for assets transacted through the OS) compared to simple data access.

The use of the data residing on Ethereum and the interaction with Centrifuge OS contracts on Ethereum are free of charge. Users can leverage the contracts of the system at large, read data from the public blockchain, and verify the authenticity of such information that is publicly available. To support the operation of the key components of Centrifuge OS and include built-in capabilities to charge and reward for data access, any payment on the P2P Layer sends a small fraction of rewards to the validators of the Centrifuge sidechain as well as Medallion stakers who actively contribute to the governance and organizational maintenance of Centrifuge OS.



Portions of a P2P Layer charge on Centrifuge OS

The actual prices for transactions on the P2P layer are very small: a thousandth of a USD equivalent or less. The price is set within the core OS contracts through governance votes. This pricing with “tiny amounts” acts, as outlined before, as the baseline for charge/reward for data providing while also allowing spam protection as each interaction costs “*something*”. The price registry also contains information about the fractions of charges

that get rewarded to the Centrifuge sidechain operators and the stakers who contribute to governance.

Added charges via applications can be distributed differently between participants (e.g., sender of data, recipient of data, application provider, etc.). However, the basic transaction costs are always split according to the public register.

Private Token Exchange

Many applications on Centrifuge OS will, at one point, require the transfer of value between business partners or the user and the provider of an application. In Centrifuge OS, as outlined previously, this exchange happens via the Cent token. Exchanging Cent tokens on a completely public blockchain, where the amount of Cent exchanged is based on the value of the involved transactions (e.g., financing of an invoice), can quickly substantiate the value of single business relationships, the creditworthiness, or health of a business. These deductions can be made by observing the amounts of token exchanged even if the documents themselves are kept private. By offering the ability of private token transfer on the Centrifuge sidechain that is linked to Centrifuge OS any DApp can charge private token amounts and, in the end, can also prevent data being publicized.

The use of the Centrifuge sidechain for private token transfer does not cost additional fees. However, the exchange from public to private tokens and back include a fee which is paid out to the network operators. This fee, as all other prices, is set by the network and voted on by holders of staked Medallion tokens.

Rewards for Validators of the Sidechain

The operation of the Centrifuge sidechain is subsidized by paying validators out of the P2P network charges, as well as the shielding/un-shielding fees for tokens.

A MORE DETAILED OVERVIEW OF TECHNICAL COMPONENTS

In this section, we provide a more detailed overview of the components on each layer and how they fit together.

Components on Ethereum

The following Centrifuge OS components are released on Ethereum:

Core OS contracts

- Pricing registry of service and OS-level;
- Publication of current exchange rate between Cent and the registered stable currency;
- TCR for Centrifuge sidechain operators;
- NFT registry;
- Governance Contracts that allow token holders to influence the central logic of the OS. It will be possible for the OS users to propose changes or updates to the OS and its parameters (e.g., price per transaction). See the Voting Specifics chapter for more details.

Public OS participant identity contracts

Corporate identity with recovery mechanisms and keys used by P2P nodes for encryption and signature to allow P2P nodes to validate data and transactions in decentralized fashion, i.e., the identity of a participant of Centrifuge OS. The ownership of identity always remains in the possession of the respective network participant. Interactions with other OS participants rely on these identities.

Public transaction level contracts

The anchor registry used to prove authenticity of document.

The registry stores a cryptographic hash on chain that proves immutability while the data itself is shared between parties on the peer to peer layer. This allows for any third party to verify the authenticity of a document by matching the cryptographic hash of a document to what is anchored on chain. These anchors are extensively used for validating data on the P2P network layer. Centrifuge OS introduces “precise proofs” as a mechanism to validate complex object structures in the form of Merkle Trees on the P2P Layer while at the same time chaining document changes to validate objects and their versions over time.

Generally, the data elements and data related contracts that are public have these characteristics:

- Data fields can be public without security restrictions;
- Low volume or immediate financial value so that the payment of Ether/Gas is justified.

Smart Contracts that fall into these categories are for example:

- Representation of a Company with the information to prove authenticity and ownership of a specific "Company";
- Relationships between Company objects that assist in generating reputation scores as well as proof of business relationships;
- KYC'ed Company information (in form of hashes) that allows data owners to access additional services.

The contracts managing the two tokens, native to Centrifuge OS:

- ERC-20 Contract for Cent tokens;
- ERC-20 Contract for Medallion tokens.

Where possible, features of zeppelin_os[24] will be used for system-level upgrades to contracts and libraries.

Components on the Sidechain

This is a publicly readable chain, allowing connections by any client. This chain only allows specific interactions:

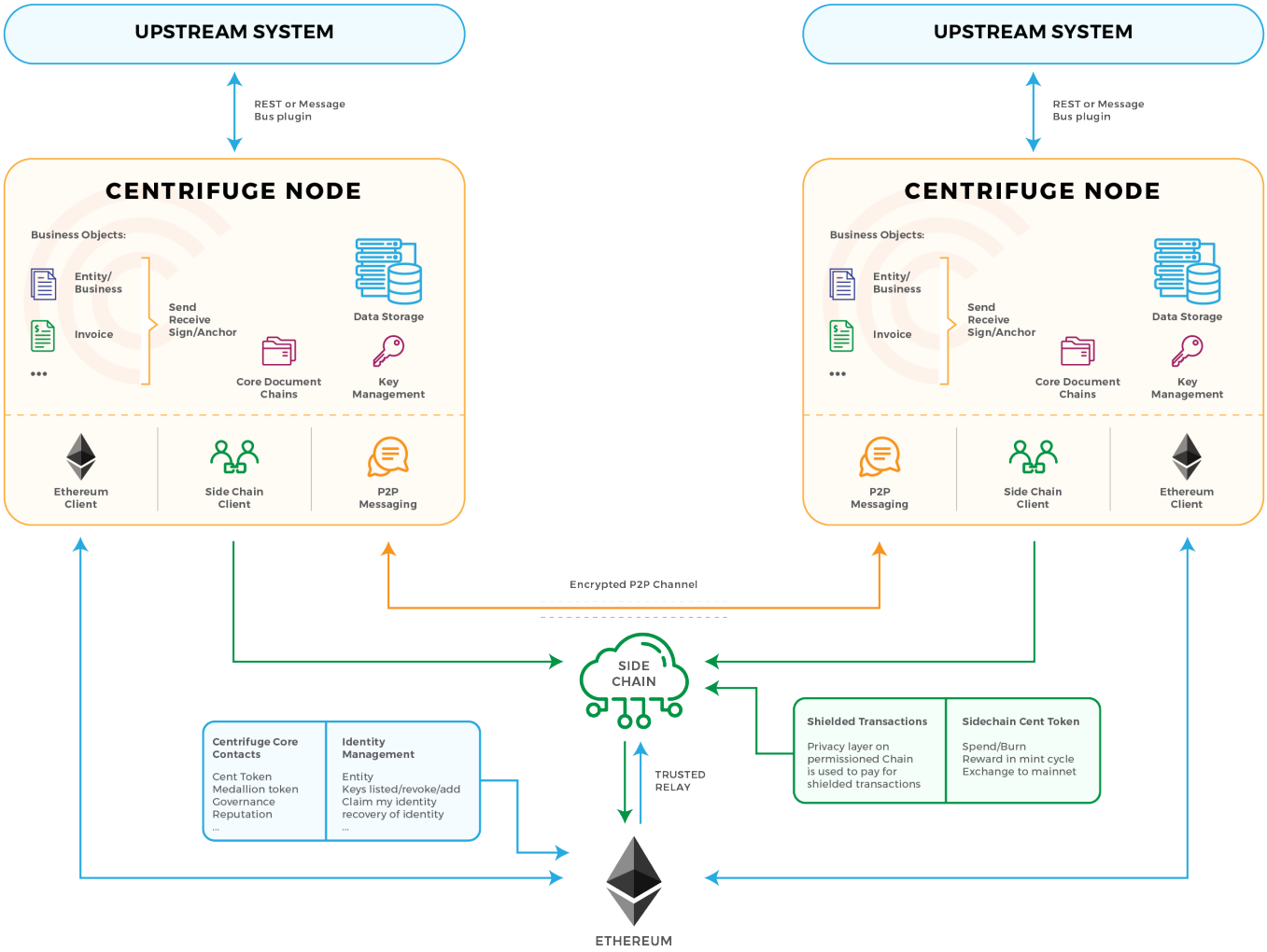
- Interaction with the Cent token contracts for value transfer;
- Shielded tokens;
- Interaction with other core Centrifuge contracts, deployed on the sidechain;
- Governance layer for the Centrifuge sidechain.

While the sidechain is based on Ethereum it is not a general purpose blockchain application platform. It does not permit clients to deploy arbitrary contract code but only allows interaction with Centrifuge specific code. The sidechain rejects transactions that are

[24] https://zeppelinos.org/

sent to unauthorized contracts. The Centrifuge governance layer is used to determine what makes an “authorized contract.”

Graphical Overview of Components



Centrifuge OS Components

MANAGING WALLETS AND KEYS

Currently, enterprises don't necessarily want to own and hold tokens or Ether in order to transact through a distributed operating system. Businesses are accustomed to paying for transactions, data transfer, storage, and services with their preferred fiat currency. Within the next few years, when holding and transacting with native tokens within business applications becomes a simpler and more integrated experience, enterprise preferences will likely shift. It will become more convenient to buy and exchange tokens of all kinds and power the services that rely on them. Until that happens, a bridge is needed to connect the world of traditional enterprise usage and payment with the new economies that rely on public blockchains and application execution and leverage tokens as part of their transactions.

Custodian Model

The solution offered by the Centrifuge team is to shield the complexity of managing wallets and holding tokens through a custodian model. Users of Centrifuge OS can work with a custodian that holds wallets and tokens for enterprises to transact within the OS (not as investment). The "interface" between the company using and paying for the use of the OS and the actual decentralized network is fiat currency. The custodian receives/sends payment from/to the business using the OS in fiat. In the example of an enterprise using Centrifuge OS, fiat currency is exchanged for Ether and Cent, which is used to fund the transactions within the OS.

The owner of a Centrifuge Identity can also set a custodian on their Identity contract allowing a 3rd-party to maintain P2P layer keys on their behalf. Medallions can also be included in a custodian model, but we foresee the majority of custodian requirements to occur related to the transaction cost and reward. Medallions are not as frequently changing hands as Cent.

Data Ownership in The Custodian Model

Besides transacting Cent by using Centrifuge OS, the users also generate data that they continue to own and can interact with. The wallets and keys that are used for signing transactions that are sent through Centrifuge become the key to this data. When a user utilizes a custodian, then the custodian is not only the interface between Cent tokens and fiat but also the de facto holder of the keys to the end-users' contracts that reside on the

Ethereum network and data in the OS. Initially, this means the data flow can be “controlled” by an entity other than the user: the custodian.

This is not much different from how enterprises transact today through e-invoicing networks or other centralized data exchanges or portals. However, with Centrifuge, the data and contracts themselves are already seeded in a decentralized fashion and allow for better sharing and transparency from day one. Over time, enterprises will become more comfortable with owning and maintaining their own wallets and holding a variety of tokens like Cent. The custodian always offers the ability to migrate existing wallets and keys to the Centrifuge OS user when user chooses to do so. This possibility of complete identity ownership and data sovereignty by choice is a vital component to foster innovation in the future where the user has control over whom to share information with. The intent is to eliminate the need for such custodian services as soon as possible to achieve a higher degree of decentralization and data ownership.

In addition to wallet management to hold Cent and Ether for transacting on Centrifuge, the participants have specific private and public encryption keys that are used for securely transacting data between the P2P Nodes. Custodians might also hold these keys and configure them in the respective nodes for encryption, decryption, and signing of data that is sent to other P2P Nodes. It is possible to cycle these keys without affecting the corporate identity on Centrifuge OS. This cycling allows transitioning public/private key ownership from a custodian to the actual user at a later time and without any network impacts.

The custodian model also allows existing business networks to operate Centrifuge OS nodes on behalf of their current user base while offering their value-added services (UI, user management, etc.) without giving up data sovereignty. At the same time, the users can start reputation building and seeding their data into the OS for additional applications to use at a later point.

THE ECOSYSTEM

On-Ramp and Connectors for Other Systems

Legacy systems will need to interact with the public blockchain and the P2P Network while operating on their existing infrastructure, with their existing execution of logic. Connectors that allow the linking of legacy systems to Centrifuge OS are hugely important to support the continuous operation of a company’s infrastructure as well as providing immediate benefits to the users of the OS.

The team behind Centrifuge will release the core P2P Node, libraries, and APIs as open source projects to allow for easy integration of existing systems with the decentralized OS. These open source tools will simplify complexities such as key management, transformation of data for transmission and storage, and more. The connectors will support direct connection to all parts of the OS. Beyond basic connectivity, existing business systems such as SAP ERP, Oracle E-Business Suite, PeopleSoft, Microsoft Dynamics, QuickBooks, and others also require translation of their internal logic and data that is then transmitted and stored via Centrifuge OS.

Given the strong background of building enterprise business networks and connecting the involved systems with online services, the Centrifuge team will also build and release first connectors for selected systems that solve logic and data translation to interact with the Centrifuge network. Aside from connecting individual legacy systems, bridges to existing business networks offer links from these networks to the OS operating on the public blockchain. The same is true for funding and bank platforms. Also, the Centrifuge team will release initial connectors in conjunction with selected network providers, banks, funders, and others to foster a strong eco-system and interoperability.

THE DIFFERENCE BETWEEN CENTRIFUGE OS AND "CENTRIFUGE THE COMPANY"

Centrifuge OS is the network and decentralized platform to power the global financial supply chain on public infrastructure. To develop a successful system of this technical and organizational scale a concerted effort of individuals and interest groups is required over longer periods. Centrifuge Inc, together with its subsidiaries and affiliated entities, brings the team together to support the initial development and deployment of Centrifuge OS. For simplicity's sake, we use the terms "Centrifuge, the company" or "the Company initially developing Centrifuge OS" to describe this group of people and partners.

While the initial development is supported by Centrifuge, the company, the network is not governed, deployed, or operated by this company. The network and Centrifuge OS at large are designed and released to be a decentralized platform from day one. The duty of Centrifuge, the company, is to build a reference implementation of Centrifuge OS components, support the initial launch, and assist OS users with their onboarding.

CENTRIFUGE, THE COMPANY, AS SERVICE PROVIDER

Centrifuge OS is designed and will be deployed as an open, decentralized system, usable by anyone who wants to join and transact on it. However, an operating system is only as useful as the services built on top of it. With decades of experience building software and services in the procure to pay and financial supply chain sector, Centrifuge, the Company, will be supporting the first use cases of the OS together with launch partners and early participants of the ecosystem.

When Centrifuge, the Company, delivers such services, they are decoupled from the delivery of the OS itself. Centrifuge, the Company, is operating within the same economic system as any other OS participant and does not receive additional financial rewards or steady payments from the network. Being one of the largest Medallion holders initially, Centrifuge, the Company, will be able to subsidize the development of the OS as well as operation of the initial infrastructure. This assures the separate development of the OS while at the same time seeding the network by solving genuine business needs for users.

DISCLAIMER

Certain statements herein may constitute forward-looking statements. When used herein, the words “may,” “will,” “should,” “project,” “anticipate,” “believe,” “estimate,” “intend,” “expect,” “continue,” and similar expressions or the negatives thereof are generally intended to identify forward-looking statements. Such forward-looking statements, including the intended actions and performance objectives of Centrifuge Inc. involve known and unknown risks, uncertainties, and other important factors that could cause the actual results, performance, or achievements of Centrifuge Inc. in its development of the system, network, its components, and the tokens to differ materially from any future results, performance, or achievements expressed or implied by such forward-looking statements. No representation or warranty is made as to future performance or such forward-looking statements. All forward-looking statements herein speak only as of the date hereof. Centrifuge Inc. expressly disclaims any obligation or undertaking to disseminate any updates or revisions to any forward-looking statement contained herein to reflect any change in its expectation with regard thereto or any change in events, conditions, or circumstances on which any such statement is based.

You are not to construe this white paper as investment, legal, tax, regulatory, financial, accounting or other advice, and this white paper is not intended to provide the basis for any evaluation of an investment in an interest.

ACKNOWLEDGMENTS

This work would not be possible without our supporters, critics, and our team. Thank you to the contributors, reviewers, and proof-readers: Philip Stehlik, Markus Ament, Martin Quensel, Lucas Vogelsang, Miguel Hervas, Maya Byskov, Lea Bauer, Toby Coppel, Jason Whitmire, Philipp Banhardt, Demian Brener, Trent McConaghy, Stefano Bernardi, Yannick Roux, Alexander Shelkovnikov, Alexis Sellier, Alexander Lange, Ravi Kurani.