Unchained

UNCHAINED RESEARCH

Bitcoin needs a network of keys

WHY UNCHAINED IS BUILDING MARKETS FOR COLLABORATIVE CUSTODY

DHRUV BANSAL

6 NOVEMBER 2023

Unchained

Contact

Follow Dhruv Bansal on twitter: @dhruvbansal

Send Dhruv Bansal an email: dhruv@unchained.com

Follow Unchained on twitter: @unchainedcom

Send Unchained an email: hello@unchained.com

Unchained

Outline

I. The past and future of collaborative custody

II. From global hubs to local neighborhoods

III. Preparing for the future

Unchained

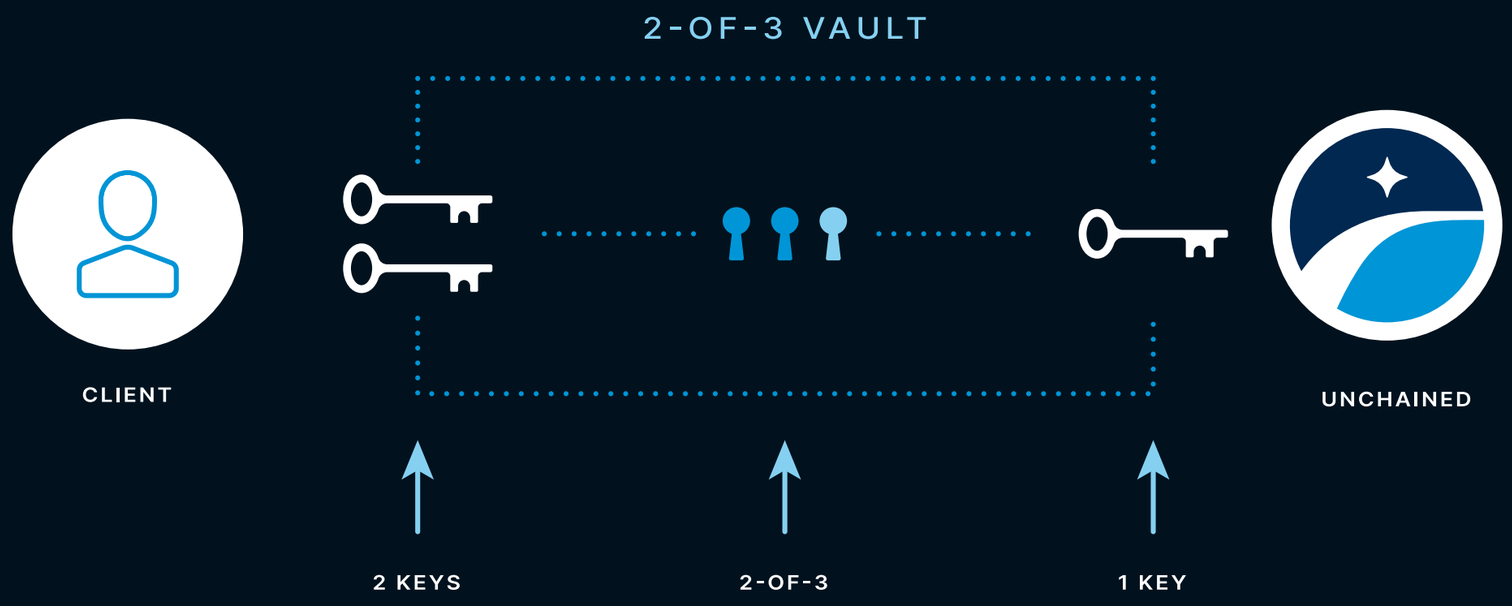
Bitcoin needs a network of keys

I. The past and future of collaborative custody

For many bitcoin holders, custody comes down to one of two choices: do it yourself or trust a custodian. If you do it yourself, you maintain full control of your funds but take on all the risk of custody yourself. If you entrust a custodian to hold your bitcoin for you, you lower your own obligations but create a single point of failure and lose control.

Unchained offers clients a third choice: collaborative custody.

Collaborative custody builds on bitcoin's native multisig capabilities to distribute the risks & responsibilities of protecting private keys across multiple parties. Platforms such as Unchained remove single points of failure and formalize the process of social key recovery for participants.



Clients using Unchained's collaborative custody vaults hold two keys themselves while Unchained holds the third key. These vaults use 2-of-3 multisig, so clients retain control of their bitcoin. But if a client loses a key, they can request that Unchained sign a recovery transaction rescuing their funds.

When we coined the term “collaborative custody” in 2018 we had a vision for how bitcoin custody should develop, but we knew many challenges were ahead of us. Standards for public keys, wallets, and transactions weren’t widely agreed upon. Hardware wallets were less capable and there were fewer companies making them. Collaborative custody was a new idea and it took time for the market to understand it.

Today, billions of dollars of bitcoin are held in collaborative custody by thousands of people and organizations worldwide. Platforms such as Unchained protect more bitcoin than the vast majority of major global exchanges. Thousands of bitcoin have been saved from loss or theft through social key recovery. Collaborative custody has succeeded.

But there is still a long way to go. Most bitcoin is still not in collaborative custody. Exchanges and custodians remain single points of failure for too many bitcoin holders. Investors with a small amount of bitcoin (relative to their net worth) may not feel the need to invest in better custody solutions. But many bitcoiners with significant holdings continue to use exchanges and custodians. Why?

Holding keys sounds scary

The most common model in collaborative custody is for clients to hold a majority of the keys in multisig wallets coordinated by a given platform. The platform provider holds a minority of keys and serves as a “key agent” to the client, signing transactions at their request. Clients in collaborative custody retain control over their bitcoin while also being able to rely on their key agent(s) for recovery. This control comes with a corresponding risk: clients who allow multiple keys to be compromised simultaneously can lose their bitcoin.

Many people and businesses just aren’t comfortable with the risk of holding a majority of their keys. They don’t want to—or can’t—be in a position where an attack on them or a mistake they make could lead to their bitcoin being lost.

New models for collaboration

Collaborative custody doesn’t require that any one party hold a majority of keys. By operating a minority of keys in their wallet, and delegating the rest to key agents, clients sacrifice control in exchange for lowering the burden of key management—without creating a single point of failure.

Clients who hold a minority of keys—even just a single key—in a multisig wallet can still verify addresses, transactions, and balances. They can sign transactions, cryptographically endorsing their intent to the key agents they collaborate with. But, if such a client’s key is compromised, this would not lead to the loss of their bitcoin.

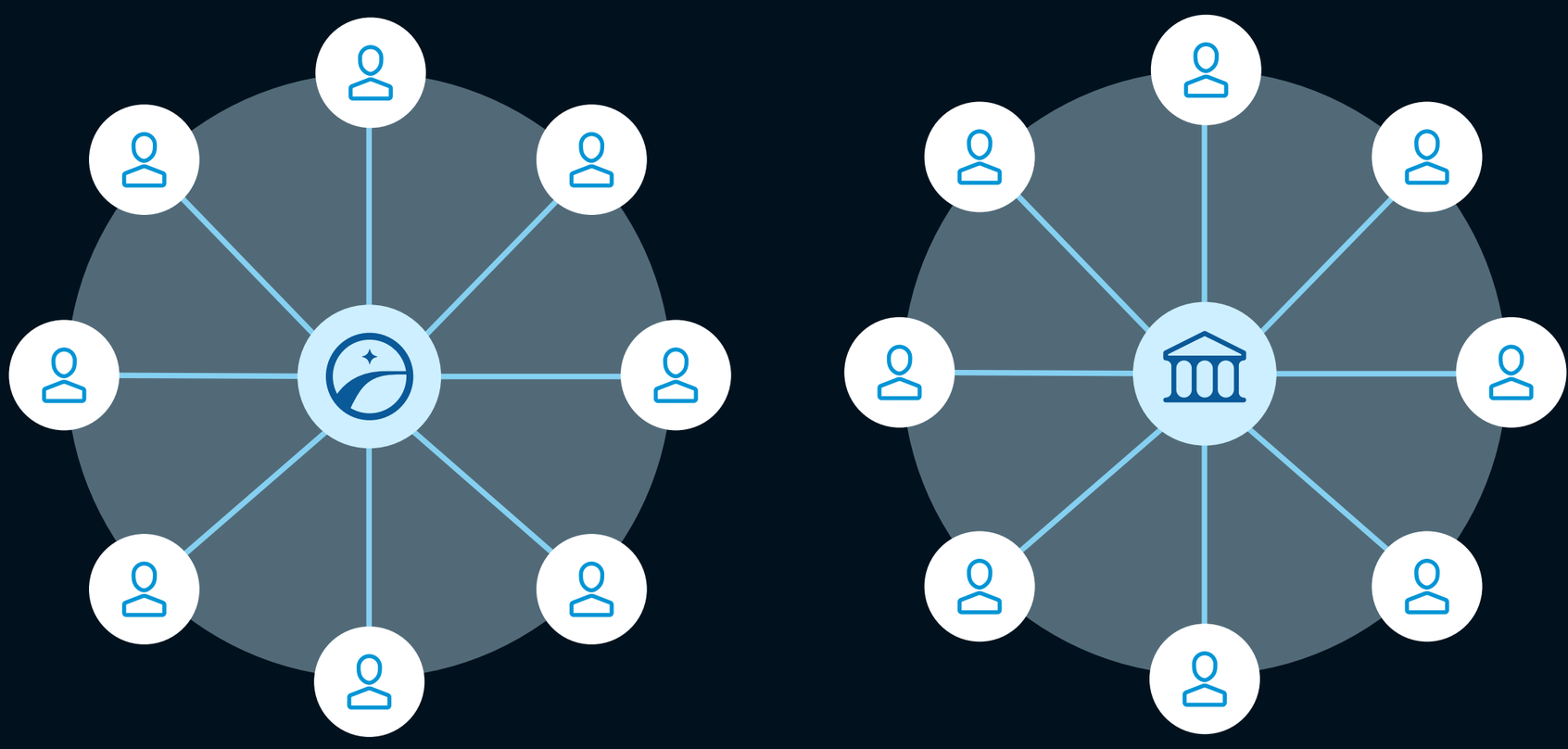
Clients who hold no keys at all can still benefit from collaborative custody. Instead of relying upon a single custodian, and creating a single point of failure, clients can delegate custody among multiple key agents in collaborative custody

Over time, as they develop the capability, clients holding no keys can start to hold a minority of keys – perhaps eventually even a majority—all while remaining within the same familiar platform.

More flexible key management models will make collaborative custody accessible to clients who aren't yet ready to operate a majority of keys themselves.

A network of keys

Most collaborative custody models today involve just two parties: the client, who holds a majority of keys, and the platform provider, who typically holds just one key and serves as a key agent to the client. This is hub-and-spoke collaborative custody—each platform provider is a hub, serving as a key agent to thousands of clients separately.



Collaborative custody today has a hub-and-spoke structure, with single platform providers serving many individual clients separately. Each platform is isolated, there are few (or no) third-party key agents, and clients do not collaborate with each other.

Clients who want to hold a minority of keys should not delegate the remaining majority to a single key agent (even a collaborative custody platform provider) as this would recreate a single point of failure, just like delegating custody to a single custodian. Instead, collaborative custody platforms must attract additional, third-party key agents to hold keys for clients who cannot hold a majority of keys themselves. The best way to do this is to make being a key agent profitable.

Bitcoin custody businesses are profitable, but building such a business from scratch requires huge upfront investments. Custodians must securely operate bitcoin private keys, develop software platforms, maintain online infrastructure, invest in compliance, succeed at marketing, and provide customer support. Relatively few companies are willing to make these investments and there are correspondingly few bitcoin custodians in the market, reducing consumer choice causing centralization.

Collaborative custody providers have already made these investments. Our platforms already provide the complex online coordination and integrations with hardware wallets required for collaborative custody.

We already have large client bases and well-earned reputations in the market. We know how to educate, onboard, and support clients.

The natural evolution of collaborative custody platforms is to become markets for key agents. Any individual or company that can securely operate a bitcoin private key should be able to sell their service directly to clients, leveraging the underlying capabilities of the platform. Lowering the barrier to entry for key agents, shortening their path to profitability, makes being a key agent more attractive, leading to a greater number of key agents in the market.

This is important for two reasons:

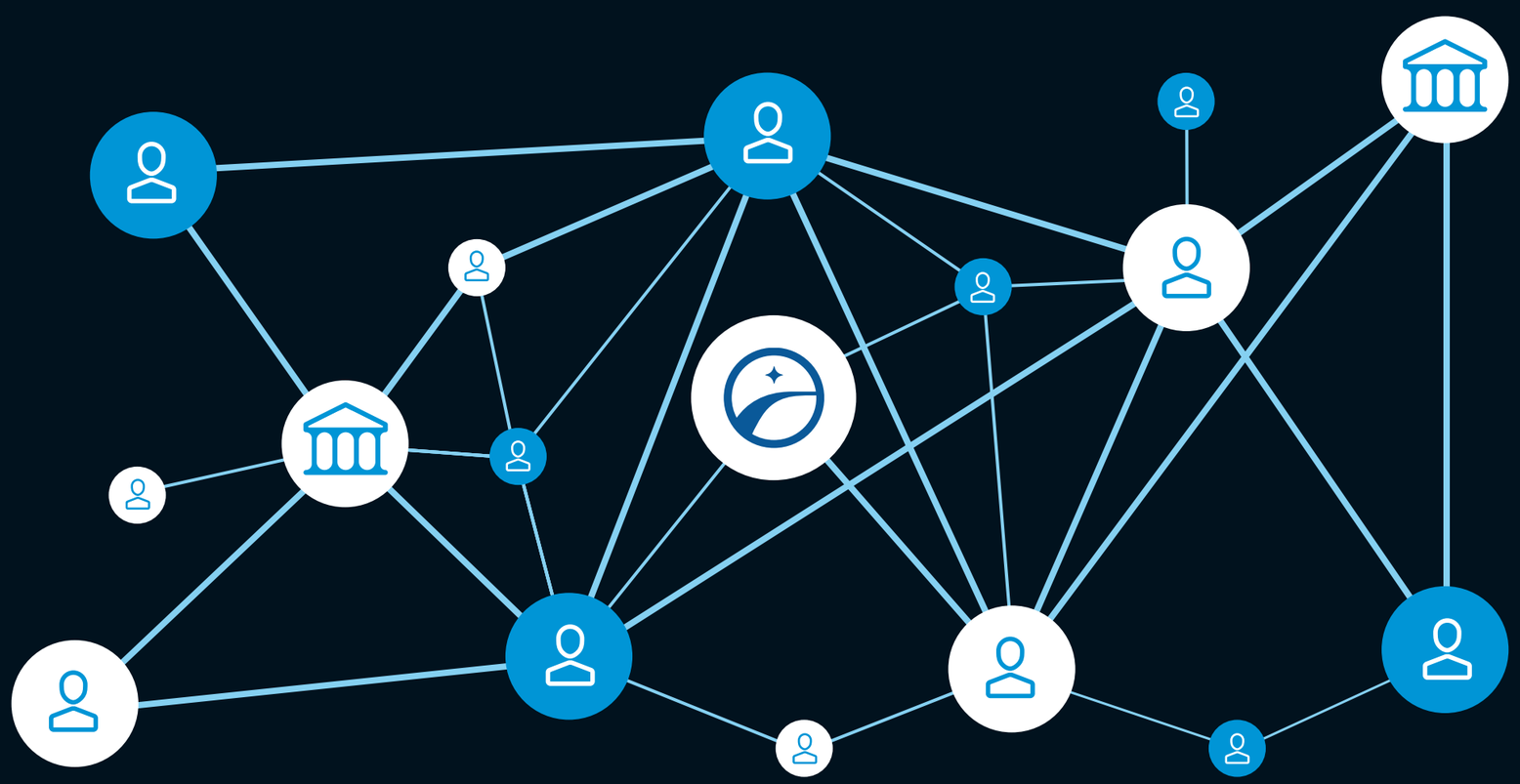
- **No single third-party key agent is best for all bitcoin holders:** Public companies holding billions of dollars of bitcoin in treasury need key agents with enterprise grade security, sophisticated key management programs, and a history of financial & security audits. The best key agents for these clients are other large companies (such as today's bitcoin custodians). Private individuals holding smaller amounts of bitcoin do not have these requirements and may not be willing to pay for them. The best key agents for individuals may be professionals such as financial advisors or attorneys – even friends and family. The more key agents that join the market, the more clients will find a match to their own needs and budgets.

- **A market with more key agents provides a more robust custody offering:** All other things being equal, more key agents means less bitcoin protected per key agent. If any one key agent were to be compromised, fewer clients would be impacted. And, because the market incentivizes the participation of many, competing, high-quality key agents, clients that are impacted should find it easy to replace their key agent with another.

Markets for key agents will cause today's collaborative custody platforms to evolve past separated hub-and-spoke configurations to become a network of keys.

Nodes in this network are people and companies practicing collaborative custody and links between nodes represent key agency relationships.

Networks create resiliency through offering redundant pathways for routing. If some hub fails, nodes can route around it through other nodes they are connected to. Nodes in 4/ real-world transportation, power, and telecommunications networks seldom rely



A network of keys is more robust than a hub-and-spoke model. Disruptions due to the failure of individual key agents or collaborative custody platforms impact fewer clients and recovery is easier.

upon a single link to access the network—more connections means more robust service. A network of keys is no different. More key agents serving as hubs and a greater number of interconnections means more trusted relationships that can be leveraged for safe custody of bitcoin.

Networks are also multiscale. They have tiers consisting of global hubs, regional centers, and local neighborhoods. A network of keys will have similar structures. Different kinds of key agents will be appropriate for the different scales of bitcoin holders that populate these tiers.

Links in a network of keys represent high-trust, valuable, real-world relationships—this isn't a social network, it's a social key recovery network. Connected nodes understand how to verify each other's real-world identity and intent. The strength of these connections means that a network of keys is also a scaffold for distributing financial services that benefit from trusted relationships. Trading, lending, insurance, inheritance, and payments are all easier to orchestrate when counterparties are in the same network.

Traditional custodians will not build this network. Their platforms were designed with the assumption that they would always control the bitcoin because their business model usually requires rehypothecating client assets behind the scenes to earn revenue for themselves. They are not incentivized to practice collaborative custody because it would damage their own bottom line.

It is collaborative custody platforms such as Unchained that have both the capabilities and the incentive to build the network of keys.

II. From global hubs to local neighborhoods

What follows is Unchained's roadmap towards a network of keys, ordered by market segment.

Custodians must become key agents for large holders

The global hubs of the network of keys are key agents that service clients that hold millions of dollars in bitcoin. Examples of such clients include (U)HNW individuals, trusts and family offices, public companies and other large enterprises or non-profits, and operating businesses that deal with bitcoin such as exchanges and funds. These clients aren't numerous but they collectively hold most bitcoin and have unique needs compared to other market segments.

These clients are accustomed to managing traditional assets where questions of custody are already settled. Banks such as BNY Mellon, JP Morgan, and State Street have strong reputations and long histories and already custody "systemically important" fractions of US wealth. When choosing a custodian, if some banks are considered "too big to fail," why would you trust anyone else to hold your assets?

Clients at this scale seek bitcoin custodians that look as much like the traditional banks they're used to dealing with as possible. They look for healthy financials, qualified custody, insurance policies, licenses, and audits because these are indicators of the maturity of a traditional custodian's infrastructure and processes. This leads them to choose one of a few major US bitcoin custodians who they trust to protect—to control—their bitcoin holdings.

Clients applying this reasoning should remember that, in bitcoin, no one is too big to fail. There is no government or money printer capable of restoring lost coins, so there are no bailouts.

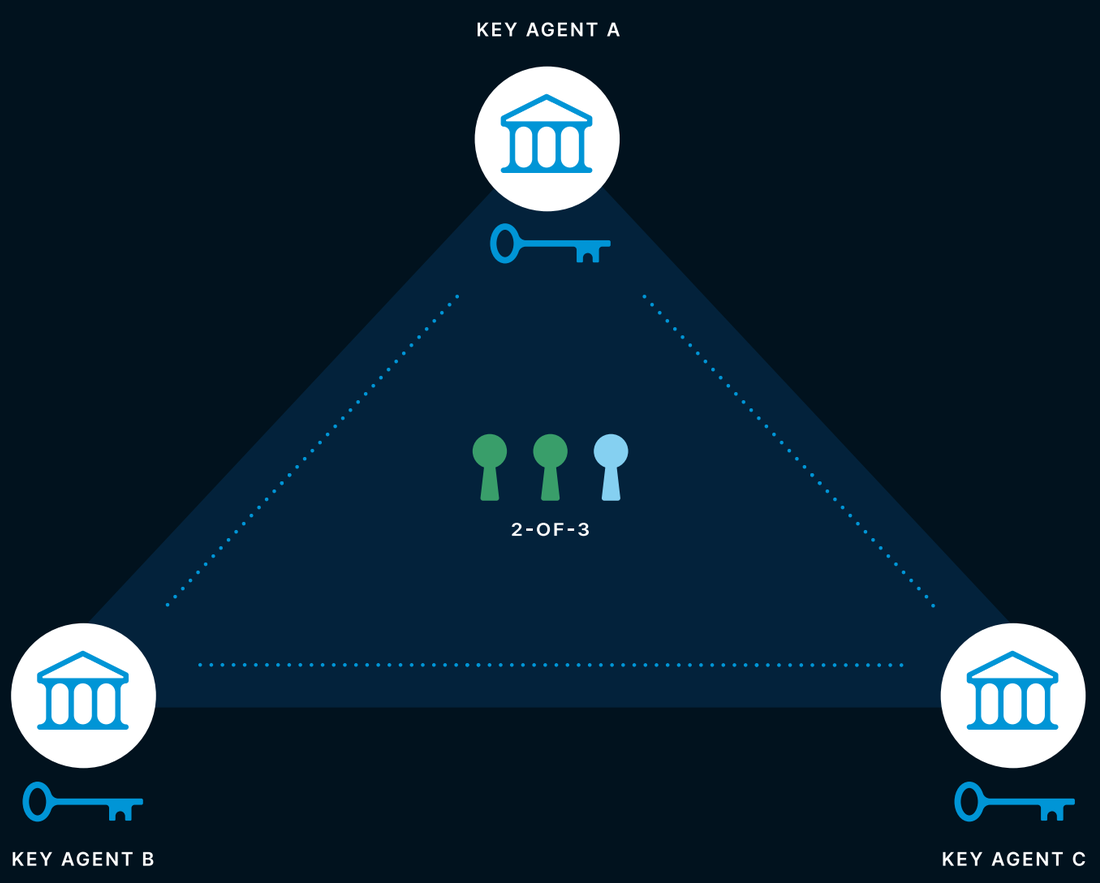
Trusting a single company, no matter their qualifications, to protect your bitcoin creates significant counterparty risk.

Some people ignore, rationalize, or accept this counterparty risk. Others attempt to mitigate it by splitting their bitcoin holdings among multiple custodians: putting their eggs into multiple baskets.

But bitcoins aren't eggs! Bitcoin is programmable digital money—unlike the dollar, it isn't restricted to being in a single basket held by a single custodian.

Unchained's *Delegate* model

Instead of balancing counterparty risk across multiple custodians, Unchained's Delegate model allows clients to balance risk across multiple key agents.



Unchained's Delegate model distributes control over your bitcoin between three enterprise-grade key agents, ensuring that you can recover funds if any one of them fails.

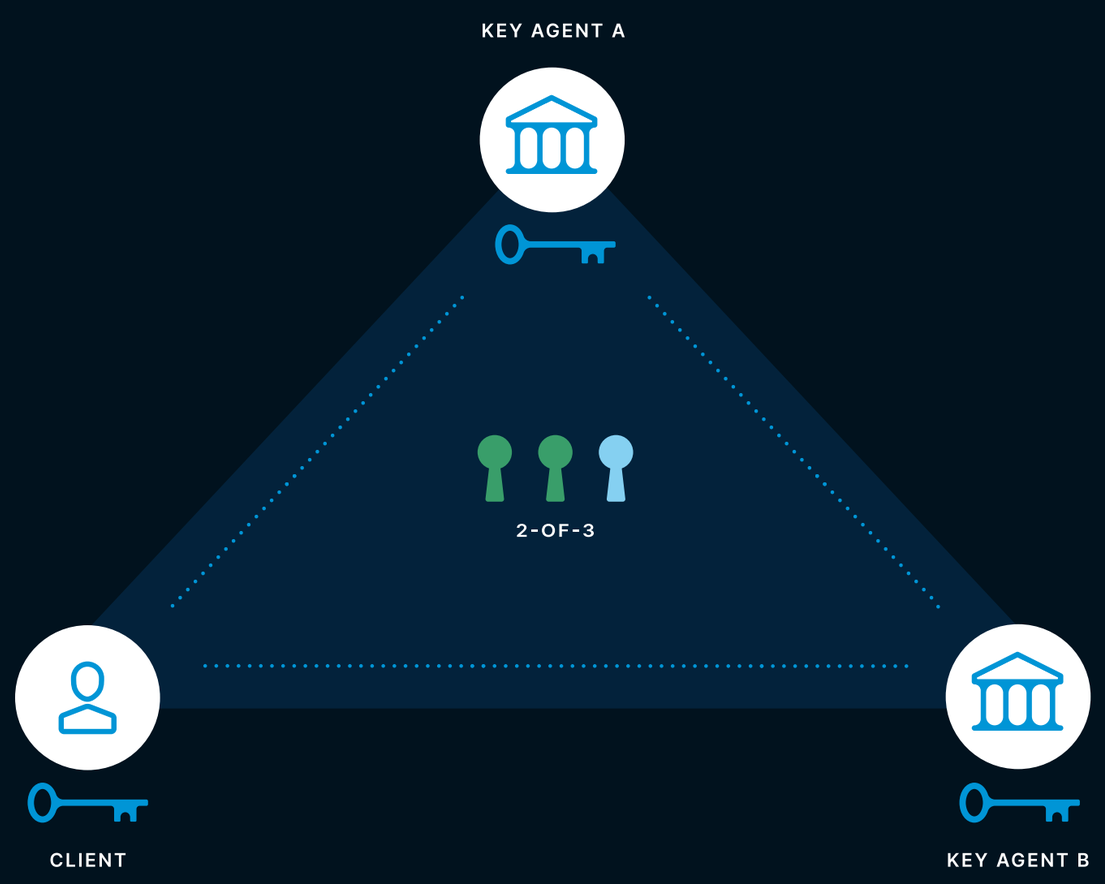
If a particular key agent fails or their key is compromised, no bitcoin is lost—clients can choose another key agent and sweep bitcoin to new wallets. In contrast, if a client is relying on multiple custodians, and a particular custodian fails, the bitcoin that custodian was protecting is now at risk.

Collaborative custody is built on multisig, a basic capability of the bitcoin blockchain, and uses open standards such as HD keys and PSBTs to define wallets and transactions. In contrast to proprietary MPC-based methods, wallets protected through collaborative custody can be recovered in a variety of opensource tools operating on a shared standard. If Unchained or our platform itself fails, key agents can use these tools to recover client bitcoin. Schedule some time with us if you are interested in learning how you can benefit from collaborative custody and our Delegate model.

From *Delegate* to *Partner*

We hope our Delegate model will attract clients who can't yet hold their own keys away from custodians. But our ambition is to help these clients eventually transition to using our Partner model.

Holding even just a single key allows clients to verify the addresses, transactions, and balances Unchained exposes using their own private keys. They can sign transactions using their key, which is a strong indicator of their identity & intent to other key agents they are collaborating with.



Unchained's Partner model requires you to hold a single key. You can verify addresses, balances, & transactions but an attack on you or your key will not directly lead to loss of bitcoin.

Managing a private key is challenging for individuals. There are many decisions to be made about devices and backup strategies with conflicting sources of advice. Businesses have an ever harder time. Retail hardware wallets are designed to be used by one person, not by a treasury management team within a public company. And organizations, unlike individuals, must deal with staffing changes among those with access to private keys.

Unchained, as a business with a long history of operating keys in collaborative custody since 2018, understands how to solve these problems for individuals and organizations. We offer consulting & training to help our clients build secure key management programs of their own.

Schedule some time with us if you want to explore how we can help you learn to protect your own key.

But we don't just want to help you learn how to hold keys, we want to incentivize you to do it, so we price our Partner model below our Delegate model. By managing a key yourself, you are decreasing the risk other key agents bear and deserve a lower carrying cost.

We hope this acts as an incentive for our clients to take on the challenge of learning to hold their own keys.

Expanding the marketplace

Unchained's platform today offers clients several key agents to choose from, as well as Unchained ourselves. Each key agent has experience protecting bitcoin private keys and using them to securely sign bitcoin transactions on behalf of clients.

We are already in conversations with several other major custodians, trust companies, and bitcoin firms to join our platform as additional key agents. Look out for coming announcements from us on this front and reach out to us if you are a current bitcoin custodian who is interested in exploring being a key agent on Unchained's platform.

Professionals and small firms are key agents for the middle market

Regional centers in the network of keys are key agents that service clients holding $100k – $1M of bitcoin. Examples of such clients include individuals, operating businesses, non-profits, and smaller funds.

Clients at this scale have the same concerns as the clients of global hubs, albeit with smaller budgets. It's no surprise that many small businesses thus follow in the footsteps of larger organizations and trust centralized custodians. Unfortunately many clients in this segment don't want to pay the fees for a toptier custodian and wind up relying on secondrate custodians or, worse, exchanges.

The counterparty risk for these clients is also more severe. They can seldom afford the cost or time required to spread their portfolios out across multiple custodians. They are also less capable of recovering from a loss induced by the collapse of their chosen custodian.

Clients in this segment often retain the advice and services of professionals such as financial advisors, accountants, estate planners, and attorneys. Most of these professionals do not know much about bitcoin and, what they do know, they often don't like – or aren't allowed to like by their firm.

But just as the population of bitcoin holders is growing, the number of professionals and firms who understand and engage with bitcoin is also growing. Professionals and firms that can advise their clients about bitcoin have an edge in the market—they are certain to be recommended from bitcoiner to bitcoiner. As adoption grows, professionals and firms that have a history of working with bitcoin will accrue even more clients.

We see a valuable market opportunity in enabling professionals to serve as key agents for their own clients. Clients who have retained a trusted advisor for years have also developed a relationship with that person that is difficult for attackers to subvert. If you trust your financial advisor to manage your investments, or your attorney to execute your will, would you trust them to hold a key to your bitcoin?

For clients who aren't ready to hold one or more keys in their wallet, involving a trusted advisor can be a great way to reduce their operational and security burdens while still retaining the benefits of collaborative custody.

Professionals who believe collaborative custody is important have brought Unchained many clients over the years. But many of these professionals also provide consistent feedback on how to improve the support we offer them in viewing their clients' holdings, managing their vaults, or holding keys for them.

We will soon be remedying this lack by adding he capability for professionals to obtain reporting and provide asset management & key agent services to their clients through the Unchained platform. We will also be offering training & certification programs to professionals serving as key agents.

If you are a professional interested in providing these services to your clients, please reach out to us. Our vision is to enable the growing number of professionals, present in every major city, who understand bitcoin to become nodes in our network of keys, serving bitcoiners in their local community.

Friends and family are key agents for each other

Most participants in the network of keys will have less than $100k in bitcoin. Bitcoin holders at this scale may not be willing to pay for the services of a professional key agent but they still benefit from using collaborative custody. The right key agents for this tier of the network are other individuals –

– friends, family, and colleagues protecting each other in local neighborhoods of collaborative custody.

Many of Unchained's clients are already "the bitcoin person" for their family or friend group. They are relied upon for advice on everything from where to buy bitcoin and how to protect it to using a hardware wallet and backing up keys. As Unchained clients, they naturally want to see their friends and family eventually onboard into collaborative custody with Unchained. But they recognize, correctly, that their parent or sibling or best friend may not yet be ready to hold a majority of their own keys.

As a result, vault names such as "Smith family vault" or "Alice and Bob's vault" are common on our platform. Clients use a single Unchained login and account but distribute the corresponding keys among multiple individuals in the real world. We want to replace this informal, off-platform approach with a dedicated set of features for peer-to-peer collaborative custody.

We want clients to easily be able to onboard their friends and family into collaborative custody with Unchained, including serving as a key agent to them if it helps them get started.

Our vision is to grow collaborative custody virally, with existing participants growing the network of keys in each local neighborhood.

III. Preparing for the future

Too many bitcoin holders today are still making a false choice between taking on all the risk and responsibility of key management themselves or outsourcing it to a custodian. The current "network" of keys consists of a few giant custodial hubs and many disconnected nodes in self-custody. This leads to single points of failure.

If one of today's major global custodial hubs were to be compromised, a significant fraction of the current bitcoin supply would be at risk of loss. The holdings of millions of people and businesses would be in jeopardy. Most individuals who self-custody don't have a social key recovery plan. If they lose a key or pass away, their bitcoin is at risk of loss.

Collaborative custody replaces custodians with key agents. Bitcoin holders decide how to share control and risk between themselves and their chosen key agents. Collaborative custody platforms such as Unchained have empowered clients who want to hold a majority of their keys to eliminate single points of failure.

Unchained

To scale to the millions of new people and businesses that will want to custody bitcoin, but aren't yet ready to hold a majority of their keys, collaborative custody needs new key agents. As a leading collaborative custody platform provider, we believe Unchained can build the markets that incentivize today's existing bitcoin custodians, professionals, and experts to offer their services as key agents.

We want these markets to evolve our platform beyond its current hub-and-spoke configuration into a network of keys. In such a network, the compromise of a major global key agent would be disastrous for that key agent but would not lead to the loss of any funds. Clients would merely sweep funds to wallets with other key agents—the network routes around damage.

Individuals and businesses can choose key agents in the network to hold keys for them without creating single points of failure. As clients develop the confidence to take on the burden of key management, they can begin to hold a minority of keys and eventually grow into holding a majority, while continuing to leverage key agents for social key recovery.

We want to offer clients an incremental path from holding no keys to taking on full-control of their bitcoin, all within the same platform, with help and support from the Unchained team and our key agent partners. Our hope is this path makes the journey of key management less daunting and encourages more bitcoin holders to take the first step.