CITADEL

Bridging the adoption gap between Decentralized Ledger Technology and the Consumer Services Economy

Whitepaper Version 0.1

Citadel Research & Development Team
September 16, 2018

Abstract

Citadel is a peer-to-peer, open access cryptographic network of value for delivering distributed digital services to users around the world. Citadel's primary focus is to create an open and flexible digital ecosystem that fosters innovation and creates economic opportunities for businesses and consumers around the world, by reducing service costs, mitigating transaction risks and lowering barriers to entry.

The Citadel project comprises two primary entities - the Citadel Network, being the underlying Blockchain-based, cryptographically-secure infrastructure for sending economic value in the form of CTL coins between users, and the Citadel Platform, a diverse and flexible ecosystem of digital, identity and e-commerce services for consumers globally.

The Citadel Network

The Citadel Network is:

A. A peer-to-peer decentralized cryptographic network where users can transact by sending economic value to one another. All transactions are stored on a secure, shared public ledger known as the Citadel Blockchain, while being completely anonymous and reveal no information about the sender and receiver. The Network's robust distributed infrastructure serves as the backbone for the multi-layered, decentralized digital services architecture known as Citadel Platform;

B. Private By Default - As Citadel takes user privacy very seriously; all transactions performed across the Citadel network are fully anonymous and untraceable. Using the peer-reviewed, cryptographically-sound CryptoNote protocol with a stealth addresses implementation, Citadel Network ensures that identities of both the sender and receiver remain hidden and can never be traced. Citadel's privacy means that usage is risk free and that you are safe from any de-anonymization attacks.

C. Truly Decentralized - Citadel utilizes the time-tested Proof-of-Work (PoW) network consensus in order to ensure the integrity of its shared ledger, the Citadel Blockchain, where all transactions are immutably stored and cannot be corrupted. By using a uniquely modified variant of PoW, the Citadel Network greatly reduces the advantage that certain actors attempt to gain through dedicated hardware equipment meant to concentrate network share, as seen in the case of Bitcoin and other well-known cryptocurrency networks. This ensures a more level playing field for honest participants using general purpose CPUs and creates a far more democratic participation opportunity for contributors globally.

D. Threat Resistant - Citadel takes security a few steps further and introduces a hardened cryptographic mining algorithm variant (CryptoNight V7+), a dynamically evolving memory-heavy verification challenge (Citadel Adaptive Scratchpad) and a robust difficulty adjustment algorithm (DAA) known as Zawy's Linear Weighted Moving Average (LWMA). These components are all of which work in unison to prevent any attackers from being able to compromise the network's operational continuity and guarantees its reliability.

E. Fungible - Funds that are stored on the Citadel Network are represented as Citadel coins (CTL), its innate cryptographic currency. As the network is completely private and there is no way to determine any coins transactional history, CTL coins are completely indistinguishable from one another and cannot be singled out or blacklisted. This makes CTL the equivalent of safe and convenient digital cash.

F. Fully Open - Citadel is an open access, open source, public network with no barriers to entry. Anyone can participate in securing the network, using its services or acquire CTL coins to transact with their peers. Users can choose whether to run a full Citadel Blockchain node, a Sentinel service node, create their own Sentinel Application, register their identity or simply use a wallet to store their funds securely and privately. 3rd party developers can and are encouraged to contribute to any aspect of growth, ranging from contributions to its core architecture to creating and publishing decentralized applications.

G. Scarce - Citadel Network relies on a disinflationary economic model designed to support its coin's long term value. A very tightly controlled inflation schedule is in place to ensure that only a certain number of coins are created every day to compensate miners who participate in verifying blocks and securing the network, as well as depositors via Citadel Vault - an interest-yielding term deposits and withdrawals service that rewards long term holders and creates long-term market liquidity used to fuel the Citadel economy. All of this resolves in making the Citadel Network a resilient store of value and hedge against economic volatility.

H. Commercially Applicable - The Citadel team is constantly working on service provider and merchant adoption to generate real-world usability for coins held by users. Services such CTL Pay, a network of e-commerce and Point-of-Sale integrations, will allow users to pay directly for goods and services consumed using their CTL coins, which can be received via either mining, depositing or services rendered on the Citadel platform, creating a sustainable chain of value free of economic bottlenecks.

The Citadel Platform

The Citadel Platform is a secure, cost-effective and multi-faceted architecture for delivering digital services to anywhere in the world. Its primary application ecosystem, known as the Sentinel Framework, will serve as an open, flexible and fully programmable network of distributed nodes where decentralized applications (Sentinel Apps) can be hosted and run.

Leveraging the power of Citadel Network's underlying decentralized infrastructure and expanding its scope with the infinite flexibility that is afforded by the Sentinel Framework, allows the platform to create a wealth of immutable digital services with a cost-friendly commercial profile ready for mass business and consumer adoption.

Key Components of the Citadel Platform

1. Sentinel Network

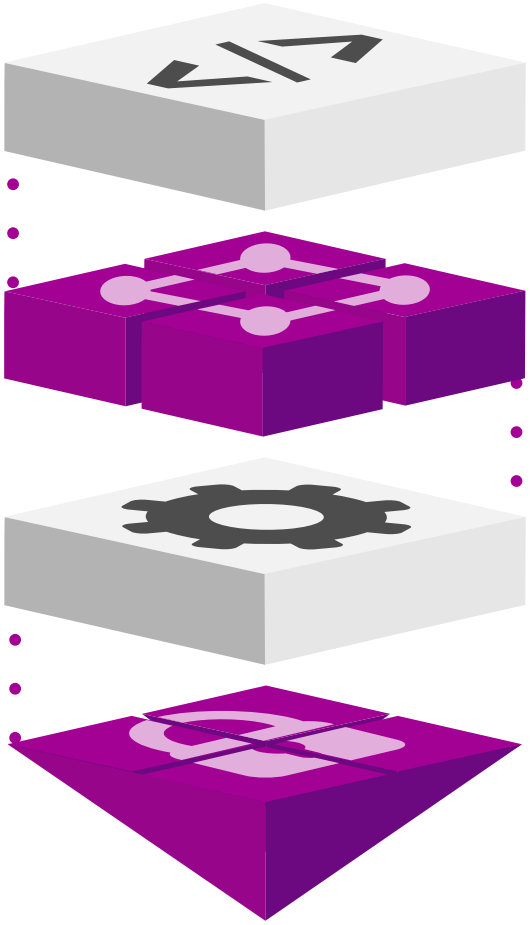
Sentinel Network is:

Citadel Platform's robust, open, digital services architecture where developers can author decentralized applications (Sentinel Apps) using a set of built-in development tools, publish them to thousands of active, high-redundancy Sentinel Nodes around the world and have millions of users engage and collaborate with complete privacy.

Sentinel Nodes are Citadel Platform's main driver of scalability. These nodes are run trustlessly by network participants who receive a fee for on-demand service delivery and operation by consumers directly. As there are no centralized intermediaries involved and services are only consumed on-demand, the ecosystem creates the economic conditions needed to keep both consumers and service providers equally motivated to participate.

Citadel's redundant network architecture allows Sentinel Apps to seamlessly switch between multiple Sentinel Nodes in the event of node failure, eliminating the risk of database corruption and reduced availability. This allows applications to have operational and security assurances that are essential to mission critical business functions. The unique benefit afforded by this architecture is having a rich digital library of smart applications, without the need for a trusted third party, without performance trade-offs and without having your data trail collected without your knowledge or consent.

For mission-critical enterprise applications, publishers and can opt for using Citadel's Private Sidechains (CPS), which creates a private corporate environment that is permissioned and cannot be accessed by unauthorized entities. Due to Citadel Network's innate privacy features, private sidechains are truly private and their existence cannot be determined or tracked by any outsiders. This invariably leads to an increase in operational efficiency and lowers costs, making CPS-hosted Sentinel Apps well suited for driving large scale business adoption.



Sentinel Framework - (Creation Layer)

Sentinel Nodes - (Hosting Layer)

Sentinel API - (Interaction Layer)

Sentinel Apps - (Application Layer)

Sentinel Network Layers

2. BitKYC protocol

BitKYC Protocol is Citadel Platform's Smart Identity Management Service (SIMS), and is an on-chain identity registration, encryption and verification service. The purpose of BitKYC is to create a viable mechanism through which digital identities can be created, administered and recognized by any service provider worldwide.

Each user's identity, once verified, grants the registrant a unique cryptographic key (C-Key) with which all services can be accessed seamlessly and securely. Such identities will be persistent and reusable across all services provided by Citadel Platform at first, and later on integrated into large scale, traditional ID-based services such as the ones provided by world governments, law enforcement agencies, financial and commercial service providers, regional authorities and others, and in doing so, Citadel aims to disrupt the fractured global landscape and create a consistent and unified method of identity management with equal participation for every global citizen.

BitKYC ensures that each person's unique identity corresponds to a cryptographic key that cannot be altered, cannot be compromised and cannot be stolen. Furthermore, due to Citadel Network's unique privacy-by-default nature, any identity issued by Citadel cannot be detected or discovered even before, after and during verification using BitKYC.

3. Private Smart Contracts

With the introduction of private smart contracts, Citadel aims to provide a framework for creating, executing and verifying cross-party agreements with special commercial terms. Understanding that sensitive commercial and financial data must not be compromised, Citadel leverages its audit-resistant Blockchain infrastructure to ensure that contractual content remains invisible to unauthorized parties or publicly at all times, while allowing authorized parties to verify that agreed-upon term is satisfied.

The ability to store data privately and securely on the Citadel Platform coupled with the ability to perform advanced conditional computation results in a very wide range of cross-industry business applications, such as enforcing real-world contracts, ensuring delivery-on-payment and counterparty compliance.

4. Private Side Chains

Citadel's empowers business and individuals to create their own uniquely-tailored private Blockchains that suit their individual needs. Every Citadel launched sidechain will be a derivative of the main Citadel Blockchain, and have a two-way peg back to it, allowing for seamless exchange of information on-demand. Private Side chains will be a store of data and value and can be run on any number of nodes around the world, making them ideal for use by decentralized applications and consensus-backed issued assets.

The main benefit is that Citadel side chains will be private and not publicly visible, as well as have a set of custom configurable governing parameters that dictate each chain's nature, behavior, requirements, structure and pre-defined assets. Conversely, having dedicated chains for specific applications will offload computation and storage requirements from the main chain, allowing the Citadel to assign resources to more general purpose operations and network-wide data validation.

5. Citadel Assets

Citadel Assets provide individuals, businesses and organizations with a mechanism to solidify ownership over both digital and physical real-world assets using the power of Citadel Network's trustless consensus.

As assets are issued on the Citadel Blockchain, being a decentralized and trustless public ledger, any risk of database corruption for any centralized organizations, whether governments or otherwise, is therefore eliminated. This ensures that any asset retains a persistent representation on the Citadel Blockchain that can be transacted and transferred at any time. Transferring of asset ownership can be supervised using Citadel's private smart contracts mechanism to ensure that ownership is retained until all contractual terms are fully carried out, creating powerful safeguards that are incorruptible or subject to individual interpretation.

To further solidify individual ownership, assets can be coupled with identity-based C-Keys, to protect against re-issuance under a different identity (asset double spend), and require a C-Key signature for any pending transaction involving the assets in question, adding a much needed layer of security against digital property theft. As identity association is strictly optional, Citadel Assets will allow anyone to own any asset without having to disclose their identity publicly, and will open the door to billions of unbanked world citizens in need of such a platform.

6. Citadel's Encrypted Messenger

Citadel's Encrypted Messenger is a decentralized service for sending end-to-end encrypted data-rich communication between users. Its architecture has no singular points of failure, and allows you to restore your entire communication history using your private view key, without relying on any centralized or cloud hosting services.

While currently available as an in-wallet service, future platform enhancements will allow developers to make use of advanced APIs to create rich interactive experiences between peers, communities and corporate entities, making the service more scalable, cost-effective and cross-device friendly.

The service includes two primary communication functions:
- **Citadel Messaging** - encrypted, self-destructing untraceable on-chain messaging, enabling multiple communication channels between peers and wide distribution lists.
- **Citadel File Share** - send and receive files using the distributed, storage-efficient and persistent IPFS internet infrastructure. Sent files are encrypted and anonymous, ensuring that only the relevant parties can locate and access sent data.

7. CryoSyS

Linux based operating system that is meant to run off a USB drive as a fresh installation on every launch. It is a clean, malware free, privacy focused environment with application sandboxing capabilities, advanced built-in privacy and security features to form the safest user environment.

8. NoteAlias

A unique, one-to-one, persistent address aliasing mechanism on the Citadel network. Using NoteAlias, users will be able to create an alias (User ID) for their public address and receive funds directly to their chosen alias, eliminating the need to send long, unintuitive public addresses for payment. NoteAlias is Citadel's adaptation of the OpenAlias protocol for the CryptoNote sphere.

DarkBazaar

DarkBazaar is Citadel's simple, fee-free, privacy-centric online marketplace for exchanging goods and services. There are no listing fees or approval processes for vendors and sold items, and no restrictions on shopping activities. DarkBazaar allows users to buy directly from merchants without needing a centralized intermediary, reducing costs overall and making the service an attractive alternative to major e-commerce players in the field.

DarkBazaar's privacy features ensure that no-one can know what you buy, who you are buy from and how much you spend on each purchase. While a clear aim is to protect user privacy, such that no identifiable records are kept of any purchase, shoppers and vendors will be given an option to use and link their C-Key identities to maintain an operational record and establish trust, as well as verify identities for physical delivery.

DarkBazaar's primary method of payment will be using CTL coins directly, giving the currency a real-world use and increasing its commercial viability.

CITADEL

Whitepaper Version 0.1

Citadelplatform.io