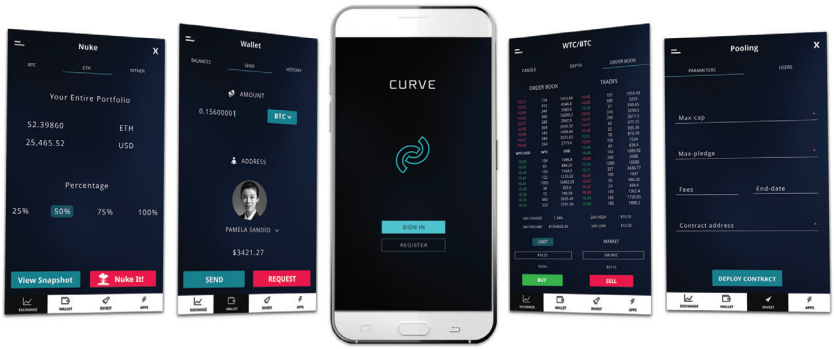
CRYPTOCURVE

THE BROWSER TO BLOCKCHAIN

PRIVATE COMMERCIAL PAPER

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.

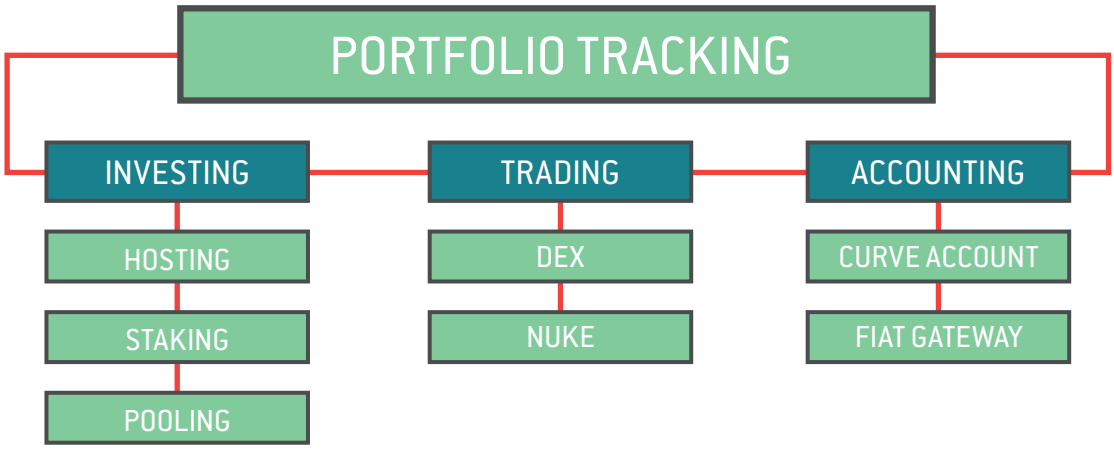
Cryptocurrency investors, whether new or experienced, face daunting barriers. To keep pace with highly volatile currencies across multiple platforms in exchanges that move far too slowly, transactions must use clumsy and non-intuitive management tools. The general public hears horror stories about massive 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 commercial paper describes Curve Wallet -- a multi-blockchain platform that provides a frictionless experience, facilitating cross-chain transactions and smart contracts in a simple and clean UI/UX. Curve Wallet simplifies and accelerates adoption for seasoned investors and the general public. 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.

Envisioned to be available via both a desktop site and a mobile application, Curve Wallet is a turnkey product for all blockchain-consumer needs.

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

OVERVIEW



Packed with features designed for real-world utility and designed by and for cryptocurrency investors, Curve Wallet provides an integrated, secure, simple-to-use platform, constructed to appeal to new and experienced users alike.

In creating Curve Wallet as the central integration point for technology and ideology, the CryptoCurve team set out to resolve the main issues that have stunted the mass adoption of cryptocurrency and blockchain technology: fragmented ecosystems, security vulnerabilities, and high barriers to entry.

Curve Wallet caters to investors of all types by offering an integrated, secure, intuitive way to Invest, Trade and Manage Accounts:

+ Curve Wallet will use CURV, a token with multiple utilities. For example, by using CURV tokens, investors will enjoy reduced trading fees and unlock enhanced capabilities like the Nuke function.
+ Invest and trade directly from inside Curve Wallet, monitor their portfolios over time, and fund accounts through a bank or credit card.
+ Easily participate in new ICOs as well as join investing pools that require no manual admin management.
+ Stake CURV tokens, receiving tokens from any ICOs launched on Curve Wallet.
+ Advanced portfolio analysis allows users to track, monitor, and analyze holdings over time.

SECURITY

Security, more than any collection of attractive features, defines a crypto 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 exchanges directly on the platform. Enjoying safekeeping for cryptocurrency assets in a secure, simple Wallet, users will no longer need multiple accounts on different platforms.

> 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.

A significantly deeper look at our security protocols can be found in the Appendix. Below, we briefly outline some of the critical 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 CryptoCurve Wallet keystore vault provides both inexperienced and expert-level investors options for powerful, secure key storage. New users may prefer that CryptoCurve store their keys, while seasoned investors may choose customized controls for keystore files.

For ease of use, the CryptoCurve keystore vault encrypts, shards, and replicates keys across multiple distributed key store 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 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 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. 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[2] 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 & Face Recognition ·

In 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 ·

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.

[2] http://motp.sourceforge.net

CURVE WALLET

Designed and built by seasoned cryptocurrency users, 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.

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.

The CryptoCurve platform will also offer capabilities for: Investing, Trading and Accounting.

INVESTING >>

+ ICO HOSTING: Initial Coin Offerings (ICOs) will be able to be hosted directly on Curve Wallet
+ STAKING: Investors will be able to stake CURV tokens and receive tokens of new ICOs hosted through the platform
+ POOLING: Automated pools will increase ease and efficiency for participants

<< ICO HOSTING >>

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

ICOs that host directly on 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 is partnering 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.

3RD PARTY VALIDATOR >> KYC / AML STORED ONCE >> STAYS IN CRYPTOCURVE

· Use Any Cryptocurrency to Invest ·

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

<< STAKING >>

+ Receive new ICO tokens by staking CURV tokens
+ Actively invest in ICOs

ADD 10,000 CURV TO BE ADDED TO NEXT TIER

By staking or locking away CURV tokens, investors will receive tokens from newly hosted ICOs. A single investment into CryptoCurve unlocks the ability to actively invest in every ICO hosted through the platform. The more CURV tokens staked, the more an investor will earn. As the CryptoCurve ecosystem grows, the CURV investor's portfolio will grow with it.

Users will fall into tiers based on how many CURV tokens staked and then proportionally receive coins from each ICO launching on the platform. By being in a higher tier, a user will receive proportionally more ICO tokens.

<< POOLING >>

+ Smart pools, trustless process, early access
+ Run ICO investing pools automatically
+ No expertise needed to be an admin - just hold CURV tokens
+ Trust the blockchain, not an individual

‹ 1 › An administrator creates a pool and selects a hard cap, a pledge cap if necessary and pledge dates

‹ 2 › The administrator invites other CryptoCurve users to the pool

‹ 3 › Members pledge to the pool

‹ 4 › The administrator approves pledge amounts

‹ 5 › Pledgers contribute to the pool

‹ 6 › Tokens are distributed to pool members

Users who stake 10,000 CURV tokens will be able to create custom ICO pools.

Pools are implemented by smart contracts deployed on the Wanchain network. Pool parameters

(whitelist, max pledge, and so forth) validate in Curve Wallet and protect against fraudulent interference.

Users can contribute to these pools using any supported cryptocurrency. Curve Wallet will automatically convert them to designated denominations.

Note: The administrator has the option to charge pool members a small fee in exchange for his or her work. In this case, CryptoCurve will assess the administrator a 10 percent fee.

TRADING >>

+ DECENTRALIZED EXCHANGE: Provides liquidity and saves time
+ NUKE BUTTON: Liquidate holdings at any time into Bitcoin or Ethereum

<< DECENTRALIZED EXCHANGE (DEX) >>

+ Trade directly from inside 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

< 1 > Connect to CryptoCurve Ethereum node clusters

< 2 > Connect to CryptoCurve 0x relayer

< 3 > Retrieve the current 0x exchange contract address

< 4 > Retrieve the Wrapped Ethereum (WETH) and ZRX token addresses

< 5 > Setup an account

< 6 > Set a spending allowance (user configurable)

< 7 > Generate WETH (Converts ETH into ERC20 compatible WETH)

< 8 > Transact with the relayer

Curve Wallet will integrate with the 0x protocol. 0x implements an off-chain order relay with on-chain settlement in which off-chain relayers are distributed hosts that keep and broadcast the order books. Market makers release signed orders (backed by

on-chain confirmation), and market takers buy them. Once bought, orders are backed by on-chain settlement.

This allows Curve Wallet to:

+ Provide low fees (CryptoCurve has its own relayer and will provide discounted rates for Curve Wallet users)
+ Make and take orders
+ Find the best-matching orders for takers

<< EXCHANGE INTEGRATION >>

Curve Wallet users will be able to add their current supported exchanges directly in the CryptoCurve ecosystem. Two phases of implementation are currently in development for this:

+ Phase 1: Users add trade keys directly. This allows full user control because keys are stored with the user who can interact directly with their exchange wallets.
+ Phase 2: A shared-state channel in which users simply activate an exchange service and give full functionality access.

<< INSTANT TRANSFERS & LOW-FEE TRANSACTIONS >>

Due to our use of state channels that were originally designed as a scaling mechanism for on-chain settlement, Curve users will enjoy instant transfers with marginal fees. A state channel can be explained as follows:

> Alice and Bob are both Curve Wallet users. Alice transfers 1 WAN to Bob, and Alice signs the transaction. Bob accepts receipt of funds, 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.

CryptoCurve will allow for multi-channel interparty state channels. This allows Curve Wallet users to enjoy instantaneous, low-fee transactions.

<< NUKE BUTTON >>

+ Liquidate any or all holdings into Ethereum, Bitcoin, or a stablecoin with the click of a button
+ Save critical time during drastic market shifts
+ Easily revert to previous holdings with the Snapshot feature

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 need to consolidate their holdings into currencies like Ethereum and Bitcoin.

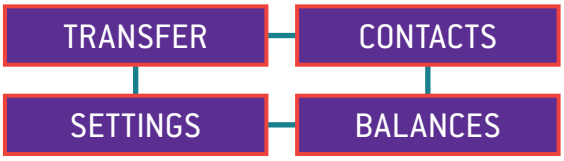
Users will be able to Take a Snapshot of their portfolio prior to Nuking to revert to previous positions with proportional accuracy.

ACCOUNTING >>

+ CURVE ACCOUNT: Transfer currencies instantly with no fees
+ FIAT GATEWAY: Invest using a bank account or credit card

<< CURVE ACCOUNT >>

+ No transfer fees when sending coins and tokens inside Curve Wallet
+ Instantaneous transfers of coins and tokens inside Curve Wallet



The Curve Account will provide a single storage point for a user's tokens of any type. It will allow users to send coins and tokens within Curve Wallet instantly, with zero fees. Users will have control over their contacts, security, and preferences.

<< FIAT GATEWAY >>

+ Fund a portfolio with a bank account or credit card
+ No need to transfer funds through another platform, thus reducing spending on gas and other network transfer fees, as well as time and effort
+ Easy tax tracking
+ No level of expertise needed to begin using cryptocurrency

Inside the Wallet, users will be able to fund a portfolio using credit cards and bank accounts. KYC/AML information used to verify identity for participating in ICOs will also verify identity for fiat withdraws, eliminating redundancy and saving time.

UI / UX: USER INTERFACE / USER EXPERIENCE

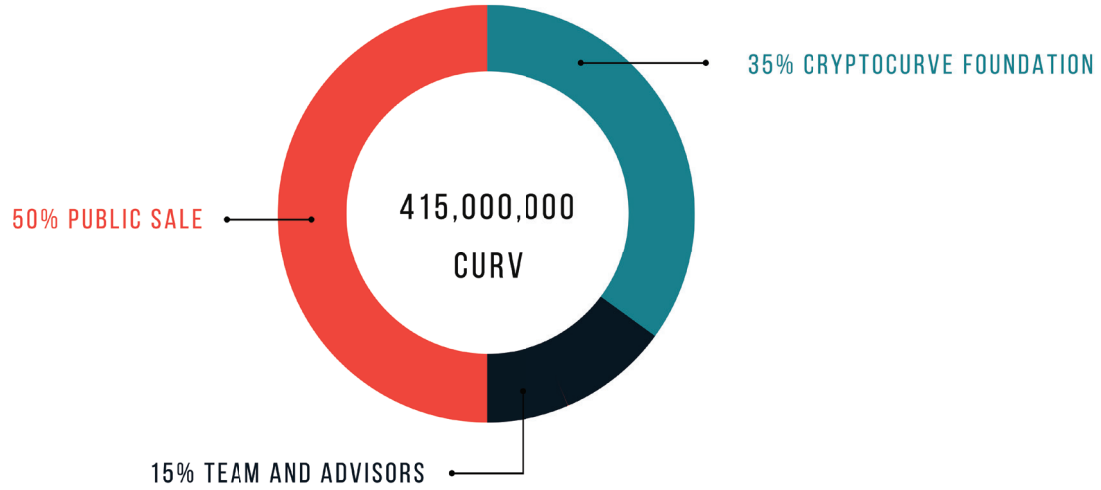
Cryptocurrency platforms are not currently known for being easy to use; rather, the opposite is often true with many apps and exchanges suffering from clunky interfaces, confusing color schemes, and unintuitive design. Curve Wallet will change that. From the beginning, the focus for Curve Wallet has been simplicity. We believe the management and use of assets should be easy and require very little acclimation.

<< RESOURCES >>

For more images, visit our Pitch Deck:
https://cryptocurve.io/documents/cryptocurvepitchdeck.pdf

TOKEN STRUCTURE

TOKEN STRUCTURE >>

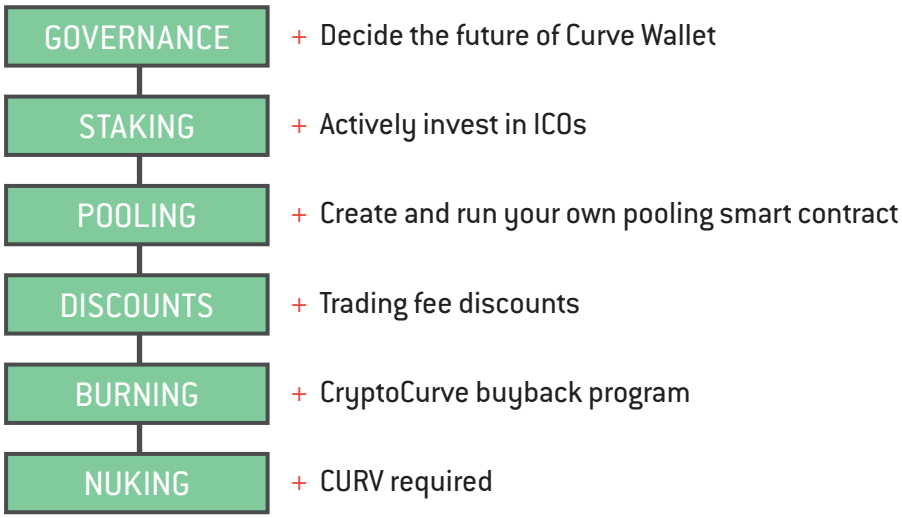


TOKEN METRICS >>

+ Name: Curve Token
+ Symbol: CURV
+ Website: https://cryptocurve.io
+ Social Media:
  - @cryptocurve on Telegram / Facebook
  - @crypto_curve on Twitter / Instagram
+ Token Type: WRC-20
+ Fundraising Goal: $32m
+ Private Sale: $26m
+ Public Sale: $6m
+ Max supply: 415 million CURV
+ Circulating Supply : 207.5 million CURV
+ Token Rate: 1 CURV = $0.20
+ Contribution Method:
  Private Sale (ETH) & Public Sale (WAN)
+ Token Distribution:
  - 50% Public Sale
  - 35% CryptoCurve Foundation
  - 15% Team & Advisors

TOKEN UTILITY >>

Some examples of our token utilities are:



THE CRYPTOCURVE MISSION & VISION

Our Mission is to provide an integration point between users, third-party technologies, and foundational technology so as to democratize financial fairness, promote financial freedom, and drive global adoption of blockchain technology.

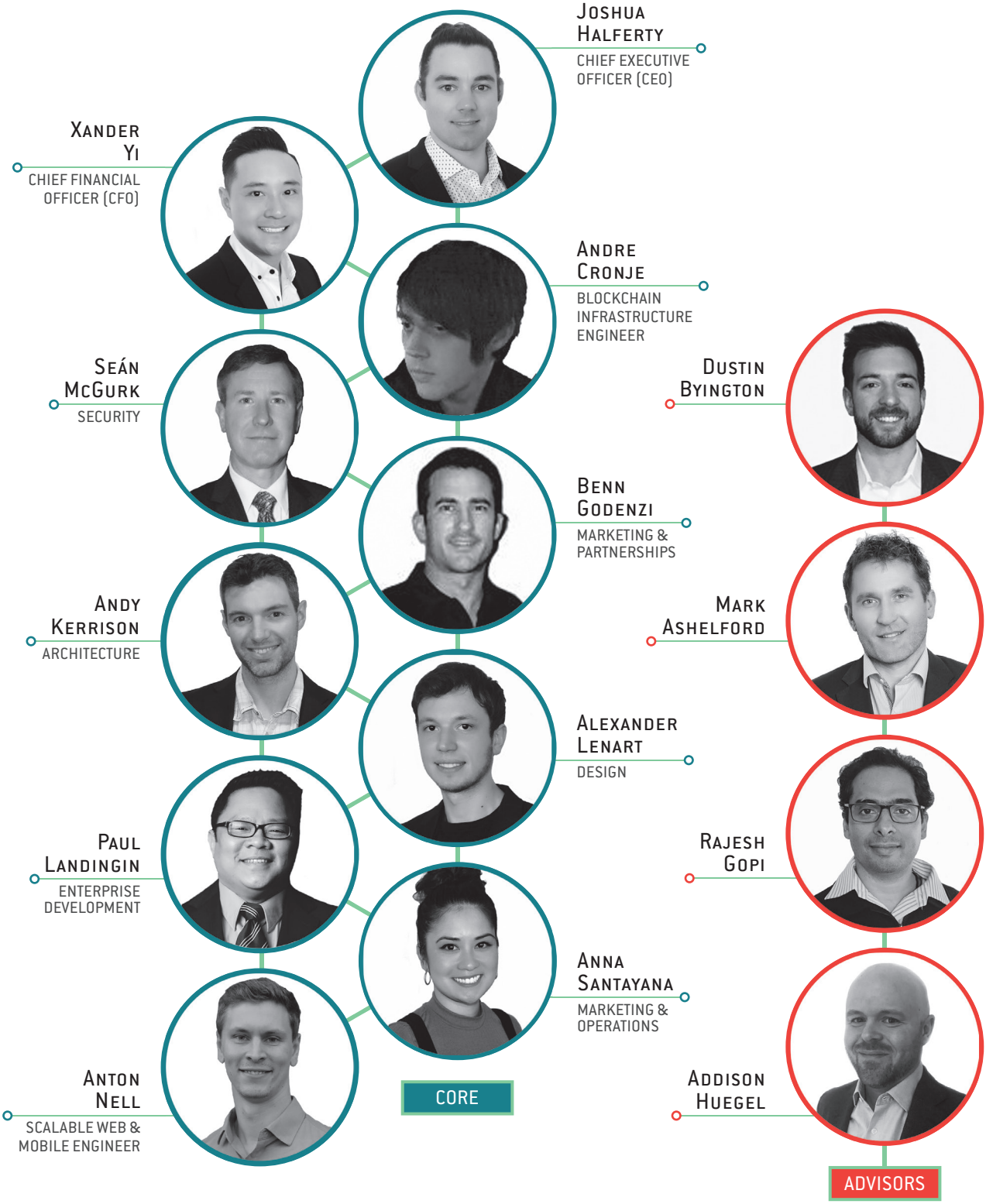
The first step in this mission will be achieved by Curve Wallet allowing anyone in the world to transact with and use any and every single digital asset.

Our Vision is to be the world's front end for blockchain by using a standards-based approach to provide infrastructure and flexible platforms that allow interaction and compatibility with other solutions.

To achieve our Mission and Vision, we look to **Best Practices and Standards**, which form the foundation for any product, company, or industry. Blockchain must adopt best practices and standards for design, development, and user experience. Through industry-wide standardization, end users can more readily make educated decisions about which services to use.

Through a standards-based approach, Curve Wallet is designed to optimize reliability, scalability, authentication, authorization, design, development, and testing.

TEAM


Joshua Halferty
CHIEF EXECUTIVE OFFICER (CEO)
Xander Yi
CHIEF FINANCIAL OFFICER (CFO)
Andre Cronje
BLOCKCHAIN INFRASTRUCTURE ENGINEER
Seán McGurk
SECURITY
Dustin Byington
Benn Godenzi
MARKETING & PARTNERSHIPS
Andy Kerrison
ARCHITECTURE
Mark Ashelford
Alexander Lenart
DESIGN
Paul Landingin
ENTERPRISE DEVELOPMENT
Rajesh Gopi
Anna Santayana
MARKETING & OPERATIONS
Anton Nell
SCALABLE WEB & MOBILE ENGINEER
Addison Huegel
CORE
ADVISORS

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

Q3 2017

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

Q2 2018

+ Curve Token Sale: CURV public token sale
+ Wanchain Wallet Functionality: Basic wallet functionality on Curve main site

Q3 2018

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

Q4 2018

+ Wanchain Interoperability: Cross-chain functionality
+ Ethereum ICO Pooling: Ethereum ICO pooling on Curve
+ Portfolio Tracking: Allow users to track their assets on the Curve platform

Q1 2019

+ Wanchain Decentralized Exchange: Cross-chain trading on the Curve platform
+ Nuke Function: Allow users to liquidate percentages of their portfolio automatically into BTC, ETH or a stable coin

Q2 2019

+ Fiat Gateway: Allow users to purchase cryptocurrency directly through mobile application with bank account or credit card

Iterative mobile releases after these milestones are released on the Curve Wallet website.

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.

0x Protocol >>
An 0x 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 0x protocol defines a standard format for off-chain order relaying via web services or other suitable communications mediums. A consumer of the 0x 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[3].

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[4].

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[5].

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[6].

[3] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[4] https://steemit.com/exchange/@nyinyinaing/decentralized-exchange-vs-centralized-exchange
[5] https://en.wikipedia.org/wiki/DMZ_(computing)
[6] https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ECS_instances.html

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[7].

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[8].

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[9].

Mobile OTP ››
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 0x platform are referred to as Relayers as they host off blockchain order books and can charge fees for their services[10].

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[11].

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[12].

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 [13].

[7] https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html
[8] https://jwt.io/introduction
[9] https://en.wikipedia.org/wiki/Know_your_customer
[10] https://blog.0xproject.com/a-beginners-guide-to-0x-81d30298a5e0
[11] https://en.wikipedia.org/wiki/Salt_(cryptography)
[12] https://cryptocurrencyfacts.com/maker-vs-taker-cryptocurrency
[13] https://aws.amazon.com/vpc

SOURCES

< 01 > https://aws.amazon.com/vpc

< 02 > https://cryptocurrencyfacts.com/maker-vs-taker-cryptocurrency

< 03 > https://www.cnbc.com/2017/12/04/cyberattack-temporarily-hits-bitcoin-exchange-bitfinex.html

< 04 > https://www.ccn.com/bitcoin-exchange-shapeshift-hacks-sees-230000-lost

< 05 > https://www.wired.com/2014/03/bitcoin-exchange

< 06 > http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

< 07 > https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ECS_instances.html

< 08 > https://en.wikipedia.org/wiki/DMZ_(computing)

< 09 > https://steemit.com/exchange/@nyinyinaing/decentralized-exchange-vs-centralized-exchange

< 10 > https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

< 11 > https://www.investopedia.com/terms/p/proof-stake-pos.asp

< 12 > https://en.wikipedia.org/wiki/Salt_(cryptography)

< 13 > https://blog.oxproject.com/a-beginners-guide-to-ox-81d30298a5e0

< 14 > https://en.wikipedia.org/wiki/Know_your_customer

< 15 > https://jwt.io/introduction

< 16 > https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

APPENDIX: SECURITY

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 architectured 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:

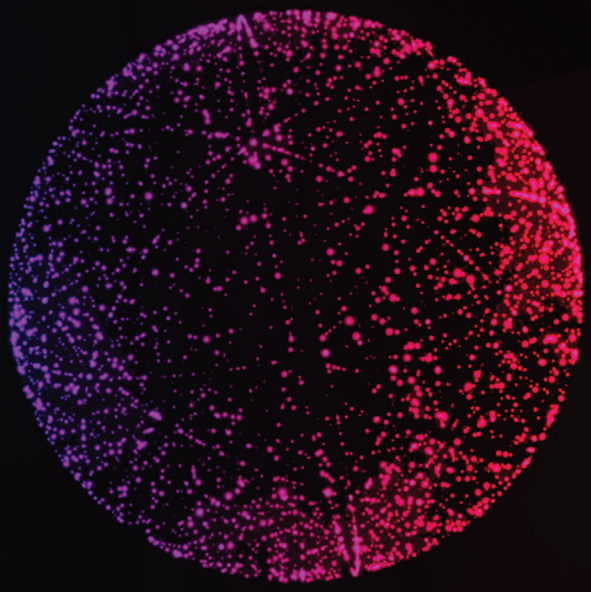
+ One-off IAM accounts for ECS instances
+ APIs are stateless and side effect free
+ No data is stored locally
+ Data is actively purged from memory after usage
+ All clusters are VPC controlled and only available behind DMZ
+ All access is IP- and port-controlled
+ Microservices architecture for role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

<< LAYER 3: STORAGE >>

Storage is arguably the 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

CRYPTOCURVE.IO



@CRYPTO_CURVE | @CRYPTOCURVE