Unlocking the Value of Digital Assets

How to ensure bulletproof protection, instant availability and total autonomy over all your digital assets

Curv Whitepaper

February 2019 | info@curv.co

© Curv 2019 All Rights Reserved

Blockchain – the Promise of the Digital World?

Blockchain has got everyone's attention. The globally distributed ledger, which allows the permanent and immutable recording of data, could be one of the most disruptive IT technologies seen in decades. It's being heralded as the potential democratizer of economies, eradicator of inefficiencies, and transformer of business models, across industries[1].

What is it? Blockchain is a continuously growing list of records, called blocks, that are linked together and secured using cryptography. These blocks record transactions between two parties. Each block contains a timestamp, record of the transaction data, and a cryptographic hash of the previous block, so it cannot be retroactively changed, without altering all subsequent blocks.

This ensures the integrity of the chain and irreversibility of transactions, which is good, until it's not. The public key cryptography used by blockchain gives organizations complete, and consequently permanent control, over a blockchain address and all the digital assets associated with it, but it also introduces a single point of failure – private keys.

Organizations have to safeguard and manage the private keys they use to sign and register a transaction. Some owners of cryptocurrencies, the first global-scale blockchain application, have seen firsthand what happens when keys are compromised or used for unauthorized transactions - more than one billion dollars-worth of digital assets were reported stolen in the first half of 2018 alone[2].

For mass adoption of blockchain to occur - the World Economic Forum estimates 10 percent of global GDP will be stored on blockchains by 2027 - the private key weakness must be addressed. It's the only way the full potential of blockchain technology will ever be realized. Then, and only then, will institutions be able to fully adopt these new asset-classes.

For more background on the challenges financial institutions face with the rise of new digital assets:
check out "Custody in the Age of Digital Assets" at https://bit.ly/2QSmn9v

The Trouble with Securing Private Keys

For years, vendors and service providers have been trying to come up with solutions to protect the private keys used by blockchain applications. Unfortunately, all the different offerings available are simply workarounds - they don't tackle the problem head on to eliminate the single point of failure; worse yet, they result in compromises that force organizations to choose between varying levels of security and availability.

Typically, one of the first choices that organizations must make is whether they want their assets to be more secure or more accessible.

[1] *"Blockchain beyond the hype: What is the strategic business value?" by Brant Carson, Giulio Romanelli, Patrick Walsh, Askhat Zhumaev, McKinsey, June 2018, https://mck.co/2K4oTWZ*

[2] *"$1.1 billionin cryptocurrencies has been stolen this year, and it was apparently easy to do," by Kate Rooney, June 7, 2018, CNBC, https://cnb.cx/2HvuKTc*

[3] *"Deep Shift: Technology Tipping Points and Societal Impact," World Economic Forum, Sept. 2015, www.weforum.org*

© Curv 2019 All Rights Reserved

Cold Wallets

Offer greater security because they are isolated from the Internet. Access requires physical proximity to the server/hardware on which the assets are held. This usually means an organization must grant access and trust a handful of employees to manage those assets, which negates the decentralization benefits of blockchain and can introduce other types of risks (internal threats and physical damage).

Hot Wallets

Offer greater accessibility to assets, because they are connected to the Internet. That connection, however, makes them an easy target and vulnerable to cyberattacks. To try to strengthen the security of the hot wallets, some providers are offering multi-signature, "multisig," services that require additional private keys to perform transactions.

Autonomy	**Security**	**Liquidity**
Full Autonomy Build Own	Cold Wallet	Hot Wallets
No Autonomy Service Provider	Cold Storage Custodian	Exchanges
	More secure but not fast	**Faster** but not secure

These multisig wallets can't scale to protect all an organization's digital assets because they are protocol-specific (support for Bitcoin, but not Ethereum, for example). For those protocols that don't support multisig (e.g Ethereum), providers can implement a software-based smart contract that enables several signatures, but these contracts have been prone to bugs and exploits and were not intended to be a security layer, as their code is open and attackable by all. Overall, the additional complexity and cost introduced by the combination of multisig wallets and smart contracts likely overshadows any incremental security benefits they might deliver.

Another consideration for organizations is whether they want to try to manage their private keys and wallets themselves or turn them over to a custodian or exchange. Again, the tradeoffs are high:

Do it Yourself "DIY"

Comes with big operational costs and delivers questionable security returns. The reality is most organizations do not have the time, skills, or resources to effectively take on the ongoing management of all their digital assets and private keys, which limits adoption.

Custodians

Manage crypto vault services on behalf of customers. While making things simple for the organization, these services force organizations to centralize control of their digital assets and hand them over to a third-party, which ultimately negates many of the benefits associated with using blockchain in the first place. The SLAs offered by these vendors are usually measured in hours, sometimes even days.

Exchanges

Manage digital assets on behalf of customers. While these services simplify an organization's ongoing operations, they too require the organization to hand over control to a third-party, which means the organization loses the value of a distributed ledger and their autonomy. Most exchanges only support specific protocols, so organizations are often limited in which digital assets they can use. In addition, because exchanges hold assets in hot-wallets, they are also susceptible to cyberattacks and insider threats.

One benefit of a custodian and exchange is that, if attacked, they will try to cover the loss (e.g. Coinrail [4]). The reality is organizations must really trust the custodian or exchange they use to do the right thing. The middleman is back. This is something that blockchain is supposed to remove – the value of the distributed nature of blockchain is that everyone is in control of their own assets, there is no need for intermediaries, no unnecessary lags, no inefficiencies.

To eliminate these contradictions and trade-offs and fully realize the benefits of blockchain, organizations need to eliminate the single point of failure. The only way to do that is to eliminate the concept of the private keys altogether. This is what Curv does, with the industry's first Institutional Digital Asset Wallet Service.

[4] https://bit.ly/2R9IIUC

© Curv 2019 All Rights Reserved

curv

Curv - Securely Enabling Blockchain Adoption

Curv's unique decentralized security model eliminates the need for private keys, replacing them with multi-party computation (MPC) protocols that enable transactions to be securely signed in a distributed way to eliminate any single point of failure. As a result, customers can confidently adopt and take full advantage of the speed, efficiency and autonomy that blockchain applications offer to transform their business.

Curv customers include:

Exchanges, Brokers, and Over-the-Counter (OTC) Markets

Digital asset liquidity providers and brokers who need to securely manage and trade all types of digital assets.

Digital Asset Fund Managers

Hedge funds, venture capital firms, and other asset managers who need to securely hold digital assets, short and long-term.

Custodians and Banks

Fiat custodians entering the digital asset space who are looking to securely manage digital assets and/or the currency-specific infrastructure for their clients.

Enterprises

Companies looking to manage and secure valuable data, cryptocurrencies, and other digital assets that can be exchanged on a public or private blockchain.

Consumer Wallet Vendors (both hot and cold)

Vendors offering a consumer wallet who want to be able to easily manage and secure their customers digital assets and integrate with one or more blockchain protocols, via a simple SDK.

To enable all these different institutions, vendors, and enterprises to adopt digital assets or roll out high value digital asset services, Curv provides a Institutional Digital Asset Wallet Service.

Industry's First Institutional Digital Asset Wallet Service

The Curv Institutional Digital Asset Wallet Service is the first to give organizations the control, security and instant access they need to adopt and use whatever digital assets they need - no tradeoffs, no compromises. The software-only cloud-service makes it easy for institutions and enterprises to confidently add these new asset classes to their portfolios because it is:

Mathematically Secure

Eliminating the concept of private keys to allow organizations to sign transactions in a secure, distributed way. Curv's mathematically-proven MPC protocols protect against cyber breaches and insider collusion, ensuring every user is authenticated and each transaction validated against a pre-defined policy, so only authorized transactions are completed and recorded.

Operationally Efficient

Providing a scalable cloud-based service that replaces the need for both cold and hot wallets. In addition, Curv sets up, manages and maintains the blockchain IT infrastructure for customers, making it easier than ever for organizations to adopt new digital assets.

Easily Customizable

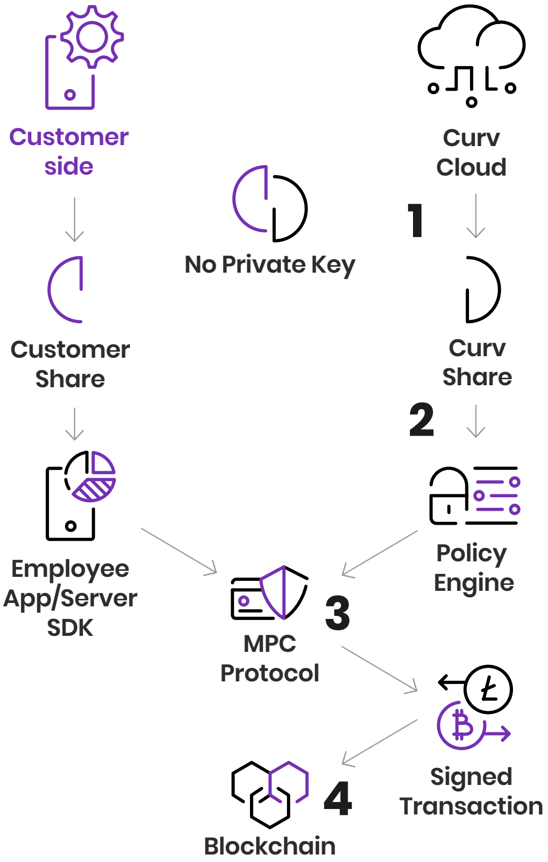
Offering a flexible enterprise-grade policy engine that allows institutions to define risk profiles and enforce granular policies that meet their varied requirements. For the first time, customers can adapt the transaction approval policy to the risk it introduces. The protocol-agnostic services also give customers the freedom to use whatever digital assets, protocols, and tokens they want, now and in the future – **Curv is the first to support Bitcoin (BTC), Ethereum (ETH), and all ERC-20 tokens, out-of-the-box, with the ability to easily add support as needed.**

[4] "Digital assets" include cryptocurrencies (e.g. BTC, ETH, ZEC), utility tokens, security tokens, private / permissioned blockchain assets created by enterprises – i.e. any blockchain-based asset.

© Curv 2019 All Rights Reserved

How the Curv Institutional Digital Asset Wallet Service Works

The Curv Institutional Digital Asset Wallet Service uses Curv's unique mathematically-secure, decentralized model, which retains the inherent benefits of blockchain, while making it easy to manage and secure all an organization's digital assets and transactions. Customers start by generating a secure wallet that gives them complete control and easy access to their digital assets.



1 The customer and Curv will individually generate secret shares, executing multi-stage communications over secure channels that generate a new public key. The public key is revealed to all parties, while the shares remain confidential, known only to their respective party. The corresponding private key is never generated or materialized - it remains latent, with the information to construct it inherently distributed between the secret shares.

The customer's shares will be used to jointly sign transactions with Curv. They can be distributed across any number of user devices (desktop, mobile, etc.) and servers running a local Curv SDK or app. Once the wallet is generated, digital assets can be deposited to its public key.

2 When a request to transfer funds outside of the wallet is made, the requesting party (user or machine) will be authenticated and the request validated to ensure it adheres to the customer's pre-defined policy.

To sign a transaction, all parties need to be convinced of the transaction's legitimacy and participate in the signature protocol. Participation will only be authorized if the transaction meets all the rules set in the Curv policy engine. These are defined by the customer and can include checks pertaining to identification, transaction volume, destination wallet etc.

The customer may also choose to place their own additional checks before allowing participation with their backend share. Likewise, an authorized employee may supervise transactions and restrict or approve share participation through the mobile app.

3 Once approved, Curv's MPC protocol runs between the customer's devices and Curv to jointly sign the transaction, without ever constructing the private key or revealing the shares to the other signing parties.

4 Curv maintains all the infrastructure required to transact with different blockchains. Once signed, Curv will upload the signed transaction to the relevant blockchain and monitor its execution.

BIP32 HD-Wallet support:

Curv can generate BIP32 addresses in a distributed way, without reconstructing the private key.

© Curv 2019 All Rights Reserved

The Benefits of Using Curv's Shares – Achieve Strong Security & the Ability to Transact with Confidence

Curv's use of independently generated shares creates a secure, distributed mechanism that eliminates the need for private keys, eradicating blockchain's single point of failure. Customers and Curv independently generate a number of random secret shares that will be used to sign transactions jointly, while maintaining the privacy of the underlying public/private pair (only one wallet address/ public key will appear on the blockchain). These shares make it easy for institutions and enterprises to:

Secure Assets

If an attacker compromises a share from one party, the assets remain safe - the corresponding share from the other party is needed before assets can be accessed or a transaction signed. The shares are continuously rotated, making it virtually impossible for an attacker to compromise the right share pairs from both the customer and Curv at the right time. The rotation also eliminates the risk an attacker accumulating key shares or any useful information over time. Unlike competing solutions, Curv's key rotation scheme does not require costly and unnecessary on-chain transactions.

Restrict Access

Granular customer-defined polices determine exactly who has shares and how they can be used to sign specific transactions. Every employee or machine generates and owns their own unique set of shares, unlike multi-sig solutions where all employees access and use the same key. A simple access list change, via the policy, can revoke a user's permissions entirely or prevent them from continuing to access a particular wallet. By destroying their respective shares, any cryptographic material the user obtains or records immediately has no use, mitigating the concerns of an insider attack.

Scale

When customers want to add a new user, they simply initiate the joint share generation using existing users.
If a user loses their share, Curv can issue a new one based on the existing shares to replace it.

The Control Delivered by Curv's Enterprise-Grade Policy Engine – Remain in Complete Control

Curv provides a flexible enterprise-grade policy engine that gives institutions and enterprises visibility and total control over their digital assets. It enables customers to define risk profiles and enforce granular policies for each of their wallets to ensure only valid and authorized transactions can be signed. Customers can:

Customize Enforcement

Policies can be defined by the customer to require multi-factor authentication (MFA), role-based access control, and multiple sign-offs for transactions, depending on their size, origin, destination, and even time of day. The customer may also choose to place their own additional checks before allowing participation with their backend share. Likewise, the authorized employee may supervise transactions, by restricting or approving share participation through the app.

Confidently Transact

While anyone can initiate a transaction, organizations can be sure only validated, authenticated requests that are within their pre-defined policy will be completed. For every transaction, the MPC protocol involves Curv's participation, with its shares, before it can be signed. The policy engine will only permit participation, if the customer-defined rules are met.

© Curv 2019 All Rights Reserved

Receive Alerts

For anything that is suspicious or violates policies, Curv will generate an alert that allows the customer to get ahead of and shut down issues.

Audit

Customers have a complete audit log of every transaction - not just previously signed transactions, but also the party who initiated the transaction, the policy steps taken, and the factors of authentication used. Audit log activity can be exported, filtered, and searched through.

Full API Support

All capabilities support both app usage by an employee and machine usage through an SDK. All capabilities and policies can be programmatically defined and controlled.

The Simplicity of Using Blockchain with Curv – Execute with Speed

The Curv service handles the onboarding and ongoing management of the blockchain IT infrastructure, greatly simplifying and speeding an institution's or enterprise's adoption of a wide variety of blockchain apps. Building out the IT infrastructure to integrate with blockchains can be cumbersome, expensive, and time consuming - organizations need to deal with a wide array of open source software and community-based support, and stay on top of all the upgrades, forks, and other protocol changes.

Curv eliminates this operational overhead for customers, by deploying, monitoring, and maintaining the entire wallet infrastructure across all the major digital assets and protocols, such as Bitcoin (BTC), and Ethereum (ETH) on an ongoing basis. Curv is continuously adding digital assets to accommodate current and future adoption requirements.

Curv also takes care of managing all the nodes and broadcasts transactions securely for customers. For customers who wish to maintain their own nodes, Curv can support the digital signature and policy enforcement service for practically all blockchain protocols.

This frees customers up to focus entirely on operating their digital asset business and managing their transactions through Curv's easy-to-use software interface. Customers can submit transactions using the Curv infrastructure through a web interface, cloud APIs, the Curv app, or SDK integrations – the app and SDK can be deployed on containers, mobile devices, or desktops/laptops, supporting various operating systems, including IOS, Android, Windows, OSX, and Linux.

© Curv 2019 All Rights Reserved

The Added Security of Curv's Built-in Backup – Maintain Unilateral Autonomy Over Assets at All Times

Curv has a unique patent-pending built-in backup that enables customers to retain full control over their wallet and unilaterally recover in the face of worse case scenarios. For the extreme cases in which the service is shut down, software is no longer functioning, or there are not enough active shares to be able to securely sign transactions, a physical backup key can be used to recover the digital assets.

The backup is generated initially by the customer and stored physically with a third-party or within a separate security infrastructure of the customer's choice. It exists explicitly to support this catastrophic failure, otherwise it will never be needed. Unlike with single-point-of-failure solutions, Curv empowers the customer to maintain total independent control over the backup key. The backup key on its own poses no risk, as it has no cryptographic significance without secrets that are generated jointly with Curv and the customer.

Looking Ahead

The private key security weakness is relevant for any entity holding or exchanging digital assets on a public or private blockchain. Traditional workarounds only force compromises between security, access, and ease of use. To actually address the issue, the private keys need to be eliminated, so organizations can realize the full value of their blockchain applications.

Curv's unique distributed security approach is setting a new standard for institutional digital asset security, eradicating the single point of failure to enable institutions and enterprises to easily and confidently adopt blockchain. Today, it's digital assets, tomorrow it could any number of applications. For example, supply chain, identity, and financial securities applications all entail a value transfer of some kind, making them well suited for blockchain.

With Curv, organizations have the security, efficiency and flexibility they need to adopt these blockchain applications – knowing they can transact with confidence, execute with speed, and always remain in complete control.

For More Information

If you would like to learn more or
see a demo of the service in action,
please contact **info@curv.co**

© Curv 2019 All Rights Reserved