Blockchain Security Issues and their Impact on the Global Capital Markets

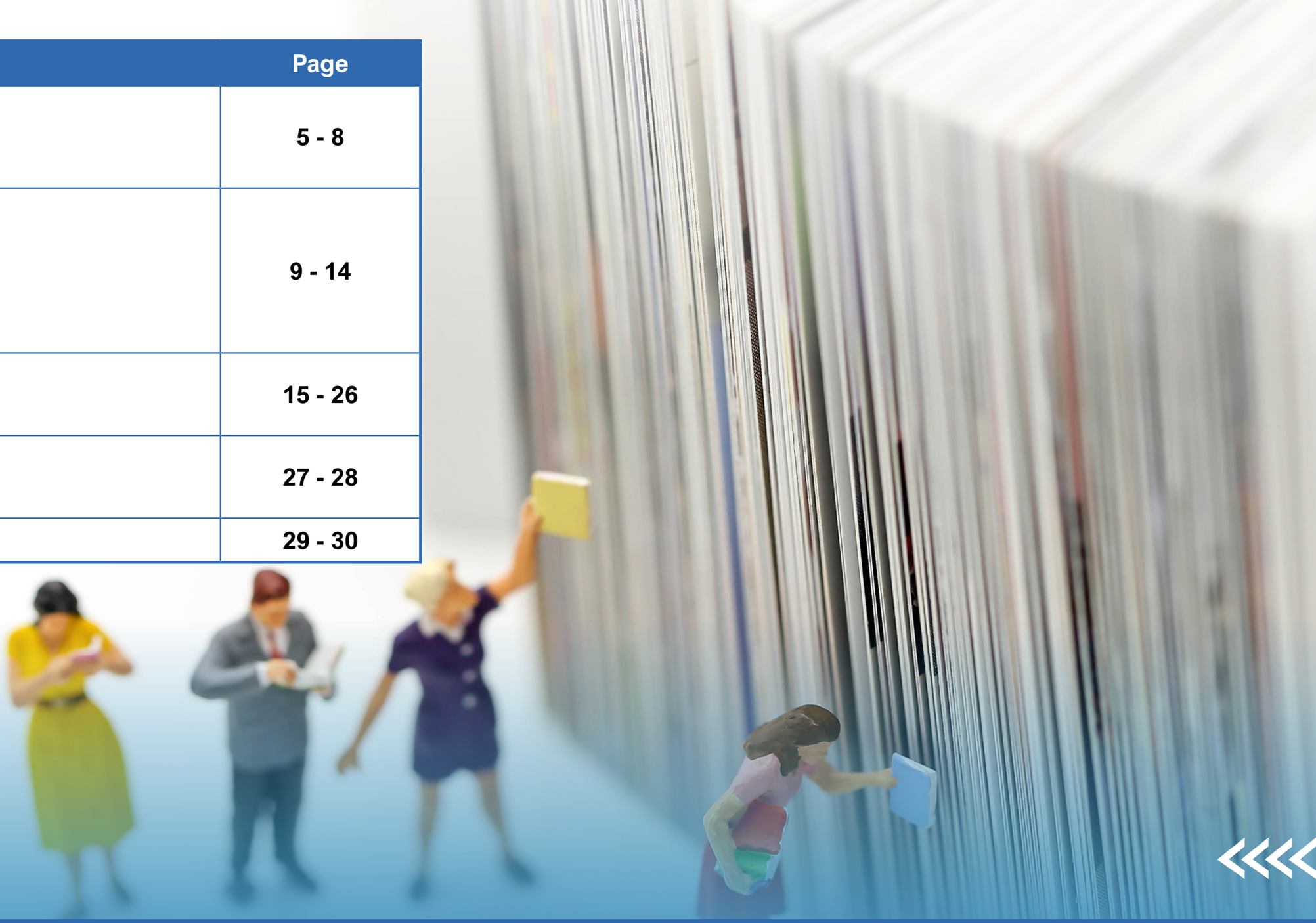
Capital Markets Industry – Sutherland Global Services

Christopher Rigg
Armstrong Wolfe Industry Advisor,
Sutherland Global
February 13, 2022

SUTHERLAND

ARMSTRONG WOLFE

Contents



Introduction

In a recent podcast interview Vitalik Buterin, the founder of Ethereum, described his experience trying to liquidate and donate a large chunk of the cryptocurrency called Shiba Inu that he was given by its founders. The experience Buterin portrayed sounded like a spy novel. He had stored the tokens in a cold wallet, which means that the cryptographic hash code representing his ownership of the tokens was not stored anywhere where it could be accessed on the internet. Buterin took the hash code, essentially an 80 digit number, and divided it into two numbers that if added would result in the correct key. He stored one of the values on a laptop in his home in Canada and the other on a piece of paper that he carried around at all times. To access the tokens in the wallet while Buterin was traveling in the United States, and unable to return to Canada due to the pandemic, he had to call his family, on a burner phone of course, and ask them to read out the stored number. He then purchased a new laptop from a local Target store, connected it to the internet, and entered the sum of the two numbers into an interface on the distributed crypto-asset exchange app known as UniSwap, which allowed him to trade the Shiba Inu tokens for Ethereum tokens, ETH, which could then be donated or traded for US dollars. This may seem extreme but the estimated value of the tokens in his cold wallet was over 1 billion US dollars. He expressed how intensely stressful the experience was for him because any errors in the process could result in a material loss of value.

Buterin's story portrays the current state of the crypto-asset market with its cloak and dagger practices and ridiculous valuations. The risk that Buterin exposed himself to was caused by the fact that crypto-assets, in this case, Shiba Inu coins, are on public networks accessed via anonymous codes, and UniSwap, the exchange service he used to trade the assets, is a smart contract, which is a piece of software that runs autonomously and its actions cannot be reversed. Even with these known issues, the crypto-asset market has become increasingly attractive to the companies and investors that participate in the institutional capital markets.

Starting with the introduction of Bitcoin in 2009, the cryptocurrency, crypto asset, and distributed finance (DeFi) space have taken off as evidenced by the increase in value of Bitcoin and related products, the volume of venture capital invested in companies providing crypto-related services, and the overall hype in the popular and business media [Chang, Baudier, Zhang, Xu, Zhang, and Arami 2020]. The technology underlying the crypto space, blockchain, is believed to provide significant value from automating the exchange of value via a shared and secured transaction ledger [Karame 2016]. The blockchain data structure uses an append-only concept where blocks in the chain cannot be modified, only added, are linked to the previous block in the chain through a hash value of the previous block that is stored in the current block[Kovalchuk, Kaidalov, Nastenko, Shevtsov, Rodinko, and Oliynykov 2018]. This approach is perceived to be highly secure as it requires significant computing power to modify a block in a way that would resolve all of the hashes linking the chain together. Many proponents of Bitcoin highlight that it has "never been hacked", but over 20 percent of the Bitcoin in circulation has been either stolen or are inaccessible because the owner has lost access to the appropriate cryptographic keys to access it [Gervais, Ritzdorf, Karame, and Capkun 2015]. Bitcoin, and its associated infrastructure, are often referred to as "Blockchain 1.0" because of the very limited functionality it provides. Bitcoin, which is based on the Bitcoin protocol, is essentially a payments system with an associated token to store the value that is exchanged by the payment system. There are many additional cryptocurrencies that are implementations of the Bitcoin protocol, including the now-infamous Dogecoin made popular by Elon Musk.

In December of 2013, a group of developers created Ethereum which is a public blockchain-based network that extends the core concept of a blockchain by adding a dynamic data structure called a smart contract. Smart contracts allow for the automated exchange of tokenized value on the blockchain providing the potential for additional automation of the activities that are associated with a transaction. The additional functional capabilities introduced by smart contracts are referred to as "Blockchain 2.0" as it represents an incremental increase in Blockchain capability. There are over 3,000 companies that are members of the Enterprise Ethereum Alliance, a group dedicated to the development and promotion of Ethereum based solutions. While the use of the blockchain data structure and associated cryptography has the potential to provide significant security features, there are many cybersecurity risks associated with blockchain, smart contracts, and the related infrastructure that surrounds them.

A further delineation in the blockchain is the concept of public vs private blockchains. Ethereum is an example of a public blockchain and these are called permissionless because anyone can participate on these blockchains by simply adding a node on the network that can implement the protocols established by the Ethereum standard. There are private blockchains, called permissioned blockchains, that use blockchain technology but implement it in a private network where all of the nodes on the network are known to the network owners and there is some authoritative figure that controls who can and cannot access private blockchain network [Zhang, Xue, and Liu. 2019].

Two key features of the blockchain and smart contract space that significantly increase the risk of their adoption by institutional capital markets participants are the anonymous encrypted transaction signature that allows anyone with that key to impact the crypto assets stored on the chain and the immediate and irreversible execution of smart contracts. The net impact of these two features is an increase in the potential impact from an inadvertent error and the exploitation of a vulnerability [Mense and Flatscher 2018, Bissias, Levine, and Kapadia 2017, Luu, Chu, Olickel, Saxena, and Hobor 2016].

In the electronic trading space, there is a concept called an auto-execute algorithm. These algorithms interact with electronic messages in the securities market and make decisions on whether to execute a trade, including the price and quantity traded, without any human intervention. This is similar to a smart contract in that once the code is released to a production environment, it is executed automatically. On August 1st, 2012, one of the largest electronic market makers in the US Equity market, Knight Capital, was essentially bankrupted by a defect in an auto-execution algorithm that made trading decisions resulting in over 15 billion dollars of transactions in 40 minutes. Knight did not have sufficient capital to survive the settlement cycle of these trades and had to be rescued by external investors who ultimately forced Knight to merge with another company and replace a significant portion of its management.

The fact that a well-established and highly-profitable company could be destroyed in 40 minutes by a software defect rippled through the institutional capital markets industry forcing every participant - banks, broker-dealers, exchanges, hedge funds, to ask themselves – "Could this happen to us?" and "What do we need to do to make sure it doesn't?" As a result of the Knight Capital incident virtually all capital markets participants adopted new and enhanced controls to prevent the introduction of software defects into their algorithmic trading infrastructure, monitor the outputs of the auto-execution algorithms, and created procedures and capabilities to shut-down trading immediately if errant behavior is detected.

The Bitcoin cryptocurrency is by far the most adopted blockchain implementation in the institutional capital markets. Goldman Sachs, one of the world's largest investment banks and trading organizations, recently announced that it was opening a crypto trading desk that would provide market-making and other trading services to institutional clients. Coinbase, a recently listed public crypto trading platform company, provides a range of institutional crypto services including trading and custody. Many other providers of traditional financial services have implemented or announced the implementation of crypto-related services, although most of them are targeted at the retail space.
Microstrategy, a publicly-traded software company, recently started to use Bitcoin as an asset on its balance sheet as part of its corporate treasury. Companies use their corporate treasury as a vehicle to manage the financing of their day-to-day operations. The rationale provided by the Microstrategy CEO, Michael Saylor, was that Bitcoin provides a better hedge against inflation than US Dollars or other government issues currencies so he had a fiduciary obligation to hold Bitcoin in the Microstrategy treasury. Tesla, a publicly traded electronic vehicle and battery manufacturer, also started to use Bitcoin as an asset for a portion of its corporate treasury. As of March 1st, 2021, Microstrategy had acquired over 2.19 billion US dollars of bitcoin and is holding it in their treasury. Michael Saylor has subsequently hosted a series of conferences advocating the corporate community the virtues of using Bitcoin as a corporate treasury store of value.

Corporations that choose to use crypto-assets in their treasury function will have to make sure that the processes and infrastructure supporting the movement and conversion of those assets are secure. Citibank, one of the largest banks in the world, accidentally wire transferred 900 million US dollars to several companies that had loaned money to one of its clients, Revlon. The bank was supposed to wire 1/100th of that amount as an interest payment on the loan but the operator accidentally added two zeros to the amount. When Citibank tried to get the money back from the lenders, several of them refused because they had legitimate concerns with Revlon's ability to repay the loan and decided to keep the payment as a return of principal. Citibank took the matter to court and was not able to recover all of the money. This is another very good example of how mistakes in the institutional capital markets can have significant consequences. The crypto asset infrastructure does have the same level of controls that the US wire transfer does, increasing the potential of an error.

Generalized Blockchain Security Issues

Academic and industry research has explored the cybersecurity issues related to Bitcoin, Blockchain, and Smart Contracts. Multiple surveys have been conducted that identified and classified key security issues related to blockchain [Amiet 2021, Saad, Spaulding, Njilla, Kamhoua, Shetty, Nyang, and Mohaisen 2019, Lee and Kim 2020, Toufaily, Zalan, and Dhaou 2021, Biryukov, Khovratovich, and Pustogarov 2014, DuPont and Squicciarini 2015, Kwon, Kim, Son, Vasserman, and Kim 2017] including:

- The 51 percent attack where an attacker can compromise the core operation of a blockchain if they can gain control over 51 percent or more of the underlying computing power applied to the network.
- Denial of service attacks where the nodes on a public blockchain network are occupied handling erroneous traffic that an attacker can force the network to fork created a separated chain that could be controlled by the attacker and capturing ownership of the tokens on that portion of the network.
- Pseudo anonymity where the identity of a blockchain wallet holder, who is supposed to be anonymous, can be identified through the harvesting of additional non-encrypted information that is carried with a transaction.
- Smart contract vulnerabilities where defects in smart contracts expose the underlying blockchain to attacks that can corrupt the network or extract the tokens within it.

Ethereum Specific Security Issues

The Ethereum public blockchain network is the second-largest blockchain implementation after the Bitcoin network and it is the primary platform for smart contract implementations [Luu, Chu, Olickel, Saxena, and Hobor 2016]. The smart contract feature on Ethereum is supported by an object-oriented programming language called Solidity. Solidity applications are compiled into byte code and inside an Ethereum virtual machine. In a 2020 survey, Chen, et al, identified and analyzed 40 vulnerabilities related to the Ethereum network [Chen, Pendleton, Njilla, and Xu 2020]. These vulnerabilities were classified based on which component of the Ethereum architecture was impacted, including the application layer, the data layer, the consensus mechanism, and the network layer. Many of these vulnerabilities have led to direct financial loss by companies that provide or use Ethereum based solutions. Because many of the cybersecurity incidents on Ethereum, tools, and methodologies have been created to assist developers in identifying defects and producing higher quality and more secure smart contract code [Luu, et al. 2016, Bissias et al.2017, Jiang et al. 2018, Mense and Flatscher Mense and Flatscher 2018, Lai and Luo 2020, Durieux, Ferreira, Abreu, and Cruz 2020, Brent, Grech, Lagouvardos, Scholz, and Ghaleb and Pattabiraman Ghaleb and Pattabiraman2020, Garfatta, Klai, Gaaloul, and Graiet 2021].

Blockchain Adoption Research

There has been some research on the adoption challenges associated with Blockchain technology. In an exploratory study, Toufaily et al. (2021) interviewed 46 individuals across the public sector, private sector, and expert community to analyze the challenges to adopting blockchain in the financial services industry [Toufaily et al. 2021]. Security and Privacy issues were identified by the participants in the study, especially as it relates to the financial services industry, the challenge of protecting customer data, and the risks associated with the movement of money. Ali et al. (2020) performed a literature review of 87 articles on blockchain implementation in financial services to understand the benefits, challenges, and desired functionality [Chang et al. 2020]. Data security and privacy were identified in this study as a material challenge to the adoption of blockchain technologies in the financial services space.

Research Design

Providing crypto-asset services creates asymmetric risks to the providers from the unique characteristics of crypto-asset structures and the underlying blockchain technology. These risks are derived from the fact that crypto-assets are essentially bearer instruments, possession = control, and transactions are irreversible. If crypto assets, including cryptocurrencies, smart contracts, and other tokenized assets, are going to become a material part of the financial management toolkit for global corporations, they must be adopted by the capital markets institutions that provide market-making, payments, financing, and other related services. The rapid digitization of the global capital markets over the past 20 years required institutions to develop and adopt new risk frameworks to identify, manage, and mitigate the unique risks associated with electronic trading. The crypto-asset space introduces a new set of cybersecurity risks that must be factored into the core management processes of the organization. This paper focuses on the cybersecurity risks introduced by crypto assets and the mitigation approaches being considered and implemented by the primary capital markets participants.

Since the inception of crypto-assets, starting with Bitcoin in 2009, Ethereum in 2013, and then the explosions of coins, Dapps, and DeFi services in the past few years, billions of dollars of value has been stolen, lost, or destroyed by the exploitation of vulnerabilities in the crypto ecosystem by malicious actors. Many of these incidents are well known, like the Mt. Gox hack, the Ethereum DAO fork, and the Parity Wallet hack. There has been extensive academic research on these vulnerabilities and the potential strategies to manage and mitigate them.
The crypto-asset vulnerabilities that are most relevant to the institutional capital markets are classified across different layers of the ecosystem:

- **1 - Custody -** Crypto-assets are essentially bearer instruments meaning if an attacker is able to access the cryptographic keys that represent your assets on a blockchain, they can steal the assets. All blockchain implementations, both public and private, must interact with traditional IT infrastructure that is prone to extensive vulnerabilities as evidenced by the recent Solarwinds attack or the Microsoft Exchange exploitation. These attacks can lead to account takeovers or wallet theft which leads to all of the value in the wallets being confiscated without any recourse to get a refund.
- **2 - Core Infrastructure -** Blockchains rely on a core infrastructure that uses cryptography and network processing that has the potential to be brute force interrupted or penetrated. This includes the 51 percent attack, denial of service attacks that can disrupt mining operations, or new technologies, like quantum computing, that could break the SHA256 encryption that most blockchain implementations use.
- **3 - Smart Contracts -** Smart contracts are written in scripting languages, like solidity, that are compiled into byte code that is executed in the virtual machine infrastructure on the nodes of the blockchain network. Both the language compiler and the code can introduce vulnerabilities that could be exploited to cause transactions that drain wallets instantaneously, similar to the Knight Capital defect in their market-making algorithms that inadvertently traded over 15 billion dollars in securities in 40 minutes and essentially bankrupted the company.
- **4 - AML/KYC -** The pseudo-anonymity offered by blockchain implementations creates an exposure that legitimate actors could unknowingly trade with malicious actors and the pseudo-anonymity can be compromised through heuristic analysis of combined data sets between blockchain activity and non-blockchain activity can expose client identities impairing their ability to achieve the best price or other harm to their market interaction.

Research Questions

This paper seeks to answer the following questions:

- **RQ1 -** How are the known security issues related to Blockchain negatively impacting its adoption in the institutional capital markets?
- **RQ2 -** Are the perceived differences in the cybersecurity issues between Permissioned vs Permissionless Blockchains material enough to warrant different mitigation approaches?
- **RQ3 -** What specific strategies are capital markets institutions deployed to mitigate crypto asset security risks?

Assumptions

- **1 -** The demand for crypto-asset related services will force traditional capital markets institutions, including banks, broker/dealers, exchanges, asset managers, and wealth managers to enter the market at scale.
- **2 -** Crypto assets are based on blockchain technology, both public and private, that includes features based on cryptography, the blockchain data structure, and pseudo-anonymity.

Limitations

- **1 -** The crypto-asset space is new and the technology is rapidly changing creating the potential for newer technologies or features that address the vulnerabilities considered in this paper and obviating the results.
- **2 -** The competitive nature of the capital markets industry creates a strong desire of the participants to conceal vulnerabilities in their infrastructure and strategies to leverage technology for economic gain.

Delimitations

- **1 -** This study is limited to individuals who are focused on, or have experience in, delivering capital markets services, including corporate and investment banking, brokerage, custody, market making, and advice, to institutions. It is not focused on the retail aspects of the market.

Research Method

The research described in this paper was a descriptive study that interviewed selected individuals with experience and expertise in the institutional capital markets. These individuals have a combination of extensive experience in the space and have a role in the consideration or adoption of crypto-asset-related services to the market.

Research Instruments

The primary research instrument was a structured interview with industry professionals who are currently working on institutional capital markets adoption efforts for crypto-asset services. The following question prompts will be used to structure the interviews with the selected participants:

Demographic Questions

What role(s) have you played or are currently playing in the capital markets industry?

- Trader
- Risk or Compliance Manager
- Sales Person
- Technology Manager
- Operations Manager

What part of the capital markets industry have you been employed in?

- Sell-Side Bank or Broker-Dealer
- Exchange or Market Infrastructure Provider
- Buy-Side Asset or Wealth Manager
- Consultant or Advisor
- Hedge Fund or Proprietary Trading Firm

How many years have you worked in the industry?

What is the highest level of seniority you have achieved?

- Individual Contributor
- Executive
- Supervisor or Manager
- Principal

Risk Appetite

Risk appetite is defined as the relative amount of risk that an organization is willing to take on as part of its core operations. The risk appetite of many institutional capital markets has changed over the years. In the years leading up to the global financial crisis in 2008, many companies steadily increased their risk appetite, demonstrated by the significant addition of many high-risk assets onto bank balance sheets.

- **1 -** How well do you think the responsible executives at capital markets companies understand the core principles, including the math, cryptography, and computing model, that underpin crypto assets?
- **2 -** Why are so many traditional capital markets companies entering the crypto asset space now given that they were very reluctant to do so in the late 2017 and early 2018-time frame when the price of Bitcoin reached 20,000?
- **3 -** Which risk areas are traditional capital markets institutions most concerned with related to the provisioning of crypto-asset services? (Financial Loss, Reputation, Regulatory Compliance)
- **4 -** How well do think the principals of institutional capital markets companies understand the risks associated with crypto assets?
- **5 -** How are capital markets companies sharing the risk management strategies around crypto-asset services across Risk, Compliance, Operations, Sales, and Technology?
- **6 -** How are capital markets companies balancing the risk emanating from crypto assets and the potential revenue from providing crypto-asset services?

Custody

Custody is defined as providing a safekeeping service for assets so that they are protected from theft or destruction while also being available to the asset owner so that they can be used in typical financial transactions, including sales, trading, lending, and borrowing?

- **1 -** What risks do capital markets companies associate with providing custody of crypto assets?
- **2 -** How are most companies approaching the provision of crypto-asset custody to their clients or internal organizations? Insource? Outsource? Build from scratch? Partner with external custody providers?
- **3 -** What role is insurance playing?
- **4 -** What guarantees are financial services companies going to provide to their clients?

Smart Contracts

Smart contracts are programs written in a computer language, like Solidity that is provided by the Ethereum Network, that allow for a series of conditions to be defined and then creates an automated exchange of value if and when the contract conditions are met. Smart contracts live inside of the blockchain networks and are executed on the network's nodes. A defect or vulnerability in a smart contract can expose that contract to attack resulting in a loss of value from the crypto-assets associated with the smart contract being transferred to or destroyed by the attacker.

- **1 -** Do you believe that institutional capital markets companies are going to implement smart contracts as part of their crypto-asset services offering?
- **2 -** How are companies managing the risk derived from the deployment of smart contracts?
- **3 -** How is the systems development life cycle (SDLC) of smart contracts different than other application development efforts within the industry?
- **4 -** What testing methods are financial institutions deploying to ensure that smart contracts are safe?

AML/ KYC

AML/KYC risks are associated with the regulatory obligation that financial services institutions have to ensure that they are not participating in money laundering, the drug trade, or terrorist financing. Companies in this space are required to validate the identity of their clients to understand their role and potential connection to illegal activities or political manipulation. They are also required to monitor their client transaction to detect and prevent suspicious activity. Crypto asset activities have increased potential to facilitate illicit transactions because the core platform is anonymous. There is no guarantee that the counterparties an institution is trading with known and verified identities.

- **1 -** How are institutional capital markets companies ensuring that their clients are not trading with suspect counterparties?
- **2 -** What specific strategies are capital markets companies using to screen the marketplaces and other venues they trade crypto assets one?
- **3 -** What techniques are traders using to obfuscate their crypto-asset positions from the blockchain analysis tools.

Results

Six industry professionals were interviewed for 1 hour each. The demographic makeup of the interviewees is in the following Table 1:

Participant	Role	Experience	Level
P1	Sell-Side Trader	25	Executive
P2	Consultant/ Attorney	7	Manager
P3	Blockchain Developer	12	Manager
P4	Operations	27	Executive
P5	CTO/ CISO	23	Principal
P6	Salesperson	10	Manager

Interview Results Summaries

Key points raised by the interviewees are listed here with a subsection for each participant.

Participant 1 Results

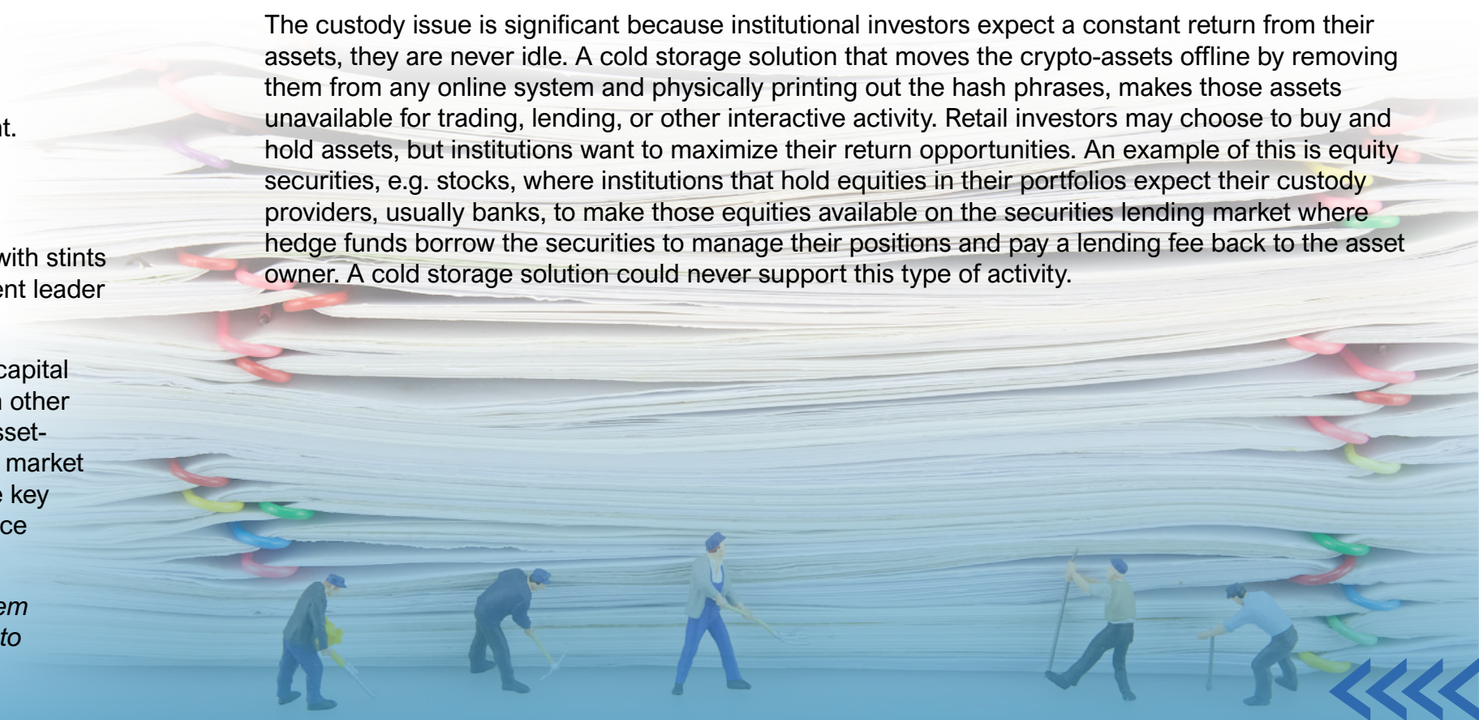
Participant 1, P1, had a long career as a sell-side trader in the fixed income marketplace with stints at both banks and derivative exchanges. He is currently working as a business development leader for a startup focused on providing blockchain-based solutions for institutions.

The first section of questions on the interview focused on the risk appetite of institutional capital markets participants. P1 was able to opine on the ”Why now?” question. There have been other inflection points during the past 10 years where institutional interest in providing crypto-asset-related services was demonstrated, but most providers at that time chose not to enter the market in any material way. Many industry professionals believe that this time seems different, the key question is why? P1’s perspective on the risk appetite of institutional capital markets service providers is highlighted below:

- *Institutional investors want exposure to crypto-assets and need services to help them achieve their goals. The price action over the past 12 months has forced investors to consider crypto.*
- *Banks are being dragged into this space by both their clients and the senior executives who both believe they are missing out on a huge money-making opportunity.*
- *Most executives and managers do not understand the underlying technology, cryptography, or math related to crypto-assets.*
- *Hedge funds are struggling to justify their 2 and 20 (the fees they charge based on the amount of assets they manage). Clients are looking at crypto as a highly volatile component of a diverse portfolio.*
- *Banks and hedge funds are used to spending a lot on technology and many of them have recently hired experts in distributed computing and cryptography to get more comfortable with these risks and issues.*
- *The introduction of insurance that provides a certain level of risk absorbing backstop has made a big difference between now and 2017.*
- *Custody is one of the most important issues, but there are significantly more services available now than in 2017.*
- *Institutional capital markets participants need their assets to be continuously available, it is impractical for them to use cold storage or other mitigation that introduces a lag between when they need access to an asset and when it can be available.*

The implication of P1’s description of the motivation of institutional capital markets players for entering the crypto-asset services space suggests that even if the risks are material and difficult to mitigate, many providers are going to offer services anyway. Capital markets companies are risk-taking organizations and are comfortable taking significant financial risks if they believe there is a monetary benefit to be gained from those risks. Companies that provide services to institutional investors, like hedge funds, are under constant pressure to justify their fees and are always looking for opportunities to find better financial returns.

The custody issue is significant because institutional investors expect a constant return from their assets, they are never idle. A cold storage solution that moves the crypto-assets offline by removing them from any online system and physically printing out the hash phrases, makes those assets unavailable for trading, lending, or other interactive activity. Retail investors may choose to buy and hold assets, but institutions want to maximize their return opportunities. An example of this is equity securities, e.g. stocks, where institutions that hold equities in their portfolios expect their custody providers, usually banks, to make those equities available on the securities lending market where hedge funds borrow the securities to manage their positions and pay a lending fee back to the asset owner. A cold storage solution could never support this type of activity.



Participant 2 Results

Participant 2, P2, started out as an attorney focused on the banking industry and its compliance with global anti-money laundering (AML) and know your customer (KYC) requirements. After several years advising banks on compliance issues, participant 2 joined a top-tier management consulting firm where he helped financial services clients identify crypto use cases and build crypto capabilities. His prior focus on banking regulatory issues makes him a good source to provide input on how the crypto-asset space is impacting the global financial services industry efforts to combat terrorist financing and the illicit drug trade. He is now working for a startup that provides crypto-asset custody services to financial institutions.

The interview with P2 focused on the AML/KYC and custody issues related to crypto-assets. Key points captured during the interview include:

- *The idea that when bitcoin is stolen it is lost for good is a common misconception. The pseudo-anonymity provided by encrypted data transmissions and anonymous participation is hampered by the fact that the financial details, the amount of crypto exchanged between anonymous accounts, are public information.*
- *Sophisticated fraudsters use mixers and other techniques to try to hide the movement of crypto-assets across the public networks.*
- *The state of the forensics capabilities in the blockchain is so good that they can see through these obfuscation techniques.*
- *From one transaction to the next you can't always know who controls the wallet. You can trace wallet to wallet until you hit a known wallet, like an exchange, the exchanges are conducting KYC you can learn the identity of the wallet owner.*
- *Users are out of luck if they lose the password to a local hardware-based cold wallet solution.*
- *There are so many crypto scams that you would think it was fiction.*
- *Multi-level marketing mixed with crypto assets creates a reward structure to sell crypto packages. Amazing too good to be true prices.*
- *Number one question? Custody. Mismanagement by a centralized exchange. Hot wallets are required for active traders.*
- *There are solutions that allow for secure crypto storage including insurance solutions.*

P2's perspective on how the blockchain forensic space is increasing its capability to analyze the transactions on the public blockchain demonstrates an important issue for certain segments of the institutional capital markets. From a banking regulatory perspective, more capability to trace transactions and ownership increase the ability to ensure that crypto-asset transactions are not financing illicit activity. But institutional investors often take large positions because of the size of the assets that they are required to manage and making material changes to these positions creates a significant financial risk that the market signals created by their trades will move the prices of their assets in an unfavorable direction. If a hedge fund wants to sell a large block of Microsoft stock without causing the price to drop, it can use the services of a dark pool that will execute the trades anonymously, saving the fund considerable costs. If a public blockchain investment can be exposed through analyzing the available information on the chain, large institutional investors face potential exposure of their trading strategies, which negatively impact its effectiveness.

The P2 interview also identified perspectives on the custody issue, including:

- *Cold storage solutions that print out hash phrases on paper are being phased out.*
- *Large custody providers like Bank of New York Mellon and Fidelity have invested heavily in their crypto custody capabilities through partnerships with specialist companies like Fireblocks and Anchorage.*
- *The key challenge is to balance the availability vs security of the assets.*
- *Crypto custody providers are focused on reducing the time window from when an asset is needed to when it is online and available to a network. SLAs have gone from as high as 48 hours down to 20 or 30 minutes.*
- *The availability of insurance to protect crypto-assets that are under custody is a huge game-changer.*
- *90 to 95 percent of assets in cold storage can be protected and up to 50 million dollars in a hot wallet.*

P2's perspective on custody highlights the level of investment in that space targeting the institutional investor market. Institutional investors manage very large positions increasing the value of potential loss from an account takeover or custody breach. Their requirements are very robust as they need ready access to their crypto-assets and the ability to deploy into various use cases. The focus on custody also demonstrates how the industry views this as one of the most important obstacles to the institutional adoption of crypto-assets. What is not clear is whether these investments have resulted in sufficient capabilities to allow large regulated financial services companies, like banks and asset managers, to meet their regulatory, fiduciary, and shareholder obligations to effectively manage the risks to their business. The increasing availability of insurance is critical as most regulated organizations require a financial backstop for financial risks that are seen as asymmetric.

The last area where P2 was able to provide insight on was smart contracts and the risks associated with developing and deploying them on a private or public blockchain. In his role as a risk and compliance advisor to large financial institutions, P2 has seen firsthand the evolution of smart contract development in the institutional space. Key highlights from P2's smart contract perspective include:

- *Most large banks are not comfortable deploying smart contracts on a public blockchain, the risk of loss is just too great.*
- *There are smart contract audit firms, like Open Zeppelin, that offer a range of services, including auditing and libraries of audited smart contract components that clients can incorporate into their own code. I have heard that as much as 70 percent of the in-production deployed smart contracts are based on pre-audited library code.*
- *One of the biggest problems is that there are no standards for smart contract audits, which limits the ability of traditional auditing firms, like the big 4, to provide these services in a way that protects both the auditor and the client from excessive liability.*
- *There is also an emerging set of services focused on the economic analysis of smart contracts providing stress testing and simulation of the financial behavior of the contracts.*

P2 was the only interviewee that was comfortable opining on the smart contract space suggesting that public blockchain implementations of smart contracts are not currently being widely adopted by institutional capital markets participants. The DeFi space is the area most associated with smart contracts and most large institutions are not actively participating in the DeFi markets.

Participant 3 Results

Participant 3, P3, has been a Blockchain developer, advisor, and technology executive for many financial services institutions including banks, broker-dealers, exchanges, and asset managers. He is currently working for a global investment bank developing Blockchain solutions for commercial, corporate, and investment banking.

P3's perspective on the attitude of large institutional capital markets companies entering the crypto-asset services space was a little different than other participants in that he believes there are still issues that are causing firms to avoid the space. His perspective is that Bitcoin as an asset that investors can hold in their portfolios to mitigate inflation or provide an alternative exposure, the so-called digital gold concept, is the only viable use case for crypto that will be widely adopted. The DeFi concept of a smart-contract-driven autonomous function is a bridge too far for today's institutions. Highlights of his perspective include:

- *The risk-reward trade-off for autonomous smart contracts does not make sense.*
- *Large banks have huge software development organizations that are slow but provide protections and risk and compliance issues. Smart Contracts are essentially software that no one can shut down, which is not good.*
- *Bitcoin is not practical as a currency, it is too volatile and too expensive to transact in. The proof-of-work consensus mechanism in Bitcoin has been extensively tested and is highly unlikely to change. This helps Bitcoin because assets that are acting as a store of value should not change.*
- *The capabilities of NYDIG, Fireblocks, and Anchorage are a huge improvement in the custody space.*
- *Banks and institutional investors are not going to self-custody their crypto, too risky. Institutional custody is extremely complex.*
- *Bitcoins competition is gold and other commodities, not the US Dollar.*

The conversation with P3 then moved to Central Bank Digital Currencies (CDBCs) which are crypto-assets issued by the central banks of countries, like the US Federal Reserve (The Fed), the European Central Bank (The ECB), or the Chinese Central Bank (The CCB). Many capital markets participants believe that CBDCs provide a tacit endorsement of crypto-asset technology and are therefore an indicator of further corporate crypto adoption. Participant 3 sees CBDCs as something different, just a way to improve the efficiency of the payments system. His perspective included:

- *CBDCs are like the private blockchains of 2016, they are implemented as private networks with only known participants.*
- *Blockchain as a technology is really just crypto hashed linked list. Not sure if it is the best technology to base a payments system upgrade on.*

The last area that P3 was able to provide input was the AML/KYC issue. His perspective includes:

- *No one, institutions anyway, is buying Bitcoin or other tokens from an unregulated exchange, they can't risk the compliance issue.*
- *Some institutions are trying to create the concept of a "walled garden" where institutions only buy crypto-assets where the prior ownership is known to help ensure AML/KYC compliance.*

Participant 4 Results

Participant 4, P4, has been a capital markets operations executive for over 20 years at one of the leading global investment banks. He has recently transitioned from that role into a consulting partner at a top-tier management consulting firm focused on helping capital markets institutions improve their operational capabilities. This work has brought him into the crypto-asset space as more and more of his clients are seeking advice on how to enter the business. One of the interesting perspectives is that P4 is not an advocate of crypto-asset technology or services but because his clients, who are primarily securities operations managers from large sell-side investment banks, are moving into that space, he is designing and implementing solutions to address the challenges. Key points that surfaced during the P4 interview include:

- *Six months ago all of my investment banking clients thought Bitcoin was a Ponzi scheme and they had no interest in entering the space. Now over half of them are taking active steps to provide services and believe there is something real there.*
- *It's not the wild west like it was a few years ago.*
- *Coinbase is making the largest investment in capabilities directed at the institutional capital markets space.*
- *Attitude among capital markets companies toward AML/KYC issues varies widely. Most traditional banks that are regulated by the OCC the FCA are not yet comfortable with anonymous transactions.*
- *Some banks are focused on only acquiring Bitcoin, or other tokens, from miners that are known to limit their AML/KYC exposure.*

The key aspect that P4 is able to provide is the operational requirements that institutional capital markets companies need to satisfy. As companies enter the crypto space they often start with some type of proof-of-concept, a joint venture with a small company, or another experimental project. These efforts do not require extensive involvement of the operations department is busy managing the trading and settlement flows of the core business, which for a large bank or asset manager is millions of trades per day. The fact that operations managers are now getting involved in crypto-asset services is an indication that these institutions are starting to move into the space more seriously.

Participant 5 Results

- *Bitcoin is the largest PKI implementation in the world. Public blockchains, like bitcoin and Ethereum, are extremely resilient. None of the losses have been caused by Blockchain vulnerabilities. The biggest security issue is the custody component. How the individual user is protecting their keys when interacting with counterparties and service providers?*
- *Merkle tree and public/private key cryptography are 30-year-old technologies.*
- *A DeFi company got hacked for 25M. Even though the bitcoin protocol has never been hacked, the ecosystem surrounding it is immature.*
- *Lazarus group – North Korean hacking group focused on financial services was were able to hack Swift and ATM networks. They focused on crypto because it is easier to move. They are a very skilled advanced persistent threat. Providers need a defense in-depth approach.*
- *Secure multi-party computation (MPC). Don't have a private key on a single server or computer or phone. A decentralized system of endpoints. As long as all devices are not compromised, the system is secure.*

- *HSM – Hardware security model – separates the main operating system from the security chips is a critical element of how we approach hardening our custody offering.*
- *Distributing the system across multiple cloud providers. Which would require collusion among cloud providers to compromise the system.*
- *Dozens of banks get hacked every day and we never hear about it. Crypto hacks are more publicized. 10's or 100's of billions of dollars have been hacked from traditional banks over the past 20 years. Crypto is held to a higher standard.*
- *Cyber Insurance – cold storage insurance does not protect against cyber attacks. Errors and Omissions insurance is critical to insure against accidental damage.*
- *Institutions must have their crypto assets available to earn a return.*
- *Some customers don't want their keys stored in the US or in Europe.*
- *Money will always go to where it is used the most efficiently.*
- *Over 3B US dollars spent by traditional banks in 2019 on cybersecurity capabilities. JP Morgan spends 150M per year on cybersecurity.*

Because of his role and mandate, P5 is clearly an advocate of crypto-asset services and believes the technology and processes they have developed have significantly improved the ability of large institutions to enter the space. As has been highlighted previously, institutional requirements are more robust because of the scale of their operations. Global banks are required to operate in many countries which subjects them to many different regulators and compliance requirements. According to their website, the crypto-asset custody provider, Fireblocks, has received over 179 million dollars in investment capital since its founding in 2019. The Bank of New York Mellon (BNYM), the largest provider of asset custody services in the world, was one of the lead investors in Fireblocks' latest round of capital raising which is another clear indicator that the institutional capital markets providers are moving into the crypto-asset space very aggressively.

Participant 6 Results

Participant 6, P6, was a sell-side currency trader for a global investment bank and then moved on to become a business development executive for a crypto-asset custody provider. While she was a currency trader, P6 focused on helping large multinational organizations manage their foreign currency exposure emanating from their supply chains. This role exposed her to the challenges of serving large institutions in the global capital markets.

Given her role as a salesperson for a crypto-asset custody provider, the interview with P6 centered on the challenges of providing institutional-grade custody services that meet the needs of large global clients that are moving into the space. P6 is also based in Asia reflecting the global nature of the crypto space and how institutional investors there are also entering the market aggressively. Some of the salient points of her interview are listed below:

- *Institutional users are able to get more scale out of their operations with improved custody offerings. Automation can drive bespoke workflows. Maintaining the same bottom line.*
- *From the bank's perspective, they are using native digital players to understand the potential of the space. Banks are listening and looking. Trying to understand the bottom line opportunity. Security and custody issues are important.*
- *The Metamask wallet that many retail investors use is not fit for purpose for institutional clients.*
- *Cold storage will become obsolete. Settlement needs to be on an active wallet construct to support automated delivery assets and the processing of fiat payments.*
- *Multi-Party Computation (MPC) and other new protocols are being enhanced to allow for greater security but also more automation.*
- *Insurance entering the space is critical as that allows these players to offset a portion of their financial risk and take on larger positions.*
- *Regulators getting more comfortable with the space and will likely produce guidance that banks can rely on.*
- *Blockfi – replicating the traditional banking infrastructure – this provides a playbook for other traditional players to enter the capital markets for crypto*

P6 was the last interview for this research effort and many of the points she was able to provide were redundant with the others. It is also apparent that P6, like P5, is an advocate for the crypto-asset services that her organization provides. One area that was unique in the P6 interview was the focus on how some of the banks in Asia are evaluating the different business models in the institutional crypto space. The reference to Blockfi is significant because it is a startup that is attempting to offer a full suite of financial services using crypto-assets. Blockfi is essentially providing all the services that a traditional bank offers, loans, deposits, payments, trading, but with a defined set of crypto-assets as the base currency. This is the furthest any institution has gone to provide a comprehensive financial institution in the crypto space.

Findings

All of the interviewees expressed the belief that institutional capital markets companies are either directly moving into the crypto-asset services space or are strongly considering it despite the fact that there are known cybersecurity issues that create significant financial and reputational risks.

P1 highlighted the fact that most of the senior executives of the providers in this space, banks, broker-dealers, and asset managers, do not understand the underlying technology, cryptography, or advanced mathematics associated with crypto-assets. He emphasized that these executives were entering the crypto-asset market out of necessity to produce returns for their shareholders and to provide the services their clients were demanding. One indicator is that each of the interviewees had successful careers in the financial services industry before the introduction of crypto-assets and are now spending the majority of their time in the space, either because they believe it is the future of capital markets or because their clients are demanding it. Because these individuals are profiting from crypto-asset activity, it casts some doubt on the objectivity of their assessments of risks and benefits from providing services in this market.

Findings Related to Crypto-Asset Custody Risks

The first cybersecurity issue identified for this research was the custody issue. The unique characteristics of crypto-assets, they are pseudo-anonymous bearer instruments with irreversible transactions, create the need for a custody solution that supports the requirements of an institutional capital markets participant. All of the interviewees identified custody as a critical issue that must be addressed for companies to be comfortable entering the space. Institutional investors, and the banks, broker-dealers, and advisors who serve them, manage very large amounts of capital for their clients, and that capital, when deployed in the marketplace, results in very large asset positions. The significant value of these positions creates an attractive target for attackers looking to exploit vulnerabilities for monetary gain.

One of the traditional approaches to securing crypto-assets is the cold wallet or cold storage concept where the cryptographic keys associated with an account that can contain crypto-assets are printed out on paper or stored on a computer that does not have any access to the internet. This approach separates the key from the public network entirely. The challenge with this approach is the lag time introduced between the time when an asset owner chooses to access the assets and the time they are made available. Providers of cold wallet solutions often have service level agreements (SLAs) associated with this lag time that can extend to 24 or 48 hours. Long lag times to access an asset is generally not acceptable to an institutional capital markets company as they need to move their positions frequently and leverage their assets for all available avenues of return, including lending those assets to other companies or pledging those assets as collateral against a loan.

All the interview participants identified custody as a major issue impacting institutional capital markets companies and a significant amount of financial and management resources are being directed to solve the above-listed challenges. The results of the interviews identified two primary vehicles that institutional capital markets companies are using to address the cybersecurity risk associated with custody:

- **1 - Specialized Custody Providers -** Companies like Fireblocks, NYDIG, and Anchorage have developed sophisticated technical capabilities that allow crypto-assets to be stored securely in an electronic vault that provides a combination of security and availability. Most of these solutions have emerged in the last few years and incorporate advanced security techniques such as multi-signature wallets, multi-party computation, multi-cloud infrastructure distribution, and hardware layer security.
- **2 - Insurance -** Although cybersecurity insurance has been around for several years, carriers are now offering products that are specific to cryptoassets and the related custody risks. Companies can insure significant balances allowing them to offset the financial risk associated with the custody exposure of crypto-assets. Insurance is critical as many institutional capital markets companies are highly regulated entities and they have to substantiate to their regulators that they are effectively mitigate the financial and operational risk inherent to their business model.

Findings Associated with Core Infrastructure Risks

As was articulated in the introduction to this research, public blockchain networks provide an ever-growing attack surface for hackers to attempt to compromise. Although the Bitcoin network, the largest and oldest public blockchain network, has never been successfully breached, there are potential vulnerabilities that institutional capital markets participants should consider when evaluating their appetite to enter the market for crypto-asset services. These include:

- **1 -** The 51 percent attack allows a coordinated set of malicious actors to force a change to the blockchain data structure if they are able to gain control of 51 percent of the computing power applied to the network. Although rare, there have been successful attacks on other public blockchain networks resulting in a destruction in value of the underlying assets.
- **2 -** The SHA-256 encryption algorithm used by Bitcoin and other public blockchain networks could be overcome at some point in the future if computing power, like the power that is forecast in quantum computers, continues to advance. Although this risk is relatively low, institutional investors often hold positions for very long time periods. Life insurance companies are one of the largest categories of institutional investors and their position duration is often 30 years or greater.

With the exception of P5 who stressed the fact that the Bitcoin network has never been compromised, none of the other interviewees had a defined opinion on the core infrastructure issues associated with crypto-assets. The fact that the interviewees did not have significant input on this issue could be because most of them are not technology infrastructure experts or that this issue does not raise to the level inside the industry that the prior academic research suggests it should.

Findings Associated with Smart Contracts

Many blockchain implementations provide an embedded capability to develop programs that can impact the movement of the crypto-assets on the blockchain. These programs are called smart contracts, are written in a high-level computer language, and are usually executed inside of a virtual machine on the nodes of the blockchain network. There are specific aspects of smart contracts and the way they are implemented on a public blockchain that introduces risks that need to be considered, including:

- **1 -** Smart contracts can move crypto-assets between wallets and, as has been noted previously, blockchain transactions are irreversible. If a smart contract inadvertently moved assets to the wrong account, there would be no way to move the assets back.
- **2 -** Smart contracts execute autonomously and once they have been deployed to a public blockchain, they can never be shut down.
- **3 -** Blockchains are immutable meaning that existing data structures cannot be modified. If a smart contract has a recognized defect, it cannot be patched in the traditional way that other software is patched. This would leave the defect online and available forever.

Similar to the core infrastructure issues, most of the interviewees did not have material input on the smart contract issues. When pressed, P1 highlighted that the organization that he is working for has hired technical experts with experience in this space and had contracted a smart contract development firm. He also stressed that their offerings were not leveraging public blockchain network implementations of smart contracts, they are leveraging a private blockchain. P2 provided the most input on smart contract issues and focused on the smart contract auditing services that are emerging and believed that capability was going to provide significant comfort to financial services executives as they evaluate the decision criteria around implementing smart contracts onto public blockchain networks.

Findings Associated with AML/ KYC Risks

Another key cybersecurity risk associated with providing crypto-asset services to institutional clients is the identity and counterparty exposures derived from the pseudo-anonymous nature of crypto transactions. Pseudo anonymity presents two different issues that institutional capital markets companies must address:

- **1 - Transaction Counterparty Identification -** Regulated financial services institutions are required to take meaningful steps to ensure that they are not transacting with counterparties that are associated with illicit or illegal activity, including terrorism and drug trafficking. To meet this obligation, companies verify the identity of all of their clients and they rely on the other companies participating in the market to do the same. That way if a bank trades with another bank they are relying on each other's identity verification processes to ensure that their trades are compliant. Since crypto-asset transactions are pseudo-anonymous, the company facilitating the transaction cannot verify the identity of the counterparty and is unable to ensure that they are an authorized entity.

- **2 - Position Exposure -** Even though crypto-asset transactions are pseudo-anonymous they are executed on a public network that can be interrogated via capturing the non-encrypted metadata associated with a transaction. The wallets on public blockchains are available and the individual transaction amounts are known to all network participants. Additional information, such as IP address, is also often available because blockchain nodes require an on-ramp for a user to access them. As more and more transactions are executed, the volume of associated metadata increases, and wallet ownership becomes revealed. Adversarial counterparties can analyze this information to approximate the value of institutional investor positions and can then devise trading strategies to work against those positions, reducing the opportunity of the investor to achieve the desired return from their crypto-asset investments.

The interview results identified two relevant factors associated with pseudo-anonymity:

- **1 -** Some banks, and other players, are looking to create a capability to help ensure that the crypto-assets traded in the marketplace are from validated and authorization counterparties. This concept would require that all crypto-assets provenance be established and the market-making companies would provide guarantees of compliance. This can involve purchasing crypto-assets from miners who have newly created assets that were never owned by an unknown counterparty and then tracking them as they move from one counterparty to another. The challenge with this approach is that as more and more transactions are executed in a particular crypto-asset, the amount of newly created assets shrink and there may not be enough to satisfy the needs of large institutional investors who require large positions in their portfolios. Also, the network of authorized providers would need to be constantly monitored to ensure that a rogue element does not gain access.

- **2 -** There is a bifurcation in the approach to pseudo-anonymity emerging between highly regulated institutions, such as a bank, and lesser regulated institutions, such as a trading app (e.g. Robinhood or Coinbase). The highly regulated entities are not as comfortable and are approaching the crypto-asset services space more cautiously by restricting access to these services to a select group of clients and through a smaller array of services that can be monitored effectively. The less-regulated companies have opened up a broad range of crypto-asset services to virtually all of their clients.

Discussion

In many ways the concept of crypto-assets as serious tools employed by institutional investors and multi-national corporations is ridiculous, very few people actually understand how they work, they are incredibly vulnerable to many forms of cybersecurity exploitation techniques, and there is no limit to supply, as new assets can be created at will by anyone, globally. But it is also clear from the interview results that many, if not most, institutional capital markets participants, including banks, broker-dealers, exchanges, and asset managers, are going to provide some crypto-asset services to their clients. As more traditional companies enter the space they drag a network of next-tier startups and other small companies that aim to provide specialized services to the larger players. All of this activity will cause the value of crypto-assets to increase but since there is no control on the supply of newly created crypto assets, the price action in the market will be highly volatile. The volatility will create opportunities for professional traders to profit from the action at the expense of the smaller participants. The end result of all of this activity is an ever-growing ecosystem of companies with highly variable technology capabilities. That ecosystem represents a major attack surface and a very attractive target for malicious actors, including those that are supported or controlled by nation-states.

Similar to both e-commerce and online banking the direct exposure of technology to the public internet creates a set of challenges that cybersecurity professionals need to address because they are hired by the business to do so. The demand for crypto-asset security solutions is driving massive venture capital and private equity investments, according to CB Insights, an industry research firm, over 25 billion dollars has been invested in blockchain solutions over the past few years. A significant component of this investment will be directed at solving the cybersecurity issues associated with the space. It is incumbent upon cybersecurity industry professionals to continue to invest in understanding how these new capabilities address the underlying risks and issues.

The two biggest issues identified and verified by this research were custody and pseudo-anonymity. The custody solutions identified by the interviewees have complicated services built on very technical infrastructure. The more technology that is applied to the problem, the more potential for vulnerabilities to be introduced. The pseudo-anonymity issues are trending toward a resolution where institutional market participants restrict their operations to a subset of the market that contains known actors. This approach may result in a bifurcation of the crypto-asset market with a controlled and transparent market for regulated institutions and an dark market for everyone else. One issue is that the transparent market is unlikely to provide the action that institutional investors and their facilitators want. The challenge for the cybersecurity professionals is to provide solutions that allow companies to take advantage of the economic opportunities available in the crypto-asset market that effectively mitigates the risks from taking on the associated exposure to the bad actors that are so prevalent in the space.

Implications

A recent article on the Bloomberg financial news website [Mochizuki and Furukawa Mochizuki] profiled the extremely rigorous measures that the technology company Payward Inc., that operates the crypto-asset exchange Kraken, requires their employees to implement to ensure that their services are not compromised. The measures included requiring children to sign non-disclosure agreements and not connect their video game consoles to the internet, executives dressing in disguise, and employees are not allowed to tell anyone they work there or tell their families the address of the office. Payward's approach to security can seem over the top but it highlights how risky it is to provide crypto-asset services when the value of the underlying assets are measured in the billions, soon-to-be trillions, of dollars.

Armored car drivers, who transport cash from banks to depositories and fill the automated teller machines, carry guns, and are authorized to use deadly force to prevent theft. Where there is money to be stolen, there will be criminals looking to steal it. Jamie Dimon, the CEO of the largest bank in the world - JP Morgan Chase, is probably one of the most visible and famous bankers in the world. He has management control and influence over 2.5 trillion dollars of assets. When he travels, he uses a corporate jet and has significant personal security, likely mandated by the JP Morgan Chase board of directors. Although that level of security is certainly warranted, no one believes that if they kidnapped Dimon or members of his family, they could extract the keys to the 2.5 trillion. Unfortunately, that is not the case for the crypto-asset world, and it demonstrates how challenging operating this space can be.

Prior to the creation of Bitcoin, moving billions and trillions of dollars of value electronically was the domain of the Swift network, a consortium of banks that cooperate on a private technology infrastructure that allows banks to exchange currencies among each other. As the internet has matured and payment services like Wechat, Alipay, PayPal, Zelle, and Venmo have emerged they still need to go through the traditional bank system to settle a transaction that involves a government-issued currency, like the US dollar. An individual can Venmo money to another individual and they can spend the value in their account at a merchant, but eventually, it gets converted into a dollar, and that step requires a bank. Bitcoin, and the numerous other cryptocurrencies in circulation, bypass that infrastructure entirely, which is why it has become the preferred payment mechanism for hackers and other criminals.

The traditional financial services institutions that drive the global capital markets, banks, broker-dealers, exchanges, and asset managers, have demonstrated on many occasions that they are willing to take extreme risks for monetary gain, even if it results in significant damage to the global economy. The global financial crisis of 2008 proved what can happen if the markets are left unsupervised. The crypto-asset phenomenon has captured the attention of the institutional capital markets and the intersection of these two worlds is likely to create significant challenges for the entities and individuals charged with their security.

Limitations

The primary limitations to this research are the very small sample size of interview participants and the fact that the crypto-asset space is changing so rapidly any insights captured today could be irrelevant tomorrow.

End of Article

References

[Amiet 2021] Nils Amiet. 2021. Blockchain Vulnerabilities in Practice. Digital Threats: Research and Practice 2, 2, Article 8 (March 2021),
7 pages. https://doi.org/10.1145/3407230

[Biryukov, Khovratovich, and Pustogarov 2014] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. 2014. Deanonymisation of Clients in Bitcoin P2P Network. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (Scottsdale, Arizona, USA) (CCS '14). Association for Computing Machinery, New York, NY, USA, 15–29. https://doi.org/10.1145/2660267.2660379

[Bissias, Levine, and Kapadia 2017] George Bissias, Brian N. Levine, and Nikunj Kapadia. 2017. Market-Based Security for Distributed Applications. In Proceedings of the 2017 New Security Paradigms Workshop (Santa Cruz, CA, USA) (NSPW 2017). Association for Computing Machinery, New York, NY, USA, 19–34. https://doi.org/10.1145/3171533.3171541

[Bistarelli and Santini 2017] Stefano Bistarelli and Francesco Santini. 2017. Go with the -Bitcoin- Flow, with Visual Analytics. In Proceedings of the 12th International Conference on Availability, Reliability and Security (Reggio Calabria, Italy) (ARES '17). Association for Computing Machinery, New York, NY, USA, Article 38, 6 pages. https://doi.org/10.1145/3098954.3098972

[Brent, Grech, Lagouvardos, Scholz, and Smaragdakis 2020] Lexi Brent, Neville Grech, Sifis Lagouvardos, Bernhard Scholz, and Yannis Smaragdakis. 2020. Ethainter: A Smart Contract Security Analyzer for Composite Vulnerabilities. In Proceedings of the 41st ACM SIGPLAN Conference on Programming Language Design and Implementation (London, UK) (PLDI 2020). Association for Computing Machinery, New York, NY, USA, 454–469. https://doi.org/10.1145/3385412.3385990

[Chang, Baudier, Zhang, Xu, Zhang, and Arami 2020] Victor
Chang, Patricia Baudier, Hui Zhang, Qianwen Xu, Jingqi Zhang, and Mitra Arami. 2020. How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees. Technological Forecasting and Social Change 158 (2020), 120166. https://doi.org/10.1016/j.techfore.2020.120166

[Chen, Pendleton, Njilla, and Xu 2020] Huashan Chen, Marcus Pendleton, Laurent Njilla, and Shouhuai Xu. 2020. A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses. ACM Comput. Surv. 53, 3, Article 67 (June 2020), 43 pages. https://doi.org/10.1145/3391195

[DuPont and Squicciarini 2015] Jules DuPont and Anna Cinzia Squicciarini. 2015. Toward De-Anonymizing Bitcoin by Mapping Users Location. In Proceedings of the 5th ACM Conference on Data and Application Security and Privacy (San Antonio, Texas, USA) (CODASPY '15). Association for Computing Machinery, New York, NY, USA, 139–141. https://doi.org/10.1145/2699026.2699128

[Durieux, Ferreira, Abreu, and Cruz 2020] Thomas Durieux, Joa˜o F. Ferreira, Rui Abreu, and Pedro Cruz. 2020. Empirical Review of Automated Analysis Tools on 47,587 Ethereum Smart Contracts. In Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering (Seoul, South Korea) (ICSE '20). Association for Computing Machinery, New York, NY, USA, 530–541. https://doi.org/10.1145/3377811.3380364

[Garfatta, Klai, Gaaloul, and Graiet 2021] Ikram Garfatta, Kais Klai, Walid Gaaloul, and Mohamed Graiet. 2021. A Survey on Formal Verification for Solidity Smart Contracts. In 2021 Australasian Computer Science Week Multiconference (Dunedin, New Zealand) (ACSW '21). Association for Computing Machinery, New York, NY, USA, Article 3, 10 pages. https://doi.org/10.1145/3437378.3437879

[Gervais, Ritzdorf, Karame, and Capkun 2015] Arthur Gervais, Hubert Ritzdorf, Ghassan O. Karame, and Srdjan Capkun. 2015. Tampering with the Delivery of Blocks and Transactions in Bitcoin. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (Denver, Colorado, USA) (CCS '15). Association for Computing Machinery, New York, NY, USA, 692–705. https://doi.org/10.1145/2810103.2813655

[Ghaleb and Pattabiraman 2020] Asem Ghaleb and Karthik Pattabiraman. 2020. How Effective Are Smart Contract Analysis Tools? Evaluating Smart Contract Static Analysis Tools Using Bug Injection. In Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis (Virtual Event, USA) (ISSTA 2020). Association for Computing Machinery, New York, NY, USA, 415–427. https://doi.org/10.1145/3395363.3397385

[Jiang, Liu, and Chan 2018] Bo Jiang, Ye Liu, and W. K. Chan. 2018. ContractFuzzer: Fuzzing Smart Contracts for Vulnerability Detection. In Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering (Montpellier, France) (ASE 2018). Association for Computing Machinery, New York, NY, USA, 259–269. https://doi.org/10.1145/3238147.3238177

[Karame 2016] Ghassan Karame. 2016. On the Security and Scalability of Bitcoin's Blockchain. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (Vienna, Austria) (CCS '16). Association for Computing Machinery, New York, NY, USA, 1861–1862. https://doi.org/10.1145/2976749.2976756

[Kovalchuk, Kaidalov, Nastenko, Shevtsov, Rodinko, and Oliynykov 2018] Lyudmila Kovalchuk, Dmytro Kaidalov, Andrii Nastenko, Oleksiy Shevtsov, Mariia Rodinko, and Roman Oliynykov. 2018. Number of Confirmation Blocks for Bitcoin and GHOST Consensus Protocols on Networks with Delayed Message Delivery: Extended Abstract. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (Munich, Germany) (CryBlock'18). Association for Computing Machinery, New York, NY, USA, 42–47.
https://doi.org/10.1145/3211933.3211941

[Kwon, Kim, Son, Vasserman, and Kim 2017] Yujin Kwon, Dohyun Kim, Yunmok Son, Eugene Vasserman, and Yongdae Kim. 2017. Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (Dallas, Texas, USA) (CCS '17). Association for Computing Machinery, New York, NY, USA, 195–209. https://doi.org/10.1145/3133956.3134019

[Lai and Luo 2020] Enmei Lai and Wenjun Luo. 2020. Static Analysis of Integer Overflow of Smart Contracts in Ethereum. In Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy (Nanjing, China) (ICCSP 2020). Association for Computing Machinery, New York, NY, USA, 110–115.
https://doi.org/10.1145/3377644.3377650

[Lee and Kim 2020] Suhyeon Lee and Seungjoo Kim. 2020. Proof-of-Stake at Stake: Predatory, Destructive Attack on PoS Cryptocurrencies. In Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems (London, United Kingdom) (CryBlock '20). Association for Computing Machinery, New York, NY, USA, 7–11. https://doi.org/10.1145/3410699.3413791

[Luu, Chu, Olickel, Saxena, and Hobor 2016] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. 2016. Making Smart Contracts Smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (Vienna, Austria) (CCS '16). Association for Computing Machinery, New York, NY, USA, 254–269. https://doi.org/10.1145/2976749.2978309

[Mense and Flatscher 2018] Alexander Mense and Markus Flatscher. 2018. Security Vulnerabilities in Ethereum Smart Contracts.
In Proceedings of the 20th International Conference on Information Integration and Web-Based Applications amp; Services (Yogyakarta, Indonesia) (iiWAS2018). Association for Computing Machinery, New York, NY, USA, 375–380.
https://doi.org/10.1145/3282373.3282419

[Mochizuki and Furukawa 2021] Takashi
Mochizuki and Yuki Furukawa. 2021. One Crypto Exchange Is Going to Extreme Lengths on Cybersecurity.
https://www.bloomberg.com/news/articles/2021-06-08/kraken-cryptoexchange-is-going-to-extreme-lengths-on-cybersecurity

[Saad, Spaulding, Njilla, Kamhoua, Shetty, Nyang, and Mohaisen 2019]
Muhammad Saad, Jeffrey Spaulding, Laurent Njilla, Charles Kamhoua, Sachin Shetty, DaeHun Nyang, and Aziz Mohaisen. 2019. Exploring the attack surface of blockchain: A systematic overview. arXiv preprint arXiv:1904.03487 (2019).

[Toufaily, Zalan, and Dhaou 2021] Elissar Toufaily, Tatiana Zalan, and Soumaya Ben Dhaou. 2021. A framework of blockchain technology adoption: An investigation of challenges and expected value. Information Management 58, 3 (2021), 103444. https://doi.org/10.1016/j.im.2021.103444

[Zhang, Xue, and Liu 2019] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and Privacy on Blockchain. ACM Comput. Surv. 52, 3, Article 51 (July 2019), 34 pages. https://doi.org/10.1145/3316481

ARMSTRONG WOLFE

SUTHERLAND

Christopher Rigg
christopher.rigg@sutherlandglobal.com

Gwen Wilcox
g.wilcox@armstrongwolfe.com

Find us on LinkedIn - Armstrong Wolfe

www.armstrongwolfe.com