KPMG

Cracking crypto custody

Custody businesses founded on four key building blocks will be poised for growth in the expanding crypto ecosystem

kpmg.com

The crypto winter came. Now, the spring thaw has arrived, and the incredible innovation in bloom may propel the $200+ billion cryptoasset class into the trillions.

The improving performance, scalability, privacy and interoperability of the blockchain infrastructure—which enables crypto transactions—is driving the increasing tokenization of traditional assets and enticing institutional investors and large pension funds to grow their allocations and positions in cryptoassets. [1, 2]

To drive growth in the new crypto economy, many traditional custodians and crypto-native startups are looking to develop capabilities to engage with cryptoassets owners, requiring them to build or buy custody solutions designed to meet their specific needs. However, the technical and operational requirements of cryptoasset custody, security and exchange create unique challenges for enterprises looking to transform.

This paper uncovers four critical building blocks of winning crypto custody models: next-gen security and resilience, comprehensive compliance, third-party trust, and value-added custody.

Both custodians of traditional assets and emerging crypto custody businesses will gain clear and pragmatic advice for integrating these building blocks into their custody solutions in order to profit from the surge of investors entering the crypto waters.

KPMG

Crypto custodians have tremendous growth potential

In the broad financial ecosystem, cryptoassets are no longer an exotic instrument, bit player, or side show. There is broad market acceptance that permissionless blockchains, native tokens, and cryptoassets will enable robust new ecosystems of commerce and trade.

Although once firmly rooted in the jurisdiction of fringe retail investors, cryptoassets are now attracting the attention of institutional investors. As they increasingly compete for investment dollars against legacy asset classes, traditional financial institutions are reading the signs. Major banks, asset managers, broker/dealers, qualified custodians, exchanges, fintechs, and others are joining upstart entrants in launching a new wave of institutional grade crypto products and services. These innovations are spurring the rise of a tokenized economy made up of natively digital assets.[3,4]

This expanding crypto ecosystem is poised to alter the financial services landscape as we know it. But it's also complex and in a continued state of disruption. As financial institutions consider new business models to capitalize on the rise of crypto, where should they place their bets?

As the crypto economy continues to accelerate and mature, one area stands out as a critical core capability: custody.

Custody—the management of the cryptographic private keys that cryptoasset owners use to execute transactions—is a critical building block for crypto institutionalization. It is fundamental to earning customer trust in cryptoassets and allowing the market to scale. As cryptoassets proliferate, custodians have a tremendous opportunity to profit—both by earning management fees for delivering straightforward custodian services, and also by offering adjacent services only possible in the emerging crypto ecosystem.

To fully appreciate the opportunity, just consider the simplest economics. Demand is surging: Every new participant in the market needs a way to safely store and move their cryptoassets; institutional investors, especially, will not risk owning cryptoassets if their value cannot be safeguarded in the same way their cash, stocks and bonds are. And supply is short: There are only a few established financial institutions currently offering institutional custody services to crypto investors and it remains to be seen if crypto custody offerings by dozens of specialized service providers are truly ready for institutional-grade investments.

Every new participant in the market needs a way to safely store and move their cryptoassets; institutional investors, especially, will not risk owning cryptoassets if their value cannot be safeguarded in the same way their cash, stocks and bonds are.

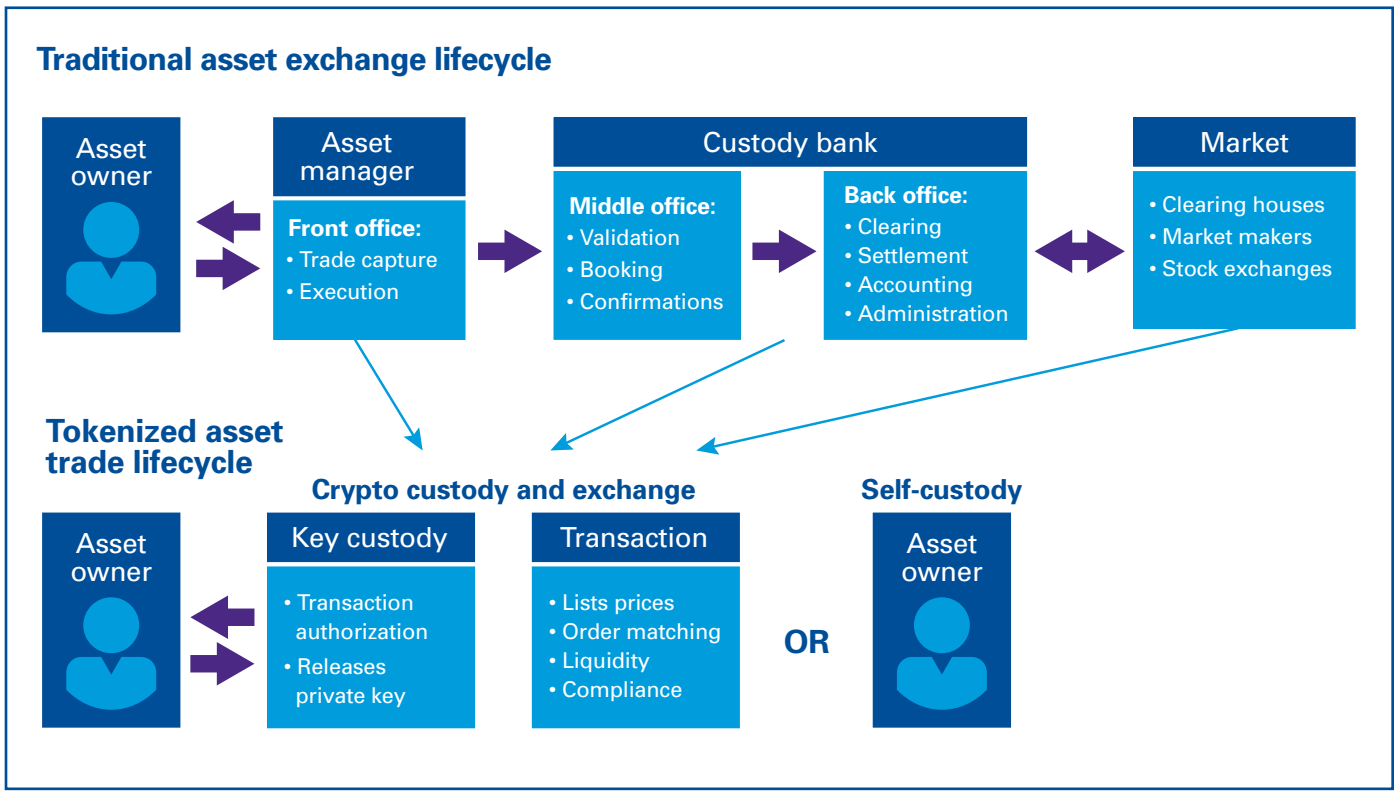
Evolving custody models for crypto customers

So why hasn't anyone completely cracked crypto custody? Because custody of cryptoassets is fundamentally different than custody of traditional financial assets.

Cryptoassets are a unique kind of bearer instrument. Traditional bearer instruments, such as cash and certain types of bonds, are issued in physical form to the purchaser. Unlike registered assets—which account for most securities issued today—no ownership records exist. That means whoever holds the physical asset is presumed to be its owner.

Crypto assets expand the definition of bearer instruments to a new digital frontier. On a blockchain network, control of cryptoassets resides with the holder of a cryptographic private key which unlocks a public key wallet address used to execute transactions and move assets, or tokens, on the network. Custodians maintain ownership rights for those private key holders with internal custody systems of record

Figure 1:



The ownership and control model for cryptoassets marks a significant departure from traditional assets, and therefore has major implications on how they should be custodied.

Evolving custody models for crypto customers

(continued)

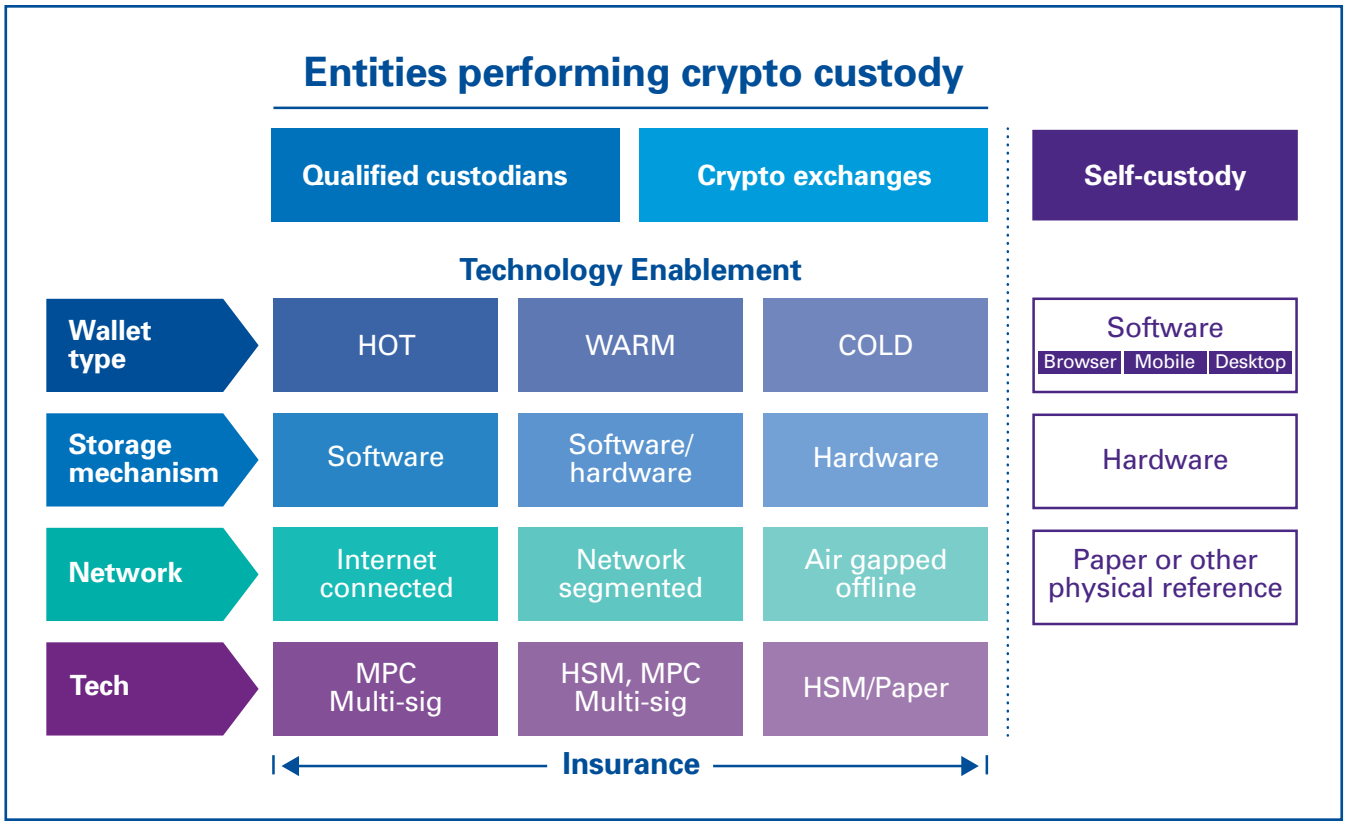
Types of crypto custody

Qualified custodians[5] deliver fully-managed custody services to institutions that own and trade cryptoassets. Traditionally, qualified custodians are banks or trusts that are chartered by a regulatory body (e.g., New York Department of Financial Services, South Dakota Division of Banking) to operate on an institutional scale and are subject to specific regulatory requirements for infrastructure, governance and controls. Qualified custodians maintain control of private keys as part of their role alongside record of asset ownership. The formal definition of and requirements for qualified custodians of cryptoassets is still evolving.

Crypto exchanges offer digital wallets to hold and protect cryptoassets while making them available for asset exchange through a central order book and matching engine. They cater mostly to retail investors, traders and private investment funds and typically offer additional services beyond cryptoasset storage—namely trading.

Self-custody solutions are in-house or commercial off-the-shelf software and hardware solutions that store and protect cryptoassets. Building or buying these solutions gives owners complete control of their cryptoassets. But with no third-party intermediary, cryptoasset owners are solely responsible for their assets and may have no ability to retrieve lost cryptoassets.

Figure 2:



Why are these building blocks so critical?

- Cryptoasset hacks have resulted in $9.8 billion in losses since 2017.
- Compliance failures have stripped crypto businesses of the licenses they need to operate.[6]
- The world's first external audit of a crypto custodian is complete, setting a new industry standard.[7]
- Crypto competitors are already expanding their service offerings in innovative ways to drive value for customers.[8]

Four building blocks of institutional-grade crypto custody

Custody solutions must evolve to better meet the unique needs of cryptoasset owners—especially at the institutional level. But what makes for best-in-class crypto custody capabilities across the solution and service landscape? What should financial sector business and technology leaders prioritize as they reshape existing custody capabilities or develop new business models around crypto custody?

We believe crypto custody capabilities founded on **four key building blocks** will be best positioned to meet institutional needs and seize the incredible opportunity in the custody space. Whether institutions build custody solutions from scratch, transform existing custody solutions for non-digital assets, or contract with a third-party custody service provider, these are the building blocks business and technology leaders should emphasize as they enter the crypto custody business. We'll explore each in the following pages:

1 **Next-gen security and resilience**

2 **Comprehensive compliance**

3 **Third-party trust**

4 **Value-added custody**

Four building blocks of institutional-grade crypto custody

(continued)

1 Next-gen security and resilience

Many cryptoasset transactions are executed on public blockchains, which have no central management or governance in place. Transactions executed on public blockchains are final: Without trusted intermediaries to capture, confirm, clear, settle, and account for the transaction, there is no recourse for owners to recover an underlying asset once it has changed hands.

The finality of public blockchain transactions significantly raises the stakes for custodians in charge of safeguarding private keys controlling cryptoassets. With no central authority, the risk of loss to crypto participants is enormous: Since 2017, hacks and compromises of cryptoassets native to public blockchains have resulted in at least $9.8 billion in losses (see figure 3, page 10) at current valuations, and that doesn't account for losses that haven't been revealed to the public. And the risk becomes even greater on an institutional scale, compelling crypto custodians to obtain extensive and costly insurance policies. The insurance landscape for crypto coverage is evolving and asset coverage has implications for how custodians manage assets across their wallet tiers.

Since 2017, hacks and compromises of cryptoassets native to public blockchains have resulted in at least $9.8 billion in losses (see figure 3) at current valuations.

Crypto custodians can't tackle security at scale for the tokenized economy by creating webs of controls and physical isolation. Instead, crypto custodians are challenged to deliver enhanced security without sacrificing transaction processing speed and resilience—both areas crypto customers typically value to an even greater degree than owners of traditional financial assets due to the 24/7 nature of cryptoasset exchanges, persistent malicious actors, and continued market volatility.

In context of these challenges, organizations are building tiered wallet architectures to minimize risk exposure of assets under custody. Advanced cryptographic mechanisms, including multi-party computation (MPC)-based solutions, are being integrated to custody capabilities, building on multi-signature (multi-sig) wallets, hierarchical deterministic (HD) wallets and key sharding approaches (i.e. Shamir's Secret Sharing-SSS). Increasingly, secure storage architectures can deliver speed and resiliency at scale to support requirements for high throughput in payments, high frequency trading, and other retail applications.

Modern security operations for crypto custody integrate industry-standard controls and processes for cybersecurity and cryptographic key management—including NIST 800-53 and NIST 800-57—which were designed to support federal government information systems and cryptographic operations. There are also established cryptographic security certifications which test and validate security controls against defined federal standards (i.e. Federal Information Processing Standard-FIPS 140-2). These approaches, which were originally designed to standardize the secure use of cryptography to protect data, are now applied to protect private keys which control cryptoassets. Robust security and resiliency will be table stakes for custody models of the future—especially for organizations aiming to serve institutions as qualified custodians.

However, current industry standards only provide a foundation. The crypto ecosystem is evolving at an incredible rate. The security ecosystem is under pressure to keep pace by enhancing standards designed for the Web 2.0 data era to secure the Web 3.0 era of value and governance. Today, researchers from academia and industry are developing innovative processes and technologies—including cutting-edge software and dedicated physical hardware—to more securely and efficiently custody cryptoassets. New leading solutions are being designed around principles of decentralization, resiliency, and "zero knowledge systems" in which participants in cryptographic processes have no information beyond what's required to execute their individual function, thereby reducing risks of a single point of failure.

So how do crypto custodians ready their security operations for the future? Successful crypto custody businesses will embrace the leading cryptographic techniques to enhance the security and resiliency of custodied cryptoassets, and focus on building customer trust through efficient and timely transaction processing. This includes developing the skills and capabilities required to both assess and design leading-edge operational and technical control environments around custody models, whether by investing in internal hiring and training or by turning to experienced advisors for guidance and support.

The crypto ecosystem is evolving at an incredible rate. The security ecosystem is under pressure to keep pace by enhancing standards designed for the Web 2.0 data era to secure the Web 3.0 era of value and governance.

Four building blocks of institutional-grade crypto custody

(continued)

Figure 3

Major hacks and compromises of crypto asset exchanges

Hack	Value (Crypto)	Value (USD at time of attack)	Value (USD as of January 7, 2020)	Attack Vector	Potential security/ mitigation approach
Mt Gox (2011 – 2014)	850K BTC[9]	680 Million[10]	6.9 Billion[10]	Online accessible hot wallet, unencrypted private key[9]	Tiered storage approach with limited fund exposure to hot wallets
Bitfloor (2012)	24K BTC[11]	250 Thousand[11]	195 Million[10]	DDOS/power failure to exchange server, unencrypted backup key[11]	Tiered storage approach, limited fund exposure to hot wallet, encrypted backup keys
Poloniex (2014)	97 BTC[12]	116 Thousand[12]	790 Thousand[10]	Simultaneous withdrawal requests; no queuing utilized[12]	Implement a queuing and sequence process for all transactions and order methods
Cryptsy (2014)	13K BTC, 300K LTC[13]	9.5 Million[13]	120 Million[10]	Simultaneous withdrawal requests via Trojan Horse placed in a vulnerable server	Secure code reviews, queuing and sequentially processing withdrawals, tolerance/balance checks
Bitstamp (2014)	19K BTC[14]	5.2 Million[14]	155 Million[10]	Phishing attack[14]	Email filters, lock-down communication channels, education and awareness
Bittfinex (2016)	120K BTC[15]	66 Million[15]	978 Million[10]	Software bug in multi-signature wallet solution[15]	Limit exposure of funds to hot wallets, recovery through second key
DAO (2016)	3.6mm Ether[16]	70 Million[16]	522 Million[10]	Smart contract bug[16]	Robust smart contract/ DApp source code review and testing procedures
BitGrail (2018)	17mm Nano[17]	195 Million[17]	11 Million[10]	Exchange software vulnerabilities exploited[17]	Software security testing and review
Coincheck (2018)	523mm NEM[18]	500 Million[18]	15 Million[10]	Funds stored in hot wallet without multi-sig configuration[18]	Tiered storage, multi-sig protection
Bithumb (2018)	Not Disclosed[19]	31 Million[19]	N/A – Asset not disclosed	Exchange hacked after security update, possible phishing attacks[19]	Tiered storage solution, improved cyber security governance, increased security education and awareness
Binance (2019)	7K BTC[20]	40 Million[20]	57 Million[10]	Phishing attacks, viruses[20]	Additional verifications for suspicious and/or large asset transfers

2 Comprehensive compliance

Financial services is one of the most heavily regulated industries. So it's little surprise that in most jurisdictions, organizations that deliver custody products and services for digital assets must comply with certain regulatory requirements. In addition, cryptoassets are becoming widely used mediums of value exchange across e-commerce, which has been covered in the media due to illicit activities and enforcement actions.

Some regulatory challenges facing crypto custodians are an extension of those facing traditional institutional custody providers. For example, one of the biggest compliance hurdles for crypto custodians is Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations, which require custodians to assess asset provenance and monitor transactions for potentially suspicious activity. Similarly, the Financial Action Task Force (FATF), an intergovernmental organization, recently extended guidance based on the Bank Secrecy Act's Travel Rule to apply to crypto institutions, proposing that cryptoasset institutions share customer information when they transfer funds between firms.

Financial services regulatory compliance is data-intensive, requiring extensive infrastructure and robust processes. But when applied to cryptoassets, they become more so. Even established financial institutions which already have mature AML and KYC compliance programs in place are challenged to enhance their methodologies to address the unique considerations for cryptoassets and related data management challenges. Two of these challenges include foundational aspects of KYC and AML: determining customer asset provenance and meeting transaction monitoring requirements.

Commercially available blockchain analytics tools are able to assist KYC and AML teams with addressing these foundational aspects. However, organizations will still have to build defensible risk-based programs including detailed policies and procedures that explain *why* and *how* their programs will detect potentially suspicious activity.

Another challenge is the regulatory push to implement licensing requirements for qualified custodians of cryptoassets. Under the Custody Rule of the U.S. Registered Investment Advisers Act of 1940 and subsequent amendments, asset managers must custody client assets meeting certain conditions with qualified custodians—typically licensed banks, trusts or brokerdealers. However, the unique risks around cryptoasset security have triggered regulators around the world to redesign custody business licensing requirements to guarantee market integrity and investor protection without stifling financial innovation.

The risks of noncompliance are steep. Failure to meet licensing requirements have prevented some crypto companies from conducting business, such as Bittrex, which saw its license application denied by the New York State Department of Financial Services due to deficiencies in customer due diligence, transaction monitoring and compliance department staffing.[21]

Four building blocks of institutional-grade crypto custody

(continued)

Further adding complexity is the fact that the regulatory environments affecting crypto custody businesses vary greatly from one jurisdiction to the next. Differences in rules at the state, national and international level are creating substantial compliance challenges for global financial institutions that deliver custody solutions. For example, regulators in the nations of Malta and Gibraltar and the U.S. states of Wyoming and New York all recently passed different rules regulating institutions performing custody, exchange and other services for cryptoassets. Although cryptoassets are global in nature and their risks are clearly best managed across jurisdictions, a consistent, coordinated and interoperable global regulatory framework is still on the distant horizon.

For crypto custodians trying to manage this regulatory complexity, an informed and detailed view of the changing regulatory landscape is paramount. Given the steep variation in the clarity and nature of different regulatory environments, decisions based on existing law and policy should be carefully calculated, weighing the risks and benefits of each course of action.

We recommend looking forward at product and capability road maps to see how evolving regulations may apply to current and future business activities. Crypto custodians that watch for trends and signals in the market to anticipate regulatory change will be better prepared to strategically align their future compliance operations. Meanwhile, those that proactively engage policymakers and legislators can actually help guide the development of effective regulatory structures that both foster the innovation on which their businesses rely and protect investors and market integrity.

Crypto custodians that watch for trends and signals in the market to anticipate regulatory change will be better prepared to strategically align their future compliance operations.

3 Third-party trust

Given concerns about the risks of cryptoassets, many financial institutions have been cautious about transforming their business models to serve the growing number of crypto users. For this reason, third-party trust is essential to the growth of the crypto economy. It will also be integral to the success of the custody businesses that support it.

Third-party trust is supported by independent reviews including attestation and certification. Engaging in these assessments is necessary for crypto custodians to earn the trust and business of cryptoasset owners. Third-party trust is critical for crypto businesses—especially qualified custodians operating on an institutional scale. Without independent reviews, cryptoasset owners have limited ways to evaluate which custody services will best protect and manage the owner's assets to suit their business needs.

In addition, Gemini recently became the world's first crypto business to complete an in-depth external review of its security compliance capabilities, further raising the bar for the industry.[22]

For custodians serving traditional financial institutions or publicly-traded companies in the U.S., third-party attestation is typically delivered through System and Organization Controls (SOC) examinations[23], which are used by asset owners to assess and monitor service providers. SOC reports provide assurance on the design, implementation and/or operating effectiveness of internal controls over financial reporting (SOC1) as well as information relating to technology security, availability, processing integrity, confidentiality and privacy (SOC2). Similarly, established security certifications, such as the U.S. Federal Information Processing Standard (FIPS) 140-2, and security control frameworks, such as NIST 800-53 and ENISA, serve as baselines for third-party security audits. There is an extensive level of effort required to obtain and maintain current certifications and compliance with these certifications and frameworks.

Now, leading accounting, auditing and information security standards organizations are actively working to apply existing third-party attestation, assurance and certification approaches to crypto custody business models. SOC report guidelines are in the process of being reviewed specifically for blockchain-related platforms, including cryptoasset custodians, which may identify additional risks for consideration by management and service auditors. Management of crypto custodian organizations will be responsible for the determination of controls to mitigate these identified risks.

The winning custodians of the future will invest in control environment optimization and rationalization to mature and meet third-party requirements, helping competitively differentiate their crypto custody services. Similarly, custody providers will benefit from having high standards for service providers that are critical to building trust in their business. For service providers, this may require investments in new risk and governance talent who possess the expertise to design and implement comprehensive control environments for cryptoasset custody platforms. These new resources can augment existing skill sets in risk and audit functions to perform risk-based assurance work.

4 Value-added custody: What's next in crypto custody

In the next few years, next-gen security and resilience, comprehensive compliance, and third-party trust will differentiate successful crypto custody businesses from the pack. But looking further ahead, even best-in-class crypto custody models that embrace these foundational elements will almost certainly become commoditized. Such is the nature of technology-based solutions in today's dynamic and sometimes volatile business world.

But that doesn't mean the prospects for crypto custody businesses will dim. Rather, crypto custody models present exciting opportunities for financial services companies to connect custody with adjacent front, middle and back office services that have traditionally operated in silos.

Many traditional qualified custodians offer services for their customers beyond safekeeping, ranging from fund administration to tax reporting, which also apply to crypto custody businesses. Custodians may initiate a number of process design and technology enablement activities to integrate these existing asset services into new crypto custody capabilities. It is important to have an effective integration strategy to connect cryptoasset custody capabilities and core asset services in a secure and compliant manner.

In addition, there are net new opportunities for crypto custody businesses to enable asset owner participation in permissionless blockchains to realize economic and strategic benefits. In traditional financial markets, owning a share of stock in a publicly traded company can give the investor the right to vote on certain aspects of governance in that company. Crypto markets are evolving to work much the same way: owning certain cryptoassets can give the owner the right to participate in the consensus model and governance of the public blockchain network. As such, network participation refers to the asset owner's ability to participate in activities on a public network which they are entitled to through ownership. Today, examples include participation in staking, a proof-of-stake consensus process to realize monetary rewards, and participation in the governance of a protocol through a voting process.

For example, Coinbase recently launched a new staking rewards program which gives its customers new ways to earn income on their cryptoassets.[24]

As blockchains evolve there will continue to be new opportunities for asset owners to participate in consensus processes, governance decisions, and other rights afforded to them. Crypto custodians that support customers in exercising their rights as asset owners and using their assets in custody to the greatest economic advantage will gain the competitive edge. They may also face requirements stemming from asset managers' fiduciary responsibilities to pursue revenue generating opportunities on behalf of asset owners. As such, winning crypto custodians will focus today on two fronts: building out core capabilities for secure, resilient and compliant custody capabilities, and keeping pace with rapid technical changes that may drive new revenue opportunities and future competitive advantages.

Winning crypto custodians will focus today on two fronts: building out core capabilities for secure, resilient and compliant custody capabilities, and keeping pace with rapid technical changes that may drive new revenue opportunities and future competitive advantages.

Advice for establishing winning crypto custody solutions

The institutionalization of cryptoassets is well underway, with new crypto custody models as an essential foundation. A necessary precursor for at-scale institutional engagement with the crypto economy, custody is fast becoming an exciting area of technological innovation and progress.

Yet, the magnitude of the business transformation required of traditional custodians to successfully operate and scale a crypto custody business is significant. Crypto-native startups face similar challenges as they look to establish institutional grade custody solutions for cryptoassets.

By starting with the four building blocks described in this paper, and keeping an eye on future revenue growth opportunities, both will be ready to seize the incredible opportunity in the crypto custody space.

These are key actions that cryptoasset custodians and aspiring organizations should start doing today to build a sustainable business model in this emerging financial ecosystem.

Next-gen security and resilience

– Design and enhance security operations and controls to provide layered defenses aligned to industry-standard frameworks

– Incorporate leading cryptographic techniques for cryptoasset security and availability, including multi-sig, sharding and MPC, and dedicated physical hardware (HSMs)

– Track emerging developments in cryptoasset security and develop the technical and operational agility to quickly embrace new innovations

Comprehensive compliance

– Optimize processes through a unified compliance program to comply with existing financial regulations, compliance requirements, and customer commitments

– Closely monitor regulatory changes across jurisdictions and develop a plan to rationalize future compliance operations with new rules

– Proactively engage with legislators and regulators to facilitate learning which drives an ecosystem defined by market integrity and investor protection

Third-party trust

– Implement and monitor a control environment to achieve attestation and security standards, including SOC reports, FIPS, NIST, and ENISA

– Stay abreast of updates to existing security frameworks under consideration by leading standard-setting organizations

– Proactively seek out independent auditors to help prepare for and execute third-party attestation and certification requirements

Value-added custody

– Develop a robust strategy to efficiently integrate front, middle and back office services into crypto custody capabilities to realize efficiency benefits across traditional silos

– Launch services that support customers in participating in consensus processes, governance decisions, and other rights afforded to cryptoasset owners

– Keep pace with rapid technical changes and think broadly about how they might drive future revenue opportunities

How KPMG can help

As adoption of crypto increases, KPMG's Cryptoasset Services practice helps crypto custody businesses develop a suite of core capabilities to support institutional requirements for engagement in the ecosystem.

We work with startups, fintechs, and large financial services organizations to help develop the key capabilities of institutional-grade custody solutions, built with security, resilience, and compliance at their core. Crypto custodians count on our insights and guidance through every phase of custody transformation, including strategizing products and services, delivering custody services to customers, protecting cryptoassets under custody, understanding regulatory and reporting requirements, and serving as an independent auditor for crypto attestation services. As experienced system integrators with close strategic relationships with leading technology providers, we recognize what it takes for crypto businesses to implement third-party custody solutions into existing environments.

KPMG's Cryptoasset Services practice brings a broad range of specialized business and technical skills to the table. Our team includes a variety of ecosystem participants including crypto specialists, cybersecurity professionals, technology architects, data scientists, capital markets specialists, smart contract developers, regulatory compliance and financial crimes professionals, technology auditors, tax professionals, and accounting advisors.

Authors

Tegan Keele is a Director in KPMG's Innovation & Enterprise Solutions practice and US Blockchain Program Leader. She has a background across the full life cycle of IT project delivery and considerable project and program management experience with software implementations and infrastructure projects. Tegan has been at the forefront of emerging technology consulting for several years, with experience in electronic medical records, big data, advanced analytics, and now blockchain and cryptoassets. She currently runs the Blockchain Center of Excellence at KPMG, managing blockchain and cryptoasset strategy, go to market approach, and solutions across numerous industries and functional areas.

Mike Krajecki is a Managing Director for KPMG's Emerging Technologies practice and a recognized specialist in disruptive technology strategy and digital risk management. His experiences include leading and delivering KPMG's solutions related to cryptoassets, the Internet of Things (IoT), mobile apps, and intelligent automation. He has helped organizations across a variety of industries responsibly implement and manage emerging technology platforms founded upon the principles of "trust by design." He also has extensive experience leading global System and Organization Control (SOC) reporting covering complex digital products and services, including cryptoasset custodian services.

Sal Ternullo is a Director in KPMG's Innovation & Enterprise Solutions practice and Co-leader, Cryptoasset Services. Drawing on his deep technical background in cryptocurrencies, blockchain, robotic process automation, and public cloud computing, Sal helps companies across industry lines develop, design, implement, and manage products and services for the crypto economy.

Sam Wyner is a Director in KPMG's Innovation & Enterprise Solutions practice and Co-leader, Cryptoasset Services. Sam helps clients evaluate and manage operational and security risks driven by the implementation of emerging technologies, including cryptoassets and blockchain. He has extensive hands-on experience helping companies identify, manage and mitigate risks related to emerging technologies.

References

1 State Street: 38% of clients will put more money into digital assets in 2020 (Coindesk, Dec. 6, 2019)

2 Pension funds double exposure in Morgan Creek's fund to 1% (Coindesk, Nov. 8, 2019)

3 Custody: Crypto Assets' Unique Challenge and Opportunity (CoinDesk, July 2019)

4 Institutionalization of cryptoassets (KPMG LLP, 2018)

5 Investor Bulletin: Custody of Your Investment Assets (SEC.gov, March 1, 2013)

6 NYDFS: Why We Rejected Bittrex's Application for a BitLicense (Coindesk, April 18, 2019)

7 Gemini Completes SOC 2 Review — A World's First For a Cryptocurrency Exchange and Custodian (Medium.com, Jan. 29, 2019)

8 Introducing Staking Rewards on Coinbase (Coinbase, Nov. 6, 2019)

9 The History of the Mt Gox Hack: Bitcoin's Biggest Heist (Blockonomi, June 7, 2019)

10 CoinMarketCap Historical BTC Pricing Data

11 Bitfloor Hacked, $250,000 Missing (Bitcoin Magazine, September 5, 2012)

12 Poloniex Claims All Customers Repaid Follow March Bitcoin Hack (Coindesk, July 2, 2014)

13 Cryptsy Threatens Bankruptcy, Claims Millions Lost in Bitcoin Heist (Coindesk, January 15, 2016)

14 Details of $5 Million Bitstamp Hack Revealed (Coindesk, July 1, 2015)

15 The Bitfinex Bitcoin Hack: What We Know (And Don't Know) (Coindesk, August 3, 2016)

16 The Story of the DAO – Its History and Consequences (The Startup, December 24, 2017)

17 Bitgrail will refund $195M worth of stolen Nano – but only if you promise not to sue (The Next Web, March 15, 2018)

18 How to Steal $500 Million in Cryptocurrency (Fortune, January 31, 2018)

19 Bithumb $31 Million Crypto Exchange Hack: What We Know (And Don't) (Coincheck, June 20, 2018)

20 Hack Brief: Hackers Stole $40 Million from Binance Cryptocurrency Exchange (Wired, May 8, 2019)

21 NYDFS: Why We Rejected Bittrex's Application for a BitLicense (Coindesk, April 18, 2019)

22 Gemini Completes SOC 2 Review — A World's First For a Cryptocurrency Exchange and Custodian (Medium.com, Jan. 29, 2019)

23 American Institute of Public Accountants System and Organization Controls www.aicpa.org/soc

24 Introducing Staking Rewards on Coinbase (Coinbase, Nov. 6, 2019)

Contact

Tegan Keele
US Blockchain
Program Leader,
KPMG LLP
T: 1-781-708-3298
E: tegankeele@kpmg.com

Mike Krajecki
Managing Director,
Emerging Technologies
KPMG LLP
T: 1-312-665-2919
E: mkrajecki@kpmg.com

Sal Ternullo
Co-leader,
Cryptoasset Services,
KPMG LLP
T: 1-617-988-1153
E: sternullo@kpmg.com

Sam Wyner
Co-leader,
Cryptoasset Services,
KPMG LLP
T: 1-212-954-4903
E: swyner@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates and related entities.

kpmg.com/socialmedia