CRYPTOCURVE

WHITEPAPER VERSION 1.0

TABLE OF CONTENTS

ABSTRACT

In 2015, the World Economic Forum predicted that by 2025 approximately 10% of the global Gross Domestic Product (GDP) will be stored on cryptocurrency blockchain technology[(1)]. Positive impacts of this shift include increased transparency, disintermediation of financial institutions, and financial inclusion.

Blockchain carries the potential to shape industry, privacy, security, and the global economy. But it currently lacks an easy entry point, which has delayed adoption.

Cryptocurrency investors, whether new or experienced, face daunting barriers. To keep pace with highly volatile currencies across multiple platforms in exchanges that move far too slowly, transactions must use clumsy and non-intuitive management tools. The general public hears horror stories about massive hacks, black market dealings and fortunes being lost when a computer crashes. The more knowledgeable blockchain enthusiast is all too familiar with DDoS attacks, exchanges crashing, limited fiat gateways and an arcane system of hex addresses. These limitations lead to an environment of fragmented ecosystems, significant security vulnerabilities, and high barriers to entry. This Whitepaper describes CryptoCurve's solutions: the Curve Wallet and the CurveSDK.

The Curve Wallet is a multi-blockchain platform that provides a frictionless experience, facilitating cross-chain transactions and smart contracts in a simple and clean UI/UX. The Curve Wallet simplifies and accelerates adoption for seasoned investors and the general public by serving as a turnkey product for all blockchain-consumer needs. Intuitive features in Investing, Trading and Accounting allow for custom pooling, advanced asset tracking and management, securities-compliant ICO investing, in-app trading via a decentralized exchange, and easy transactions through fiat gateways.

As with the barriers to mass adoption from a user's perspective, there are similar concerns with obtaining adoption at a developer level. Current dApp developers must maintain their own nodes and infrastructure, all the while lacking resources and ready-made tools, costing in time and effort. CryptoCurve accelerates development by creating the CurveSDK -- an all-inclusive and standardized environment similar to the convenience provided by Amazon Web Services. By providing the infrastructure and the ecosystem, CryptoCurve will allow developers to focus their efforts on the blockchain solutions their dApps are looking to provide.

The Curve Wallet and CurveSDK solutions described in this Whitepaper are the first steps toward building an ecosystem that will break down existing technological barriers and drive global blockchain adoption.

MISSION + VISION

CryptoCurve's **mission** is to accelerate the positive global impact of blockchain technology through an ecosystem of user-experience-driven products and programs that help individual investors, software developers, and corporate entrepreneurs achieve their goals with blockchain technology. Our **vision** is to be the world's blockchain front-end solutions leader and a preeminent global thought leader in the blockchain industry.

CHALLENGES

USER ADOPTION BARRIERS

TIER 1 CONCERNS & CONSIDERATIONS

These are initial concerns for new users and are often the first barriers to entry.

PRIVATE & PUBLIC KEYS

+ Key storage/management are not meant for non-technical users. Storage methods vary widely from platform to platform -- one preferring mnemonics, another passwords, and another JSONv3 format.
+ This leads to lost keys and dormant wallets with no recovery options.

SECONDARY SECURITY MEASURES (2FA, Biometric, Dual-linked devices)

+ Base wallet implementations lack secondary security mechanisms. These protect transfers, sensitive data, and transactions, while creating peace of mind.
+ Standard mechanisms used in financial trade include: Two-Factor Authentication (2FA), biometrics (fingerprint and facial recognition), dual-linked devices (web and mobile), secure passphrases and One-Time Passwords (OTP).

TRANSFERS ARE CUMBERSOME

+ Transfers are a terrifying task for new and veteran users, using complex public keys. When a large sum is involved, this is particularly daunting.
+ Keys are complex and not designed for ease of use. To service the financial sector, we have created an abstraction for account numbers by leveraging beneficiaries. This allows for comfort, ease of use, and a secondary authentication step.

NO AHV OR CDV

+ Account Holder Verification (AHV) and Check Digit Verification (CDV) is standard for normal financial trade, yet these simplistic tools are missing in cryptocurrency.
+ CDV is already possible and can be further implemented to allow for check digits of Curve users. AHV also becomes possible as accounts are registered to specific Curve users.
+ Disconnected Environments (Wallets, Explorers, Web, Mobile, Online, Offline, Hardware)
+ A single transfer can involve multiple wallets, offline transaction, offline signing, online broadcasting, or an explorer to see the transfer. All of these tools can be consolidated into a single platform.

FRAUD DETECTION

+ There are basic security mechanisms that can be put in place for fraud detection, aside from AHV, CDV, or secondary security. Other possibilities exist.
+ Accounts will be whitelisted or blacklisted for transfer, a wallet identified via public consensus will be triggered for investigation. Machine Learning tools will be implemented for fraud detection. Wallet trust factors will be implemented based on age, transfer history, and the interconnectedness of a wallet to trusted sources.
+ An index of all accounts will be built with each having a rating based on age, total transfers, value transferred, and whether they interact with other highly-rated accounts. This score will be made transparent for the purpose of identifying accounts.

FIAT TO CRYPTOCURRENCY

+ First-time cryptocurrency purchases are often cumbersome and include bank transfers, clearing times, and banks not allowing for cryptocurrency-related charges or deposits. Being able to get in and out of cryptocurrency is a critical hurdle for cryptocurrency to reach mainstream adoption.

TIER 2 CONCERNS & CONSIDERATIONS

At this point, a user has gained some comfort with cryptocurrency and has started to expand their portfolio.

MULTI-CRYPTOCURRENCY TRACKING

+ All Tier 1 concerns are specific to a single cryptocurrency, and those issues are compounded when adding multiple cryptocurrencies. Tracking multiple cryptocurrencies across different exchanges and wallets can become an arduous task.

MULTI-CRYPTOCURRENCY WALLETS ARE UNINTUITIVE

+ The few multi-currency wallets that currently exist are cumbersome and difficult to use.

PORTFOLIO MANAGEMENT

+ Even if cryptocurrencies are stored across multiple wallets, data management is complex and requires specialized software.

EXCHANGE VETTING & IDENTIFICATION

+ With over 200 exchanges it can quickly become difficult to identify which to use and trust with your data.

ASSET DEPENDENCY

+ Crypto assets are often specific in requirements. For example, a user must possess ETH to participate in an ERC-20 ICO, or BTC for a Bitcoin network ICO. Users are unable to successfully abstract their assets and need to keep multiple assets for crypto engagement.

TIER 3 CONCERNS & CONSIDERATIONS

These are users that currently hold multiple assets across multiple exchanges and wallets.

INITIAL COIN OFFERING IDENTIFICATION (only vetted ICOs can join the platform)

+ As of the time of writing, 828 ICOs in 2018 translates to 5.25 ICOs to vet per day for a single person.

ICO PARTICIPATION

+ Lotteries, questionnaires, KYC, Proof of {Insert Term}, and multiple distributed platforms

KNOW YOUR CUSTOMER

+ KYC is inconsistent across platforms. One may require a selfie, another requires you to take a selfie holding a defined written message, another with you holding your ID, and the list goes on.

DEVELOPER ADOPTION

User adoption is parallel to developer adoption. Without continuous improvement and new applications, Blockchain will become stagnant and unable to attain mass adoption. In the developer ecosystem the following issues exist.

CONCERNS & CONSIDERATIONS

SELF-MANAGED NODES

+ As a dApp developer, you need to manage your own nodes and infrastructure to host applications.

UNSTRUCTURED APIs

+ One solution implements REST, another JSON-RPC, one HTTP, another HTTPS, another Web Sockets, often requiring multiple API inclusions and types for simple applications.

DEVELOPER ECOSYSTEM

+ A standard developer stack consists of nodes, cloud infrastructure, explorers, wallets, testnets, multiple API stacks, and multiple connectivity tools.

LACK OF DEVELOPER RESOURCES

+ Developers often have no point of contact for developing documentation and resources, how-to's, and Hello World's.

END-TO-END TESTING SOLUTIONS

+ Testnets exist, but often you are unable to replicate from the live environment. Thus, testnets are a step towards the right direction, but must include the ecosystem, infrastructure and up-to-date data.

CONSOLIDATED APIs

+ API standardization is required, talks towards unstructured APIs as well.

DOCUMENTATION

+ Documentation for API, ecosystem, testing, compliance and developer resources are spread out across multiple sources.

SOLUTION

To address user adoption, we have architected the following high level solutions:

+ Key Management System
+ Two Factor Security
+ Dual Linked Security
+ Beneficiaries
+ AHV and CDV
+ Account Fraud Detection System
+ Secure Wallet Vetting (with certificate and stamp)
+ Consolidated UI for Wallet, Explorer, Web, Mobile, Online, and Offline systems
+ Multi-asset tracking
+ Portfolio Management
+ ICO Pooling
+ ICO Hosting
+ DEX and CEX integration

To achieve the above, we created a set of developer tools. Instead of keeping these tools in house, we opted for open source to provide these tools to the community. These tools include:

+ Interoperable Hosted Nodes
+ Interoperable Offline Wallets
+ Interoperable Online Wallets
+ Interoperable Explorers
+ Enterprise Service Bus (ESB) Mapping for Consolidating APIs
+ Replicated End-to-End Testnet Environments
+ Consolidation and Documentation of Exposed APIs

We will not discuss each component in detail. Rather, the purpose of this document is to explain how we are solving new problems. We will not focus on items that have already been addressed in other papers.

THE CURVE WALLET

The Curve Wallet will be available on the following devices:

- Web
- Android
- iOS
- Mobile Web
- API
- Cold Storage (Vault)

Designed and built by seasoned cryptocurrency users, the Curve Wallet will serve as a powerful, simplifying tool for new and experienced cryptocurrency investors. For example, the wallet will offer simple portfolio tracking that allows investors to monitor holdings over time.

SECURITY

Security, more than any collection of attractive features, defines a cryptocurrency wallet. Much of the negative PR surrounding blockchain and cryptocurrency involves security vulnerabilities in which individuals lose large amounts of cryptocurrency.

Until now, cryptocurrency investors have needed multiple storage points for their investments with hardware and online wallets (both often also secured by paper wallets), as well as uninsured exchanges.

CryptoCurve has invested significant resources into creating the most secure wallet on the market. Curve Wallet users will be able to manage assets from multiple blockchains and perform peer-to-peer exchange directly on the platform. Users will no longer need multiple accounts on different platforms and will enjoy safekeeping for cryptocurrency assets in a secure, simple Wallet.

Below, we briefly outline some of the critical security standards and features that we have implemented.

SECURITY FEATURES

We have five critical security features that we want to highlight:

- Key Storage Flexibility
- Beneficiaries
- Multi-Sig Capability
- Mobile OTP
- Biometric Data

KEY STORAGE FLEXIBILITY

The Curve Wallet keystore vault provides both inexperienced and expert-level investors options for powerful, secure key storage. New users may prefer that the Curve Wallet stores their keys, while seasoned investors may choose customized controls for keystore files.

For ease of use, the Curve Wallet keystore vault encrypts, shards, and replicates keys across multiple distributed keystore instances. More experienced users can either store their own keystore files (like other wallets) or utilize dual storage by simultaneously storing keys personally and on the Curve Wallet.

BENEFICIARIES

A beneficiary is any user to whom another user sends coins or tokens. One significant example of our security standards involves beneficiaries that Curve Wallet users will be able to add, remove, and manage. (A beneficiary must be added before payment can occur.) Beneficiaries will have privatized trust scores that allow for more informed decision making. For example, an account that has not received any transactions would have an uninitialized (or low) score, and a warning will be provided to the user making the transfer. The beneficiary system also allows for blacklisting certain accounts. If an account is confirmed as fraudulent, that account will be blacklisted and will no longer be allowed transfers via the Curve Wallet.

MULTI-SIG CAPABILITY

Standard wallets require only a single user to confirm a transaction before it is sent to the blockchain. In a multisignature wallet, multiple users must confirm a transaction. This allows for greater security when a large pool of funds is owned by a number of different users. The Curve Wallet will support multisignature via smart contracts: when a user with sufficient privileges initiates a transaction, other users with approval rights will receive a push notification. Those users will be able to view unapproved transactions in the Wallet and grant approval. When the number of approvals meets the required threshold, the transaction will be sent to the blockchain.

MOBILE OTP

Multi-factor authentication is a recommended best practice for protecting sensitive data. Providing an extra layer of authentication and verification, multi-factor authentication goes beyond the basic username and password security model. With the release of our mobile app, we will enforce OTP and in-app validation of transfers. While we allow for Two Factor Authentication (2FA), it can be cumbersome; OTP will push an authorization request to the user. If the user approves, the transfer will go through.

BIOMETRIC DATA

FINGERPRINT AND FACE RECOGNITION

Curve Wallet users will be able to integrate features currently used on many bank and credit card mobile applications -- such as fingerprint or facial recognition -- in lieu of traditional passwords. Fingerprint and facial recognition are stored locally on the device, which means a user's biometric data will never be vulnerable.

VOICE RECOGNITION & VOCAL SEED PHRASES

The Curve Wallet will integrate voice recognition and vocal seed phrases of the user's choice to ensure that only the user has access to their assets and transactional history.

SECURITY: IN DETAIL

CryptoCurve has an end-to-end approach to security. Security considerations are made from the application layer to infrastructure layer.

LAYER 1: COMMUNICATION

This is architected with end-to-end encryption in mind. To facilitate this, we implement the following security protocols:

+ All communication is HTTPS with a minimum of TLSv1.1_2016
+ All payload transfers are random seed AES-cbc encrypted
+ Mnemonic phrases are used for random seeds
+ Time based payload signatures are implemented to prevent replay attacks
+ Payloads are signature-signed to prevent tampering
+ All passwords are random-seeded SALT
+ All endpoints are secured via basic authentication
+ All function calls are secured via endpoint authentication
+ Session management is controlled via JWT
+ Web application firewalls are implemented to protect against vulnerabilities
+ Sites and APIs are externally scanned for XSS, SQL injection, and other released vulnerabilities
+ Content-Security-Policy header is used to prevent cross-site scripting
+ Allow-Control-Allow-Origin only allows approved whitelisted domains
+ Access-Control-Allow-Methods only allows the minimum set required
+ Access-Control-Allow-Headers is strictly controlled
+ X-Powered-By headers are stripped of content
+ Public Key Pinning is implemented to prevent man-in-the-middle attacks
+ Strict-Transport-Security enforces secure connections
+ Cache-Control and Pragma headers are used to disable client-side caching

+ X-Content-Type-Options are implemented to prevent MIME-sniffing
+ X-Frame-Options are used to prevent clickjacking
+ X-XSS-Protection to enable the CSS filter in browsers
+ IP access is filtered and controlled to prevent DDoS
+ Multi-location hosting to prevent single point of failure

LAYER 2: PROCESSING

After transmission has occurred, the processing phase begins. The following protocols are implemented to ensure security during processing:

+ One-off IAM accounts for ECS instances.
+ APIs are stateless and side effect free.
+ No data is stored locally.
+ Data is actively purged from memory after usage.
+ All clusters are VPC controlled and only available behind DMZ.
+ All access is IP- and port-controlled.
+ Microservices architecture for role encapsulation.
+ Minimum access user roles.
+ Processing occurs in single-boot instanced VMs.

LAYER 3: STORAGE

Storage is arguably the single most critical single point for any security-centric system. To ensure a secure protocol layer we implement the following security protocols:

+ All data stores are key encrypted
+ Data stores are split into read-only and write-only systems
+ Access control is meticulously audited and logged
+ Sensitive data is dual-encrypted by user key and randomly-generated one-off keys
+ Keys are stored in protected JSONv3 standard
+ Passwords are random-seeded and SALTed
+ Keys are sharded and stored in distributed key stores
+ Keys are only made whole during creation and in-memory access
+ Minimum-access user roles are used to ensure that only a single role has access to its minimum feature set

EXCHANGE INTEGRATION - DECENTRALIZED

+ Trade directly from inside the Curve Wallet
+ No need to manually track trade history
+ Save time by using only one trading platform
+ Users will be able to trust in the blockchain - not a centralized database

+ Decentralized back end, ease of use similar to a centralized interface
+ Wide variety of liquidity pools provides consistency

The first of these integration partners will be Øx protocol. Øx implements an off-chain order relay with on-chain settlement. Øx started as an OTC platform for peer to peer order matching, it further expanded upon this by creating the Øx protocol. Øx implements the concept of off-chain relayers. These are distributed hosts that keep and broadcast the order books, similar to how a blockchain is distributed and decentralized. Market makers release signed orders (backed by on-chain confirmation) and market takers buy these. Once bought it is backed by on-chain settlement.

INTEGRATION

+ Connect to CryptoCurve Ethereum node clusters
+ Connect to CryptoCurve Øx relayer
+ Retrieve the current Øx exchange contract address
+ Retrieve the WETH and ZRX token addresses
+ Setup an account
+ Set a spending allowance (user configurable)
+ Generate WETH (Converts ETH into ERC20 compatible WETH)
+ Transact with the relayer

BENEFITS

+ Low fees (The Curve Wallet has its own relayer and will provide discounted rates for users)
+ Make orders
+ Take orders
+ Find best matching orders for taker

DECENTRALIZED EXCHANGE

+ Spot trading
+ Margin trading
+ Futures

EXCHANGE INTEGRATION - CENTRALIZED

For further ease of use, users will be able to add their current supported exchanges directly into the ecosystem. There are two phases of implementation in development.

+ **Phase 1:** Users add trade keys directly. This allows full user control. These keys are stored with the user and they will interact directly with their exchange wallets.
+ **Phase 2:** Shared state channel. Users will simply activate an exchange service and be given full access to the functionality.

INSTANT TRANSFERS & LOW-FEE TRANSACTIONS

Transfers between users will be instantaneous and have a marginal fee. This is accomplished via state channels. State channels were originally designed as a scaling mechanism for on-chain settlement. A state channel can be explained as follows.

Alice and Bob are both Curve Wallet users. Alice transfers 1 WAN to Bob. Alice signs a transaction to that end. Bob accepts receipt of funds and co-signs the transaction and publishes the co-signed transaction back to Alice. At any point in time Bob can now withdraw his 1 WAN with the co-signed transaction as both Alice and Bob have agreed on the state of their financial transaction.

The Curve Wallet will allow for multi-channel inter-party state channels. This allows for Curve Wallet users to have instantaneous, low-fee transactions among other Curve Wallet users.

PAYMENT PROCESSING

The multi-channel state channel will allow for third parties desiring to receive payment in cryptocurrency to accept payment via state channels. This allows for low-fee, instantaneous payments. This benefits the Payment Processor as well as the users.

BENEFICIARIES

Standard best practice security measures will be implemented, which includes the addition of beneficiaries. This will allow Curve Wallet users to add, remove, and manage beneficiaries. A beneficiary will need to be added before payment can occur. Beneficiaries will also have a privatized trust score. For example, an account that has not received any transactions would have an uninitialized (or low) score, and a warning will be provided to the user making the transfer.

This also allows for blacklisting certain accounts. If an account is confirmed for fraudulent activity, that account will be blacklisted and will not be allowed to make transfers via the Curve ecosystem.

Extra safety and security measures such as these are implemented from an application layer to ensure the safety of the user's funds.

TRANSFER LIMITS

Users can set daily, weekly, and monthly transfer limits per currency. These limits will be hard-enforced unless a user actively changes them.

DETAILED REPORTING

Managing cryptocurrency assets across multiple exchanges, platforms, and blockchains becomes a complex administrative endeavor. To facilitate easier usage, full reporting dashboards and statements

will be provided for ease of use and management.

The Curve Wallet will record a user's transaction history, including pricing information for buys and sells. Users will be able to create an electronic transaction form at the end of the year for tax purposes.

MOBILE OTP & BIOMETRIC AUTHORIZATION

With the release of our mobile app, we will enforce OTP and in-app validation of transfers. While we will allow for 2FA, it can be a cumbersome process on mobile due to the need to switch applications. Instead, this will push an authorization request to the user, and the transfer will be completed only if it is approved.

This will be further extended to biometrics (fingerprint, and facial recognition) where supported.

NUKE BUTTON

The Nuke feature allows users to liquidate any percentage of their portfolio into Ethereum, Bitcoin, or a stablecoin with the click of a button. This will save critical time during periods (such as sharp market corrections) when users want to consolidate their holdings into currencies like Ethereum and Bitcoin.

Users will be able to 'Take a Snapshot' of their portfolio prior to 'Nuking' to recover previous positions with proportional accuracy.

ICO HOSTING

+ Investors will have access to new ICOs launching directly through the Curve Wallet
+ CryptoCurve will ensure that a project's KYC/AML methods meet regulatory requirements

ICOs that are hosted directly on the Curve Wallet will gain an immediate user base, organizational tools to organize funding, and trustworthy, audited smart contracts.

KNOW YOUR CUSTOMER / ANTI-MONEY LAUNDERING (KYC/AML)

CryptoCurve partners with third party compliance and KYC companies, enabling users to register for KYC/AML once, save that KYC/AML information to their account, and then use that information to register for future ICOs. The investor need only complete this process once on the platform.

USE ANY SUPPORTED CRYPTOCURRENCY TO INVEST

Currently, investors must trade for Ethereum or Bitcoin to invest in ICOs. On the Curve Wallet, users will be able to use any supported cryptocurrency to participate in ICOs.

CurveSDK

As an ecosystem, Ethereum has wide adoption. The goal of Ethereum has always been to develop for developers. For that reason, a lot of time, effort, and energy is spent around the Ethereum ecosystem. The Ethereum ecosystem can be split up into the following components: developer tools, convenience tools, infrastructure tools, distributed storage tools, and data convenience tools.

DEVELOPER TOOLS

- Web3.js
- Node IPC & RPC
- Third Party APIs
    - Etherscan.io
    - Ethplorer.io
- Documentation sources
    - https://web3js.readthedocs.io/en/1.0/
    - https://github.com/ethereum/wiki/wiki
    - https://etherscan.io/apis
- Puppeth
- Open Source
- Infura
- Truffle

CONVENIENCE TOOLS

- Mist
- Metamask
- MyEtherWallet
- MyCrypto
- Etherscan
- Ethplorer
- Block Explorers
- Token Explorers

INFRASTRUCTURE TOOLS

- Øx
- Kyber Network
- OmiseGO
- Bancor
- Raiden Network

DISTRIBUTOR STORAGE TOOLS

+ IPFS
+ Swarm

DATA CONVENIENCE TOOLS

+ Bluzelle
+ Fluence.ai
+ PepperDB

These tools allow for developers to be able to prototype, develop, and build products at a rapid pace. These tools are also evolving. Block explorers are turning into full-service third party APIs and being changed from pull request protocols to streaming request protocols. Developer, and specifically dApp adoption can only happen when these tools are in place, abstracted, well documented, and easy to use.

Furthermore, it is difficult to consolidate all of these sources and each one needs to be interrogated separately. Standards also deviate vastly between projects, as each is maintained by their own parties.

CryptoCurve's solution is to build an all-inclusive, documented, and standardized infrastructure ecosystem. This will allow us to foster developer adoption, allow a single hub of information, and allow us to foster standards between systems to integrate easily.

This infrastructure is still in its infancy and will evolve to include payment solutions, content distribution, and off-chain storage with on-chain proofs.

CryptoCurve's mission is to create solutions that allow product compatibility, ease of use, and integration across different technologies and systems among these services. This is similar to the convenience of AWS, Google Cloud, or Azure, where the underlying infrastructure is obfuscated from the developer who can simply focus on their end product.

If the developer wishes to build a dApp, they can pick from the storage and integration options, while leveraging specific components they would like to use.

The infrastructure as a whole is being built to include, but is not limited to:

- Consolidated API development resources
- Hosted load-balanced node solutions for all ecosystems that CryptoCurve will support
- Metamask, MyEtherWallet & MyCrypto support for all ecosystems
- Block Explorers, Token Explorers and consolidated APIs
- Ease of use enhancements and abstraction for infrastructure projects
    - IPFS
    - Swarm
    - NeoFS
    - Bluzelle
    - Fluence
    - PepperDB
- Ease of use enhancements and abstractions for protocol projects
    - Øx
    - Bancor
    - Raiden
- Smart Contract deployment tools
- Tutorials on
    - dApp development
    - Best Practices
    - Blockchain Integration
    - Setting up and hosting Nodes

As more niche blockchain solutions come to the foreground, we want these solutions to focus on their core value proposition, while CryptoCurve takes care of the infrastructure and the ecosystem.

By leveraging and allowing this, CryptoCurve will provide adoption from the developer community, furthering adoption from end users.

DEVELOPER ADOPTION

In our current blockchain iteration, user functions include:

- Exchange buy/sell
- ICO investing
- Pool funds
- Masternodes
- Portfolio tracking
- Transfer value
- Key management

In our current blockchain iteration, developer functions include:

+ dApp Development
+ Smart Contracts
+ ICOs

Seasoned developers and users need to leverage a variety of third party services in order to accomplish these specific functions. For Ethereum alone, they need to use:

+ Etherscan
+ Ethplorer
+ MyEtherWallet
+ Trezor
+ Ledger
+ Exchanges
+ Prima Block

Developers need domain-specific knowledge on all the current blockchain solutions, need to understand the underlying architecture, and they need to be able to boot up and host their own nodes. Additionally, developers have to rely on disconnected third-party services that do not have standards or policies. This all prohibits effective application development, which is critical for developers to incentivize a user base for their applications.

A FULLY-FUNCTIONAL BLOCKCHAIN ECOSYSTEM

+ Fault-tolerant nodes
+ Online accessible public APIs
+ Block explorers
+ Online wallets
+ Offline wallet
+ Hardware wallets
+ Available on exchanges
+ Allows for pooling
+ Allows for standard transfer of value functionality

Currently, the main blockchain value-add is the transfer of value. Future blockchain business will exist because of what they are offering on top of this transfer of value. Companies like Amazon exist not because you can pay them in fiat, but rather, users are willing to pay for the services they offer. Therefore, a set of standards and protocols need to be defined in order to interact with this transfer of value.

First, let's discuss the basic interaction of a state-driven blockchain.

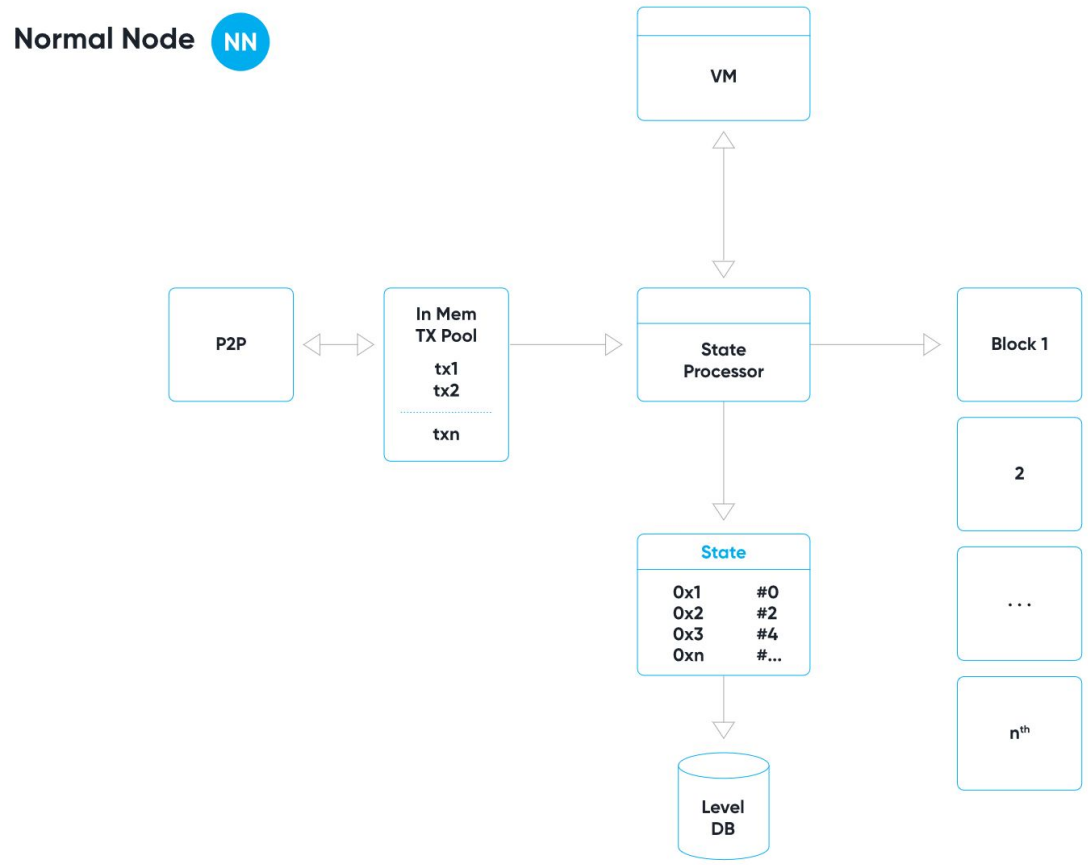


Fig. 1

Nodes communicate with one another via Peer-to-Peer (P2P) propagation. P2P propagation takes time to slowly propagate through each network's starting and entry point, slowly creeping across the entire network. This is especially true for blocks.

A Normal Node (NN) receives transactions via P2P and stores these locally in memory (and disk) within a transaction pool. A state processor sorts transactions and validates them via the Virtual Machine (VM). If the outcome is successful, their net result is applied to the state in memory (and disk). From here a block has been created, and consensus occurs. Consensus is domain specific and not important for the purposes of this explanation. Post state transition and consensus blocks are again propagated via P2P.

This is the structure of a NN. As a user, you do not need to understand this layer, and as a developer you interact with this via the CLI (Command Line Interface), RPC (Remote Procedure Call), or IPC (Inter-process communication).

At this point, what issues have we identified?

+ P2P propagation is a slow and time consuming process.
+ Developers need domain specific and direct awareness to interact.
+ Developers need to host nodes locally.
+ Nodes are designed for state processing and not API interaction. While it is capable of doing this, it does not allow for memory caching, distribution, and other API processes we have come to take for granted.

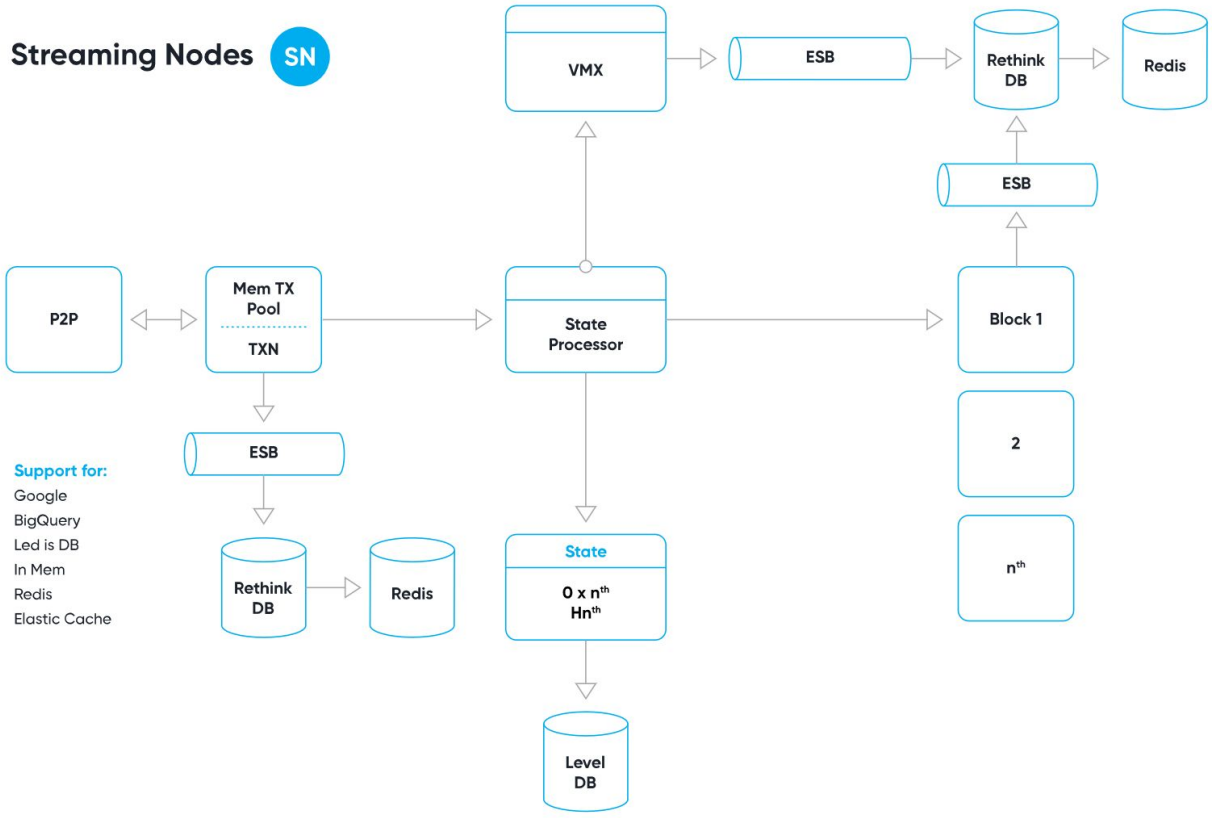


Fig. 2

The Streaming Node (SN) is a Node where the underlying process has been modified with API streaming in mind. Two services are particularly good at this, Redis (in-memory value key storage engine) and RethinkDB (subscriber-based streaming database).

Both have also been chosen for their schemaless storage capability. Another concern is that each blockchain implementation has domain-specific change or modifications to the transaction payload.

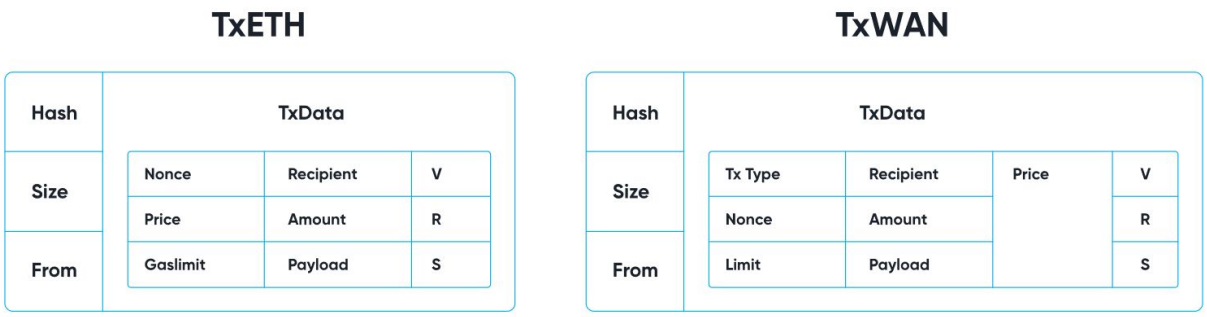


Fig. 3
An Ethereum transaction versus a Wanchain transaction.

The Transaction Type (to indicate a normal transaction or a private transaction) has been added to Wanchain but is not present in Ethereum. A generalized solution was required without schema enforcement to allow for multiple node object mapping.

The core of the SN node has been left mostly untouched. However, at any data change touchpoint, this data is sent to the ESB.

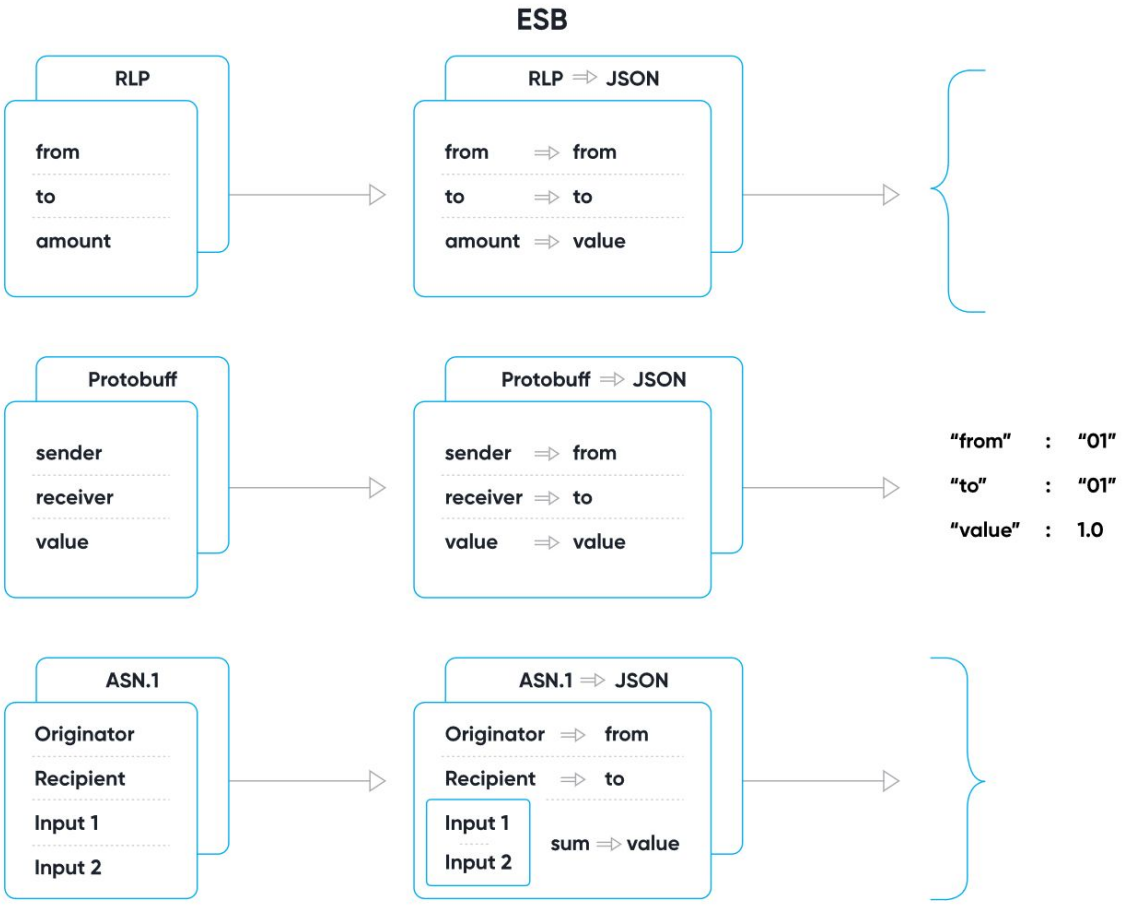


Fig. 4

The ESB is responsible for decoding and mapping of domain-specific values. This aligns inputs in different formats and with different naming standards into a single, agreed-upon standard and structure. This allows for data consumption from different systems to all be available in the same format.

Memory and disk cache support has been added for Google BigQuery, Ledis DB, Redis & ElasticCache, Rethink, and RDS postgres and Dynamo support to follow soon.

A single node however is not fault tolerant. To allow for fault tolerance, scalability and availability, we have designed the following infrastructure.

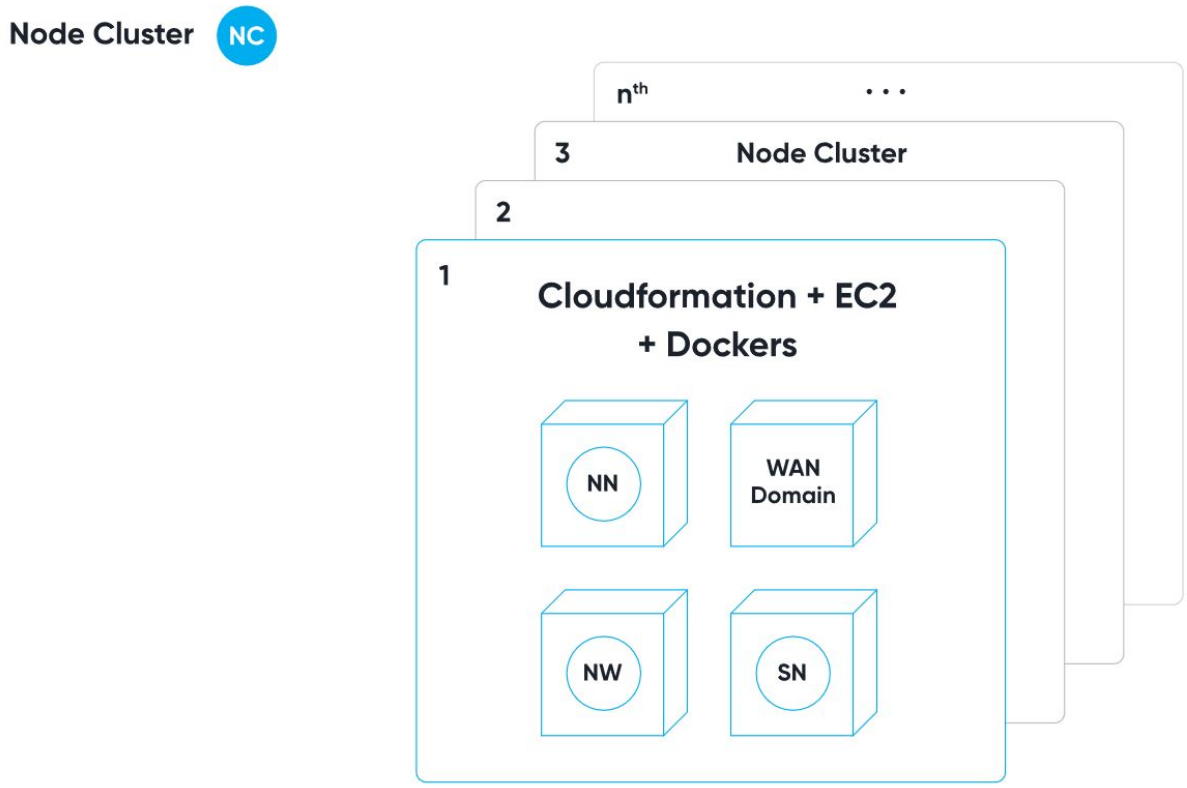


Fig. 5

Cloudformation scripts and docker builds have been developed to allow for multi-cluster deployments of domain-specific nodes. This allows for fast, scalable, and secure deployment of multi-region SNs and NNs. Cloudformation scripts and Docker builds will be open sources to allow others to deploy the same infrastructure.

With the above in mind, consider the following infrastructure:

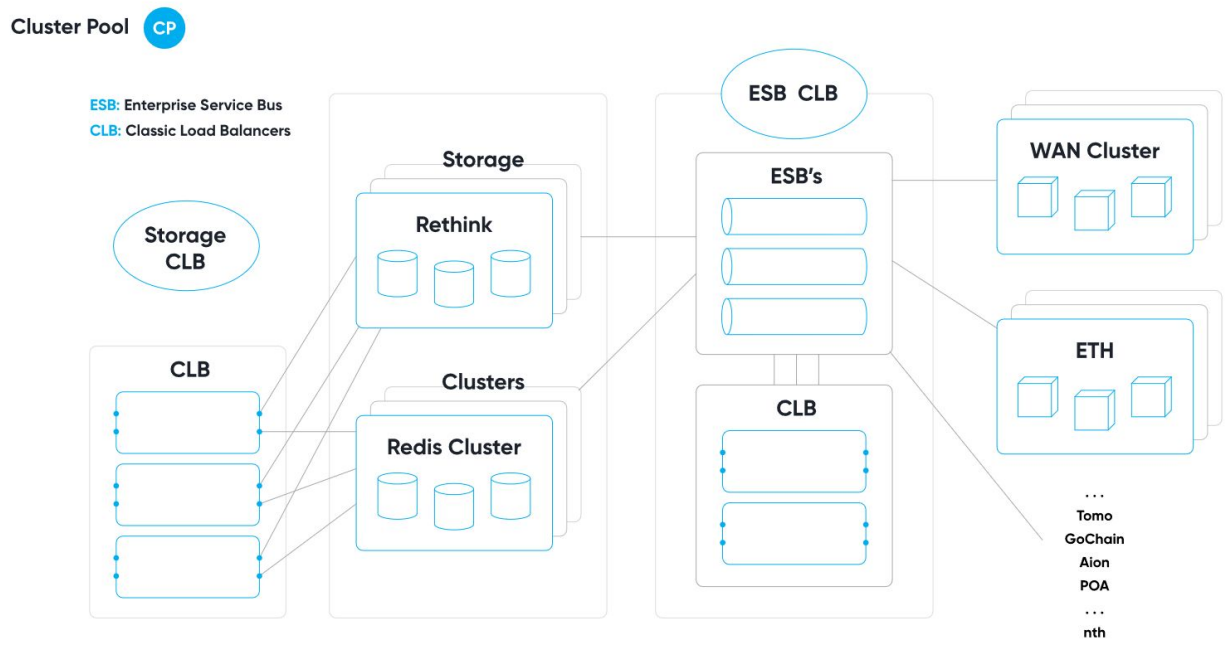


Fig. 6

The above is the Cluster Pool (CP). The CP is comprised of domain-specific clusters as described above. Current support has been built in for Wanchain, Ethereum, TomoChain, PoA, and Aion with support to follow soon for GoChain and Fusion.

All communication originates at the Classic Load Balancers (CLB). These interact with the ESB CLB (EC) where, for read data, it directs traffic to the Storage Clusters (SC) comprised out of load-balanced, autoscaling, multi-region Rethink, and Redis storage. For stateful data, the EC delegates to the relevant Node Cluster (NC).

Doing the above allows for a generic standard of interaction to any supported Node. This allows integrators and developers to have fast, fault tolerant, reliable and standardized interaction. Developers (ourselves included) can focus on their value proposition and not the underlying domain-specific infrastructure (except where a specific service is to be leveraged, for example private transactions in Wanchain).

In front of the EC, we still want to offer additional value adds; this includes tools that developers are used to, as well as further security and accessibility. With this in mind we add the following infrastructure in front:

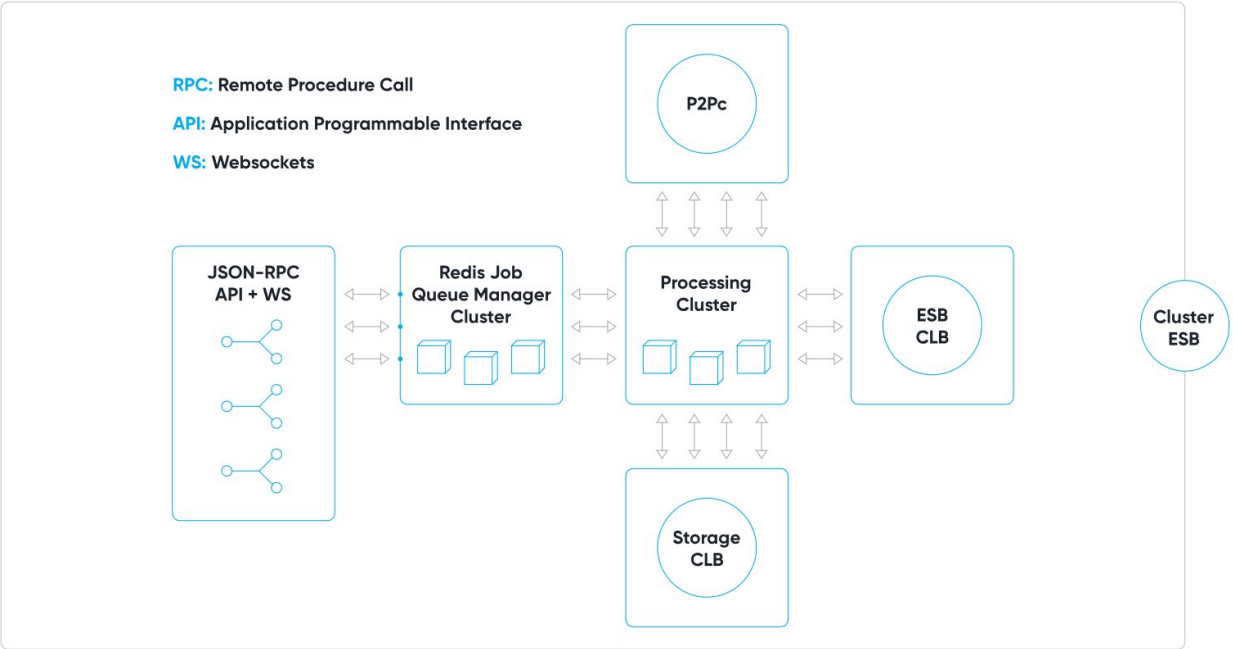
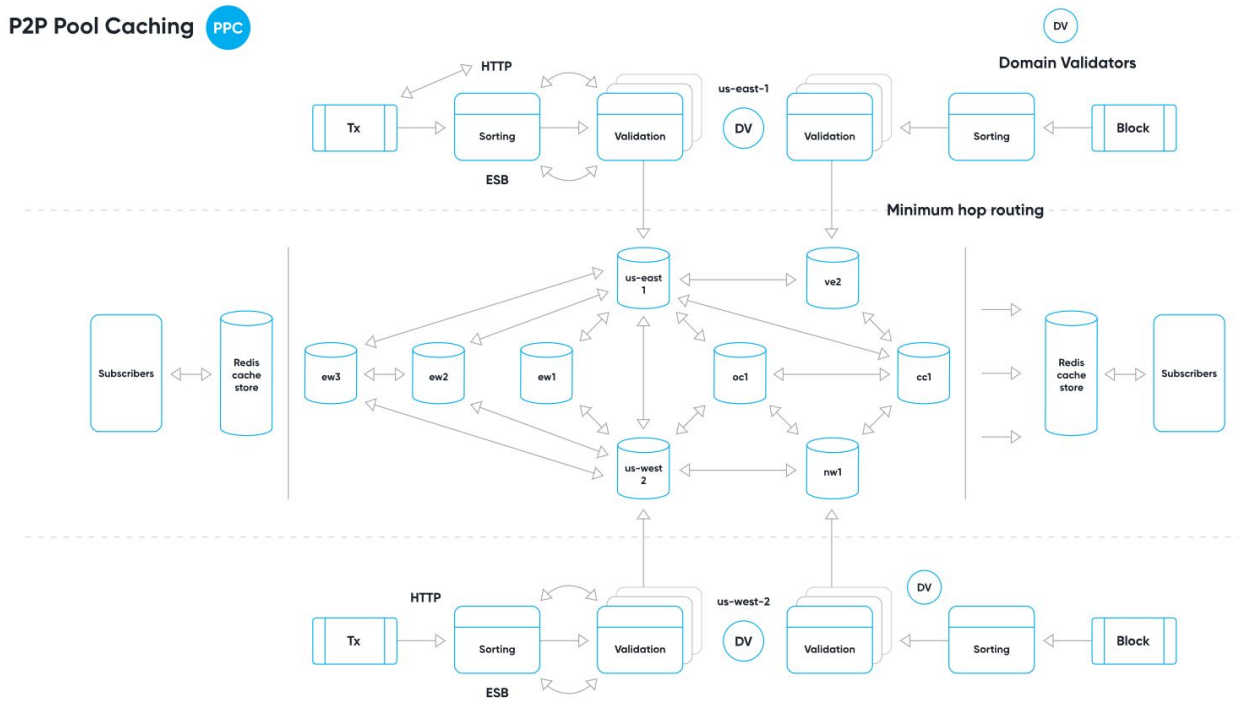


Fig. 7

HTTPS APIs, standardized and documented JSON RPC calls, as well as WebSocket (WS) interfaces are made available. All requests are load balanced, validated, and stored in a Redis-based job manager queue cluster. Job executors running in the Processing Cluster (PC) will monitor the queue and initiate events based on incoming requests. They will then either delegate to the Storage CLB, EC, or P2PC

.



Flg. 8

This brings us to the P2P pool caching engine (PPC). Both transaction and block propagation are slow processes. For this purpose, we have designed the P2PC. Transactions are received via the CP, a sorting engine does an indexed lookup on the recipient domain, when confirmed these are sent to the Domain Validators (DV) to confirm domain-specific validation on the transaction. There are P2PC endpoints in all the primary regions, specifically;

+ us-east-1 (ue1)
+ us-east-2 (ue2)
+ us-west-1 (uw1)
+ us-west-2 (uw2)
+ eu-west-1 (ew1)
+ eu-west-2 (ew2)
+ eu-west-3 (ew3)
+ ca-central-1 (cc1)
+ eu-central-1 (ec1)

Each environment is set to use minimum hop routing (shortest route routing) to propagate to all other edge locations as fast as possible with transactions and blocks. These are stored in memory-optimized Redis stores that allow subscribers of these stores to quickly consume

transactions and blocks without having to wait for P2P propagation to occur in the underlying system. This subscription service will allow nodes to quickly and efficiently consume blocks and transactions, instead of having to spend time on P2P propagation.

All the above allows for a generalized, documented, scalable, high availability, high throughput, multi-blockchain environment. This will allow developers to have a single source of truth for all interactions, as well as allow nodes to faster consume and thus process transactions. Read-only data is made available in an asynchronous and push-based fashion to allow consumers to quickly be notified of data changes. Stateful data is propagated faster and to high-availability nodes while abstracting the underlying infrastructure to developers.

This allows us to quickly and efficiently add new domain-specific blockchains, while the interaction from a developer or user perspective remains the same.

So, let's consider a standard transaction flow.

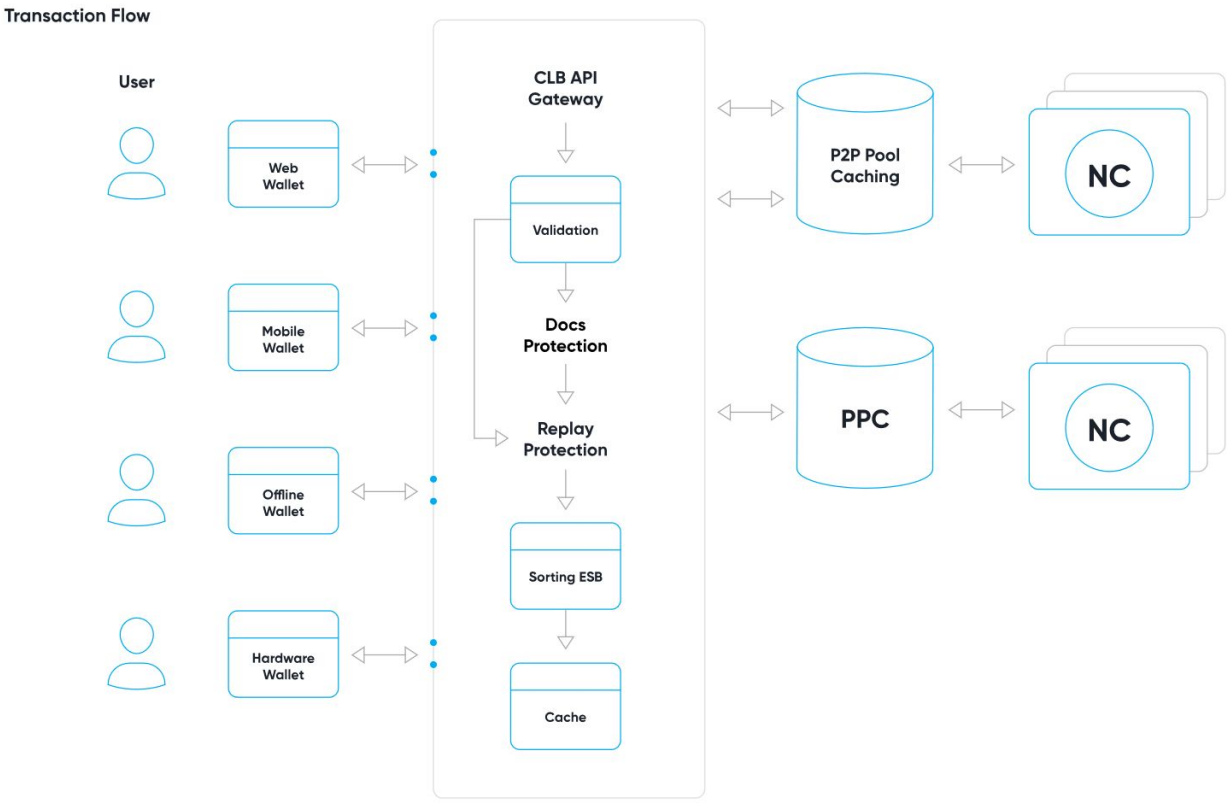


Fig. 9

A user initiates a transaction event via a web wallet, mobile wallet, offline wallet, or hardware wallet. The transaction (for multiple systems) is sent to the same CLB API Gateway (CAG). Built-in DDOS protection is provided, followed by an index-based lookup for replay protection, sorting, followed by domain validation. At this point a transaction is deterministically hashed and cached (for replay protection and validation) and transmitted to the CE which sends it to the P2PC, as soon as available via the P2PC Node Clusters (NCs) can subscribe to events and have immediate awareness.

This assumes an already signed transaction. Let's look at the CryptoCurve solution:

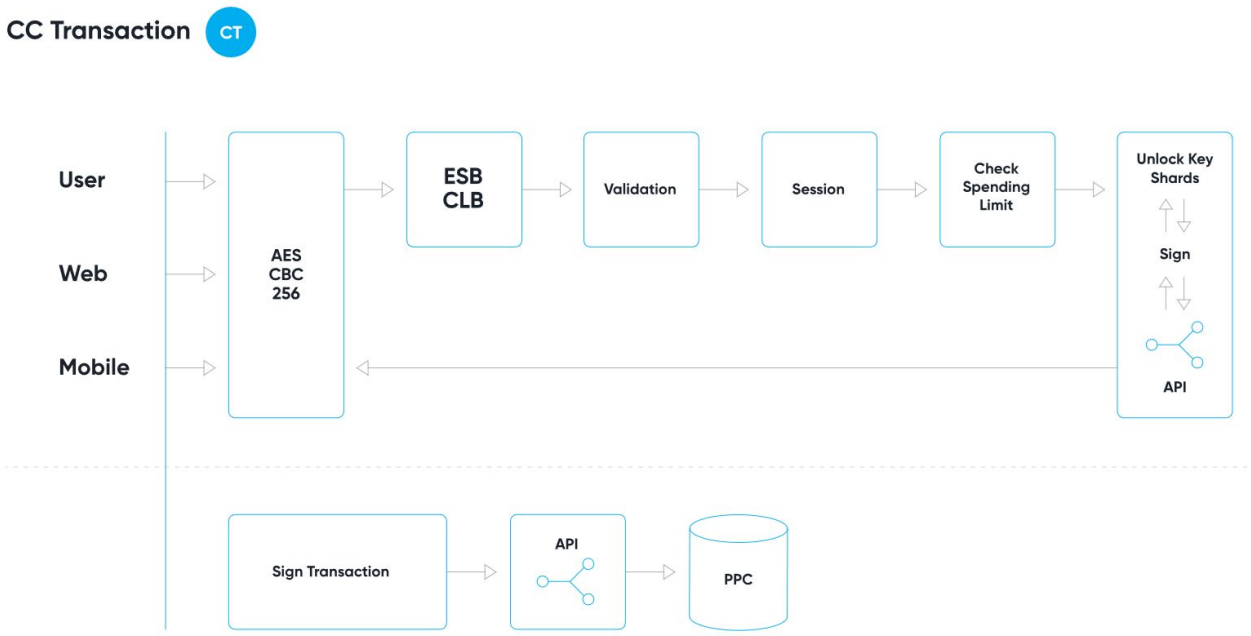


Fig. 10

Signed transactions are simply sent to the CAG and transmitted to the P2PC. Where CryptoCurve is facilitating the user, their data is first AES-CBC-256 encrypted (this includes time-stamped signatures, as well as mnemonic seeded one-off seed keys and is transmitted over TLS). This allows for end-to-end encryption. The event is received at the EC, where the work is delegated to the PC. The PC will validate the basic structure, followed by session validation, after this domain-specific validation occurs (such as confirming maximum spend limits and if a user is exceeding their limits, or if a "from" party is an approved beneficiary to send to). If confirmed, the multi-sharded and replicated key stores are requested from the distributed key vaults, signing occurs in memory (and immediately removes the key from memory) and a normal signed transaction follows.

From a transaction point of view, this allows the user to have additional security while not needing to know about the underlying abstraction of private keys or signatures, while also adding additional functionality such as spending limits and beneficiaries.

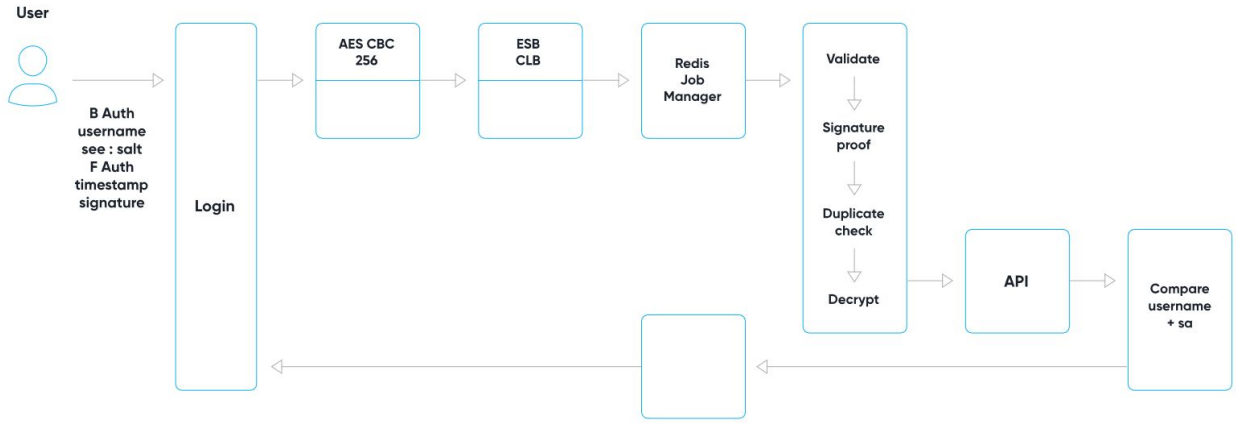


Fig. 11

Login as another example. A payload is constructed with Basic Authentication (to be allowed to talk to the API), cross-origin controlled (only specific origins are allowed to interact with the API), function authentication (even if you are allowed to talk to the API you have to prove you are allowed to talk to the function), with username and a mnemonic seeded SALT password. Off of this, a timestamp and signature are created to prevent tampering or replay attacks. The payload is AES-CBC-256 mnemonic seed encrypted and sent to the EC for the Redis Job manager running in the PC. Validation, signature proofs, index duplication lookup, and decryption occurs after interaction is allowed with the DMZ API which will compare the username and SALT to what is currently stored in the encrypted data store. The data itself (for example username) is encrypted with the users SALT and a user specific random seed, once these two values have been compared then authentication is approved.

So, what does the data flow look like?

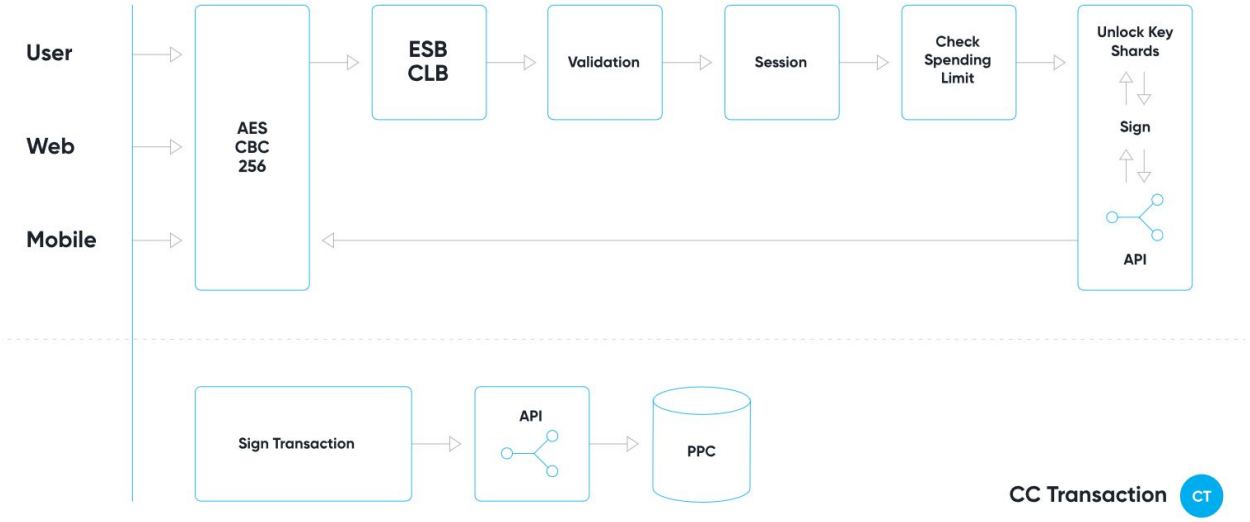


Fig. 12

We can split this into stateful (a change should occur) and stateless (read-only data). Static data is served via the CCHW (explained next). A request is made to the API CLB which goes through the standard process of Redis Queue and Docker Job manager. This delegates to the relevant role-specific microservice, which can then interact with the data store. Role specific is defined on a data store schema level. So, for example, Login will have a Login IAM user and a Login RDS user which only has write access to the Login service and Login schema.

The data store is a multi-AZ (across multiple regions), read replica, key-encrypted, RDS data store. Stateless data is only allowed to interact with the read replica and does not have any access to the stateful systems.

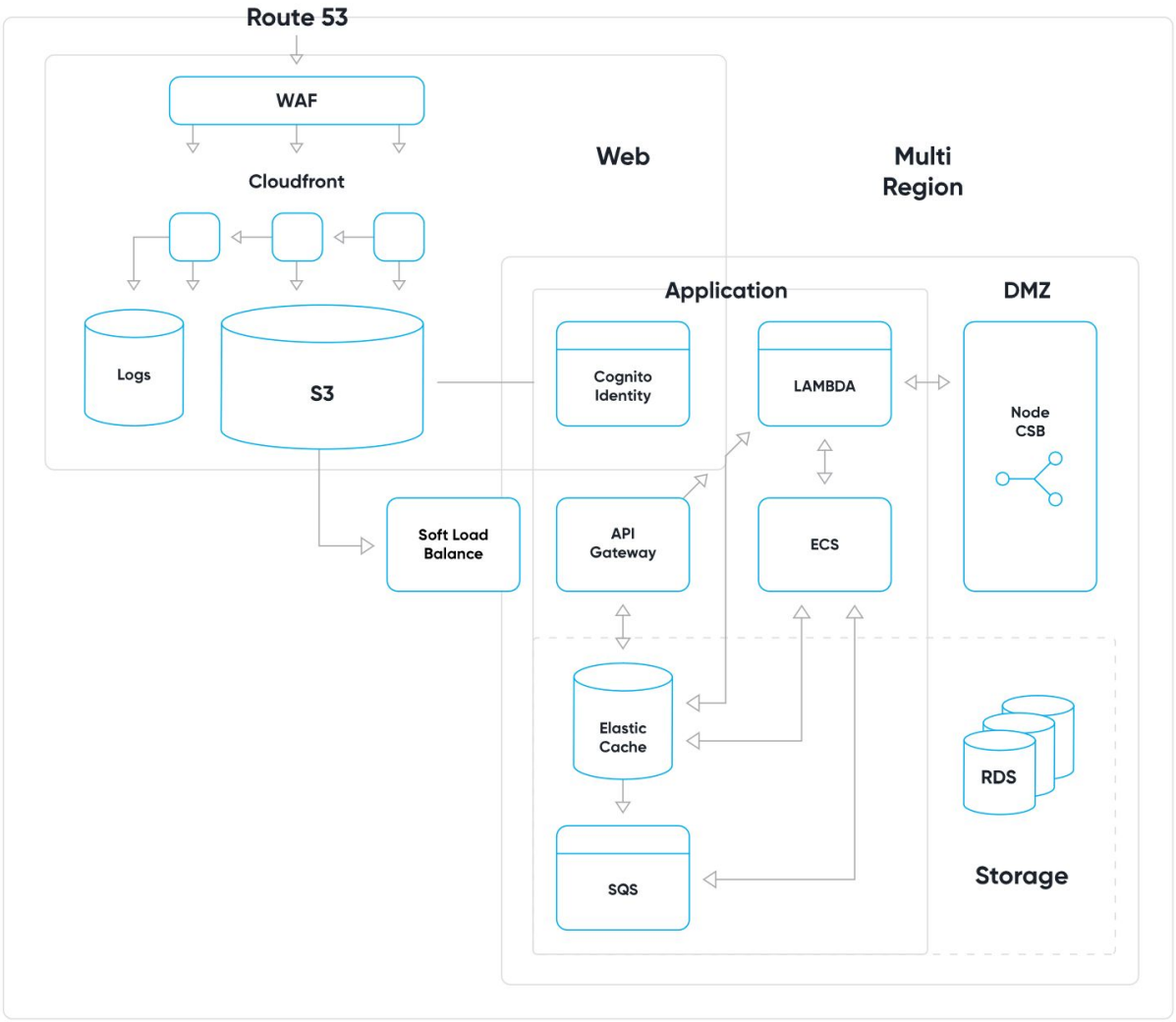


Fig. 13

The CCHW (CryptoCurve Hosting Web) is a subset of the Auto Web Architecture (AWA). The CCHW starts at Domain Name System (DNS) lookup via Route 53. This request is then delegated to Cloudfront (Load balanced and stored across 116 locations across regions) with requests validated via Web Application Firewall (WAF). Cloudfront stores logs in S3 and hosts static data from S3. This allows for interaction with the static data provided by CryptoCurve (Web wallet, Offline Wallet, Block explorer, API documentation, Wiki).

User access and management is handled via IAM and Cognito identify. The S3 solution interacts with Software Load Balancers (SLB) that spread communication across multi-zone API Gateways. Requests are saved in Elastic Cache and SQS for job specific processing. These are then executed via

Lambda for synchronous events or via ECS managed Job services. These services will then either interact with the Node ESB, or with the Storage Clusters depending on requirement. This solution is the Auto Web Architecture.

With the knowledge of all of these components, we can look at the high-level architecture:

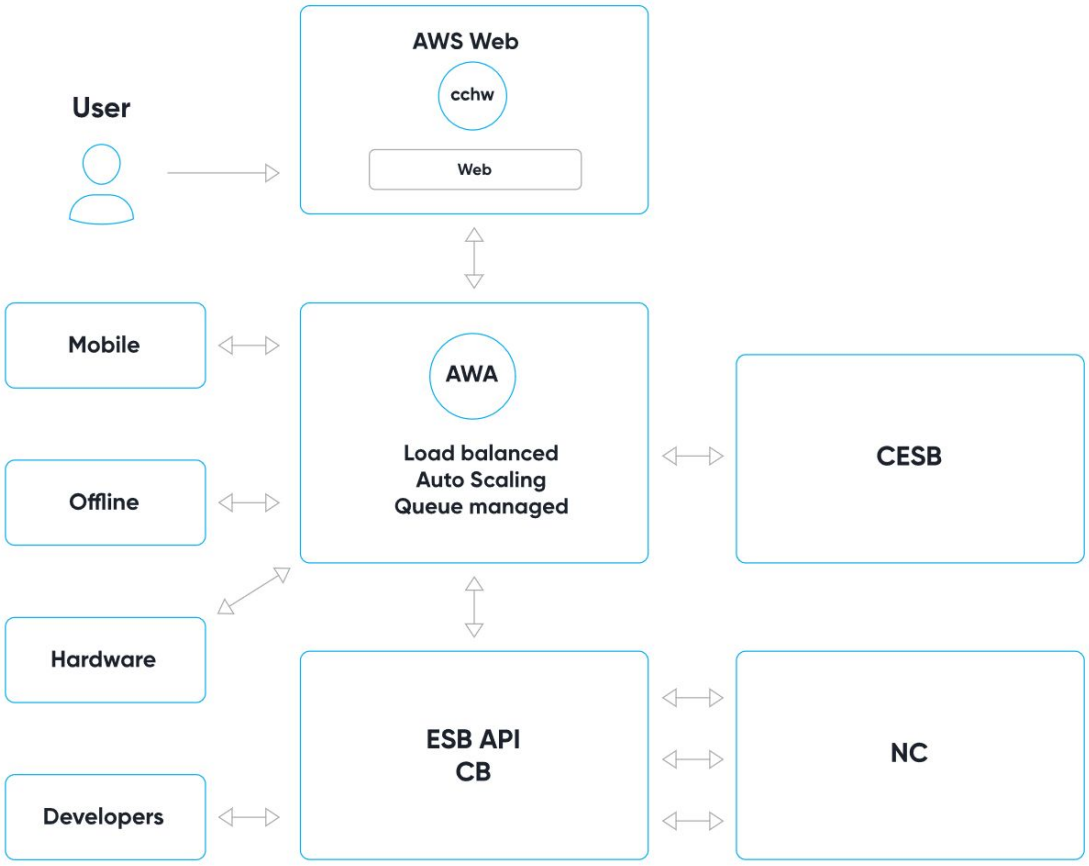


Fig. 14

Users interact via the CryptoCurve mobile app, website, or directly via their offline wallet, hardware wallet, or via third-party developers that integrate with CryptoCurve services.

The CryptoCurve webapp is provided via the CCHW which interacts as part of the AWA. From here, events will either be sent to the CP or CE dependent upon requirement.

This design architecture allows for:

+ Scalability
+ Availability
+ High throughput
+ Security
+ Standardized interaction with Nodes
+ No need for Node-specific domain knowledge
+ Easily integrating third-party services into the CE
+ Integrating services such as Kyber, Øx, Bancor, or other third-party exchanges easily without needing to change the underlying architecture
+ Allow for addition of domain-specific blockchains
+ Allows a well-documented standard set of protocols for developer interaction
+ As we integrate new services for our own products they become available for the generalized developer community via the standard set of APIs and protocols

This architectural abstraction further allows for the addition of CryptoCurve modules, these are domain-specific infrastructure modules that can be added as plug and play modules with the EC.

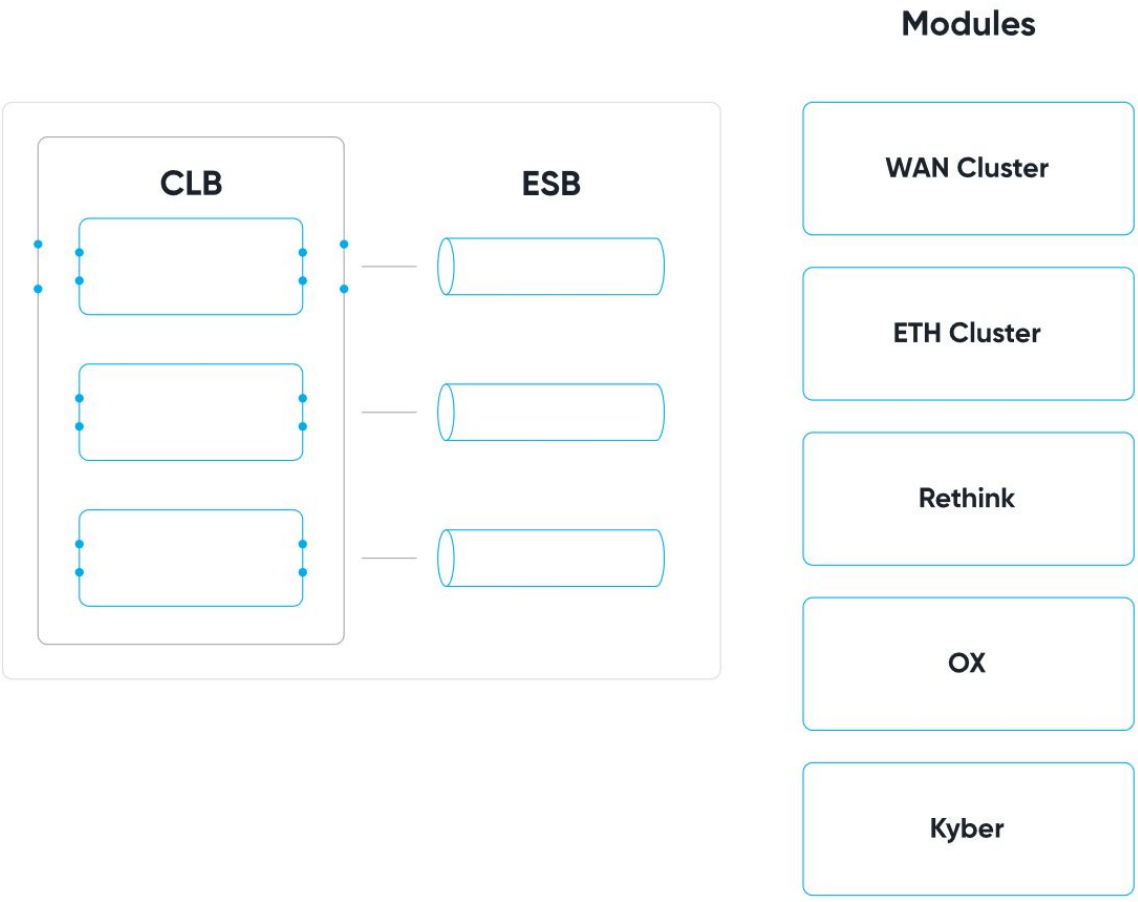


Fig. 15

The EC handles the abstraction, scalability, security, and availability, while domain-specific integrations only need to focus on their domain knowledge. This allows us to build in Øx, Kyber, or other exchanges by plugging them in as modules into the existing infrastructure.

The overall architecture allows for generalized and standardized interaction to all of these modules, so that dApp developers can focus on their value proposition and less on domain knowledge.

As we expand these modules we will be adding in protocols such as:

+ IPFS
+ Swarm
+ Bluzelle
+ PepperDB

This can also be expanded to current dApp solutions, such as:

+ DAO
+ Origin
+ NuCypher
+ Phantasma

Or dApps we don't even know about yet.

The end result will be a plug and play standardized API that will allow developers to pick and choose with regards to their interaction. You simply decide that you want to transact on Wanchain, while storing data in Bluzelle, and securing data with NuCypher.

Surely that's a problem though? Wanchain needs WAN, Bluzelle needs BLZ, and NuCypher needs NKMS? Well, remember, we have exchange modules as well, creating a few sub expenses, we will convert them for you on the fly to feed all your services--via the CURV token.

MARKETING PLAN

Since April 2018, along with our partners, including Wanchain, we have been actively engaged in a marketing campaign to attract investors. Using a strong network of influencers including the networks brought to us through our investors and advisors, we have gained significant awareness and interest from cryptocurrency investors.

Looking forward, our marketing efforts will grow and evolve significantly as we (1) roll out new marketing priorities targeting user adoption and brand promotion, (2) engage with new market segments, (3) activate new digital and traditional media channels, and (4) further invest in marketing team members, partnerships, and technologies.

MARKETING PRIORITIES

CryptoCurve's marketing programs will shift to focus on three core areas that will complement each other to maximize reach and effectiveness in support of CryptoCurve's mission and revenue goals.

USER ADOPTION

User adoption is a top priority for accelerating CryptoCurve's revenue generation and maximizing profitability. Programs focused on user adoption will focus on the features and advantages of CryptoCurve products and platforms. Goals are to reach, engage, and retain users with our software and achieve user adoption rates from the first year that will be used as a benchmark for goal-setting for subsequent years.

BRAND PROMOTION

Distinct from direct promotion of CryptoCurve platforms and products, separate programs will influence, organize, and mobilize current evangelists and non-users to interact with all digital assets seamlessly, lowering all barriers of entry to blockchain, inspiring/growing blockchain enthusiasts in target populations and in priority countries. These programs are a crucial secondary vehicle for achieving brand impact. Goals are to drive CryptoCurve's brand and awareness to influence knowledge, attitudes, beliefs, and behaviors around blockchain among the target population; increase CryptoCurve's brand and mission relevance within culture; and monetize the CryptoCurve brand to generate revenue for CryptoCurve.

POLICY INFLUENCE

Marketing programs targeted directly at government policymakers and regulators will be essential to paving the way for continued mass adoption. Continued user adoption and brand promotion will be critical to success in the policy sphere, but these programs will also drive and draw from independent

research initiatives aimed at demonstrating the positive social and economic impacts of blockchain technology. Goals are to build awareness of the CryptoCurve brand and of blockchain and cryptocurrency technology more broadly among policy decision makers to result in a positive regulatory environment for the continued growth of CryptoCurve's ecosystem.

MARKET SEGMENTS

Thoughtful market segmentation is the engine that powers CryptoCurve's marketing strategy. By tailoring marketing programs and content to the unique experiences of each segment, we will drive awareness and adoption of all of the products and platforms in CryptoCurve's ecosystem. The key initial areas of segmentation are by audience, geography, and blockchain experience.

AUDIENCE

Three core audiences make up the core of CryptoCurve's strategy, Investors, Developers, and Emerging Companies. Tailored marketing campaigns will be developed to attract and engage each segment, particularly in the realm of user adoption and brand promotion. The Investor segment will be the primary focus in the short term, but targeted programs for the Developer and Emerging Companies segments will follow soon thereafter.

+ **Investors:** As CryptoCurve's core market, most of our marketing programs will be primarily geared toward Investor engagement and adoption of CryptoCurve's products and platforms. Programs have and will include attending global conferences and exhibitions, maintaining active online communities, engaging with key influencers, publishing valuable content through owned and affiliate blogs and social media, and investing in strategic sponsorships and advertising campaigns.

+ **Developers:** Targeting Developers through the endowment of a comprehensive set of developer tools provides both a strong addition to our revenue model as well as a valuable addition to our community of users. Initial programs targeting the Developer segment will center around a "reach-out" program for developers that will feature a schedule of online and offline community engagements including incentivized (reward) development campaigns for individuals and groups, bug fixing bounties, and a series of hack-a-thons to take place in key locations around the world.

+ **Emerging Companies:** Growth of CryptoCurve's Investor and Developer user base will make our ecosystem a valuable destination for both projects preparing for their ICOs and blockchain companies that have already moved past the ICO stage. While the CryptoCurve Accelerator helps companies mature from ideation to execution, marketing also focuses on business-to-business campaigns including online and offline broad channel and direct marketing.

GEOGRAPHY

Blockchain and cryptocurrency investor and user markets are intrinsically global, but effective marketing strategies must incorporate elements of the regional and local. For this reason, our marketing programs will focus on tailoring messages to markets around the globe. Particular care must be given as select countries may be less receptive to cryptocurrencies and blockchain technology. Initial programs will include targeting of audiences in East and South East Asia.

BLOCKCHAIN EXPERIENCE

CryptoCurve's initial investors, advisors, and current target audiences are predominantly drawn from the ranks of blockchain and cryptocurrency evangelists. But to achieve our mission of mass-adoption of blockchain technology, we will develop marketing programs specifically targeting investors and users from outside the blockchain sphere-of-influence.

CHANNEL STRATEGY

Numerous digital and traditional media channels will be activated to ensure that CryptoCurve's marketing programs maximize their reach and effectiveness. Whenever possible, programs will be coordinated to develop valuable cross-channel and omni-channel experiences for our audiences.

+ Digital Communities
+ Influencer / Affiliate marketing
+ Event/conference marketing
+ Content marketing
+ Email marketing
+ Sponsorships / Partnerships
+ Traditional media
+ Social media

MARKETING RESOURCES

The majority of the marketing strategy will be designed and executed by CryptoCurve's experienced core marketing team and network of advisors. Strategic partnerships with other cryptocurrency organizations, affiliates, agencies and vendors will increase our ability to quickly bring our programs to scale. Lastly, all marketing programs will be made more effective and efficient through utilization of a full marketing technology ecosystem. Early technology investments will include: a Customer Relationship Management (CRM) database, email marketing platform, social media management platform, marketing automation platform.

THE CURV TOKEN

TOKEN METRICS

- Name: Curve Token
- Symbol: CURV
- Website: https://cryptocurve.io
- Social Media:
    - @cryptocurve on Telegram / Facebook
    - @crypto_curve on Twitter / Instagram
- Token Type: WRC-20
- Private Sale Hardcap: 37,000 ETH
- Public Sale Hardcap: $6m
- Max Supply: 415 million CURV
- Circulating Supply : 207.5 million CURV
- Private Sale Token Rate: 4,175 CURV per ETH
- Public Sale Token Rate: 1 CURV = $0.20
- Contribution Method: Private Sale (ETH) & Public Sale (WAN)
- Token Distribution:
    - 50% Token Sale
    - 35% CryptoCurve Foundation
    - 15% Team & Advisors (Team tokens are locked for 2 years)

TOKEN UTILITY

The CURV token is the fuel for the CryptoCurve ecosystem allowing: real time transfers with low fees; low fee cryptocurrency payments to payment integrators; and allowing developers to abstract the underlying infrastructure from the tools they are building.

CURV allows ease of use, abstraction, and inclusiveness. The same design principles as CryptoCurve.

Some examples of our token utilities are:

EXCHANGE INTEGRATION

The DEX integration allows CryptoCurve to exchange tokens. This seems simplistic at first, but what this allows is a multi-token abstraction layer. With an integrated exchange, a CURV token can represent any other token via token abstraction.

THE CURV TOKEN IS A REPRESENTATION FOR EVERY TOKEN AVAILABLE VIA THE EXCHANGE INTEGRATION.

STATE CHANNELS

The Curve wallet implements state channels to allow for instantaneous, millisecond finality, low fee transactions between Curve users and Curve payment providers. To enable these transactions CURV tokens will be used to pay the fees.

PLATFORM INTEGRATION (Putting It All Together)

With the multi-layer abstraction of the infrastructure layer, CryptoCurve allows developers to plug and play with different blockchain solutions. They can hand pick Wanchain for OTA transfer, Ethereum as a store of value, Bluzelle as a data store, or PepperDB as a key value store all in one solution.

This would require developers to hold tokens for each underlying system, WAN for OTA transfer and BLZ for data storage. To use the infrastructure a user has to be a Curve wallet owner. Being a Curve wallet owner allows for token abstraction. So instead of needing to own WAN and BLZ, the owner just needs to hold enough CURV tokens to pay for the fee of the underlying tokens.

This infrastructure along with the token abstractions allows the user to obfuscate the underlying infrastructure and instead enjoy a plug-and-play environment.

STAKING

Only by staking CURV tokens within the Curve Wallet will users be eligible to receive airdrops for ICOs launching on the Curve Wallet platform.

Staking rewards will be tier-based:

+ Tier 1 - top 20% of CURV holders will receive 40% of total airdrops
+ Tier 2 - mid 40% of CURV holders will receive 40% of total airdrops
+ Tier 3 - bottom 40% of CURV holders will receive 20% of total airdrops

Within these tiers, the rewards are distributed 100% proportionally within that tier. It will be required to stake CURV tokens for 1 quarter (3 month period) to be eligible for the airdrops from that quarter.

NUKE BUTTON

CURV will be required within the Curve Wallet to: activate Nuke functionality; take a portfolio snapshot pre-Nuke; and to revert a portfolio post-Nuke.

CUSTOM POOLING

Admins are required to hold 10,000 CURV tokens during the creation and execution of custom pools.

TRADING FEE DISCOUNT

Half-priced trading fees when fees are paid for with CURV.

GOVERNANCE

Decide the future of the Curve Wallet.

TEAM

CORE

+ Joshua Halferty: Chief Executive Officer (CEO)
+ Xander Yi: Chief Financial Officer (CFO)
+ Andre Cronje: Blockchain Infrastructure Engineer
+ Seán McGurk: Security
+ Benn Godenzi: Marketing & Partnerships
+ Andy Kerrison: Architecture
+ Alexander Lenart: Design
+ Paul Landingin: Enterprise Development
+ Anna Santayana: Marketing & Operations
+ Anton Nell: Scalable Web & Mobile Engineer

ADVISORS

+ Dustin Byington
+ Mark Ashelford
+ Rajesh Gopi
+ Addison Huegel
+ Moe Levin
+ Tim Bukher

BIOS

Joshua Halferty, CEO

Mr. Halferty is an expert in leading large, geographically dispersed, development teams through all phases of project delivery while successfully maintaining timeline and budgetary requirements. For the last two years, Mr. Halferty has provided leadership in product and project management positions for Hewlett Packard Enterprise. Prior to that, Mr. Halferty led multi-million-dollar software development projects for the US Navy and Marine Corp. He holds a Bachelor's degree from Virginia Tech in Industrial and Systems Engineering.

Xander Yi, CFO

As Founder and Partner at the Law Offices of Gutierrez Yi, Mr. Yi has broad legal experience and brings valuable leadership and legal, business, and financial experience to the company. Mr. Yi graduated with a Juris Doctorate from Arizona State University and served as a clerk for the Arizona Attorney General's office. He also previously launched a successful eCommerce business.

Andre Cronje, Blockchain Infrastructure Engineer

With more than 13 years of experience in core technology leadership roles, Mr. Cronje has lent his expertise to various entities as a lecturer, CTO, and Head of Technology, and Technical Team Leader. He has many years of blockchain experience, including serving as Chief Crypto Code Reviewer at CryptoBriefing and as Head of Technology at Freedom, which works to innovate technology in financial services. In these roles, Mr. Cronje has scaled and innovated financial service technologies, including neural nets, deep learning, and Big Data.

SeáN McGURK, Security

Mr. McGurk has over 37 years of experience in advanced systems operation, cyber threat intelligence and information systems security. His experience includes multiple senior-level leadership roles such as Director of the National Cybersecurity and Communications Integration Center at the Department of Homeland Security and Chief Security Officer for Web Operations at Amazon Web Services.

Benn Godenzi, Marketing & Partnerships

As an early investor in Bitcoin since 2010 and 8 years of experience in entrepreneurship, Mr. Godenzi leads marketing and partnerships for CryptoCurve. Previous experience within the cryptocurrency space includes managing marketing for Aion, STK Token, Wanchain, Edenchain, Gochain and Quarkchain, along with helping others raise awareness and funding. He focuses full time on ICO management, fundraising, networking, private investor relations and social media growth within the space. Mr. Godenzi is a co-founder of the Interoperability Alliance between AION, ICON and Wanchain, and is the founder of Outlast Nutrition.

ROADMAP

We will be keeping our community up to date with development and plans which can be followed dynamically on our website.

Q3 2017

+ Company Founded: CryptoCurve was conceptualized
+ First Product: Uncapped ETH ICO pooling

Q2 2018

+ Curve Token Sale
+ Wanchain Wallet Functionality: Basic wallet functionality on Curve main site

Q3 2018

+ Integrated KYC
+ Wanchain ICO Pooling: Allow custom pooling for Wanchain ICOs
+ Buy Into ICOs From Curve Wallet: Allow users to participate in ICOs directly from wallet
+ ICO Staking

Q4 2018

+ Decentralized Exchange Integration
+ Nuke
+ Ethereum Pooling

Q1 2019

+ Curve SDK

Q2 2019

+ Fiat Gateway

GLOSSARY

CryptoCurve
The parent company of the Curve ecosystem.

CURV
Ticker symbol for the native currency of the CryptoCurve ecosystem.

Curve Wallet
The first product produced by CryptoCurve.

Øx Protocol
An Øx relayer is any system which has implemented the standard order format and process and made those orders publicly available via a suitable communications medium (such as a web service). The Øx protocol defines a standard format for off-chain order relaying via web services or other suitable communications mediums. A consumer of the Øx protocol is able to read those orders from any number of different relayers (since they all share a common format), and then fill orders as needed.

AES
The Advanced Encryption Standard (AES), also known by its original name Rijndael, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001[(2)].

Decentralized Exchange (DEX)
A decentralized exchange is an exchange market that does not rely on a third party service to hold customers' funds. Instead, trades occur directly between users (peer to peer) through an automated process[(3)].

DMZ
In computer security, a DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN): an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled. The DMZ functions as a small, isolated network positioned between the Internet and the private network and, if its design is effective, allows the organization extra time to detect and address breaches before they penetrate internal networks. The name is derived from the term "demilitarized zone," an area between nation states in which military operation is not permitted[(4)].

ECS

An Amazon ECS container instance is an Amazon EC2 instance that is running the Amazon ECS container agent and has been registered into a cluster. When running tasks with Amazon ECS, tasks using the EC2 launch type are placed on active container instances[5].

IAM

AWS Identity and Access Management (IAM) is a web service that helps securely control access to AWS resources. IAM is used to control who is authenticated (signed in) and authorized (has permissions) to use resources[6].

JSON

JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret key (with the HMAC algorithm) or a public/private key pair using RSA[7].

KYC/AML

Know Your Customer (alternatively know your client or 'KYC') is the process of a business identifying and verifying the identity of its clients. The term is also used to refer to the bank and Anti-Money Laundering regulations that govern these activities[8].

Mobile OTP /

One-Time Password (alternatively 'OTP') is a free "strong authentication" solution for Java-capable mobile devices like phones or PDAs. The solution is based on time-synchronous one-time passwords. It consists of a client component (a J2ME MIDlet) and a server component (a Unix shell script).

Relayer

Parties building on top of the Øx platform are referred to as Relayers as they host off blockchain order books and can charge fees for their services[9].

SALT

In cryptography, a salt is random data that is used as an additional input to a one-way function that "hashes" data, a password or passphrase. Salts are closely related to the concept of nonce[10].

Taker

When an individual places an order that is immediately filled in its entirety (for example a market or stop order) that individual becomes a "taker," and pays a "taker" fee[11].

VPC

Amazon Virtual Private Cloud (Amazon VPC) lets a user provision a logically isolated section of the AWS Cloud where the user can launch AWS resources in a virtual network that is defined by the user. The user has complete control over the virtual networking environment, including selection of the user's own IP address range, creation of subnets, and configuration of route tables and network gateways. Users can use both IPv4 and IPv6 in VPC for secure and easy access to resources and applications [12].

FOOTNOTES

1
http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

2
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

3
https://steemit.com/exchange/@nyinyinaing/decentralized-exchange-vs-centralized-exchange

4
https://en.wikipedia.org/wiki/DMZ_(computing)

5
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ECS_instances.html

6
https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

7
https://jwt.io/introduction

8
https://en.wikipedia.org/wiki/Know_your_customer

9
https://blog.0xproject.com/a-beginners-guide-to-0x-81d30298a5e0

10
https://en.wikipedia.org/wiki/Salt_(cryptography)

11
https://cryptocurrencyfacts.com/maker-vs-taker-cryptocurrency

12
https://aws.amazon.com/vpc

SOURCES

https://aws.amazon.com/vpc

https://cryptocurrencyfacts.com/maker-vs-taker-cryptocurrency

https://www.cnbc.com/2017/12/04/cyberattack-temporarily-hits-bitcoin-echange-bitfinex.html

https://www.ccn.com/bitcoin-exchange-shapeshift-hacks-sees-230000-lost

https://www.wired.com/2014/03/bitcoin-exchange

http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ECS_instances.html

https://en.wikipedia.org/wiki/DMZ_(computing)

https://steemit.com/exchange/@nyinyinaing/decentralized-exchange-vs-centralized-exchange

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

https://www.investopedia.com/terms/p/proof-stake-pos.asp

https://en.wikipedia.org/wiki/Salt_(cryptography)

https://blog.0xproject.com/a-beginners-guide-to-0x-81d30298a5e0

https://en.wikipedia.org/wiki/Know_your_customer

https://jwt.io/introduction

https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

SOCIAL MEDIA

URL

+ CRYPTOCURVE.IO

Instagram / Twitter

+ @CRYPTO_CURVE

Facebook / Telegram

+ @CRYPTOCURVE

DISCLAIMER

IMPORTANT NOTICE

PLEASE READ THIS SECTION CAREFULLY. IF YOU ARE IN DOUBT AS TO THE ACTION YOU SHOULD TAKE, PLEASE CONSULT YOUR FINANCIAL, LEGAL, TAX, TECHNICAL OR OTHER PROFESSIONAL ADVISORS.

This whitepaper ("Whitepaper") gives a summary of the sale of CURV Tokens ("CURV") during the pre-sale and public sale of CURV (collectively, the "Token Generating Event") by Stichting CryptoCurve, a Dutch foundation ("CryptoCurve"). The purpose of the Token Generating Event is to raise funds for the development and commercialization of the proposed business model of the CryptoCurve Wallet ("Wallet").

As detailed in the Token Generating Event Terms and Conditions accessible at cryptocurve.network ("Terms"), CURV carry no rights other than a limited right to use and interact with the Wallet if, and to the extent that, the Wallet is successfully developed and deployed. Please read the Terms carefully and ensure that you understand the nature of your rights and obligations and the risks you are undertaking in respect of your purchase of CURV or participation in the Token Generating Event.

CURV are not intended to constitute securities in any jurisdiction. Further, this Whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction.

The Token Generating Event and distribution of CURV to each purchaser will be subject to and governed solely by the Terms. In the event of any conflict or inconsistency between the Terms and any other document, including this Whitepaper, the Terms shall prevail.

All trademarks included in this Whitepaper other than trademarks representing the "CryptoCurve" name is included for the convenience and education of the reader and fall within the "fair dealing "copyright use exception. CryptoCurve asserts no ownership of any third-party trademarks presented here.

No part of this Whitepaper is to be reproduced, distributed or disseminated without including this section titled "Important Notice".

DISCLAIMER

The information contained in this Whitepaper is of a descriptive nature for information only and is not binding. Such information has been compiled from sources believed to be reliable. Some of this information may be forward looking in nature and based on certain assumptions. All statements other than statements of historical facts included in this Whitepaper, including, without limitation, statements regarding business strategy and plans, estimates of returns or performance, and objectives for future operations, are forward looking statements. In addition, forward looking statements can generally be identified by the use of forward looking terminology such as "may", "will", "should", "expect", "anticipate", "estimate", "intend", "continue", or "believe", their respective negatives and other comparable terminology.

Unless expressly provided by CryptoCurve in writing, no information contained in or referred to in the Whitepaper shall be construed to be part of the Terms or any representation, warranty or undertaking from CryptoCurve.

None of the information set out in this Whitepaper has been reviewed or approved by any regulatory authority and the information in this Whitepaper is subject to material updating, revision, correction, completion and amendment from time to time. This Whitepaper may not be transmitted to any country where distribution or dissemination of such information may be prohibited.

ELIGIBILITY

As detailed in the Terms, you are not eligible to purchase CURV during the Token Generating Event if you do not meet the eligibility conditions set out in the Terms. For example, you will not be eligible if you are (i) a citizen, resident (tax or otherwise) or green card holder (as the case may be) of the People's Republic of China, the United States of America, or Canada; or (ii) a citizen, resident (tax or otherwise) or a person located or domiciled in any geographic area or country in which your participation in the Token Generating Event may be prohibited or restricted by the applicable laws (including, without limitation, any laws relating to anti-money laundering and combating the financing of terrorism).

It is your responsibility to inform yourself about and to observe any restrictions and laws which may apply to you in respect of any purchase, ownership, receipt or possession of CURV or participation in the Token Generating Event.