



Bitcoin custody from the ground up

River's first-principles approach
to protecting your bitcoin



Bitcoin custody from the ground up

I started River in 2019 with the mission of building the world's most trusted financial institution, knowing that this trust must be earned through a track record of operational excellence, transparency, and an extreme focus on security and risk management.

River's number one focus (by a mile) is to keep your Bitcoin safe. River's custody system is built in three layers, each following a core security principle:

1. **Build an indestructible core:** The core custody system does not rely on any third parties and has been designed and built to protect against obvious risks like theft and loss of keys as well as non-obvious risks like Electromagnetic Pulses (EMPs), natural disasters, and nuclear war.
1. **Maximize client security:** Our clients must be protected against scams, hacks, and unforeseen risks to their security.
1. **Trust follows transparency:** You deserve the tools to verify the quality and integrity of our operations. We provide transparency about River's services while ensuring the privacy of clients.

In this paper, you will learn the details of how River has built each of these three security layers over the past six years. We will never stop working to improve our security and client satisfaction.

- Alexander Leishman, Founder, CEO, & CTO

Layer 1: Build an indestructible core

What does it mean to have an indestructible core? Simply put, it means having a custody infrastructure secure enough that River employees can sleep well at night, confident that all bitcoin under custody is safe.

In practice, River employs three strategies to ensure its core security.

1. Minimize dependencies

Many businesses in our industry have chosen to outsource their custody services to a third party as a quick and convenient way to launch. This decision comes with a tradeoff—limiting their ability to fully understand and control the security of their infrastructure.

At River, we prioritize building and maintaining our infrastructure in-house to minimize external dependencies. River maintains its own cold storage custody; no third parties ever have access to private keys. While this approach may result in a slightly longer development timeline, it enables us to provide a higher level of security assurance to our clients.

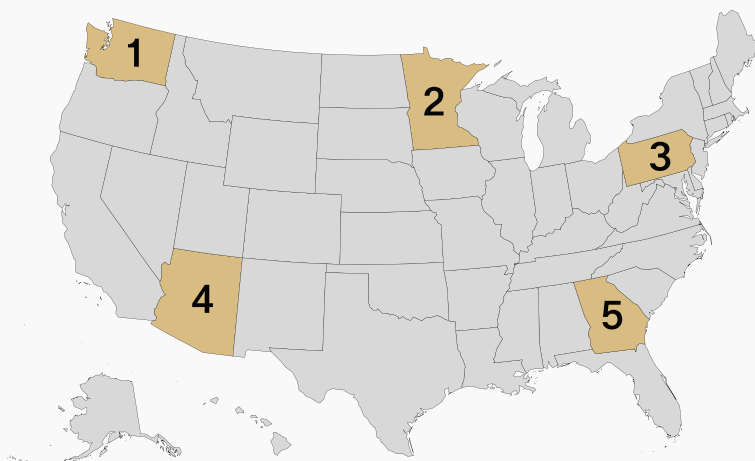
2. No single points of failure

River's custody solutions are implemented with maximal redundancy—cold storage keys are generated in separate locations, each having a physical and digital backup. The backups are then stored in different physical locations.

Geographically distributing backups is a form of geo-redundancy: these practices work to mitigate unforeseen, external events that are rare. Consider a scenario where the keys for a multisig vault are all generated and stored in the same location; if there is a natural disaster or a fire, the keys could be gone, and funds might be lost.

If the keys for the vault in the above scenario were physically backed up—non-digital media—then funds would still be secure even if all electronic systems failed. Our cold storage is designed such that, even if unexpected events happen in multiple locations across the US, client funds would be secure. Further, geo-redundancy measures are taken to ensure that private keys associated with the vault are generated and secured in separate geographic locations.

Geographically distributed bitcoin custody



- Set up as a 3-of-5 multisig
- Keys distributed across the US
- Each key has a digital and physical backup

River's cold storage vault uses Bitcoin's multisig scripting capabilities; this is important because it means the basis of our custody solution has effectively had several hundred code reviews from open-source Bitcoin contributors. By building upon this transparent and well-audited resource, we maintain strong privacy for our internal systems while benefiting from the collective expertise of the Bitcoin community.

3. Verifying our own security

Security is a shared responsibility among all River employees. To support this, our dedicated security team—with extensive experience in CISO roles at leading finance and technology firms—continually reviews critical components of our applications and infrastructure.

Additionally, River enlists the help of an independent third party, Doyensec, to carry out regular security reviews of our critical software systems—not including our core custody setup. These penetration tests are carried out as white-box exercises, meaning full source-code access is provided to the auditor to help identify any defects or vulnerabilities in the implementation.

Layer 2: Maximize client security

Equally important to maintaining a robust core infrastructure is protecting clients against hacks, scams, and unforeseen circumstances. In recent years, the rise of bitcoin-related phishing scams, SIM-swap attacks, and physical theft has made the importance of client security clear. At River, we are committed to ensuring these threats never impact our clients.

Client funds and personal information are proactively safeguarded by River in two ways beyond our core infrastructure:

Deposits in cold storage

To maximize the security of client funds, client bitcoin are kept in cold storage after being purchased—remaining offline at all times to remove vulnerabilities to theft. To make this possible, River uses some of our own bitcoin in hot wallets for operations such as transfers, purchases, sales, and withdrawals.

Strict data controls

Client information is protected through strict data controls. Client data is encrypted in transit and storage. Strong encryption ensures that if data is intercepted, it cannot be recovered without associated key material held by River. Internal controls follow the principle of least privilege to ensure that personally identifiable information is only accessible to specific employees performing roles related to client service and compliance. Additionally, all River employees use modern, phishing-resistant two-factor authentication to access our internal systems. These safeguards minimize the risk of unauthorized access to our client databases.

Lastly, River's compliance with the SOC II guidelines requires extensive controls around data privacy and internal controls.

Account security features

In addition to the measures River takes to protect our clients, River offers security features to help clients protect their own funds and personal information:

Account security features



Forcefield

ForceField gives you the ability to turn off or limit withdrawals to protect your bitcoin if you are targeted by a scam or your phone is stolen.



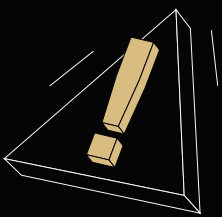
2 factor authentication

River accounts use mandatory multi-factor authentication, via one-time passcodes (specifically TOTP) or SMS.



Device verification

Any device signed into River must be verified by email. This protects you in the event that your login information is stolen.



Account notifications

Clients receive real-time notifications when security-critical actions are taken, such as a bitcoin purchase, sale, withdrawal, or deposit.



Beneficiary plans

The inheritance feature allows clients to ensure their funds are passed down to their beneficiaries in the case of an untimely death. This feature ensures that no login information needs to be shared to access your bitcoin to maximize account security.

Layer 3: Reinforce external trust

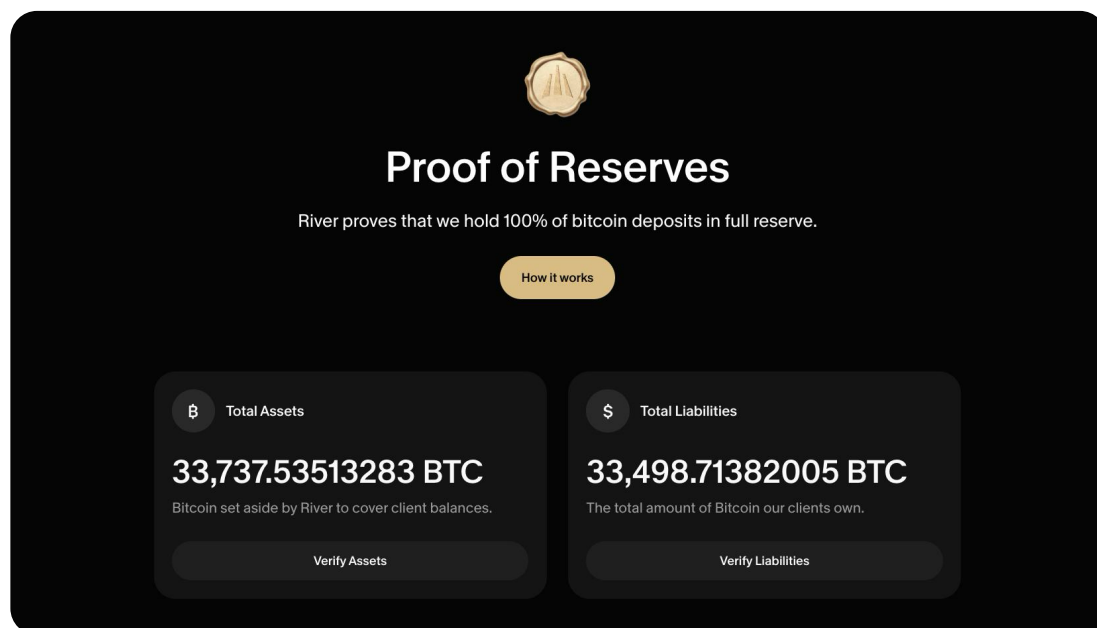
The success of any financial institution relies on the trust of clients. However, numerous bankruptcies of banks and exchanges have shown the importance of verifying what these institutions tell you.

At River we provide transparency about the state of our operations and the quality of our security so that clients do not have to trust what we say, but can verify the authenticity of our claims.

Proof of Reserves

Proof of Reserves (PoR) is a process that proves an exchange or brokerage holds sufficient reserves, or assets, to cover all customer deposits. It provides transparency and assurance to clients.

River is the only Bitcoin-only brokerage to regularly provide a Proof of Reserves both to clients and the general public. In doing so, clients can verify that River holds 100% of deposits in full reserve.



External auditing

River's security has been extensively tested by independent auditing firms. In 2024, we successfully achieved SOC 2 Type II compliance, the gold standard for vetting a financial institution's internal controls and systems.

Each calendar year, River's financials are audited by BPM, an independent accounting and auditing firm. This process provides reasonable confidence around River's financial statements and records of client cash and bitcoin balances.

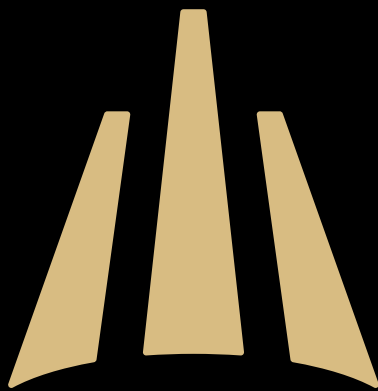
We encourage security researchers to partner with us in enhancing River's security. To report a security vulnerability or explore details about our disclosure program, please refer to our [security.txt](#) file.

Our never-ending commitment to security

Certifications and audits are an important external stamp of approval for any Bitcoin business. However, a culture of security and risk management, like the one we have at River, is the real gold standard.

We pride ourselves on being the best place for people and businesses in the United States to confidently buy, sell, transact, and of course, custody bitcoin. We do this while delivering unmatched client service, delightful user experiences, and accessible content and education. We aim to be at the forefront of Bitcoin technology and innovation.

But at the end of the day, nothing is more important than security. This is especially true in Bitcoin. As we work towards a brighter Bitcoin future, we will continue to be paranoid so that our clients don't need to.



 (888) 801-2586  [River.com](https://www.River.com)

NMLS ID#1906809