



Cryptoassets

KPMG technology risk insights

Introduction

Cryptoassets such as Bitcoin and Ethereum have made their way into the mainstream financial industry and are being sought out by retail investors as well.

Over the past two years, we've seen public companies put cryptoassets on their balance sheets, legacy financial institutions offer their customers access to crypto-related products, and retail investors buying them on an exchange. The adoption and acceptance of cryptoassets have accelerated at an incredible pace, leading to a nearly \$2.2 trillion market cap.*

But what exactly are cryptoassets? Broadly defined, they are digital units of account in which cryptography and open-source software are used to regulate the generation and distribution of units, which get tracked on a public ledger, known as a blockchain.

*CoinMarketCap.com, December 12, 2021.

Adoption and acceptance of cryptoassets have accelerated at an incredible pace leading to a nearly

\$2.2 trillion market cap



The rise of Bitcoin

The first successful cryptoasset, Bitcoin, was created in 2009 in response to the 2008 global financial crisis. Its primary objective was to solve for the monetary debasement of fiat currencies (e.g., USD, euros, British pound, etc.), which are government issued and controlled by central banks. Bitcoin is often described as a new monetary policy.

Bitcoin's solution to the government bailouts and dollar debasement coming out of the global financial crisis was to have a fixed supply (21 million) that cannot be changed by any entity or individual. Given the history and failure of previous digital currency and cryptoasset projects, Bitcoin was the first to truly solve for the double spend problem, through the use of blockchain technology. Double spending involves sending the same digital payment to two different people and, outside of blockchain-based currencies, relies on trusted intermediaries (e.g., banks) to prevent this from happening.

Since Bitcoin's implementation, thousands of other cryptoassets have come and gone. Companies have invested billions of dollars to research new and innovative ways to leverage blockchain technology; however, its primary application continues to be for the use of cryptoassets.

Blockchain

A system in which a record of transactions is maintained across multiple computers (nodes) that are linked in a peer-to-peer network. This enables digital trust and thus removes the need for intermediaries such as banks or brokers to serve as a trusted third party. Learn more by reading our companion piece [here](#).

Learn more about blockchain by reading our accompanying article [Blockchain and Risks](#)



Crypto adoption in the market

Over the past two years, institutional interest in crypto markets has exploded. Billionaire investors such as Paul Tudor Jones, Bill Miller, and Stanley Drunkenmiller have each disclosed their Bitcoin positions and made public comments praising its long-term outlook.^{1, 2} Companies such as Tesla, Microstrategy, Block (formerly Square), and SpaceX have purchased Bitcoin as a reserve asset to hold on their balance sheet. As of their 2021 Q3 filings, Microstrategy was holding approximately 114,042 Bitcoin (\$2.406 billion) and Tesla was holding approximately \$1.83 billion in Bitcoin. Additionally, legacy financial institutions have reacted to significant demand by their wealth management clients by rolling out a variety of crypto-related products such as shares of the Grayscale Bitcoin Trust, crypto related funds, and the recently approved Bitcoin futures ETF.

Safe to say, cryptoassets have gone mainstream. To meet this demand, crypto native companies have grown exponentially. In the first half of 2021, venture capital funds have poured \$17 billion into businesses operating within the crypto industry.³

This paper will describe some of the basic traits of cryptoassets, the different participants within the ecosystem, and some of the key risks that crypto companies face. We'll then describe how the KPMG Advisory, Audit, and Tax practices can help our clients navigate the complex challenges that cryptoassets present and how to address and mitigate these risks.

“As of their 2021 Q3 filings, Microstrategy was holding approximately 114,042 Bitcoin (\$2.406 billion) and Tesla was holding approximately \$1.83 billion in Bitcoin.”

¹ Paul Tudor Jones Calls Bitcoin a 'Great Speculation,' Says He Has Almost 2% of His Assets In It, CNBC.com, May 11, 2020.

² Wall Street Legend Bill Miller Reveals 'Strong' Bitcoin Recommendation Despite Massive Price Surge, Forbes, November 9, 2020.

³ Venture Capital Makes a Record \$17 Billion Bet on Crypto World, Bloomberg, June 18, 2021.



Types of cryptocurrencies

There are a number of different types of cryptocurrencies, each of which has a different purpose and use case:

Cryptoassets

Assets native to Layer 1 public blockchain protocols used to drive network incentives, process transactions, and maintain security

Examples: Bitcoin, Ethereum

Utility Tokens

Tokens issued on top of public blockchains used for governance and to access features within middleware and decentralized applications

Examples: Maker, Uniswap

Security Tokens

Security tokens issued through an initial coin offering (ICO) where tokens represent ownership interest in the underlying security instrument

Example: The Aspen Digital Security Token

Stablecoins

Asset-backed tokens issued on public and private blockchains that represent the ownership interest in underlying stable assets like fiat currency and precious metals

Example: USD Coin, Paxos Gold

CBDCs

Digital currency issued by a central bank in wholesale or retail models, many of which utilize permissioned blockchain or distributed ledger technology (DLT)

Example: Digital Yuan (China) and Digital Sand Dollar (Bahamas)

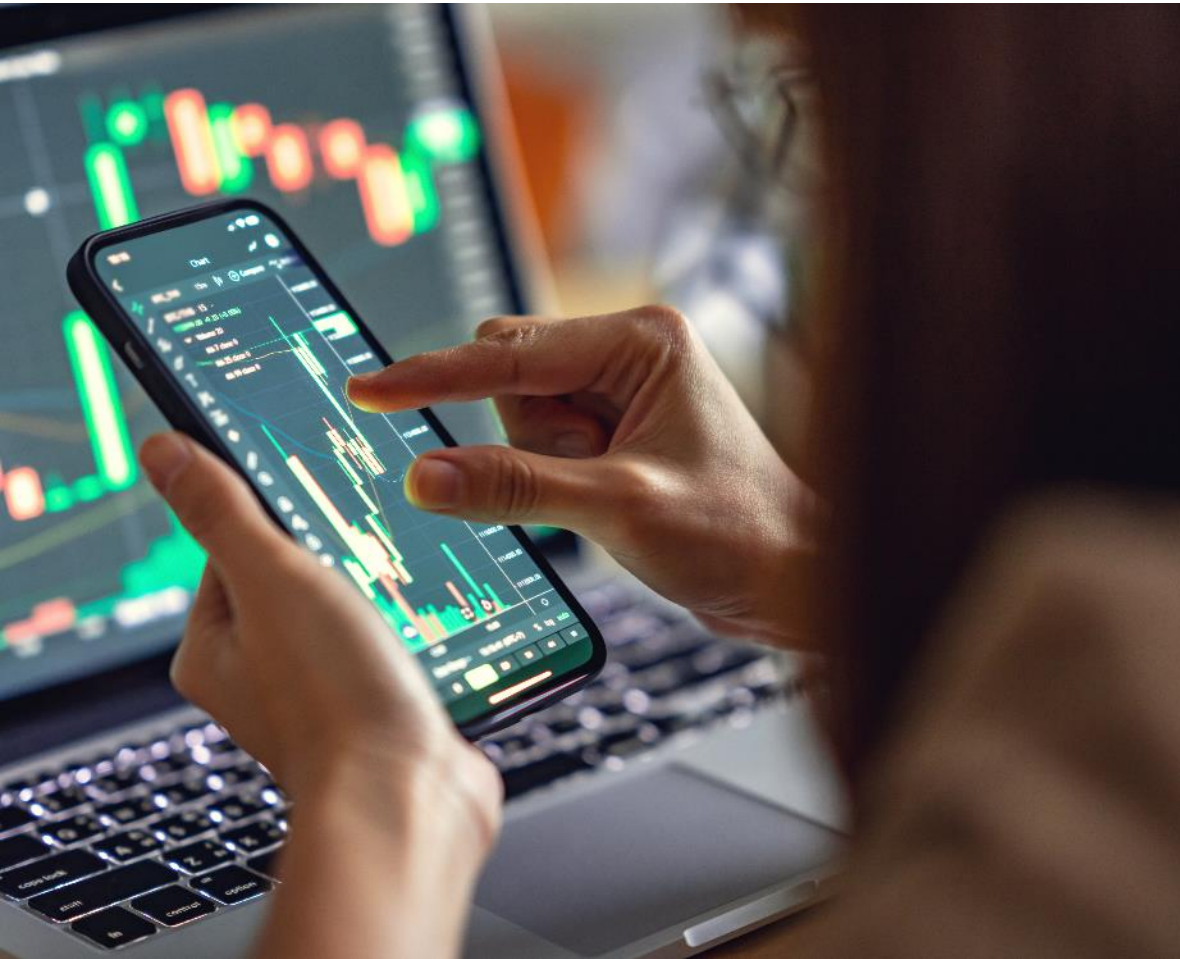
Types of cryptocurrencies

Despite the varying use cases described previously, the primary cryptoassets used today are those native to layer 1 public blockchains such as Bitcoin, Ethereum, and Solana. These assets are being sought after by both retail and institutional investors, as they are truly decentralized assets that are not owned or controlled by any single entity or central bank. However, even among layer 1 protocols, cryptoassets Bitcoin and Ethereum both have different use cases; Bitcoin was developed to be a peer-to-peer electronic cash system and Ethereum was developed to allow for the creation of decentralized applications, also referred to as smart contracts.

Both utility and security tokens are issued on top of layer 1 protocols via smart contracts. By definition, smart contracts are computer programs stored on a blockchain that automate the rules and interactions via source code. Since smart contracts are stored on a blockchain, they inherit a number of its properties such as immutability and decentralization. However, many of these tokens have come under scrutiny from regulators, such as the SEC who have questioned if they represent unregistered securities.



Stablecoins



Stablecoins initially rose in popularity given their ability to be easily transferred from one exchange to another and used as an on-ramp to crypto markets given that some exchanges could not initially get banking access in the early years of trading. Additionally, stablecoins are issued by private entities and have also come under significant regulatory scrutiny as they represent money created outside of the banking system. In November 2021, the President's Working Group (PWG) issued their report on the risks of stablecoins and suggested that issuance should be limited to "insured depository institutions" (e.g., banks).

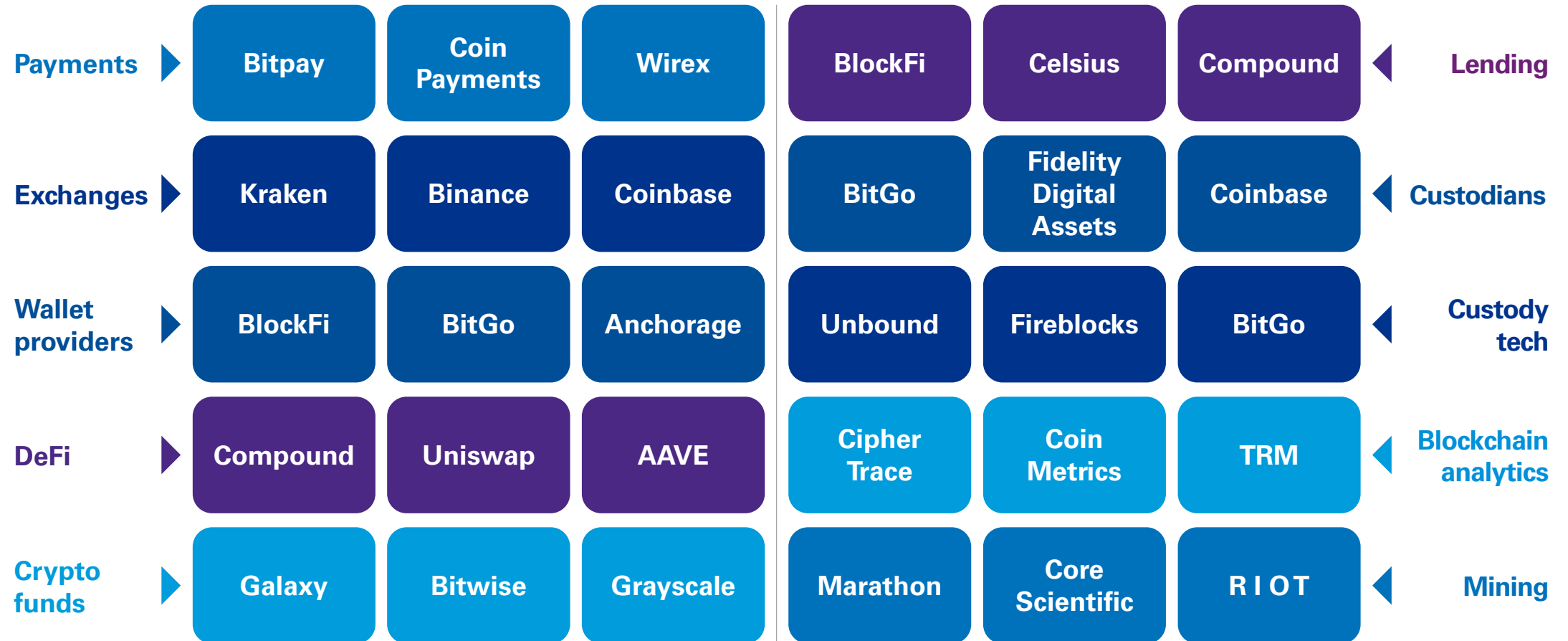
Stablecoins have seen significant growth over the past few years, and as of the time of this paper, have a market cap of approximately \$140 billion.*

*CoinMarketCap.com, December 12, 2021



Participants in the cryptoassets ecosystem

The cryptoasset ecosystem has evolved to offer many of the traditional financial services



Cryptoasset risk considerations

There are many challenges facing organizations as they institutionalize cryptoassets. Lessons learned from traditional business models are still applicable, but organizations will need to challenge these based on nuances that crypto presents. Companies will need a comprehensive framework and crypto-specific capabilities to support this transformation and prepare for a changed future.



Securing cryptoassets

Given the potentially high value of cryptoassets and their natively digital nature, crypto businesses and their customers are prime targets for cybercriminals. Possession of cryptocurrencies is based on ownership or knowledge of private keys. Since there are no intermediaries involved with the transfer of cryptoassets, all transactions are final and cannot be reversed. Properly securing cryptoassets is typically viewed as the biggest risk that companies must address.



Compliance with regulatory obligations

Cryptoasset companies have been under a considerable amount of regulatory scrutiny over the years. The SEC has challenged whether some cryptoassets represent unregistered securities (e.g., Bitcoin lending). Additionally, some states have strict compliance obligations such as those imposed under the New York Department of Financial Service's BitLicense. Companies will need to properly inventory all of their regulatory obligations to help ensure proper compliance and subsequently build out an appropriate risk management framework.



Fork management and governance

A soft fork results from an upgrade to the protocol, but a hard fork happens when significant changes are made and results in a single crypto blockchain breaking into two separate chains. Forks can have a significant impact on crypto businesses. Companies will need to decide on fork acceptance and how to continue running effectively during and after a fork event. How does a business manage the technological, operational, financial, accounting, tax, and customer relationship implications of a fork?



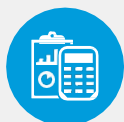
KYC and cryptoasset provenance

Crypto owners are identified not by names or account numbers but by cryptographic addresses that can be created at any time, by anyone, anywhere in the world. This presents a unique challenge to Know-Your-Customer (KYC) programs. How does a crypto business determine asset provenance and build its KYC program to prevent transactions with politically exposed persons (PEPs) and OFAC sanctioned countries?



Accounting and financial reporting

Cryptoassets challenge traditional financial reporting boundaries, and there are currently no generally accepted accounting principles in the United States (U.S. GAAP) specific to cryptocurrencies. The accounting for these assets is an emerging area, and traditional cryptoassets such as Bitcoin and Ethereum are typically accounted for as indefinite-lived intangible assets. This means that companies carrying these assets on their balance sheet must carry them at cost, subject to an ongoing impairment evaluation. However, these assets are not written back up once market prices rise.



Tax implications

Information regarding the tax treatment of crypto remains limited. Crypto businesses may face sizable tax liabilities incurred on the sale or exchange of crypto and bear significant tax accounting burdens with respect to their holdings. Unlike fiat currencies, selling a cryptoasset or using it for commerce creates a taxable event. What are the key tax implications for a crypto business?

Market features and risk management

As with any asset class, understanding the market features behind crypto is necessary to mitigate risks



Public network implications

Key considerations for market activity

- Changes in market depth and liquidity across assets
- Difficulties optimizing for transaction fees can result in price slippage
- On-chain events triggering market reactions

Mitigation solutions

- Monitor network activity to optimize fees
- Identify mempool congestion and mining pool activity



Counterparty risk

- Infrastructure system weaknesses interfering with effective trade execution and asset withdrawal
- Business continuity inefficiencies increasing likelihood that funds are inaccessible during periods of large market activity
- Custody of private keys

- Counterparty diversification
- Exchange due diligence
- Vendor risk assessments
- Segregation of duties during key generation ceremony
- Multisignature (multisig) transaction requirements



Asset class volatility

- External events triggering market reactions
- On-chain events
- Noise trader risk fueling volatility

- Adequate staffing to meet global trading needs
- Effective automation of algorithmic trading



Global nature of crypto

- 24-7 market hours strain resource requirements to effectively maximize gains
- Broader country risk to consider depending on regulatory climate of individual jurisdictions

- Adequate resources to meet global trading needs
- Currency and jurisdictional due diligence
- Regulatory inventory review per jurisdiction



Custodians and cryptoasset platforms have a number of custody models to choose from in order to manage network and market risks

Key considerations for custody and mitigation solutions



Next-gen security and resilience

- Layered security and operational defenses
- Balance key security and availability



Comprehensive compliance

- Regulation-compliant processes
- Adaptable systems to react to regulatory changes



Third-party trust

- Proof of reserve reporting
- Independent auditor attestation

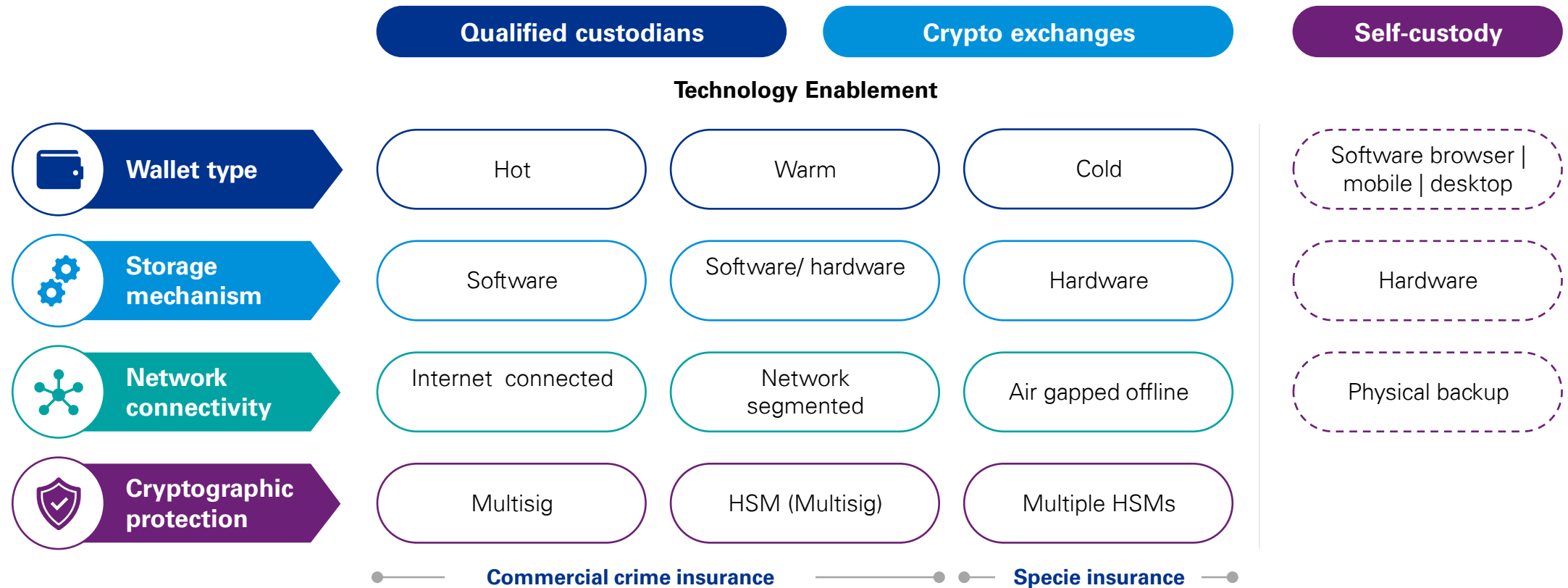


Value-adding and scalable systems

- Integrate into existing infrastructure
- Support participation in network activities

Custodians and cryptoasset platforms have a number of custody models to choose from in order to manage network and market risks

Custody Solutions Map



How KPMG can help

KPMG offers a broad set of services to help enable our clients to identify, manage, and mitigate risks posed by the adoption of cryptoassets. Whether it be legacy companies who are routinely subjected to regulatory compliance activities or start-ups looking to build out their risk management framework, our extensive experience in this space can accelerate your company's crypto strategy and help ensure that risk is aligned with business objectives.

Technology Risk Management

- | | |
|-----------------------------------------|-----------------------------------------------|
| SPAC & IPO readiness assessments | Risk, Controls, and Compliance (GRC) Programs |
| Strategy and governance | Technology Risk Intelligence and automation |
| Risk-based IT audit (IT Internal Audit) | |



Internal Audit and Enterprise Risk Management

- Readiness and gap assessments
 - Key risk and control assessments
 - SPAC and IPO readiness assessments
- Audit lifecycle
 - Audit planning and execution
 - Risk matrix
 - Strategy alignment

Cyber Security Services

- | | | |
|---------------------------|--------------------------------|---------------------------|
| Third-party security | Identity and access management | Privacy and data security |
| Threat management | Key management assessment | Smart contract assessment |
| Cyber program development | | |
| — Strategy | — Defense | — Response |

FS Regulatory and Compliance

- Filing and registrations
 - BitLicense
 - OCC charter
 - SPDI
 - Money transmitter license
 - Broker-dealer
- Establish AML/BSA and KYC policies and programs
- Custodial risk assessments
- Board reporting



Contact us

For more information, visit read.kpmg.us/TRM.



Brian Consolvo
Managing Director
Technology Risk Management
T: 804-782-4215
E: bconsolvo@kpmg.com



Ahmed Saleh
Director
Technology Risk Management
T: 402-637-5014
E: amsaleh@kpmg.com



Nana Amonoo-Neizer
Director
Technology Risk Management
T: 402-661-5316
E: namonooneizer@kpmg.com

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

kpmg.com/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.