Tech Talk: Crypto Custody

What Is It? How Is It Secure? Who Can Do It?

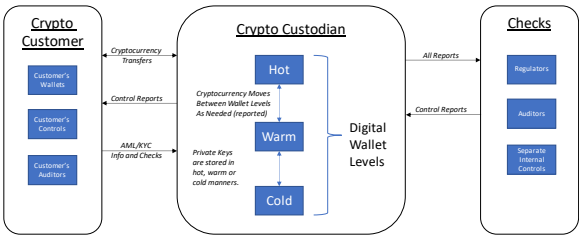
May 1, 2023
John Roy
john@watertowerresearch.com
973-666-2172

KEY POINTS

- **Following the bankruptcy of FTX and Alameda Research**, it is important to understand how security in crypto custody and trading works.
- **In crypto security, particularly by custodians, multiple levels of security should be implemented**, including physical cold storage, stock exchange level processes, multiple signature wallets, and two-factor and video authorization.
- **Trust is a key component of custody and trading.** Given the newness of the crypto market, many investors are relying heavily on government authorities to (1) outline what is appropriate and (2) certify and license those companies that have all the necessary elements. Some expect the SEC's upcoming rules to make it harder for crypto companies to become qualified custodians.
- **There are three vendors (Bakkt, Coinbase, and NYDIG)** that have both custody and trading security licenses from government authorities like the New York State Department of Financial Services (NYDFS), the Massachusetts Division of Banks (DOB), the Commodity Futures Trading Commission (CFTC), and the Derivatives Clearing Organization (DCO).
- **According to Markets and Markets, the crypto custody market is estimated to be worth $223 billion as of January 2022**, up from $32 billion in January 2019. Through 2028, estimates have it growing at a CAGR of 26.7%.
- **The growth of the market can be attributed to** the increasing adoption of cryptocurrencies by institutional investors, the rising demand for secure and compliant crypto custody solutions, and the development of new technologies in the crypto industry.
- **Tech Talk consists of short discussions of the technical issues surrounding a technology investing topic.** See previous editions of Tech Talk and other technology reports here.

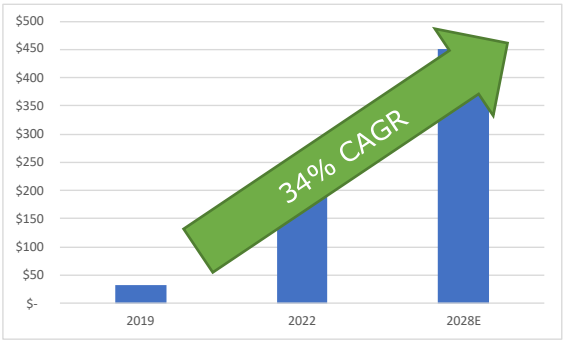
STATISTICS

Crypto Custodian Diagram



Source: WTR

Crypto Custody Market



Source: Markets and Markets, WTR

What is Crypto Custody?

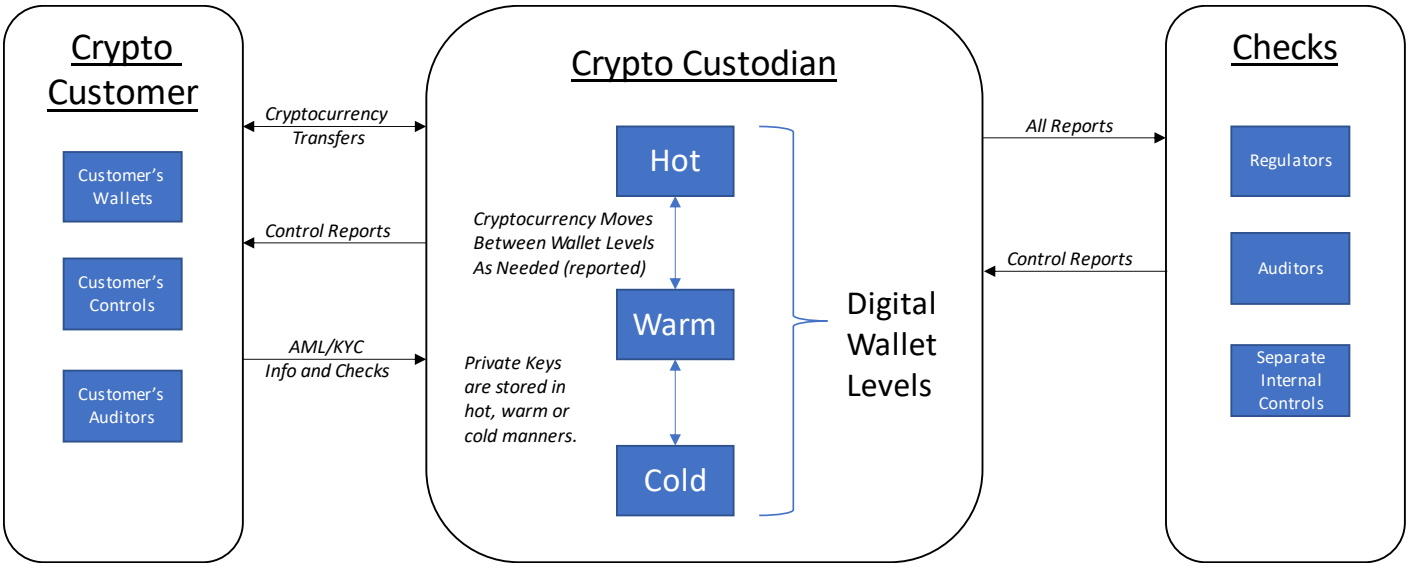
Stock or securities custody is the practice of holding and maintaining ownership of stocks on behalf of clients. It is typically performed by a custodian bank or trust company. Services include safekeeping of the stocks/securities, settlement of trades, handling dividends, and reporting transactions.

Crypto custody is similar to stock custody but with cryptocurrencies and digital assets. It is a fundamental service needed to invest in cryptocurrencies and includes some substantial technical challenges compared with traditional custody. Generally, a specialist in crypto with a team of experienced experts in digital security and compliance is used to meet these challenges.

Some key factors to consider when assessing a third-party crypto custody company are:

1. A strong security track record.
2. Deep expertise in private key management
3. Significant experience being a financial firm dealing with all applicable laws and regulations.
4. A broad set of reporting capabilities.
5. Cost of the services.

Figure 1: Crypto Custodian Diagram



Source: WTR

Typical services include the following:

- **Cold storage** is the process of storing cryptocurrency wallet private keys offline in a secure location. This is the most secure way to store cryptocurrency, as it is not connected to the Internet and is therefore not vulnerable to online attacks.
- **Warm storage** is the process of storing cryptocurrency wallet private keys online in a secure location that is accessible. However, humans need to sign the transaction and send it to the blockchain.
- **Hot storage** is the process of storing cryptocurrency wallet private keys online in a secure location. This is less secure than cold storage, as it is connected to the Internet and is therefore vulnerable to online attacks. However, it is more convenient, as it allows users to access their cryptocurrency more easily.
- **Multi-signature wallets** are wallets that require multiple signatures from different private keys to authorize transactions. This makes it more difficult for hackers to steal funds, as they would need to obtain multiple signatures from different people.

- **Compliance** is the process of ensuring that a company or organization complies with all applicable laws and regulations. This is important for cryptocurrency companies, as there are several regulations that apply to the cryptocurrency industry, including Know Your Customer (KYC), Anti-Money Laundering (AML), travel rule, and Know Your Transaction (KYT).
- **Reporting** is the process of generating reports on cryptocurrency transactions. This is important for cryptocurrency companies, as they need to be able to track their transactions and comply with reporting requirements.

These services generally come with 24/7 support, institutional-grade security, full compliance and regulatory oversight, and auditing.

How Does Crypto Custody Differ from Other Custody Services?

Crypto custody differs from other custody services in a few key ways:

- **Security.** Crypto custody is a highly specialized field and crypto custodians must take extra measures to protect their clients' funds. They use a variety of security measures, such as cold storage, multi-signature wallets, and biometric authentication.
- **Regulation.** Crypto custody is a relatively new field and there is still some uncertainty about how it should be regulated. However, the industry is slowly coming under the purview of financial regulators, which will provide greater legitimacy and protection for clients.
- **Transparency.** Crypto custody is a complex field and it can be difficult for clients to understand exactly what their custodian is doing with their funds. Crypto custodians should be transparent about their security practices, fees, and compliance with regulations.

How Is Crypto Custody Evolving?

As cryptocurrency is changing, as well as its regulation, crypto custody is keeping pace. The maturation process of any new technology can take years and cryptocurrencies are not special. Institutional investors are moving in and out of the market. Below are some trends in crypto custody:

- **The rise of institutional investors.** Institutional investors are increasingly looking to invest in cryptocurrencies, but they require a high level of security and compliance. This is driving the demand for institutional-grade crypto custody services.
- **The development of new technologies.** New technologies, such as blockchain and distributed ledger technology, are driving the need for new and innovative crypto custody solutions. These technologies offer several advantages, such as greater security and transparency. Consider Multi-Party Computation (MPC) technology, which is a cryptographic technique that allows multiple parties to jointly compute a function of their private inputs, without revealing any of their private data to other parties. This makes it an ideal solution for securing private keys in the crypto custody space.
- **The increasing regulation of the crypto industry.** The crypto industry is increasingly coming under the purview of financial regulators. This is leading to greater legitimacy and protection for investors, and it is also driving the development of new regulations and standards for crypto custody.

How Big Is the Market?

According to Markets and Markets, the crypto custody market is estimated to be worth $223 billion as of January 2022, up from $32 billion in January 2019. Through 2028, estimates have it growing at a CAGR of 26.7%. The growth of the market can be attributed to the increasing adoption of cryptocurrencies by institutional investors, the rising demand for secure and compliant crypto custody solutions, and the development of new technologies in the crypto industry.

The institutional investors segment is expected to account for the largest share of the market. This is driven by the increasing adoption of cryptocurrencies by institutional investors for investment purposes. The demand for secure and compliant crypto custody solutions is also expected to drive the growth of the market. The Asia-Pacific region is expected to exhibit the highest CAGR.

What are Regulatory Issues?

The crypto custody regulatory landscape is rapidly changing and is likely to get more complex. Expertise and experience in regulatory markets are key. Some of the key regulatory issues in crypto custody include:

- **Compliance.** Crypto custodians must comply with a variety of regulations, including AML and KYC regulations. These regulations require custodians to identify and verify their customers, and to monitor their transactions for suspicious activity.
- **Transparency.** Crypto custodians should be transparent about their security practices, fees, and compliance with regulations. This will help to build trust with their clients and to ensure that they are following best practices.
- **Interoperability.** Crypto assets are often stored on different blockchains and this can make it difficult for custodians to manage their clients' assets. There is a need for standards for interoperability between different blockchains, which would make it easier for custodians to manage their clients' assets.
- **Separation.** The provider has separated its custody entity from its exchange and provides separate custody services for institutional customers.
- **Security.** Digital assets are vulnerable to theft and fraud, and crypto custodians must take extra measures to protect their clients' assets. This includes using a variety of security measures, such as cold storage, multi-signature wallets, and biometric authentication.

US regulations are different from the rest of the world, particularly as it has several key agencies affecting the regulatory landscape, including the Securities and Exchange Commission (SEC), the CFTC, and the Financial Crimes Enforcement Network (FinCEN). These regulations require cryptocurrency exchanges and other businesses to register with the government, comply with AML and KYC regulations, and report suspicious activity.

Most other countries have different regulations, but some countries have no regulations at all. This can make it difficult for businesses to operate in multiple countries and it can also make it difficult for investors to know which countries are safe to invest in.

The US is generally seen as having more stringent regulations than other countries and this is one of the reasons why the US is a leader in the cryptocurrency industry. The strict regulations help to protect investors and ensure the long-term success of the industry.

Who are Some Leading Vendors?

Crypto custody is provided by vendors that have both trading and custody licenses.

Bakkt (BKKT)

Bakkt's approach to custody encompasses several layers of protection and risk management that are intentionally designed to minimize the ability for anyone to bypass process controls or access private keys.

From a physical perspective, as much Bakkt-custodied crypto is placed in cold storage as possible and the keys are held in a bank-grade vault across multiple secret locations, protected by guards and biometric security features. The company generates all its custodied wallets completely offline and only brings what is necessary for trading volumes online. Funds are divided between warm and cold storage, with limits to how much can be stored in each type and within each individual wallet.

Most funds are stored in deep cold storage. For example, when a consumer utilizing the Bakkt platform purchases Bitcoin, that Bitcoin is acquired and stored on a 1:1 basis in the company's cold wallet. Bakkt has the exact amount of crypto that was acquired by a customer within its vault.

From a process perspective, Bakkt has built-in additional process and technical controls. It utilizes a secure multi-signature structure for all wallets. This means that several private keys are required to enable the transfer of funds. In addition, the system requires that multiple participants give approval before a private key can even be accessed for signing. The architecture of broader blockchain design doesn't always allow multi-sig in the same way that Bitcoin does. For example, other networks like ETH require smart contacts to achieve multi-sig functionality, but Bakkt has built a distinct approach where it also follows a multi-sig approach for ether.

Once crypto currency is in Bakkt's cold storage, the company takes additional precautions to reduce the risk of unauthorized access. The crypto can only be sent from Bakkt cold storage to the company's warm wallets, preventing anyone from sending it to an external wallet. From Bakkt's pre-approved warm wallets, assets can only be withdrawn and sent to a previously authorized wallet address that has been formally approved by a customer. The process for authorizing wallet addresses with customers includes 2FA and video authorization among other controls.

As a public company, Bakkt is subject to in-depth audits from regulators and leading third-party audit firms. It also must prove the function and operation of its processes and authority structure. The company continually reviews access permissions to the custody platform to validate that only authorized staff can perform required functions based on their role. It regularly performs code reviews and penetration testing against the custody platform to determine if there are any flaws that could result in misuse of the platform.

Bakkt's custody entity also maintains a separate Governance Board. The Bakkt Trust Board is solely focused on the safe and effective operation of Bakkt's crypto custody operations as a separate, regulated entity. The Bakkt Trust Company is regulated by the NYDFS and is separate from the operating entity so that consumer funds are segregated from the rest of the business.

Bakkt holds several licenses that allow it to operate in the cryptocurrency space, including:

- **New York State Department of Financial Services (NYDFS) Virtual Currency License.** This license allows Bakkt to provide custody and execution services for Bitcoin and other cryptocurrencies.
- **Massachusetts Division of Banks (DOB) Trust Charter.** This charter allows Bakkt to provide trust services for Bitcoin and other cryptocurrencies.
- **State of Wyoming Division of Banking (DOB) Trust Charter.** This charter allows Bakkt to provide trust services for Bitcoin and other cryptocurrencies.
- **Commodity Futures Trading Commission (CFTC) Derivatives Clearing Organization (DCO) Registration.** This registration allows Bakkt to clear and trade Bitcoin futures contracts.
- **Financial Industry Regulatory Authority (FINRA) Member Firm Registration.** This registration allows Bakkt to act as a broker-dealer and provide investment advice to clients.

Coinbase (COIN)

Coinbase Custody offers features that make it a secure option for storing crypto assets, including:

- **Physical security.** Coinbase Custody stores its crypto assets in cold storage, which means that it is not connected to the Internet and therefore much more difficult to hack.
- **Audits.** Coinbase Custody undergoes regular audits by independent security firms to ensure that its security measures are up to date and effective.
- **Insurance.** Coinbase Custody's crypto assets are insured for up to $320 million in the event of theft or loss.
- **Compliance.** Coinbase Custody is a regulated custodian and is subject to security and compliance requirements.

Coinbase takes steps to ensure the security of its users' crypto assets, including:

- Coinbase stores 98% of its crypto assets in cold storage, which means that it is not connected to the Internet and therefore much more difficult to hack.
- Coinbase uses a variety of security measures to protect its users' accounts, including two-factor authentication, IP address whitelisting, and device verification.
- Coinbase has a team of security experts who are constantly working to identify and mitigate security risks.
- Coinbase is a regulated financial institution and is subject to security and compliance requirements.

Coinbase holds licenses that allow it to operate in the cryptocurrency space, including:

- **New York State Department of Financial Services (NYDFS) BitLicense.** This license allows Coinbase to provide a variety of cryptocurrency services, including trading, custody, and lending.
- **Money Transmitter Licenses.** Coinbase holds money transmitter licenses in more than 40 states in the US.
- **Electronic Money Institution (EMI) License.** Coinbase holds an EMI license in the European Union.
- **Payment Institution (PI) License.** Coinbase holds a PI license in the United Kingdom.

Coinbase provides its users with a secure and compliant platform to buy, sell, and trade cryptocurrencies. In addition to the licenses listed above, Coinbase is also a member of several industry organizations, including the Cryptocurrency Security Standards Council (COSS), the Blockchain Association, and the Global Digital Finance (GDF).

NYDIG (Private)

NYDIG is a Bitcoin company that provides custody, execution, and financing solutions for institutional investors. NYDIG's custody solution is designed to meet the needs of institutional investors by providing a secure, compliant, and scalable platform for storing Bitcoin. NYDIG's custody solution offers features that make it a secure and reliable option for storing Bitcoin, including:

- **Physical security.** NYDIG stores its Bitcoin in cold storage, which means that it is not connected to the Internet and therefore much more difficult to hack.
- **Audits.** NYDIG undergoes regular audits by independent security firms to ensure that its security measures are up to date and effective.
- **Insurance.** NYDIG's Bitcoin is insured for up to $100 million in the event of theft or loss.
- **Compliance.** NYDIG is a regulated custodian and is subject to several security and compliance requirements.

NYDIG's custody solution is targeted institutional investors who are looking for a secure and reliable way to store Bitcoin. NYDIG's custody solution offers features that make it a secure and reliable option, including physical security, audits, insurance, and compliance. NYDIG's execution solution allows institutional investors to buy, sell, and trade Bitcoin on a variety of exchanges. The company's financing solution also allows institutional investors to borrow against their Bitcoin holdings.

NYDIG takes steps to ensure the security of its users' crypto assets, including:

- NYDIG stores 99% of its crypto assets in cold storage, which means that it is not connected to the Internet and therefore much more difficult to hack.
- NYDIG uses a variety of security measures to protect its users' accounts, including two-factor authentication, IP address whitelisting, and device verification.
- NYDIG has a team of security experts who are constantly working to identify and mitigate security risks.
- NYDIG is a regulated financial institution and is subject to security and compliance requirements.

NYDIG holds several licenses that allow it to operate in the cryptocurrency space, including:

- **New York State Department of Financial Services (NYDFS) Virtual Currency License.** This license allows NYDIG to provide custody and execution services for Bitcoin and other cryptocurrencies.
- **Massachusetts Division of Banks (DOB) Trust Charter.** This charter allows NYDIG to provide trust services for Bitcoin and other cryptocurrencies.
- **State of Wyoming Division of Banking (DOB) Trust Charter.** This charter allows NYDIG to provide trust services for Bitcoin and other cryptocurrencies.

By holding several licenses, NYDIG can operate in a compliant manner and provide its clients with the confidence that they need to invest in Bitcoin and other cryptocurrencies.

ABOUT THE ANALYST

John Roy
Managing Director

Prior to Water Tower Research, John worked as a lead analyst at UBS, covering IT Hardware, Communications Equipment, and IT Services. During his 20 years covering technology stocks on the sell-side, he was also a lead analyst covering IT Hardware and Nanotechnology at Merrill Lynch; and Alternative Energy, Advanced Materials and Nanotechnology at W.R. Hambrecht, and at Janney Montgomery Scott. Before his sell-side equity research career, John was a lead software architect at J.P. Morgan, an AI sales engineer at Neuron Data, and a systems engineer and AI researcher at Hughes Aircraft.

John holds a Ph.D. in Computer Science from the University of California, Irvine, a MSEE degree from the University of Southern California, and a BSEE degree from the University of California, San Diego where he was a Regents Scholar.

DISCLOSURES

Water Tower Research ("WTR") is a professional publisher of investment research reports on public companies and, to a lesser extent, private firms ("the Companies"). WTR provides investor-focused content and digital distribution strategies designed to help companies communicate with investors.

WTR is not a registered investment adviser or a broker/dealer nor does WTR provide investment banking services. WTR operates as an exempt investment adviser under the so called "publishers' exemption" from the definition of investment adviser under Section 202(a)(11) of the Investment Advisers Act of 1940. WTR does not provide investment ratings / recommendations or price targets on the companies it reports on. Readers are advised that the research reports are published and provided solely for informational purposes and should not be construed as an offer to sell or the solicitation of an offer to buy securities or the rendering of investment advice. The information provided in this report should not be construed in any manner whatsoever as personalized advice. All users and readers of WTR's reports are cautioned to consult their own independent financial, tax and legal advisors prior to purchasing or selling securities.

The analyst who is principally responsible for the content of this report has represented that neither he/she nor members of his/her household have personal or business-related relationships to the subject company other than providing digital content and any ancillary services that WTR may offer.

Unless otherwise indicated, WTR intends to provide continuing coverage of the covered companies. WTR will notify its readers through website postings or other appropriate means if WTR determines to terminate coverage of any of the companies covered.

In certain instances, including this report, WTR will write research covering non-clients. Readers should assume that WTR may seek to turn these non-paying companies into paying clients. Likewise, WTR may seek to transform these non-clients into paying clients of it or of its affiliate, which provides services such as presenting at sponsored investor conferences, distributing press releases, advising on investor relations and broader corporate communications and public relations strategies as well as performing certain other related services ("Ancillary Services"). The companies that WTR covers in our research are not required to purchase or use Ancillary Services of WTR or an affiliate might offer to clients.

The manner of WTR's potential research compensation and Ancillary Services to covered companies raise actual and perceived conflicts of interest. WTR is committed to manage those conflicts to protect its reputation and the objectivity of employees/analysts by adhering to strictly written compliance guidelines.

The views and analyses included in our research reports are based on current public information that we consider to be reliable, but no representation or warranty, expressed or implied, is made as to their accuracy, completeness, timeliness, or correctness. Neither we nor our analysts, directors, officers, employees, representatives, independent contractors, or agents shall be liable for any omissions, errors, or inaccuracies, regardless of cause, foreseeability, or the lack of timeliness of, or any delay or interruptions in the transmission of our reports to content users. This lack of liability extends to direct, indirect, incidental, exemplary, compensatory, punitive, special, or consequential damages, costs, expenses, legal fees, losses, lost income, lost profit, or opportunity costs.

All investment information contained herein should be independently verified by the reader or user of this report. For additional information, all readers of this report are encouraged to visit WTR's website www.watertowerresearch.com.