

The Bitcoin Standard of Custody



+



TREZOR

+



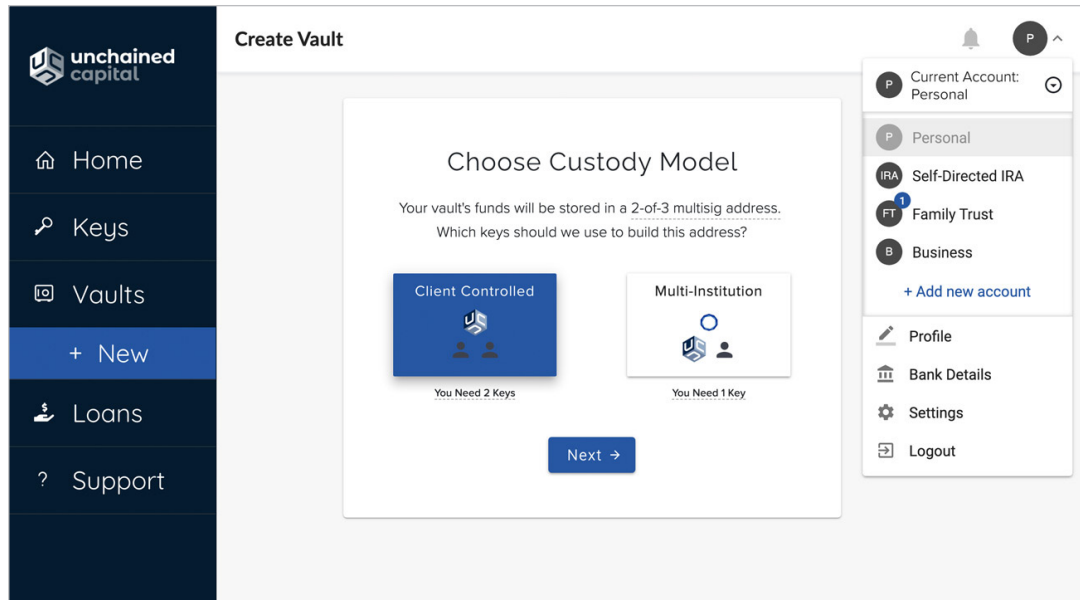
BLOCKYARD



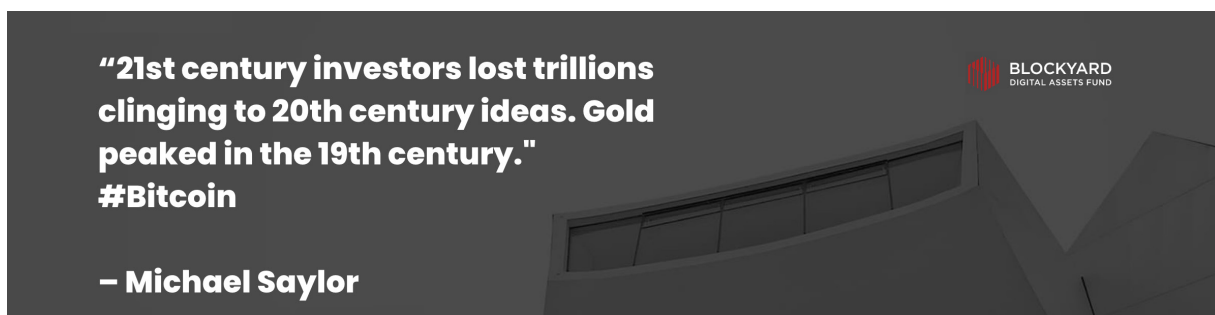
Whether you are an individual, business or investment fund holding bitcoin, there's no security substitute for private keys. While holding bitcoin with a third-party custodian is often a natural first step, bitcoin holders tend to mature to holding their own private keys over time as their holdings increase in value and as they come to better understand the immense security benefits of cold storage and key ownership. Historically, individuals have led the way both in bitcoin adoption and in the adoption of bitcoin self-custody, with businesses generally lagging behind on both fronts. Now as bitcoin matures, more and more businesses are beginning to adopt bitcoin and the same individuals that have come to understand the security benefits of private key ownership need custody solutions that work for their businesses.

While many of the same security principles hold true for both business and individuals, businesses face different challenges than individuals when securing bitcoin. Unchained Capital has invested heavily in an advanced business suite to help make private key ownership and management easy for an organization of individuals seeking to achieve a higher standard of bitcoin custody. Businesses are extensions of individuals and we know that individuals demand the same standard of care for bitcoin held by their businesses, which is core to our mission. At Unchained, our goal is to make it easy for individuals that prioritize security and understand the importance of private keys to conveniently manage both their personal and business bitcoin in one place, with incremental value delivered through a suite of financial services.

Through collaborative custody, we're delivering a solution to businesses that raises the bar for bitcoin security, while being seamlessly integrated with our consumer application. We asked one of our business clients if they would be willing to share their perspective for the benefit of others facing similar decision points. After evaluating a number of platforms, BlockYard Digital Assets Fund (BlockYard) decided to partner with Unchained Capital both as a custody and financial service provider. BlockYard works with high net worth clients that are not yet ready to take full control of private keys but want exposure to bitcoin, while demanding more direct access to the underlying asset than a product like GBTC could provide. Recognizing that security was paramount, the decision to use Unchained Capital was an easy one for the management team at BlockYard. Custody drove their process, and after evaluating a range of third-party custodians, it became clear that collaborative custody leveraging Unchained Capital and SatoshiLabs premier Trezor Model T hardware devices could not be matched from a security perspective.



BlockYard was impressed with Unchained Capital’s suite of technology and the security delivered through collaborative multisignature with Trezor Model Ts. While BlockYard was initially swayed by third-party custodians and the perceived protection provided by their insurance offerings, it became increasingly apparent that the assurances advertised by third-party custody could never replace the insurance guarantees provided by bitcoin private keys. When Unchained launched our Advanced Business Accounts, the decision for BlockYard was easy. The Unchained business suite delivered exactly what BlockYard needed as an organization: the highest standard of custody, flexibility to manage private keys across multiple team members, compatibility with leading hardware devices and value-added financial services, seamlessly integrated with custody. Now, the team at BlockYard leverages Unchained Capital and Trezors both for their personal and business needs within one easy to use interface, while taking advantage of Unchained’s lending platform and OTC trading desk for execution. The collaboration among three bitcoin companies – Unchained Capital, SatoshiLabs (Trezor), and BlockYard Digital Assets Fund- delivers the highest standard of security to the partners in BlockYard’s fund and provides high-net worth individuals and family offices with a superior alternative to investment vehicles such as GBTC.



Secure Multisig with Trezors

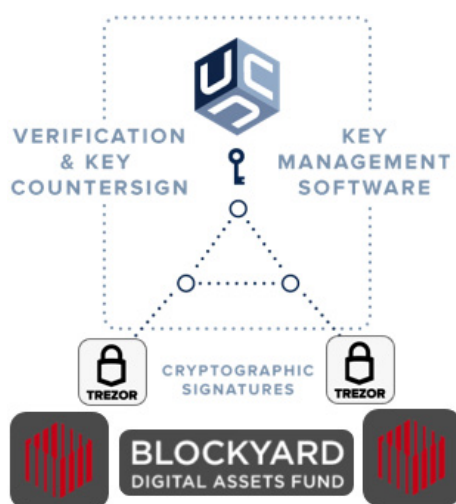
2020 was yet another year rife with exchange hacks, stolen bitcoin and frozen account withdrawals, which could be avoided by using bitcoin's native multisignature technology and distributing private keys both geographically and across multiple parties. Solving the bitcoin private key management problem for the broadest set of users is a major priority for the SatoshiLabs team, which is why they designed the Trezor Model T to be the right balance of security, functionality, and usability for multisignature.

Setting up a multisig vault with a Trezor is a 2 minute process.

JON GOODSPEED

MANAGING PARTNER/CFO, BLOCKYARD DIGITAL ASSETS FUND

Uploading public keys from a Trezor Model T to Unchained Capital to construct multisignature addresses could not be simpler. After configuring the devices and writing down the recovery seeds as recommended by Trezor, a user simply needs to give the Trezor device permission to share an extended public key, which is an easy two-step process facilitated by Unchained Capital's interface. Private key data is never shared with any third party (including Unchained Capital) and with multiple Trezors (and backups) physically secured offline in cold-storage, single points of failure are eliminated, funds are not at risk of remote account hacks and the permissionless and censorship-resistant properties unique to the bitcoin network are preserved.



- ✓ Complete control over funds, eliminate counterparty risk
- ✓ No single point of failure, native bitcoin multisig
- ✓ Keys replace weaker forms of authentication
- ✓ Account level controls augment bitcoin private keys
- ✓ Multiple members within a business can collaborate
- ✓ Best-in-class security partner, access to financial services
- ✓ External spending available by default with Caravan
- Unchained has access to financial information

In BlockYard's case, hardware devices and back ups are securely stored offline with certain executives having access to specific private keys, ensuring the most stringent financial controls are maintained at the private key level. BlockYard manages two keys in a native 2-of-3 multisig vault with Unchained Capital holding a third key, serving as both a backup recovery option and as a trusted counter-signer. Unchained Capital can collaborate with BlockYard to transfer funds, but BlockYard remains in unilateral, permissionless control of funds. In bitcoin, private keys are not just an ideology. Private keys are the ultimate form of authentication within the network; in order to transact any bitcoin, valid signatures must be produced with private keys. Without private keys, security is built on permissioned systems and weaker account level authentications. By holding 2-of-3 private keys, BlockYard eliminates counterparty risk of a third-party custodian. In order to transact, multiple executives must collaborate to create valid signatures using physically secure Trezor devices.

Bitcoin is a new technology just starting to capture the attention and imagination of the world. The companies in this space are often innovative start-ups that will mature as bitcoin adoption grows. Users who assume the solvency of their chosen custodial provider put their own or investor funds at tremendous risk. Unchained understands the need to eliminate this risk and has created a recovery solution that can be done by technically challenged CFOs, such as myself, in a matter of minutes independent of Unchained's support. Unchained's recovery process illustrates how carefully the team has considered all aspects of risk management from its customers' perspective.

JON GOODSPEED

MANAGING PARTNER/CFO, BLOCKYARD DIGITAL ASSETS FUND

To increase the security of clients using its private hosted application, Unchained Capital also developed an open source multisig wallet (Caravan) which is hosted on GitHub. By default, all Unchained clients have access to this easy-to-use tool for the best trust-minimized external recovery workflow in the industry. Caravan ensures that Unchained Capital's private hosted application and website are not a single point of failure. Open source is critical to bitcoin for a host of reasons; the libraries leveraged in Caravan are open to public code review and outside contribution. SatoshiLabs similarly open-sources their technology so that individuals can publicly review the code run by the Trezor hardware devices and collaborate with engineers to improve the functionality.

CARAVAN
MENU

My Multisig Wallet

IMPORT WALLET CONFIGURATION

Extended Public Key 1

Select Method ▼

Extended Public Key 2

Select Method ▼

Extended Public Key 3

Select Method ▼

Quorum

+
2
Required

of

+
3
Total

-

-

Address Type

- P2SH
- P2SH-P2WSH
- P2WSH

Choose 'P2WSH' for best practices, 'P2SH' for greatest compatibility.

Once you have imported all 3 extended public keys, your wallet will be generated here.the conflict.

The open source ethos of both companies has directly improved multisig functionality and security in browser-based applications. Early last year, Unchained Capital’s co-founder Dhruv Bansal contributed code to the SatoshiLabs team to allow Trezors to confirm that a multisignature address displayed in the browser is controlled by at least one key held by the device. This makes browsers significantly safer to use for all bitcoin services, since all critical information can now be easily verified by a device, rather than trusting information provided through a browser. Trezor was the first bitcoin hardware device with this functionality. While we expect all other hardware providers to follow, the collaboration between Unchained and SatoshiLabs demonstrated how more secure standards can be developed through open source leadership.

After trying a variety of hardware wallets, BlockYard decided that the ease of use, additional functionality, and the security delivered by the Trezor Model T was the best option for their needs. Before depositing any bitcoin, BlockYard executives can easily verify that addresses are controlled by company private keys on the Trezor devices themselves, without having to trust Unchained Capital or a browser. The ability to verify addresses on dedicated hardware devices enabled by Unchained Capital and Trezor significantly enhances the security assurances provided by multisig and it solved one of the critical multisig pain points for businesses like BlockYard.

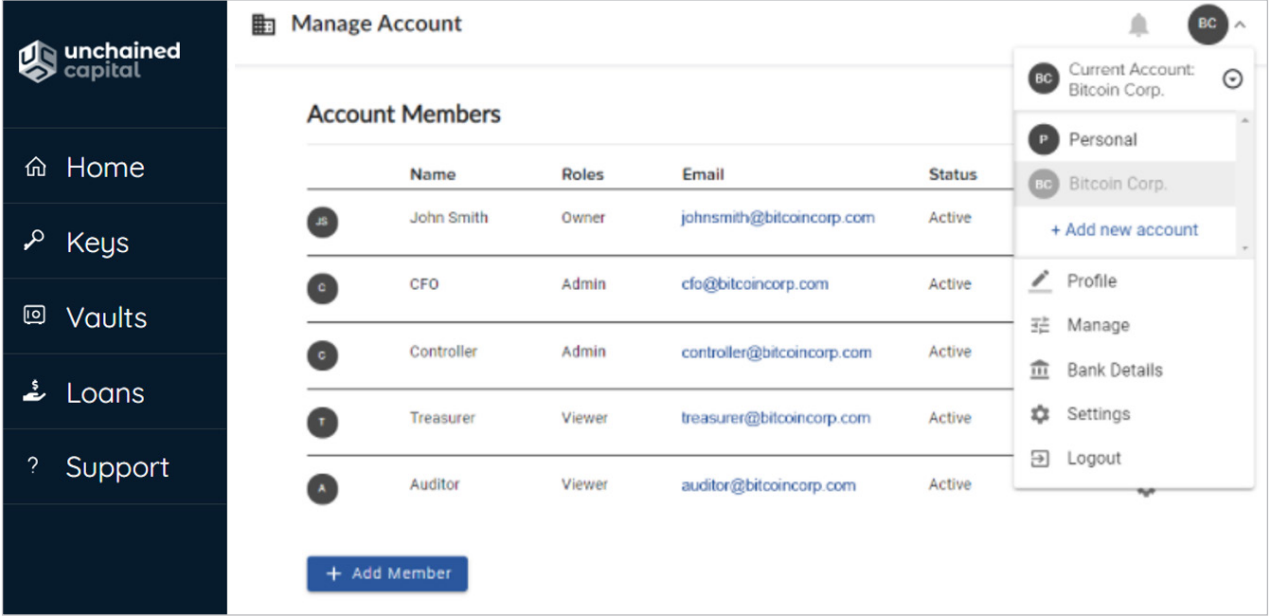
Personal + Business Accounts

Our Advanced Business Accounts provide businesses with an accessible application to secure their own private keys while creating redundancy and distributing financial controls to match the governance structure of a multi-person organization. Businesses now have a custody option that removes counterparty risk, eliminates single points of failure, and allows multiple members within an organization to easily collaborate with each other. But, more than that, individuals within businesses can easily switch contexts between personal and business use-cases to more seamlessly manage bitcoin multisignature.

Unchained and Trezor give us the combined benefit of private keys, corporate governance tools and layers of redundancy which collectively offer an unmatched level of security. We require the same standard of care for bitcoin held by our business which we demand as individuals (if not greater) and to us, collaborative custody is that standard.

HANS FREDERICK

MANAGING PARTNER, BLOCKYARD DIGITAL ASSETS FUND



Manage Account

Account Members

	Name	Roles	Email	Status
JS	John Smith	Owner	johnsmith@bitcoincorp.com	Active
C	CFO	Admin	cfo@bitcoincorp.com	Active
C	Controller	Admin	controller@bitcoincorp.com	Active
T	Treasurer	Viewer	treasurer@bitcoincorp.com	Active
A	Auditor	Viewer	auditor@bitcoincorp.com	Active

[+ Add Member](#)

- Current Account: Bitcoin Corp.
- Personal
- Bitcoin Corp.
- [+ Add new account](#)
- Profile
- Manage
- Bank Details
- Settings
- Logout

There is a reason we trust Unchained Capital's security model; it is about the approach to custody and it should be no surprise we leverage collaborative custody both as a business and as individuals.

JON GOODSPEED

MANAGING PARTNER/CFO, BLOCKYARD DIGITAL ASSETS FUND

BlockYard has demonstrated its leadership position by taking full control of their bitcoin as a business. The executive team at BlockYard thinks about security from first principles. Each understands the importance of private keys and that unavoidable risks are created when relying on permissioned systems. As individuals, BlockYard's executives recognized the benefits of holding private keys and extended that first principle thinking to their business. If they wouldn't trust their personal bitcoin with a third-party, the same principle would apply to the business. Rather than compromise, the BlockYard team chose a custody solution and financial services platform that satisfied the high bar of both their personal and business needs, and in doing so, delivered a more secure custody solution to partners in its fund by working with Unchained and leveraging Trezor.

Financial Services Integrated with Collaborative Custody

In addition to collaborative custody and advanced permissions for business accounts, BlockYard leverages the full suite of financial services offered by Unchained. BlockYard works with Unchained's OTC desk to convert US dollars into bitcoin as their fast growing fund receives more subscriptions. Separately, BlockYard uses the bitcoin held by the fund as collateral to gain leveraged exposure.

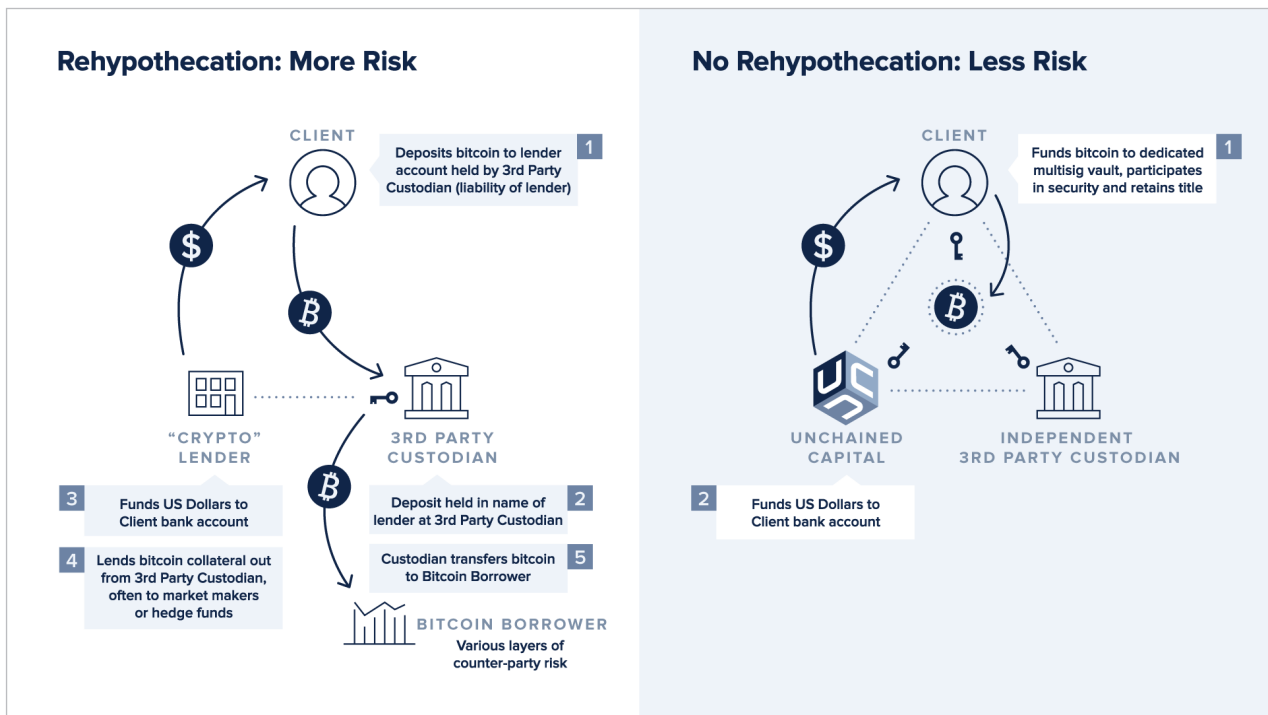
We use Unchained's OTC desk for trading and Unchained Loans for leverage; both are important tools for our investment strategy, and the integration with collaborative custody is incredibly valuable.

MAROS HAJDUK

PARTNER, BLOCKYARD DIGITAL ASSETS FUND

When BlockYard executes with Unchained’s OTC desk, the bitcoin purchased is directly deposited same-day into the corporate vault, with the company itself controlling the private keys on Trezor hardware devices and backup recovery seeds. BlockYard executives do not need to access keys to complete the trade. After a trade is executed, BlockYard wires funds, confirms its Unchained multisig vault ID number and then bitcoin is deposited without executives needing to communicate deposit addresses across insecure channels and without having to make any unnecessary additional on-chain bitcoin transactions.

When taking out leverage, the BlockYard team continues to control of 1-of-3 private keys securing the funds in a dedicated collateral address, with Unchained holding a second key and an independent third-party key agent (CitadelSPV) holding the third key. This approach allows BlockYard to easily verify at all times that collateral is segregated and not rehypothecated while preventing any single institution from unilaterally transferring funds. The ownership title to the bitcoin also never transfers and remains in the name of the fund when a loan is outstanding, which ensures that BlockYard is not subject to Unchained’s counterparty risk. This level of security is unparalleled in the bitcoin lending space, and while leverage can be risky due to price volatility, BlockYard knows that the fund’s bitcoin is secured on-chain for the duration of the loan with keys distributed among multiple institutions.



Integrating financial services on top of collaborative custody delivers incredible value. In this case, it is an example of a business having all the tools it needs within one seamless platform, but the same services and value are available to individuals as well. Custody built on the foundation of client private keys is what sets Unchained apart, and it allows us to deliver innovative and value-added financial services in ways that would not be possible if not for our first principles approach to bitcoin security. It wouldn't be possible if there weren't highly secure and easy to use dedicated hardware devices like Trezor. The sum of the parts, when combining the expertise and resources of multiple bitcoin companies, is greater than whole.

Conclusion

Through this collaboration, BlockYard Digital Assets Fund, Unchained Capital, and SatoshiLabs are setting the bitcoin standard for custody among businesses. Holding private keys requires responsibility, but it also delivers the greatest security assurance when owning bitcoin. We want to thank our friends at BlockYard for being willing to share their perspective. Understanding how sophisticated funds like BlockYard evaluate bitcoin custody helps inform other businesses weighing similar decisions. We also want to thank our friends at SatoshiLabs for continuing to advance the security of the bitcoin ecosystem, including but not limited to its investments in multisig. Collaborative custody is enabling more and more individuals and businesses to hold their own private keys with a fault tolerant approach that eliminates single points of failure. Having clients like BlockYard contributing to our product development roadmap and partners like Trezor and SatoshiLabs helping us innovate on multisig is critical to further enhancing security for all bitcoiners.

Unchained Capital, BlockYard, and SatoshiLabs invite your business to join the bitcoin native economy. You can learn more about Unchained's concierge onboarding experience for businesses at unchained-capital.com/concierge-onboarding-for-business. Concierge onboarding includes shipping and setup of Trezor devices, creating a multisig vault for your business and operational security consulting. If you are interested to learn more about BlockYard, please check out the fund website here. You may also reach out at hello@unchained-capital.com for more information or if you have any questions about our offerings.