INSURING CRYPTO: THE BIRTH OF DIGITAL ASSET INSURANCE

Adam Zuckerman[†]

ABSTRACT

In December 2020, Bitcoin hit an all-time high of over $28,000…and rising. New digital assets (also referred to as "crypto assets") are being launched seemingly every day, and more people and investors hold crypto assets than ever before. Yet, the same characteristics, such as immutability and decentralization, that make crypto assets innovative can contribute to them being particularly susceptible to costly hacks.

Digital asset insurance is a new product that provides coverage against such loss or theft. Security-oriented crypto custody providers and crypto wallets have greatly reduced the risk of hacks, but these solutions are all still relatively new, untested, and unavailable to many crypto holders. In 2019 and 2020, billions of dollars of crypto assets were stolen or lost through hacks and scams, many of which were high-profile and highly publicized. The threat of a hack, real or perceived, still acts as a strong deterrent to broader adoption and usage of crypto assets. Digital asset insurance provides a necessary backstop for holders of crypto assets while also lending legitimacy in an industry often perceived as unsafe or even nefarious.

In this paper, I provide an overview of the digital asset industry. I outline which insurers are providing digital asset insurance, how insurers are overcoming the challenges of underwriting this new insurance product, and which companies in the crypto ecosystem are obtaining coverage. I discuss several shortcomings in the new industry including the problems associated with the murky regulatory landscape, the lack of transparency for consumers, and the significant amount of bias around the crypto industry. I also propose ways in which digital asset insurance could be more efficient and effective including insurers creating industry standards and serving as a de facto regulator in digital asset storage.

[†] Associate, Latham & Watkins and recent graduate of University of Pennsylvania Carey Law School. First and foremost, many thanks to Professor Tom Baker, who oversaw my research and provided invaluable advice and guidance. I would also like to thank Sarah Downey, Yussuf Hussein, and Jeremy Sklaroff for their time and insights. Thank you also to Mia Cabello and Mike Buchwald for their helpful feedback. Lastly, I greatly appreciate the editors of the University of Illinois Journal of Law, Technology, and Policy.

In just a few short years, this insurance product has gone from nonexistent to a multi-hundred-million-dollar premium market that is growing faster than cyber insurance. Despite the insurance product's progress or importance to the broader crypto ecosystem, this paper is the first scholarly analysis of the digital asset insurance industry.

TABLE OF CONTENTS

* * *

INTRODUCTION

A jewelry store holds millions of dollars' worth of precious metals and stones. Naturally, some people would like to steal them. So, most jewelry stores hire guards, keep the jewels in locked boxes, install high tech security systems, and take any measures they deem prudent to prevent these valuable and expensive items from being stolen. Even with all of this security, there is always a chance, however slight, that the jewels can be stolen.[1] For this, the owner will likely purchase insurance.

In the last several years, a new type of insurance has become available: digital asset insurance. Digital assets are a digitally native asset class that have no physical component. In the industries' infancy, digital assets were stored in a digital wallet. These solutions, which frequently left the assets vulnerable to hacking, were the digital equivalent of an envelope hidden under a mattress.[2] Many companies have since launched innovative high-tech solutions that promise safer storage. But the security of digital assets remains a huge problem in the industry.[3]

In 2019, a record high of twelve different crypto asset exchanges were hacked[4] and over $4 billion of cryptocurrency (a type of digital asset) were stolen or scammed worldwide.[5] Recent scandals include South Korean exchange UpBit's loss of approximately $50 million worth of Ether (a popular cryptocurrency) on November 27, 2019,[6] and a few days later all funds were frozen at Chinese exchange Idax when the CEO suddenly "went missing" – a situation that remained unresolved months later.[7] New crypto exchange Altsbit received an unwelcome response to its release when it was hacked in February 2020, mere months after publicly launching its services.[8] Many of these crypto losses have occurred because companies have failed to store their digital assets in secure solutions – precisely the problem new custody providers are attempting to solve. Yet, even when security is made a priority, the technology is so new and the regulatory oversight so limited, there still remains a

[1] *See* Joshua Davis, *The Untold Story of the World's Biggest Diamond Heist,* WIRED (Mar. 12, 2009; 12:00 PM), https://www.wired.com/2009/03/ff-diamonds-2/ (discussing a multi-million diamond heist at a well-protected, seemingly secure vault).
[2] *See* Kai Sedgewick, *Bitcoin History Part 18: The First Bitcoin Wallet*, BITCOIN.COM (Oct. 6, 2019), https://news.bitcoin.com/bitcoin-history-part-18-the-first-bitcoin-wallet/ (discussing how users would merely store their private key directly on their computer).
[3] *See A Comprehensive List of Cryptocurrency Exchange Hacks*, SELFKEY, (Feb. 13, 2020), https://selfkey.org/list-of-cryptocurrency-exchange-hacks/%20 (providing an updated list of all major cryptocurrency exchange hacks).
[4] *Id.*
[5] *See* Jeb Su, *Hackers Stole Over $4 Billion From Crypto Crimes in 2019 So Far, up From $1.7 Billion in All of 2018*, FORBES (Aug. 15, 2019, 1:49 PM), https://www.forbes.com/sites/jeanbaptiste/2019/08/15/hackers-stole-over-4-billion-from-crypto-crimes-in-2019-so-far-up-from-1-7-billion-in-all-of-2018/#7762eacc55f5.
[6] *See* Tomáš Foltyn, *Cryptocurrency Exchange Loses US$50 Million in Apparent Hack*, WELIVESECURITY (Nov. 27, 2019, 5:06 PM), https://www.welivesecurity.com/2019/11/27/upbit-cryptocurrency-exchange-hack/.
[7] Eric Thomas, *IDAX Exit Scam? Users Face Withdrawal Difficulty*, CRYPTO BRIEFING (Nov. 27, 2019), https://cryptobriefing.com/idax-exit-scam-users-face-withdrawal-difficulty/.
[8] *A Comprehensive List of Cryptocurrency Exchange Hacks*, *supra* note 2.

material chance of a hack or other loss.[9] As with the storage of valuable jewels, entirely eliminating the chance of theft is impossible. And thus, the industry of digital asset insurance was born.[10]

This paper is the first evaluation of the current state of the digital asset insurance market. I hope to provide an objective overview of the industry, the players, and the insurance product for those hoping to learn about this new and exciting product. The paper is also an attempt to elucidate the role that insurance can play in the digital asset ecosystem. Blockchain technology and the underlying digital assets are evolving extremely quickly, and the laws and regulators have no hope of keeping up with the industry at its current pace. There is therefore an inevitable tension between the innovators and how the laws apply to their new technology. This creates risk for insurers as explained below. But it is also an opportunity for insurers to play a critical role in the digital asset ecosystem as a centralized governance alternative to government. Insurers can create systemic incentives that serve as an alternative to laws and regulation. Where laws and regulation are destined to fall behind technology, insurance can in some instances be a preferable alternative. I argue throughout that this new insurance product can and should act as a supplement to regulation in the digital asset security and custody industry.

Part I introduces foundational knowledge of both the digital asset space and the relevant areas of the insurance industry needed to engage with this emerging insurance product. I provide a brief overview blockchain technology, cypto and digital assets, storage of digital assets, and the relevant insurance theory.

Part II provides the most expansive overview to date of the digital asset insurance industry, including the types of companies that are obtaining digital asset insurance policies, what parties are brokering and underwriting the insurance, as well as how the insurance industry is approaching the challenge of creating policies for this new asset class. Part III enumerates several shortcomings of and factors that hinder the current approach to insuring digital assets, including a lack of loss history for insured digital assets, minimal transparency in the policy offerings, continued regulatory uncertainty, and human bias in the crypto industry.

In Part IV, I make two proposals for how I believe digital asset insurance could be more efficient, effective, and provide better value to both insurers and insureds. I suggest that those seeking digital asset insurance look to captives (a wholly-owned subsidiary that provides insurance to the parent company) as an alternative solution to third-party insurance, and I explore the possibility of the insurance industry functioning as a de facto regulator to improve digital asset storage security industry

[9] *See* Jeff Kauflin, *Lloyd's of London, Aon and Others Poised to Profit From Cryptocurrency Hacker Insurance*, FORBES (Sep. 5, 2019, 11:18 AM), https://www.forbes.com/sites/jeffkauflin/2019/09/05/lloyds-of-london-aon-and-others-poised-to-profit-from-cryptocurrency-hacker-insurance/#72a3761932aa (discussing the pervasive threat of hacks of companies with industry-leading securities, such as Binance, a security-conscious exchange with its own custody service).

[10] Insurance does not account for losses due to normal market factors such as general price volatility.

wide. Finally, I conclude by reaffirming the importance of insurance to the adoption of digital assets as a mainstream asset class.

I. AN OVERVIEW OF DIGITAL ASSETS AND THE RELEVANT INSURANCE PRODUCTS

Understanding the digital asset insurance industry first requires some knowledge of blockchains, digital assets, storage solutions for digital assets, as well as the relevant areas of insurance. **If you are well versed in these topics, feel free to skip to Part II.**

A. What is Blockchain?

A blockchain[11] is a database that is stored and shared across a number of computers, frequently called nodes.[12] These nodes perform cryptographic computations that validate transactions on the blockchain.[13] When a sufficient number of nodes (usually a majority though this can vary depending on the blockchain) validate a transaction, it and a group of other validated transactions are added to the ledger.[14] This ledger, the blockchain, is independently maintained by many or all of the nodes.[15]

While not a perfect analogy, Google Documents provide a useful starting point for understanding a blockchain. Imagine a Google Document that is open on thousands of computers all around the world at any given time. Each computer competes in a cryptographic competition to validate the new text that can be added to the Google Document by anybody, and the computer that wins the competition is rewarded. As long as the majority of other computers then verify that the text is valid, it is encoded onto a page on the Google Document. Unlike a Google Document, however, it cannot be edited, only added to. As new text is added, it is cryptographically linked to the previous page, such that if anybody tries to change the text on a prior page, it will invalidate the entire string and be rejected by the rest of the nodes.

The release of Bitcoin in 2008 marked the first functional application of a

[11] The term "distributed ledger technology," though technically different, is frequently used interchangeably with the term blockchain. *See* Hasib Anwar, *Blockchain vs. Distributed Ledger Technology*, 101 BLOCKCHAINS (Jan. 6, 2019), https://101blockchains.com/blockchain-vs-distributed-ledger-technology/ (explaining that despite their interchangeability, blockchain and distributed ledger technology differ in many respects).
[12] Maryanne Murray, *Blockchain Explained*, REUTERS GRAPHICS (June 15, 2018), http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html.
[13] *See* Ameer Rosic, *What is Blockchain technology? A Step-by-Step Guide for Beginners,* BLOCKGEEKS.COM, https://blockgeeks.com/guides/what-is-blockchain-technology/ (last visited Oct. 17, 2020) (explaining the function and importance of nodes).
[14] *Id.*
[15] *Id.*

blockchain.[16] While Bitcoin itself has gained prominence, the blockchain technology it was built on is widely believed to be far more revolutionary.[17] I will not dive into the nuances of blockchain technology (particularly as different blockchains have very different structures and purposes), but the fundamental technological breakthrough is that blockchains allow code to run autonomously without a single party having the authority to control or modify it.[18] This permits users to trust the code without trusting any individual or organization. This principle has a wide array of potentially disruptive applications.

The Bitcoin Network harnesses this technology for a very specific purpose: the transmission of digital money called bitcoin.[19] Bitcoin was the first to solve what is referred to as the "double spend problem"[20] in the digital environment. Previously, if I held $10 in my bank account, the only way to verify that I could not send the $10 to more than one different person was to rely on a trusted intermediary such as a bank, who must be trusted to ensure that I do not "double spend" the money in my account. Cash solves this problem in the physical world, as I cannot give the same $10 bill to multiple people, but the distributed ledger and validation system of a blockchain autonomously ensures that the same digital assets cannot be sent to two different people online.[21] It eliminates this specific need for a bank. For the first time, Bitcoin allowed people to trust the code rather than trusting entities such as banks and governments for the purpose of transmitting money online. If you live in a country such as Venezuela, Indonesia, Iran, Lebanon, Argentina or any other country with a highly volatile currency, untrustworthy government, or poor banking infrastructure, relying on code rather than institutions might be an extremely attractive proposition.

In addition to sending money to one another or safeguarding valuable assets without a bank, the "trustless" infrastructure of a blockchain appears valuable to any number of industries. The use cases span from mundane changes to businesses' recordkeeping systems,[22] to fundamental transformations in the way personal data is

[16] *See* Ameer Rosic, *What is Bitcoin? [The Most Comprehensive Step-by-Step Guide]*, BLOCKGEEKS.COM, https://blockgeeks.com/guides/what-is-bitcoin/ (last visited Oct. 17, 2020) (explaining how Bitcoin is a "decentralized digital currency" that "can be sent from user to user on the peer-to-peer bitcoin blockchain network without the need for intermediaries").
[17] *See* Nathaniel Popper, *The People Leading the Blockchain Revolution*, NY TIMES (June 27, 2018), https://www.nytimes.com/2018/06/27/business/dealbook/blockchain-stars.html (discussing the revolutionary potential of blockchain technology).
[18] For a good guide of how blockchains work, *see generally*, Rosic, *supra* note 13.
[19] Rosic, *supra* note 16.
[20] *See* Jake Frankenfield, *Double-Spending*, INVESTOPEDIA (last updated June 30,2020), https://www.investopedia.com/terms/d/doublespending.asp (discussing how Bitcoin "has a mechanism based on transaction logs, known as the blockchain, to verify the authenticity of each transaction and prevent double-counting").
[21] *See* Rosic, *supra* note 16 ("As each block enters the system, it is broadcast to the peer-to-peer computer network of users for validation. In this way, all users are aware of each transaction, which prevents stealing and double-spending, where someone spends the same currency twice.").
[22] *See How This Restaurant Operator Uses Blockchain to Reimagine Loyalty,* HOSPITALITY TECHNOLOGY (Jan. 2, 2018), https://hospitalitytech.com/how-restaurant-operator-uses-blockchain-reimagine-loyalty (discussing how Chanticleer Holdings uses a blockchain database rather than a traditional database to track restaurant loyalty points).

stored and shared on the internet,[23] to frivolous blockchain-enabled collectibles and games.[24] There are many practical obstacles standing in the way of broader adoption and the envisioned blockchain utopia, but many are confident that the technological benefits of blockchain will help reshape the future.[25]

B. What are Digital Assets?

Powering the blockchain-based ecosystems described above are a new asset class referred to as *digital assets.* Previously, the term digital asset was used to describe any asset in a digital form.[26] This could mean money, securities, data, music, or any other digital representation with value. More recently the term digital asset has been adopted and largely co-opted by the blockchain community to reference what is more intuitively called a crypto asset.[27]

A crypto asset is a digitally *native* form of stored value that relies on the verification properties of a blockchain. [28] Crypto asset is a broad term that encompasses digitally native assets that can take many different forms.[29] Some, such as bitcoin and ether, function as digital currencies. These are pure stores of value that are digitally native alternatives to fiat currency. Because of the cryptography required for the decentralized validation process that makes this possible, this specific type of crypto asset has been dubbed a "cryptocurrency."

Other digital assets can function more like a stock, giving the holder voting

---

[23] *See Profiles*, 3BOX, https://3box.io/products/profiles (last visited Oct. 17, 2020) (explaining how 3Box offers decentralized identity tools that allow users to maintain control of their data rather than let large technology companies exploit and profit from their data).

[24] *See* CRYPTOKITTIES, http://www.cryptokitties.co/ (last visited Oct. 17, 2020) (displaying Cryptokitties as a game where users can raise and trade digital kitties on the blockchain).

[25] It should be noted that as the industry has continued to develop, the uses and structures of new blockchains have begun to vary. Libra, for example, is a high-profile proposed stablecoin that would operate as a global digital currency. THE LIBRA ASSOCIATION, https://libra.org/en-US/association/ (last visited Oct. 17, 2020). As proposed, the blockchain would be controlled by a small group of association members rather than the decentralized format of Bitcoin or Ethereum, and the currency would be pegged to other stable assets rather than deriving its value from the network itself. *Id*. Therefore, the description above should be considered a loose but malleable definition of a blockchain.

[26] *See* WIKIPEDIA, Digital Asset, https://en.wikipedia.org/wiki/Digital_asset (last visited Oct. 17, 2020) (referring to digital assets in the traditional sense of "anything that exists in a digital format and comes with the right to use").

[27] *See* FIDELITY DIGITAL ASSETS, https://www.fidelitydigitalassets.com/digital-asset-basics (last visited Oct. 17, 2020) (referring specifically to blockchain-based digital assets not the traditional notion of digital assets).

[28] *What Exactly Is a Digital Asset & How to Get the Most Value From Them?*, MERLINONE, https://merlinone.com/what-is-a-digital-asset/ (last visited Oct. 17, 2020).

[29] *See* ICAEW, CRYPTO-ASSETS: ANTI-MONEY LAUNDERING GUIDANCE FOR ACCOUNTANTS 2 (2019), https://www.icaew.com/-/media/corporate/files/technical/legal-and-regulatory/money-laundering/guidance-on-crypto-assets.ashx#:~:text=Crypto%2Dassets%20is%20a%20broad,security%20tokens%20and%20utility%20tokens. ("Crypto-assets is a broad term covering all assets stored on distributed ledgers. This includes all cryptocurrencies as well as non-currency assets such as security tokens and utility tokens.").

rights in the digital ecosystem for which the asset was created, known colloquially as a "security token."[30] Another type, frequently called a "utility token," function like a Chuck-E-Cheese coin – a store of value designed only to be used in a specific ecosystem.[31] Still other digital assets have a different or some combination of purposes. All of these different types of assets fall into the broader category of a crypto asset as long as they are digitally native and rely on a blockchain.

I only wade into the murky waters of terminology[32] because the insurance industry has largely adopted the phrasing of "digital asset insurance" to refer to this emerging industry of insuring blockchain-based assets. This is representative of the broader trend of those in the blockchain community using the term digital asset to refer to what could be more accurately described as a crypto asset. I, therefore, use the terms "digital asset" and "crypto asset" interchangeably to refer to all digitally native assets that rely on a blockchain. Though cryptocurrency is also often used interchangeably with these two terms as it is the most popular form of crypto asset, I use it only to describe crypto assets that function as currency.

C. Crypto Storage Solutions

Digital assets have no inherent physical characteristics.[33] Instead, they are encoded onto a blockchain, and the owner of a digital asset is whatever pseudonymous account the distributed ledger (the blockchain) publicly says owns the value.[34] That account is accessed with a password known as a private key, and anybody with the private key can transfer the digital assets.[35] Storing digital assets is in essence the practice of saving and protecting the private key. If the private key is lost, the assets remain locked up forever.[36] And if the private key is stolen, the assets can be stolen.[37]

---

[30] Digital assets that have more characteristics of a stock or other security are generally referred to as a "security token." Rajarshi Mitra, *Utility Tokens vs Security Tokens: Learn the Difference – Ultimate Guide,* BLOCKGEEKS.COM, https://blockgeeks.com/guides/utility-tokens-vs-security-tokens/ (last visited Oct. 17, 2020). Whereas, tokens that are designed to be a currency for use in a blockchain-based ecosystem are called "utility tokens." *Id*. These are loose and usually self-proclaimed definitions, and frequently an asset can have characteristics of both if, for example, it can be used in an ecosystem but also is expected to gain value like a security. *Id*.

[31] *Id*.

[32] *See* Angela Walch, *The Path of the Blockchain Lexicon (And The Law),* 36 REV. BANKING & FIN 713 (2016-2017) (discussing how terminology in the blockchain world is ever-changing causing problems both within the industry and for regulators).

[33] *What are cryptoassets (cryptocurrencies)?*, BANK OF ENGLAND, https://www.bankofengland.co.uk/knowledgebank/what-are-cryptocurrencies (last visited Oct. 17, 2020).

[34] Harsh Agrawal, *What Is Cold Storage In Cryptocurrency?,* COINSUTRA, https://coinsutra.com/cold-storage-cryptocurrency/ (last updated August 12, 2019).

[35] *Id*.

[36] *Id*.

[37] This is barring extreme measures such as a fork of the entire blockchain. For an explanation of forks, *see* Nate Maddrey, *Blockchain Forks Explained*, MEDIUM: DIGITAL ASSET RES. (Sep. 18, 2018), https://medium.com/digitalassetresearch/blockchain-forks-explained-8ccf304b97c8.

The nature of a blockchain is that transactions are typically irreversible,[38] and public ownership is pseudonymous; thus, it is often impossible to determine by whom the assets were stolen, and the chance of recovery is usually very slim.[39]

Two different types of services have emerged to help store, manage, and safeguard digital assets: non-custodial and custodial services. A non-custodial service or self-hosted wallet helps users manage their private key, but the digital assets always remain in the "possession" of the user.[40] The value of the non-custodial wallet is primarily to provide a user-friendly way for people to interact with the blockchain and control their digital assets.[41] Alternatively, digital asset custody services take possession of the private key and therefore the assets themselves.[42] The difference between the two can be analogized to a home-safe versus a bank. The non-custodial service allows the user to maintain possession of the assets in a simple, easy, and relatively cheap way, whereas the custodial service takes possession of the asset but in theory provides a centralized, high-security environment. Because non-custodial services are often free and simple, they tend to be the preferred method of storage for hobbyists and those with small amounts of digital assets. Custodial services are more frequently employed by exchanges, investors, or individuals with large amounts of digital assets.[43]

Custody versus non-custody distinguishes between who maintains possession of the assets but bears no relation to the technological method of storing and securing the digital assets – this can also be broadly divided into two categories: cold storage and hot storage. *Cold storage* refers to private keys that are kept in an offline environment, not connected to the internet.[44] There are numerous techniques that would be considered cold storage. This can be as low tech as writing the alphanumeric private key on a piece of paper and hiding it.[45] Or it can be a physical device similar to a sophisticated flash drive that is kept within a safe or vault that is then protected by a security system that is then watched over by armed guards.[46] Professional

[38] A transaction can be reversed through a process called a fork. A fork essentially creates an entirely new blockchain and thus in essence reversing any transactions that occurred after the point at which the fork occurs. Forks can be applied retroactively for the purpose of negating a transaction. Forks require considerable consensus among nodes, and because of the severity of the action are seen as a momentous occasion in the life of a blockchain. Because one of the basic tenets of a blockchain is its immutability, forks often reduce trust in the blockchain and are only used as an option of last resort.
[39] BITGO, *Insurance for Digital Currencies: What Clients Need to Know* 1 (2020), http://pages.bitgo.info/rs/978-TPI-136/images/Insurance%20Whitepaper.pdf .
[40] GARRICK HILEMAN & MICHEL RAUCHS, GLOBAL CRYPTOCURRENCY BENCHMARKING STUDY 55 (2017), https://www.crowdfundinsider.com/wp-content/uploads/2017/04/Global-Cryptocurrency-Benchmarking-Study.pdf (pg 55)
[41] Chirag Bhardwaj, Custodial vs. Non-Custodial Wallets: The Working and Difference Points, APPINVENTIV, https://appinventiv.com/blog/custodial-vs-non-custodial-wallets/ (last updated Aug. 19, 2020).
[42] Hileman & Rauchs, *supra* note 40, at 55.
[43] Bhardwaj, *supra* note 41.
[44] *Hot wallet vs cold wallet: How should you store crypto?*, LIQUID (Nov. 6, 2018), https://blog.liquid.com/hot-wallet-vs-cold-wallet-how-should-you-store-crypto.
[45] *Id*.
[46] *Id*.

custodial services are hopefully closer to the latter.

Hot storage refers to solutions that remain connected to the internet. In theory, this leaves the digital assets more vulnerable to hackers who can potentially access the private key through some online vulnerability.[47] The benefit of hot storage, however, is that the assets are more liquid and can be transferred more quickly than cold storage, which may require one or more people to physically access a vault before the digital assets can be transferred.[48]

Companies will often use a combination of hot and cold storage, keeping only enough assets in hot storage to remain sufficiently liquid and the rest in cold storage. Complicating the matter further, other companies have devised hybrid solutions referred to as *warm storage*, which are neither fully online nor offline, but rather sit somewhere in between.[49] The configuration will differ depending on the particular product, but warm storage usually entails a solution that stores private keys offline until liquidity of the crypto assets is requested, at which time the system is brought online to allow the transfer of the assets.[50] Metaco, for example, a Swiss-based crypto custody solution uses custom hardware and software that essentially allows the storage to switch between hot and cold.[51]

Many different types of institutions have entered the crypto custody industry. Some such as BNY Mellon Crypto Custody[52] and Fidelity Digital Assets[53] are state chartered banks and trust companies with a long history of custody services for traditional assets that are now expanding their offerings to include crypto custody. Others such as Bakkt[54] or BitGo[55] are upstarts that began specifically as a crypto custody service. While still more were developed by companies in a different realm of the digital asset industry who needed to store large amounts of crypto assets so developed a custody solution in-house. For example, leading US crypto exchanges Coinbase[56] and Gemini[57] both developed their own custody solutions that now operate as standalone products.

Today, custody services provide digital asset safekeeping primarily for high

---

[47] *Id*.
[48] *Id*.
[49] AON RISK SOLS., CRIME INSURANCE FOR CRYPTOCURRENCIES 1 (2018).
[50] *Silo by Metaco: Unified Hot-to-Cold Storage*, METACO (May 21, 2019), https://www.metaco.com/silo-by-metaco-unified-hot-to-cold-storage/.
[51] *SILO: The Digital Asset Management Solution for Bank*, METACO, https://www.metaco.com/solutions/silo/, (last visited Apr. 4, 2020).
[52] *See* Kara Kennedy, *Crypto Custody,* BNY MELLON (Oct. 2018), https://www.bnymellon.com/us/en/insights/all-insights/crypto-custody.html (discussing how BNY Mellon, one of the world's largest custody providers for traditional assets has long indicated that they intend to enter the crypto custody industry though they currently have an ongoing partnership with Bakkt).
[53] *See* FIDELITY DIGITAL ASSETS, https://www.fidelitydigitalassets.com/overview (last visited Oct. 17, 2020).
[54] *See* THE BAKKT WAREHOUSE, https://www.bakkt.com/bakkt-markets#custody (last visited Oct. 18, 2020).
[55] *See* BITGO, https://www.bitgo.com/services/custody (last visited Oct. 18, 2020).
[56] *See* COINBASE, https://custody.coinbase.com/ (last visited Oct. 18, 2020).
[57] *See* GEMINI CUSTODY, https://gemini.com/custody (last visited Oct. 18, 2020).

net-worth individuals, institutions such as hedge funds that have large digital asset portfolios, and other companies in the digital asset industry that process or store large amounts of digital assets such as crypto exchanges – though retail custody providers are available as well.[58] Individuals or companies that have large amounts of digital assets are increasingly turning to professional custodial services such as those listed above to safeguard their assets. These custodial services can house millions or even billions of dollars' worth of digital assets and therefore have a strong interest in protecting their clients' assets.[59] The custody providers are largely driving the demand for digital asset insurance as protection in the event of a hack.[60]

D. Insurance for Digital Assets

Insurance companies are in the business of assessing risk. The basic model of an insurance company is to agree to indemnify a third-party against an unknown future loss in return for steady payments (premiums).[61] Insurers try to price the policy such that they expect to receive more in premiums than they will have to pay in losses (claims) plus overhead.[62] The precision of pricing in the insurance industry can vary dramatically. Auto insurance has troves of historical data and has experienced relatively little technological innovation that has altered the assessment of risk, so insurance companies can be quite confidant in the accuracy of the pricing.[63] Environmental liability insurance, conversely, was historically systematically underpriced causing a number of insurers to go bankrupt when a rash of asbestos claims caught insurers by surprise and forced them to pay out billions of dollars in unforeseen damages.[64]

---

[58] *See* Shiraz Jagati, *Crypto Custody Market Overview — Who Are the Biggest Players?*, COINTELEGRAH (Aug. 27, 2019), https://cointelegraph.com/news/crypto-custody-market-overview-who-are-the-biggest-players (discussing how Coinbase is dominating the custodial wallet industry and had only approximately 120 clients in mid-2019 indicating that it is large holders primarily using the services not retail users).

[59] *See* Natalie, *Leading US-based Crypto Custodian Providers for Institutional Clients*, BLOCKCHAIN4ALL (Nov. 25, 2019) https://medium.com/blockchain4all/leading-us-based-crypto-custodian-providers-for-institutional-clients-3ba9b8683c6d (explaining how Coinbase, for example, had over $7 billion worth of crypto in assets under custody in 2019).

[60] *See* Nathan McCauley, *Sealing the Gaps in Crypto Custody insurance*, MEDIUM: ANCHORAGE (May 29, 2019), https://medium.com/anchorage/sealing-the-gaps-in-crypto-custody-insurance-e6260b969ff9.

[61] Sean Ross, *What Is the Main Business Model for Insurance Companies?,* INVESTOPEDIA (June 25, 2019), https://www.investopedia.com/ask/answers/052015/what-main-business-model-insurance-companies.asp

[62] *See* RICHARD V. ERICSON, AARON DOYLE, DEAN BARRY & DIANA ERICSON, INSURANCE AS GOVERNANCE 102 (2003) (discussing how the practical realities are slightly more complicated due to the necessity of factoring in the costs of administration, loss prevention, and reinsurance; however, the basic underlying structure remains true).

[63] *Id.* at 103.

[64] *Id. See generally Liability for Asbestos Related Claims*, INSURANCE INFORMATION INSTITUTE (Feb. 3, 2010) (asbestos was widely used in homes and products for years before people understood the harmful health effects. As a result, for decades after the use of asbestos was largely banned, those who developed health problems attributable to the asbestos sued employers who exposed them to the

Storing digital assets presents a new form of risk that insurers are now attempting to evaluate. Over the last few years, insurers have begun issuing insurance policies to companies that offer commercial digital asset storage and who are willing to pay for financial protection in the event of a hack or other loss.[65] Given the nascency of the industry and the technological sophistication of the underlying product, assessing the risk of these new policies poses a number of challenges for insurers. Yet demand from those storing significant amounts of digital assets has encouraged insurers to brave the underwriting uncertainties in order to offer this new product.[66]

Digital asset insurance, like most commercial insurance, provides three primary benefits to policy holders: risk transfer, risk mitigation, and marketing. The first and most obvious benefit is the "risk transfer" from the holder of the assets to the insurer. Individuals and companies that hold millions or even billions of dollars' worth of digital assets want to protect against the risk of their assets being lost or stolen. Purchasing insurance allows them to shift a portion of the risk of theft and other such losses to an insurer for a predictable fee.[67]

If, for example, a crypto exchange – a site where users can buy or sell digital assets online – that is safeguarding hundreds of millions of dollars' worth of bitcoin for its users is hacked and assets are stolen, a digital asset insurance policy may reimburse the crypto exchange for some or all of the stolen bitcoin. What and how much is covered (i.e. how much risk is transferred) is determined by the specifics of the policy. If the exchange has a comprehensive policy with a sufficient limit of liability, a user who stores money with the exchange can be confident that if her bitcoin is stolen, the insurance company will reimburse the exchange, so she does not have to bear the loss.[68]

The second benefit of an insurance policy is "risk mitigation." In the crypto exchange example, it is in the insurer's interest to prevent the exchange from being hacked. If the exchange is never hacked, the insurer will collect the premiums and

---

asbestos and manufacturers who used asbestos in their products. Employers then turned around and relied on their workers compensation insurance or liability insurance for indemnification. As a result insurers ended up carrying much of the financial burden resulting in claims that could exceed $65 billion, nearly as much as was paid out combined from Hurricane Katrina and September 11th. This exemplifies the fundamental uncertainty in insurance. While insurance attempts to estimate and mitigate risk as best they can, ultimately there are unforeseen variables such as the unknown health effects of a widely used chemical such as asbestos).

[65] Matthew Lerner, *Insurance market adapting to provide digital asset covers*, BUSINESS INSURANCE (Jan. 28, 2020), https://www.businessinsurance.com/article/20200128/NEWS06/912332792/Insurance-market-adapting-to-provide-digital-asset-covers-Marsh-JLT-.

[66] *Id*.

[67] *See* Sasha Romanosky, Lillian Ablon, Andreas Kuehn & Therese Jones, *Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?*, 5 J. CYBERSECURITY 1, 2 (2019) (explaining how firms can either try to reduce risk or to transfer that risk to an insurer).

[68] *E.g., Digital Currency Balances,* COINBASE, https://www.coinbase.com/legal/insurance (last visisted Oct. 18, 2020) (demonstrating that Coinbase offers insurance to protect assets held in hot storage).

never have to pay out a claim – all profit for the insurer. But if the exchange is hacked, the insurer will lose money. It is in the insurer's interest therefore to offer services that help the exchange mitigate the risk of a loss event. Many insurers in this space require that a prospective insured, the exchange for example, perform measures upfront such as audits of the IT infrastructure and extensive background checks on employees before they will even consider underwriting a policy.[69] The insurer may also provide additional services such as cyber response and PR assistance to help reduce the damage should there be a theft.[70] This risk mitigation benefit is particularly valuable to the crypto exchange if the insurer (or insurance broker) has more experience in digital asset security than the exchange itself. The insurer may have a number of different clients that provide digital asset storage solutions and be able to suggest security improvements based on observed best practices or known hacking trends.[71] The value of the risk mitigation can vary according to a number of factors, such as the industry, the competency and experience of the insurer, which third-party vendors the insurer might choose to hire, and the flexibility of the insured company.[72]

Third, companies receive a marketing benefit. Companies can promote their services as insured to current and prospective clients. Countless crypto exchanges have been hacked.[73] Consumers may prefer one exchange over another because they feel more comfortable storing their digital assets with an exchange that claims to be insured. Consumers generally cannot audit a company's security, so having insurance may be the best (or only) way for consumers to feel confident that their funds will not be lost if the storage solution is hacked.

II. DIGITAL ASSET INSURANCE: NEW AND QUICKLY GROWING

In early 2018, the digital asset insurance industry hardly existed.[74] There were

[69] *See* Aviva Abramovsky, *Reinsurance: The Silent Regulator?*, 15 CONN. INS. L.J. 345, 384 (2009), available at https://digitalcommons.law.buffalo.edu/cgi/viewcontent.cgi?article=1002&context=journal_articles.

[70] Mark Camillo, *Cyber Risk and the Changing Role of Insurance*, 2 J. CYBER POL'Y 53, 55-56 (2017).

[71] Given the nascency of the industry and the relative lack of sophistication of the insurers in the space to date, this particular benefit of industry expertise by insurers has not manifested. As insurers continue to grow their supply of digital asset insurance, they will continue to gain exposure and may be able to perform this role for newer exchanges or custody solutions.

[72] *See* Shauhin A. Talesh, *Insurance Companies as Corporate Regulators: The Good, the Bad, and the Ugly*, 66 DEPAUL L. REV. 463, 472-473 (2017) (referencing the varying effectiveness of insurers to perform risk mitigation techniques across industries such as legal malpractice, medical malpractice, motion pictures, firearms, personal injury, and policing).

[73] *See* Gertrude Chavez-Dreyfuss, *Cryptocurrency Crime Surges, Losses Hit $4.4 Billion by End-September: CipherTrace Report*, REUTERS (Nov. 27, 2019, 11:31 AM), https://in.reuters.com/article/crypto-currencies-crime/cryptocurrency-crime-surges-losses-hit-4-4-billion-by-end-september-ciphertrace-report-idINKBN1Y11UP?utm_content=106779133&utm_medium=social&utm_source=linkedin&hss_channel=lcp-1857854. A list of crypto exchange hacks can be found at *A Comprehensive List, supra* note 3.

[74] *See* Kauflin, *supra* note 9 ("Two years ago, the market for crypto insurance was nonexistent . . . .");

no publicly announced digital asset policies with major insurers.[75] Within just two years, digital asset insurance has become a billion dollar industry, much of its growth occurring in late 2019 and early 2020.[76] Some experts even project that the industry's growth may continue to outpace the larger cybersecurity insurance market that has become a mainstay product for most large insurers.[77]

Yet, despite the explosion of this new insurance product, this paper is the first of its kind to perform an in-depth analysis of the digital asset insurance industry. In this section I describe (A) the general approach of the insurance industry to creating a new and novel insurance product, (B) how insurers are designing policies, (C) which companies are underwriting and brokering the policies and what types of companies have been able to secure coverage, and (D) the varying degrees of insurance protection for digital assets.

A. Creating a Digital Asset Insurance Policy

Companies in the cryptocurrency space complain that with a market cap of several hundred billion for all cryptocurrencies, the supply of digital asset insurance nowhere near matches demand.[78] The total available coverage for digital assets is projected at around $6 billion[79] with estimated $200 million to $500 million in annual premiums.[80] Why then are insurers not providing coverage for more of the over $250 billion in total value held in just the two most popular cryptocurrencies: bitcoin and ether? [81]

Olga Kharif, Brian Louis, Julie Edde & Katherine Chiglinksy, *Interest in Crypto Insurance Grows, Despite High Premiums, Broad Exclusions*, INS. J. (July 23, 2018), https://www.insurancejournal.com/news/national/2018/07/23/495680.htm (discussing how BitGo did have coverage in 2015, the first policy of its kind, but the service was discontinued a year later because of the cost).

[75] *Id*.

[76] There have been a flurry of recent announcements about large insurance policies secured including Bittrex's $300 million policy announcement and Gemini's establishment of a captive with reinsurance coverage up to $200 million. *See* Bittrex Team, *Bittrex, Inc. Secures $300 Million in Digital Asset Insurance to Enhance Protection*, MEDIUM (Jan. 29, 2020), https://medium.com/bittrex/bittrex-inc-secures-300-million-in-digital-asset-insurance-to-enhance-protection-16fff23a98d1; Ian Allison, *Winklevoss-Led Gemini Exchange Now Has Its Own Insurance Company*, COINDESK (Jan. 16, 2020, 12:00 PM), https://www.coindesk.com/winklevoss-led-gemini-exchange-now-has-its-own-insurance-company.

[77] Kauflin, *supra* note 9 ("Motta expects the market for crypto insurance to grow faster than the 20% to 25% pace at which the larger cybersecurity insurance sector is currently expanding.").

[78] Philip Martin, *A Unique Look Under the Hood of One of the World's Most Comprehensive Crypto Insurance Programs*, THE COINBASE BLOG (Apr. 2, 2019), https://blog.coinbase.com/on-insurance-and-cryptocurrency-d6db86ba40bd.

[79] Justin Grensing, *Cryptocurrency Insurance Market Shows Promise Despite Cautious Approach by Major Insurers*, AM. EXPRESS, https://www.americanexpress.com/us/foreign-exchange/articles/cryptocurrency-insurance-market-shows-promise-with-caution/ (last visited Apr. 4, 2020).

[80] Kauflin, *supra* note 9 ("Today he [Motta-a crypto insurance expert] thinks it's worth between $200 million and $500 million in premium revenue.").

[81] *See Ethereum*, *Bitcoin,* COINMARKETCAP, https://coinmarketcap.com/currencies/ethereum/, https://coinmarketcap.com/currencies/bitcoin/ (last visited Aug. 11, 2020) (displaying two links showing the total market cap for each of ether and bitcoin).

The answer requires a fundamental understanding of how insurers evaluate risk and create new insurance products. Creating and pricing any insurance policy relies primarily on determining two key variables: (1) frequency of loss and (2) severity of loss.[82] Or in other words, how often will the insurer have to pay claims and how big will those claims be? Legacy insurance products such as car insurance, health insurance, and directors and officers (D&O) insurance have decades' worth of data that insurers use to price policies.[83] Traditional insurance companies have teams of data analysts and actuaries that attempt to use this data to determine how much risk is associated with a given policy.[84] Different industries permit varying degrees of precision, but generally, more data allows underwriters to predict risk more accurately. While insurers may not be able to ascertain precisely which individual drivers may crash, for example, they can estimate how many crashes are likely to occur and the approximate amount they will need to pay out across their entire automobile insurance line. Barring a meteor striking earth and damaging millions of cars, or some other such unforeseen event,[85] their estimates are likely to be quite accurate. Underwriting D&O insurance is more variable based on the specifics of the prospective insured, but insurers have nonetheless honed modeling techniques and diversified their risk such that it has become a standard insurance product.[86]

Digital asset insurance cannot rely on historical data, as relevant data does not yet exist. There have now been several years of hacks of crypto storage solutions, but the value and relevance of this data is questionable because the companies that were hacked were generally unsophisticated and not representative of those that insurers would cover.[87] And what little data about these hacks does exist is often unreliable.[88] The insurance industry, therefore, has limited tools to estimate the expected frequency of loss and severity of loss for their digital asset policy holders.[89] Furthermore, on top of the difficulty of estimating known risks, there is always the lingering chance of an entirely unconceived risk to the insurer such as the harmful impacts of asbestos that cost insurers billions in environmental liability claims.[90]

---

[82] Tom Baker, *Uncertainty > Risk: Lessons for Legal Thought from the Insurance Runoff Market,* B.C.L. REV. (forthcoming 2020) (manuscript at 11) (on file with SSRN) (hereafter *Uncertainty*).
[83] *Id*.
[84] *Id*.
[85] Like a global pandemic that prevents people from going to work and dramatically reduces the amount of driving…though this would presumably benefit insurers.
[86] Adriana M. Rojas Mora, The Use of Quantitative Modeling in the Directors & Officers (D&O) Liability Insurance Market 1 (Oct. 2009) (unpublished master's thesis, Georgia State University) (on file with J.Mack Robinson College of Business), available at https://silo.tips/queue/the-use-of-quantitative-modeling-in-the-directors-officers-do-liability-insuranc?&queue_id=-1&v=1602870559&u=MjYwMTo2NDc6NWMwMDo2OTA6ZTBiZjo4YzUwOmIxZWU6ZDNiOQ==.
[87] Press Conference, Marsh, Digital Asset Risk Transfer Press Conference (Jan. 28, 2020), https://marsh.webex.com/marsh/lsr.php?RCID=a3f49c85ac694767a4e8612da117c0ee.
[88] *Id*.
[89] *Id*.
[90] One such risk could be systemic changes in the landscape of cryptography. Should modern cryptography become penetrable through computing advancements such as quantum computing, the entire digital asset ecosystem could be changed. Crypto assets, as the name implies, rely on

Any new type of insurance product must overcome this problem of lack of data. To do so, insurers begin by analyzing by analogy.[91] Where there is no relevant data, insurers use data from established industries that they believe have the most similar type of risk, augment the legacy policies the best they can, then rapidly iterate as they begin to receive data on the new policy type.[92] This is difficult for digital asset insurance because it is often quite different than any other insurance being offered. For example, the likelihood that loss or theft of digital assets will occur fundamentally depends on how those assets are stored and secured. Unfortunately for insurers, whether a company uses cold storage, warm storage, or hot storage dramatically alters the risk assessment.

When comparing cold storage (offline) to preexisting insurance products, the most relevant policy category is *crime insurance*. Crime insurance generally covers "cash, assets, merchandise or other property loss when someone perpetrates fraud, embezzlement, forgery, misrepresentation, robbery, theft or any other type of business-related crime."[93] Additionally, *specie insurance*, a subset of crime insurance, is a policy type used for "value in transit or at rest"[94] and frequently employed for "high value precious items such as cash, gold, diamonds, valuable documents, fine art and jewelry."[95]

Digital assets kept in cold storage are usually held in a physical device that is then protected using similar security techniques as those used for other valuable physical assets such as gold, cash, or jewelry.[96] They both use safes, vaults, alarm systems and the like, so the risk of theft is similar, and therefore the insurance product is highly analogous.[97] There are differences, however. Billions of dollars of digital assets can be kept on a device the size of a thumb drive, whereas a heist of billions of dollars in gold, cash, or jewelry may require a team of people and trucks to move the stolen goods. Digital assets kept in cold storage also have a hardware component that could be a point of vulnerability.[98] These differences between legacy specie insurance products and digital assets are controllable through the use of exclusions and insurance

---

cryptography. If the underlying cryptography becomes unsecure because of computational advancements, the assets themselves may either lose their functionality or become worthless altogether. It is worth noting, however, that this is not a risk unique to crypto assets but applies to cryptography and digital storage generally.

[91] *See* Tom Baker, *Back to the Future of Cyber Insurance*, 3 PLUS J. 1, 2 (2019) (hereafter *Back to the Future*) (describing the origins of cyber insurance as deriving from a traditional liability insurance policy adjusted as necessary for the different risk profile of liability on the internet, and mentioning how as the industry progresses, insurers iterate to better address the new risk).

[92] *Id.*

[93] Julia Kagan, *Business Crime Insurance*, INVESTOPEDIA (June 5, 2018), https://www.investopedia.com/terms/b/business-crime-insurance.asp.

[94] Martin, *supra* note 78.

[95] *Specie Insurance: Introduction*, HOLMES UNDERWRITING AGENCY, https://holmesunderwriting.com/specie-insurance/ (last visited Oct. 19, 2020).

[96] *Hot wallet vs cold wallet, supra* note 44.

[97] *Id*.

[98] Lily Hay Newman, *Cryptocurrency Hardware Wallets Can Get Hacked Too,* WIRED (May 18, 2020, 9:00 AM), https://www.wired.com/story/cryptocurrency-hardware-wallets-can-get-hacked-too/.

limits, and therefore are sufficiently analogous to legacy products to rely heavily on existing policy types and risk assessment procedures. Given the close similarities of protecting crypto assets in cold storage and traditional assets covered by crime and specie policies, insurers have become relatively comfortable underwriting crypto assets in cold storage over the past few years.[99]

Commercial crime insurance is also being used as the foundation for hot storage (online) policies, though the comparison is a bit more tenuous.[100] Insurance for assets kept in hot storage has the same fundamental goal as insurance for gold, cash, jewelry, or digital assets in cold storage: insuring the value of the assets in the event of loss or theft. The means of protecting assets held in hot storage, however, is far more similar to the realm of cyber insurance. Assets kept in cold storage are protected by physical security, whereas assets held in hot storage are primarily protected using cybersecurity.[101]

Unlike crime insurance, cyber insurance policies do not provide coverage for the stolen assets themselves because the data stolen is not itself inherently valuable. Though credit card numbers and passwords obviously have value for a hacker, they are not a store of value – credit cards can be cancelled and passwords can be changed whereas dollars, diamonds, and bitcoin cannot. Though this difference may seem trivial given both fetch a significant black-market bounty, it is elemental to devising an appropriate insurance policy. In the event of a breach, a typical cyber insurance policy covers ancillary costs such as notifying customers of the breach, resolving identity issues with effected customers, recovering lost or compromised data, repairing damaged computer systems, and sometimes compensating for losses resulting from business interruption.[102] It does not provide monetary compensation for the actual stolen assets. Digital asset insurance for hot storage, therefore, combines the theft of a valuable asset aspect of crime insurance with the cyber security foundations of cyber insurance.

After analogizing the new digital asset insurance product to the appropriate legacy ones, insurers will then consult industry experts to better understand differences between the risks of the old product and the new. They will attempt to make informed assumptions as to what modifications need to be made and customize the digital asset policies accordingly. While a new insurance product is almost always derived from an established insurance product, it may be heavily tailored and

---

[99] *See Blue Vault: An Innovative Cold Storage Solution for Digital Assets*, MARSH, https://www.marsh.com/us/services/financial-professional-liability/cold-storage-for-digital-assets-blue-vault.html (last visited Oct. 19, 2020) (demonstrating that insurers have become comfortable underwriting crypto in cold-storage because Marsh's Blue Vault system offers a relatively off the shelf insurance policy for assets held in cold storage. This shows insurers ability to create a one-size-fits all policy for cold storage as compared to the still highly customized world of hot storage insurance).

[100] Martin, *supra* note 78.

[101] *Hot wallet vs cold wallet, supra* note 44.

[102] *What is Cyber Insurance?*, NATIONWIDE, https://www.nationwide.com/lc/resources/small-business/articles/what-is-cyber-insurance (last visited Oct. 19, 2020).

customized to the new risk.

B. Digital Asset Insurance Policies Today

Estimating risk by analogy is far from perfect. It necessitates relying heavily on assumptions, which, if wrong, could dramatically alter the risk of the policy in question. For that reason, insurers typically enter new markets slowly, so they can test the new products and see how they withstand claims before they are widely sold.[103] Gradually entering the market limits exposure until the risk assessment and underwriting process can be better tested and refined.[104] Insurers underwriting digital asset policies are now balancing the desire to move quickly so as to establish themselves as industry leaders, and the need to remain circumspect and skeptical of the unknown risks of the new industry.

Only insuring the companies that are perceived to be the lowest risk also helps minimize the initial exposure to the insurers. In the digital asset industry, this means only working with the companies that have the strongest security that insurers deem least likely to suffer a loss. This creates an interesting paradox wherein the initial companies that are able to obtain insurance are arguably those least likely to need it.[105] Additionally, insurers do not have the data or experience to build precise and time-tested pricing models.[106] So new products are priced high to provide a cushion in case the risk estimates are low – a standard practice in new lines of insurance.[107] To be insurable, a company must not only be security and compliance driven, therefore, but it must also be willing and able to pay the relatively high premiums charged for digital asset insurance today.

Insurance for cold storage, which is generally deemed more secure, reportedly costs about 0.8% to 1.2% of assets covered annually, whereas a traditional commercial crime insurance policy is typically below 0.5% of assets covered.[108] Hot storage coverage is significantly more expensive at 3% to 5% of assets covered and demands a comparatively larger cushion because the risk is perceived as greater, and the analogy to existing products is more tenuous.[109] In order to be willing to pay these

---

[103] Sarah Downey, *Cryptocurrency: 5 Trends to Watch in 2020*, MARSH (Jan. 29, 2020), https://www.marsh.com/us/insights/risk-in-context/5-cryptocurrency-trends-to-watch.html?utm_source=linkedin&utm_medium=socialmedia&utm_campaign&utm_source=linkedin&utm_medium=socialmedia&utm_campaign=&sf116952995=1.
[104] *Id*.
[105] Kauflin, *supra* note 9.
[106] Press Conference, Marsh, *supra* note 87.
[107] Romanosky, *supra* note 67; Press Conference, Marsh, *supra* note 87.
[108] Virginia Hamill, *Crime Insurance: Cost, Coverage & Providers*, FIT SMALL BUS. (Dec. 12, 2019), https://fitsmallbusiness.com/crime-insurance/; *see also* Lester Coleman, *Insurance Giants See 'Big Opportunity' in Cryptocurrency Storage Coverage*, CCN (July 21, 2018, 5:33 PM), https://finance.yahoo.com/news/insurance-giants-see-big-opportunity-163341835.html.
[109] Nicky Morris, *AON Says Supply Exceeds Demand for Cryptocurrency Insurance*, LEDGER INSIGHTS (July 2019), https://www.ledgerinsights.com/cryptocurrency-insurance-digital-assets-aon-supply/.

premiums, particularly for hot storage coverage, companies must place a high priority on the security of their customers' assets. Although these costs will eventually be passed on to customers, insured companies must have sufficiently deep pockets to be able to temporarily front the cost or have security-oriented customers who immediately see the value and are willing to pay a premium for insurance.

These are precisely the type of companies that have been able to obtain sizable digital asset insurance policies from notable insurers to date. Just a few players in the digital asset space have large policies that make up much of the insurance coverage in the industry. Three of the most reputable exchanges in the US including Coinbase,[110] Gemini,[111] and Bittrex[112] have secured policies with multi-hundred-million-dollar limits. Additionally, several notable digital asset custody providers including Trustology,[113] BitGo,[114] and Anchorage[115] have inked comparably sized policies. A few smaller but well-funded start-ups including Curv, an institutional focused digital asset wallet, have secured policy limits in the $50 million-$100 million range.[116]

In addition to being security-oriented and well-funded, companies that have been able to obtain insurance also tend to be in jurisdictions known for having a stronger rule of law. Most are in countries such as the United States, United Kingdom, Japan, and Switzerland, which have stable and trustworthy legal regimes.[117] Despite the frequently vague and unclear laws surrounding digital asset companies, the companies that have secured sizable insurance policies have demonstrated earnest attempts to comply with the legal and regulatory landscape.

These industry dynamics help us better understand the reasons behind the common refrain that there is a supply shortage in digital asset insurance.[118] Companies have difficulty securing policies because the insurers' requirements are stringent and prices are relatively high.[119] This results in companies perceiving a shortage of supply while insurers struggle to find demand that they deem insurable.[120] The problem therefore is not a lack of supply or demand, but rather a mismatch between buyers' and sellers' expectations.

---

[110] Martin, *supra* note 78.
[111] *User Agreement*, GEMINI, https://gemini.com/legal/user-agreement#digital-asset-insurance (last updated Aug. 6, 2020).
[112] Bittrex Team, *supra* note 76.
[113] Scott Cook, *How Trustology Helps Cryptocurrency Owners to Secure Their Investments*, CRYPTONEWSZ (Jan. 9, 2020), https://www.cryptonewsz.com/how-trustology-helps-cryptocurrency-owners-to-secure-their-investments/55710/.
[114] *Digital Asset Insurance*, BITGO, https://www.bitgo.com/resources/digital-asset-insurance (last visited Oct. 19, 2020).
[115] McCauley, *supra* note 60.
[116] John Biggs, *Munich Re-Insures Curv's Crypto Wallet to the Tune of $50 Million*, COINDESK (May 10, 2019, 8:30 PM), https://www.coindesk.com/munich-re-insures-curvs-crypto-wallet-to-the-tune-of-50m.
[117] *See* Coleman, *supra* note 108 (discussing how Mitsumi Sumitomo Insurance in Japan has been active in offering insurance to crypto companies in Japan).
[118] Morris, *supra* note 109.
[119] Martin, *supra* note 78.
[120] Morris, *supra* note 109.

C. The Insurers (and Brokers)

Any new line of commercial insurance has higher upfront costs than more established products, but this is particularly so for digital asset insurance because of the technical sophistication of the industry. The risks of a new insurance product are also less predictable, so there is always the potential for losses for the insurer.[121] Large insurance companies are therefore well placed to develop new insurance products because they can bear the product development costs and are better able to absorb losses. The due diligence process for digital asset insurance requires significant time and resources, which has been more logical for insurers that can treat the costs as a speculative investment in future business for an industry that is quickly growing.[122] Smaller insurers will have more difficulty rationalizing spending these resources for a still relatively small pool of premiums.

In addition to the insurance incumbents, several startups hoping to tailor insurance products specifically to this new industry have emerged. These startups include Insurwave, Nexus Mutual, and Coincover, which have all taken slightly different approaches to trying to insure this novel market. Nexus Mutual, for example, bills itself as a "decentralized alternative to insurance."[123] Companies looking to Nexus Mutual for coverage present the underlying code (called a "smart contract"), which anybody can then audit and choose to pledge coverage in the event of a "material loss of value resulting from unintended uses of smart contact code" – essentially, a hack.[124] Therefore, rather than having to rely on insurers who merely underwrite based on types of losses, companies can look to the broader crypto community for coverage of the code itself.[125] These insurance startups aimed specifically at the crypto asset market are particularly exciting in the context of the exploding decentralized finance (DeFi) industry, which broadly refers to financial services based on blockchain that are automated and self-executing. Traditional insurance may prove difficult or impossible where no centralized entity exists to purchase insurance, as is often the case in DeFi, so these novel methods may be particularly attractive where legacy insurance is ill-suited. It remains to be seen whether Nexus Mutual or any of these upstarts will produce coverage comparable or superior to that of the large insurers for crypto assets, but none can yet offer the name

---

[121] *Uncertainty*, *supra* note 82, at 6.
[122] *See* BITGO, *Insurance for Digital Currencies*, *supra* note 39, at 3-4 (explaining that insurers require significant amount of information from companies that they need to understand and vet before moving forward, which is a time and capital intensive process).
[123] *See FAQ: Basics,* NEXUS MUTUAL, https://nexusmutual.gitbook.io/docs/faq (last visited Oct. 19, 2020).
[124] *Id.*
[125] This also provides significant loss mitigation benefits as those who are best at auditing this type of code can financially benefit from underwriting the safest code and offering suggestions to code perceived as less safe. Furthermore, these individuals are likely to have far more expertise in this field than insurance professionals who are likely newer to the blockchain world.

brand value associated with the legacy insurers.

Insurance brokers – intermediaries that help connect clients (companies seeking insurance) with insurers – are helping accelerate the expansion of the digital asset insurance market by performing some of the diligence and helping to educate the insurers.[126] More specifically, the two largest insurance brokers,[127] Aon[128] and Marsh[129], have both become very active in the digital asset insurance space.[130] Both have formed cross-functional teams specifically focused on digital asset insurance,[131] and one or the other has seemingly been involved in every major digital asset insurance policy to date.[132] This level of focus, sophistication, and maturity in the digital asset insurance industry is unparalleled among major insurers themselves and has allowed these two brokers to become valuable in bridging the knowledge gap between the digital asset companies and the insurance providers. Some of the large insurers such as AIG, XL Group, and Munich Re have begun to recognize the potential of the digital asset insurance market and have individuals with interest and experience in the space, but none have formed teams of comparable size or expertise to either Aon or Marsh.[133]

Most of the insurance policies themselves are coming out of Lloyds of London, a marketplace for insurance and reinsurance syndicates.[134] Lloyds is particularly well suited for emerging insurance products such as digital asset storage because the syndicate structure allows multiple insurers to co-underwrite a risk, which helps limit each company's exposure without having to individually spend the time and money to underwrite the policy.[135]

The digital asset insurance industry is still highly consolidated. Large, well-funded crypto companies are receiving the majority of the digital asset insurance supply. Aon and Marsh dominate brokerage services in the industry. And most of the insurance, while dispersed among a number of insurance companies, is funneled through the Lloyds marketplace. This lack of competition may be contributing to the perceived supply shortage of digital asset insurance, because companies have very limited options if they are locked out from these brokers and insurers. There can be

[126] Kauflin, *supra* note 9.
[127] Marianne Bonner, *15 Largest Insurance Brokerages in the World*, THE BALANCE SMALL BUS. (June 26, 2019), https://www.thebalancesmb.com/world-s-largest-insurance-brokers-462396.
[128] *Risk Transfer Solutions for Evolving Technologies*, AON, https://www.aon.com/risk-services/cryptocurrency/default.jsp (last visited Oct. 19, 2020).
[129] *Innovative Insurance Protection for Digital Assets*, MARSH, https://www.marsh.com/us/services/financial-professional-liability/innovative-insurance-protection-for-digital-assets.html (last visited Oct. 19, 2020).
[130] Kauflin, *supra* note 9.
[131] The teams are focused specifically on digital asset insurance, but the members of the teams have responsibilities outside of the digital asset team –thus, it does not appear that anybody at the brokers is focused full-time on the digital asset market.
[132] Kauflin, *supra* note 9.
[133] Coleman, *supra* note 108.
[134] Grensing, *supra* note 79.
[135] Coleman, *supra* note 108.

benefits to a small, tightly coordinated insurance market in a particular industry,[136] but the lack of market players in digital asset insurance is more likely a function of the novelty of the industry and the cost of launching a new product than it already having reached its optimal size.

D. Varying Approaches to Insuring Digital Assets

Because of the selectivity of the insurers, the vast majority of digital assets remain uninsured.[137] The two most popular cryptocurrencies bitcoin and ether have a market cap of over $250 billion, and yet likely no more than five percent of that is insured globally, despite the known risk of hacks and theft.[138] Even those companies that have announced the largest policies have limits that are substantially less than the value of the assets in their custody.

For example, Coinbase, one of the most reputable crypto exchanges in the US, has a policy that insures its assets kept in hot storage up to $255 million in losses.[139] Coinbase understandably focused on insuring the approximately 2% of funds it holds in hot storage, which it believed were the most vulnerable. 98% of its considerable digital assets in cold storage, however, presumably remain uninsured.[140] While the risk of loss for the assets in cold storage may be small, there is still a risk. Yet, a multi-hundred-million-dollar policy covering the most vulnerable assets is the current best-case-scenario for a consumer.

Some companies appear to fall into the above "insured" category but do so in name only. A number of companies, albeit impossible to know how many without access to specific insurance policies, have inked agreements that offer very limited practical risk transfer.[141] For any number of reasons, a company may agree to carveouts, limitations, and caps that dramatically weaken the value of its policy to consumers. Some companies may bargain for lower premiums by agreeing to additional exceptions, while for others, insurers may demand capitulation to terms because the company's security is deemed weaker and therefore the company riskier. This is a pervasive problem in the digital asset insurance industry.[142] A significant

---

[136] ANJA SHORTLAND, KIDNAP: INSIDE THE RANSOM BUSINESS (2019) (detailing how a tight-knit group of insurers can govern the payouts of ransoms, but this can be jeopardized by an outsider who breaks custom and issues a larger ransom thus jeopardizing the leverage of the group of insurers. One larger payout leads to more and larger ransoms curtailing the effectiveness of the tight-knit group of insurers).

[137] Grensing, *supra* note 79.

[138] *Id.* The total coverage limits for the digital asset industry is estimated at approximately $6 billion as of late 2019. *Id*. Even if this has grown to approximately $10 billion in the later months of 2020, this would be about 5% of the $200 billion total market cap. *Id*.

[139] *How is Coinbase Insured?*, COINBASE, https://help.coinbase.com/en/coinbase/other-topics/legal-policies/how-is-coinbase-insured.html?source=post_page (last visited Oct. 19, 2020).

[140] *Id.*

[141] Kharif et al., *supra* note 74.

[142] *Id.*; *see also* BITGO, *Insurance for Digital Currencies*, *supra* note 39, at 2-4 ("As a result, many companies who make public claims about their insurance coverage are not specific or transparent about what the coverage entails. This leads to significant asymmetry in what one company is able to

number of policies in the space have been so diluted that almost the entire value of the policy to the company is the ability to market the company as "insured." This trend is problematic for several reasons that I discuss further in Part III, but the most important is that consumers' assets may not actually be protected in the event of a hack.[143]

The vast majority of companies that hold digital assets, however, have no third-party insurance at all.[144] The most responsible of this group may decide to establish a formal self-insurance program that amounts to a "precautionary savings" program on behalf of its customers.[145] A self-insurance program sets aside funds to be used in the case of a loss such as a hack. Binance, a large global crypto exchange, claims to divert 10% of all trading fees into a self-managed fund that protects customers in the event of a theft[146]— and it's lucky for consumers that they do. Binance repaid its users approximately $40 million after the exchange was hacked in 2019.[147] While still preferable to offering consumers no protection at all, this type of self-insurance solution provides none of the risk transfer benefits of traditional insurance. If a loss event were large enough to jeopardize the health of Binance as an organization, its self-insurance fund may not have been able to cover the losses. Binance is also under no legal obligation to keep the funds segregated for insurance purposes. Additionally, the company does not benefit from the risk mitigation efforts of a third-party insurer that could have helped prevent such a hack in the first place (though it could purchase such services separately).

Finally, there are companies that offer consumers no protection at all in the event of a loss.[148] These companies have no predetermined method of reimbursing consumers if their funds are lost or stolen and, in many cases, companies will be financially unable to do so because money has not been set aside for such purpose. In most of the hacks to date, consumers have lost most or all of the money that was stolen.[149]

III. SHORTCOMINGS IN THE CURRENT APPROACH TO DIGITAL ASSET INSURANCE

purchase compared to another, and a "buyer beware" environment due to the opacity of policies.").

[143] *Id.*

[144] Only a handful of exchanges and custody solutions have announced insurance policies, while there are hundreds of exchanges and custody solutions around the world. *See Top Cryptocurrency Spot Exchanges*, COINMARKETCAP, (https://coinmarketcap.com/rankings/exchanges/) (last visited Oct. 19, 2020).

[145] Richard F. Denning, *Federal Taxation Concepts in Corporate Risk Assumption: Self-Insurance, the Trust, and the Captive Insurance Company*, 46 FORDHAM L. REV. 781, 786 (1978).

[146] Kauflin, *supra* note 9.

[147] *Id.*

[148] *See Are balances stored on Kraken insured?*, KRAKEN, https://support.kraken.com/hc/en-us/articles/360001372126-Are-balances-stored-on-Kraken-insured- (last visited Oct. 19, 2020) (explaining that Kraken, one of the oldest and largest crypto exchanges has no formal or informal insurance).

[149] Chavez-Dreyfuss, *supra* note 73.

In less than three years, digital asset insurance has grown from nearly nonexistent to an approximately half billion-dollar a year premium market.[150] For the digital asset industry, which badly needs improved security, better standards, and stronger consumer protections, the proliferation of digital asset insurance is a huge step in the right direction.[151] But the industry is still brand new. In Part III, I outline a number of challenges to the further growth of the industry: (A) no loss history or data; (B) the rapidly changing nature of the digital asset industry; (C) lack of transparency in policies; (D) regulatory uncertainty; (E) human bias.

A. Loss History and Data

Perhaps the largest problem in underwriting digital asset insurance is the most obvious one: there is no loss history of insured crypto assets. There is therefore almost no relevant data with which insurers can use to calculate expected frequency and magnitude of loss for the purpose of estimating the risk of a given policy.[152] This is uncomfortable for insurers, which typically price policies by analyzing historical data that provides objective predictions of future risk.[153] Without relevant data, insurers cannot rely on this primarily quantitative approach and must turn to more qualitative methods of assessment that are typically less accurate.[154] This more subjective approach to underwriting introduces significant opportunity for error that insurers attempt to avoid with more data-driven models. This is an issue that insurers face in essentially every new product line,[155] but it is more problematic when the new insurance product deviates dramatically from existing offerings, which is particularly the case with hot storage policies. The risk surrounding lack of data can be kept at acceptable levels by entering the new market slowly. Additionally, insurers generally charge higher premiums for new products to provide a small buffer for underwriting uncertainty.[156]

B. The Rapidly Changing Digital Asset Industry

The pace at which the technology surrounding digital assets is changing further complicates this problem of lack of relevant data. The underlying blockchains, storage solutions, digital asset security infrastructures, and other technology relevant when contemplating digital asset insurance is evolving at an impressive clip.[157] All these

---

[150] Grensing, *supra* note 79.
[151] Kauflin, *supra* note 9.
[152] Downey, *supra* note 103.
[153] *Id.*
[154] *Id.*
[155] *Back to the Future*, *supra* note 91, at 2.
[156] Press Conference, Marsh, *supra* note 87.
[157] *See C-Suite Briefing: 5 Blockchain Trends for 2020*, Deloitte, (Mar. 2020), https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Consulting/Blockchain-Trends-2020-report.pdf (demonstrating that the technology and suspected use cases continue to evolve extremely

technologies impact how the insurers structure their product offerings, so if the technology continues to change then the insurance product needs to be modified. The price of the insurance is a function of how the product is structured, so if the product continues to evolve, so must price.[158] If these variables are constantly moving, this poses additional challenges to gathering data. By the time there have been some claims and insurers are collecting relevant data about their digital asset insurance policies, the data may already be partially obsolete. If the insurance product has already changed because of technological developments, then data from older insurance iterations may have limited value.

Lack of relevant data is usually unavoidable for a new product line such as digital asset insurance, and it is a challenge that creative insurance professionals will have to address over time.[159] Today, underwriters are doing their best to analyze by analogy and gather what information they can to help estimate risk. Counterintuitively, insurers are eagerly awaiting a few small hacks, so they can test their assumptions and see how policies hold up under claims before expanding their coverage supply.[160]

C. Transparency

When crypto exchanges or custody solutions secure a large insurance policy, they publicize it as a victory for their users. The company can then market its funds as "insured." But details about what the policy covers in the digital asset industry usually amounts to a few vague sentences on a press release or the company website. At best, the policy will be buried in the terms of service when signing up for the platform or available upon request for clients, but usually it is not available to the consumer at all.[161] The depositor of digital asset funds is left with a legally meaningless description of the policy that provides little insight about how strong the coverage is.

Coinbase, for example, states on their website "the policy insures against theft of digital currency that results from a security breach or hack, employee theft, or fraudulent transfer."[162] This is far too fuzzy to provide any indication as to what incidents would be covered by the policy. Most events are not likely to fall neatly into a binary of clearly covered or not.

Similarly, BitGo, a leading custody solution, advertises insurance that protects against "1) Third-party hacks, copying, or theft of private keys 2) insider theft or

---

quickly).

[158] *Back to the Future, supra* note 91, at 2.

[159] *Uncertainty*, *supra* note 82, at 43-4.

[160] Downey, *supra* note 103.

[161] Coinbase, Gemini, BitGo, Trustology, and Anchorage, for example, do not make their insurance policies publicly available on their websites. COINBASE, www.coinbase.com (last visited Apr. 4, 2020); GEMINI https://gemini.com, (last visited Apr. 4, 2020); BITGO, https://bitgo.com (last visited Apr. 4, 2020); TRUSTOLOGY, https://trustology.io (last visited Apr. 4, 2020); ANCHORAGE, https://anchorage.com (last visited Apr. 4, 2020).

[162] *Insurance: Digital Currency Balances,* COINBASE, https://www.coinbase.com/legal/insurance (last visited Oct. 19, 2020).

dishonest acts by BitGo employees or executives 3) loss of keys."[163] Would vulnerabilities in the underlying blockchain code that are exploited qualify as "third-party hacks?" Would negligence by an employee be considered a "dishonest act" or would a different standard such as recklessness or intent apply?

Trustology, another crypto asset custody solution, notes on its website that policies cover "security breaches and theft of cryptoassets."[164] The lack of publicly accessible details on insurance policies is entirely understandable. Most consumers would not read nor fully understand a more detailed policy. Companies must keep their websites presentable and marketable, and long explanations of insurance policies are the antithesis of a good user experience. Without access to the entire policy, however, consumers or watchdog groups have no way of understanding with any nuance what types of events would be covered by the policy. Furthermore, because there has never been a digital asset insurance claim, there is no direct legal precedent to shed light on what types of losses would likely be covered by these vague descriptions.[165] Whether or not the consumers' assets are insured for a particular incident may be a function of whether the insurance company deems it worthwhile to fight a claim.

While commercial crime insurance policies are frequently inaccessible to the public, digital asset insurance is unusual in two ways. First, the digital asset companies purchasing insurance typically have possession of the insured assets, but they are usually merely safeguarding the assets for a third party. As such the company is actually purchasing a policy for the protection of a third-party's assets.[166] This can occur in the non-crypto context as well– for example with a traditional custodian – but the dominant purchasers of digital asset insurance are custodians. Those using the custodial services would therefore have a particularly strong interest in being able to view the policies purchased by the custodian on behalf of their assets.

Second, the crypto industry since its inception has been fraught with overpromises, misleading claims, and outright fraud that make the lack of transparency particularly worrisome given the context of the industry.[167] This was most apparent in 2017 and 2018 when a flurry of companies began selling tokens (digital assets) en masse in order to fund the development of (purportedly) blockchain-based enterprises. The top fifty of these token sales in 2017 raised over $2.5 billion collectively.[168] Recent scholarship has found that the vast majority of these top 50

---

[163] *Digital Asset Insurance: What is Covered,* BITGO, https://www.bitgo.com/resources/digital-asset-insurance (last visited Apr. 4, 2020).
[164] TRUSTOLOGY, https://trustology.io/pricing/ (last visited Apr. 4, 2020).
[165] *See* BITGO, *Insurance for Digital Currencies*, *supra* note 39, at 2-4 ("With no history of claims or best practices for analysts and underwriters to draw from, policies today are bespoke. As such, coverage will be complex and differ from company to company. In order to protect the client, transparency surrounding depth and availability of coverage is critical.").
[166] Some crypto custodians do build insurance relationships with predetermined prices, but they overcome this problem by actually allowing their clients to purchase the insurance directly from the insurer.
[167] Shaanan Cohney, David A. Hoffman, Jeremy Sklaroff & David A. Wishnick, *Coin-Operated Capitalism*, 119 COLUM. L. REV. 591, 651 (2019).
[168] *Id.* at 671. The tokens were usually purchased with either bitcoin or ether and therefore the value

Initial Coin Offerings or ICOs made substantial governance claims in their whitepapers (marketing documents that outline the details of the project and token sale) that were then not represented in the underlying code.[169]

ICOs could easily be conducted by anybody with even a moderate level of technical sophistication. And while some – probably even most – of the companies conducting ICOs did have genuine intentions of launching a blockchain-based company, the lack of skepticism and regulatory oversight of the new fundraising technique led to frequent exaggeration, misleading claims, and fraud.[170] There are many differences between the wild-wild-west ICO offerings and those securing digital asset insurance policies, but the claims of strong insurance coverage without transparent disclosures of those policies is reminiscent of the troubling ICO boom of 2017.

As with the disparity in competence and honesty of the companies that conducted ICOs, some digital asset insurance policies are undoubtedly more comprehensive than others.[171] Without transparency for consumers whose assets are being covered by the policies, mismatched market incentives should create skepticism of the policies being touted by digital asset custodians. It is in a company's short-term interests to buy a weaker policy (because it will be cheaper) and market it as a strong policy (because this will be the most attractive to customers).[172] Hillik Nissani, COO of crypto trading platform Cryptoalgo, warned of this trend suggesting that for a number of companies, "the number of exclusions can make the whole policy close to useless."[173] This lends credence to the fear that many companies are securing insurance largely as marketing ploys with little or no chance of a successful claim in the event of a loss and therefore no actual additional value to consumers whose assets are covered by the policies.[174]

Without having the insurance agreements publicly available, consumers hoping to understand the strength of a policy are forced to rely primarily on the reputation of the company and the insurer. In the cyber security industry, it is commonly said that the question of a hack is "when not if." There is no reason to believe that this mantra should be any different for digital assets held in hot storage, which uses similar security techniques. Users with large amounts of assets in a relatively untested custody solution or exchange (which is all of them at this point) should be highly invested in the insurance policy of their custodian. With the current lack of transparency, it is nearly impossible for a user to distinguish one policy from another or judge the

---

of the sale fluctuated wildly with the fluctuation of those two digital assets. *Id*.

[169] *Id.* at 635-9.

[170] *Id.* at 671.

[171] *See* BITGO, *Insurance for Digital Currencies*, *supra* note 39, at 2-4 ("With no history of claims or best practices for analysts and underwriters to draw from, policies today are bespoke. As such, coverage will be complex and differ from company to company").

[172] Ian Allison, *Underwriter Claims Crypto Custodian BitGo Exaggerated Insurance Coverage*, COINDESK (Mar. 5, 2019, 4:53 PM), https://www.coindesk.com/crypto-custodian-bitgo-exaggerated-insurance-coverage-underwriter-claims.

[173] Kharif et al., *supra* note 74.

[174] McCauley, *supra* note 60.

strength of a policy.

D. Regulatory

Much has been said and written about the lack of regulatory clarity in the crypto world.[175] Many in the industry feel that the government has been overly restrictive in regulating cryptocurrencies at the expense of innovation.[176] Regulators counter that they are trying to avoid premature regulation while still protecting consumers.[177] Regardless of their differences on the ideal regulatory approach, all parties agree that the legal landscape still has a number of uncertainties.[178] Most hotly debated is which digital assets should be deemed a security.[179] While other relevant issues include how state versus federal law will apply in regulating cryptocurrency activities, how exchanges, particularly decentralized exchanges will be regulated, how Know Your Customer (KYC) and Anti-Money Laundering (AML) laws will be adopted in a decentralized environment, among many other outstanding questions.

Progress has been made on these uncharted legal and regulatory questions. The SEC has provided guidance on what digital assets may be considered a security, such as by issuing the "Framework for Investment Contract Analysis of Digital Assets" in April 2019.[180] This was intended to provide practitioners a framework to analyze what may be deemed an investment contract and thus a security.[181] Yet, as suggested, it is just a framework and offers little guidance on how to apply the framework. For example, the framework suggests that a network that is decentralized with "an unaffiliated, dispersed community of network users" may prevent the underlying crypto asset from being a security, but it provides no further explanation as to what constitutes sufficiently decentralized, unaffiliated, or dispersed.[182] Furthermore, the courts are yet to affirm that this approach will be consistently applied across all jurisdictions. These regulatory uncertainties create legal risk that is difficult to quantify, as it can be difficult to know when one is about to cross a blurry legal line. Insurers are therefore understandably hesitant to underwrite risk that could dramatically change based on an evolving regulatory landscape and enforcement

---

[175] Carol Goforth, *The Lawyer's Cryptionary: A Resource for Talking to Clients About Crypto-transactions*, 41 CAMPBELL L. REV. 47, 85 (2019); Michèle Finck, *Blockchains: Regulating the Unknown*, 19 GERMAN L.J. 665, 666-9 (2018).
[176] Hossein Nabilou, *How to Regulate Bitcoin? Decentralized Regulation for a Decentralized Cryptocurrency*, 27 INT'L. J.L. & INFO. TECH. 266 (2019) ("[A]n aggressive command-and-control approach to its regulation would stifle the potential future innovations.").
[177] DANIEL BROBY & SAMUEL BAKER, CTR. FOR FIN. REGULATION & INNOVATION, CENTRAL BANKS & CRYPTOCURRENCIES 6 (2018).
[178] *Id*., at 7; Eric C. Chaffee, *The Heavy Burden of Thin Regulation: Lessons Learned from the SEC's Regulation of Cryptocurrencies*, 70 MERCER L. REV. 615, 626 (2019); Downey, *supra* note 103.
[179] Chaffee, *supra* note 178, at 620.
[180] *Framework for "Investment Contract" Analysis for Digital Assets,* Securities and Exchange Commission, (Apr. 3, 2019), https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.
[181] *Id*.
[182] *Id*.

strategy.[183] When asked about the impact of the regulatory haze on the digital asset insurance market, Sarah Downey, co-head of Marsh's Digital Asset Risk Transfer group, noted simply "for the underwriting community, more regulatory certainty means a greater level of comfort in offering coverage."[184]

How the regulatory uncertainty is impacting coverage, however, is not immediately obvious. Most of the outstanding regulatory issues in the digital asset industry do not appear to directly impact the risk assessment or could seemingly be disclaimed in the policy. For example, insuring digital assets that could later be deemed a security creates significant securities litigation risk that would understandably concern an insurer. Disclaiming securities litigation risk in the policy, however, would be quite straightforward. These clearly identifiable risks are not what is causing hesitation among insurers. Rather, the legal and regulatory uncertainties in the industry creates a general fog that insurers are not comfortable operating in.[185] Insurers are concerned that the lack of regulatory clarity leaves their insureds vulnerable to legal actions (such as unexpected enforcement activities by a regulator) that could lead to insolvency or messy bankruptcy proceedings.[186] This creates a counterparty risk for insurers who fear that they could face heavy claims if the company cannot return funds to all of its clients. Or the insurer may be dragged into costly and drawn-out legal proceedings as is often the case with bankruptcy. At the very least, the insurer may suffer reputational damage by insuring a company later perceived to have been acting illegally. Insurers, therefore, may prefer to avoid the industry altogether rather than subject themselves to the risk of underwriting a company in such a nebulous regulatory environment.[187]

There is hope that the regulatory barrier to obtaining insurance may become more porous as adoption of digital assets increases and the industry begins to fall more cleanly into new and existing regulatory structures. For example, Wyoming, a state that has sought to become a digital asset hub through forward thinking and crypto-friendly regulation, authorized the chartering of special purpose depository institutions (SPDIs) in 2019, which operate and are regulated essentially as banks.[188] Wyoming recently approved crypto exchange Kraken's SPDI application, making them the first crypto company to become a state-chartered bank.[189] This gives Kraken the ability to operate in other states without going through state-by-state compliance procedures as well as to interact with other financial products as a bank would.[190] This

[183] Downey, *supra* note 103.
[184] *Id.*
[185] *Id.*
[186] *Id.*
[187] Downey, *supra* note 103.
[188] *Special Purpose Depository Institutions,* Wyoming Division of Banking (last visited Dec 20, 2020), http://wyomingbankingdivision.wyo.gov/home/areas-of-regulation/laws-and-regulation/special-purpose-depository-institution.
[189] Nathan DiCamillo, *Kraken Becomes First Crypto Exchange to Become a US Bank* (Sep. 6, 2020 10:34 AM), https://www.nasdaq.com/articles/kraken-becomes-first-crypto-exchange-to-become-a-us-bank-2020-09-16
[190] *Id.*

has the tangible benefit of reducing regulatory burden, which may correspondingly reduce risk to insurers. But likely even more importantly, having a state banking charter (or other similar legal stamps of approval) should help defog the industry and improve the legitimacy in the eyes of insurers.

E. Human: Industry Knowledge and Bias

Without historical data, underwriting digital asset insurance is a heavily qualitative and time-intensive endeavor. Representatives of those seeking digital asset insurance must spend many hours with insurance professionals explaining the ins and outs of their business, the risks, the security measures, and any other facet of the business relevant to the insurers' risk assessment.[191] Requiring this level of human interaction has two significant implications in the context of digital asset insurance.

First, the insurers must understand the digital asset space. Cryptocurrencies, blockchains, digital asset storage, and the relevant technologies are new and technologically complicated. For insurers to be able to assess the risks in a digital asset business, they need to have people in-house who have a deep enough understanding of the company and its technology to be able to understand and estimate the risk. To date, most insurers do not have personnel with this capability.[192]

Companies that wish to buy a digital asset insurance policy, therefore, are tasked with educating the brokers and insurers until they are sufficiently knowledgeable to feel comfortable underwriting the policy.[193] Executives at the company seeking insurance must spend valuable time detailing their particular business model, security infrastructure, and all of the nuances that make them insurable.[194] For busy executives or start-up founders, there is a significant opportunity cost to dedicating this time to educating insurers. Even then, the insurers may (and often do) decide against insuring the risk because they still do not sufficiently understand the technology or industry.[195]

Second, humans have bias – in the case of the cryptocurrency world, a lot of bias. Cryptocurrencies have a mixed reputation. They are best known by many for being the currency of the internet underworld, the high-profile hacks of millions of dollars, and headline-grabbing price volatility.[196] These are not attractive qualities to an

---

[191] Bitgo's whitepaper outlines the different measures a custodian seeking insurance should take. Insurers need to investigate and audit all of these areas before they will be able to underwrite a policy. BITGO, *Insurance for Digital Currencies*, *supra* note 39, at 2-4. Given the nascency and sophistication of the technology, this process takes time and significant involvement on the part of the party seeking insurance in light of the "education gap." *Id*.

[192] *Id*. (siting a "general education gap around the technical features and necessary security measures of smart contracts and blockchain technology" as a primary reason that quality insurance is limited, and thus indicating the lack of individuals in the insurance industry who have a sophisticated understanding of the technology necessary to understand and underwrite policies).

[193] *Id*.

[194] *Id*.

[195] *Id*.

[196] *See* Joshuah Bearman & Tomer Hanuka, *The Untold Story of Silk Road: Part 1*, WIRED (May 2015), https://www.wired.com/2015/04/silk-road-1/ (detailing the use of Bitcoin for unsavory

insurer and can significantly impact the perception of the risk in underwriting a policy.[197] And there are truths to these perceived risks. Hacks in the digital asset industry have been rampant since its inception.[198] Billions of dollars have been lost, stolen, or frozen because of vulnerabilities in the code or security of digital asset storage solutions.[199] Furthermore, cryptocurrencies have become a favorite tool of many people hoping to act outside the confines of the law.[200] Cryptocurrencies such as bitcoin have made the sale of everything from guns to drugs to hitmen easier on the dark web.[201] And the prices of most cryptocurrencies have had periods of immense fluctuation since they garnered more mainstream attention.

These traits, however, are largely attributable to the novelty of the industry, the lack of regulatory oversight, and the reckless gold rush-like atmosphere created by the potential to make a quick fortune in the industry's early days. While the risks addressed above are far from gone, a number of tools have been developed and applied to significantly reduce the risks of interacting with illicit actors and potential hacks. [202] In many instances, merely following the same business practices that are legally required in other industries (but are often neglected in the crypto industry) can reduce the risk for insurers to that comparable to companies in traditional industries. [203]

For example, many exchanges and custodians are implementing Know Your Customer (KYC) and Anti-Money Laundering (AML) processes that require customers to present identification when using a company's services.[204] KYC and AML are standard practices in traditional banking and are legally required for any money transmission business in most jurisdictions globally. This practice eliminates the anonymity some value in the digital asset industry, but it allows exchanges and

---

purchases on the Silk Road); David Siegel, *Understanding The DAO Attack***,** COINDESK (June 27, 2016, 4:52 PM), https://www.coindesk.com/understanding-dao-hack-journalists (explaining that the DAO hack was widely reported and an example of early reporting on high-profile hacks); Jay Adkisson, *Why Bitcoin is so Volatile*, FORBES (Feb. 9, 2018, 11:40 PM), https://www.forbes.com/sites/jayadkisson/2018/02/09/why-bitcoin-is-so-volatile/#79ed484139fb (discussing how Forbes was one of many to cover the 2017 bubble and subsequent crash of cryptocurrencies such as Bitcoin).

[197] Bulletin, Lloyd's, Cryptocurrencies, Decentralised Digitised Assets and Related Transactions 1 (July 6, 2018), https://www.lloyds.com/~/media/files/the-market/communications/market-bulletins/2018/07/y5196.pdf .

[198] Chavez-Dreyfuss, *supra* note 73.

[199] *Id.*

[200] Sean Foley, Jonathan R Karlsen,& Tālis J Putniņš, *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?*, 32 THE REV. FIN. STUDIES 1798, 1800-01 (2019).

[201] *Id*.

[202] Landon Manning, *Report: Just 1 Percent of Bitcoin Transactions Involve Illicit Dark Web Activity*, BITCOIN MAG. (July 3, 2019), https://bitcoinmagazine.com/articles/report-just-1-percent-bitcoin-transactions-involve-illicit-dark-web-activity.

[203] *See* CIPHERTRACE, *Q3 2019 Cryptocurrency Anti-Money Laundering Report* (2019), https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/ (discussing how CipherTrace researchers found that two-thirds of the 120 most popular cryptocurrency exchanges have weak or porous know your customer (KYC) practices.). Implementing KYC and other such standard banking practices are prime examples of what insurers look for in a potential insured to deem them less risky. *Id*.

[204] *Id.*

custodians to far better identify nefarious counterparties and avoid servicing illicit actors. Because of the nascency of the industry and the libertarian or even anarchist tendencies of many crypto enthusiasts, still two-thirds of the largest 120 crypto exchanges have weak or no KYC/AML processes.[205] The contrast between those that have not implemented suitable KYC/AML and those that have approached compliance as if it were mainstream finance exemplifies the wide spectrum of insurability in the industry. The companies that have demonstrated a genuine commitment to security and taken reasonable measures to safely store digital assets have largely avoided the epidemic of hacks and losses which have plagued the rest of the crypto community; but still, the industry as a whole remains stained by those with more irresponsible businesses practices.

Furthermore, companies are developing new tools specifically to address the security and vulnerabilities of crypto companies. Ciphertrace, for example, is a crypto intelligence platform that helps trace crypto assets and track crypto companies' compliance measures with the goal of "protecting banks from crypto laundering risk and … making virtual assets trusted by governments and safe for mass adoption."[206] Chainalysis, another intelligence tool developed specifically for the digital asset industry, is being used by financial institutions and insurers to help determine the security vulnerabilities and risk of working with particular digital asset companies.[207] As the industry continues to grow, additional products will continue to emerge to support the security of the industry.

This is not to say that if companies take appropriate steps, there are no longer risks. There will always be risks – particularly so in a new and high-tech industry. Rather, the risks may be perceived as larger than they are because many companies in the digital asset industry have not taken the necessary (and obvious) steps to improve security and compliance. There are not yet enough individuals inside the insurers that have a sufficiently deep knowledge of the technology and industry that internalize this nuance.[208]

The solution to this problem is the continued education of insurance professionals. There is currently a network of people among insurers and brokers who focus on digital asset insurance and have been very successful in developing the market.[209] But this group is small. The digital asset industry is still new, complicated, and the utility is largely unproven, so it is entirely understandable that insurance professionals in

[205] *Id. ("*63% of exchanges that trade privacy coins have weak or porous KYC. This suggests privacy coins will find it harder to survive in a post FATF Travel Rule world if exchanges do not develop the proper KYC procedures necessary to mitigate the AML/CTF compliance risks that come with their anonymity-enhancing features.").
[206] *About Us*, CIPHERTRACE, https://ciphertrace.com/about-us/ (last visited Apr. 4, 2020).
[207] CHAINALYSIS, https://www.chainalysis.com/ (last visited Apr. 4, 2020).
[208] BITGO, *Insurance for Digital Currencies*, *supra* note 39, at 2-4 (this is precisely what is meant by the "education gap." Better educated insurers would be able recognize and better understand the difference between the more compliant and therefore less risky companies and those who have continued to flout compliance).
[209] Such as the previously mentioned teams at MARSH and Aon.

large part have not dedicated the considerable time and resources necessary to become industry experts. This will happen over time as those within the digital asset world continue educating insurers.

As education about the industry improves, the stigmas surrounding the illicit uses of cryptocurrencies and the susceptibility to hacking will begin to fade. Insurers with surface-level understanding of digital assets will learn more, and they will recognize that similar to traditional data storage, not all crypto storage solutions are equal. And just as some traditional banks have processes to avoid working with clients who tread in illicit waters, crypto custodians can employ similar tactics to avoid holding the money of the unsavory figures who may rely on crypto.

IV. AREAS OF OPPORTUNITY

This paper is primarily designed to take a comprehensive look back at the digital asset insurance industry in its early days. I hope others can use it as a resource to better understand this rapidly growing industry. But I also present two suggestions for how the digital asset insurance industry could improve its effectiveness. These are not so much responses to "problems" in the current approach as they are areas of untapped potential that I believe would benefit the digital asset ecosystem and make insurers more valuable to the industry. At the risk of prognosticating far too prematurely in the industry's evolution, I hope these two recommendations will spur additional thought, research, and development in the digital asset industry and are not an attempt to devise a fully-fledged solution.

First, I suggest that companies in the digital asset storage space explore *insurance captives* as a means of expanding the supply of digital asset insurance and broadening coverage options. A captive is an insurance company that is wholly owned by the company being insured.[210] Captives would allow digital asset companies that are either underinsured or are unable to tap into traditional third-party insurance to provide consumers desperately needed coverage.

Second, I suggest that insurers work together to create rigorous and comprehensive security standards which those that hope to obtain insurance must meet. Digital asset insurers should deliberately function as a de facto regulator by setting coordinated minimum security thresholds for companies holding digital assets who hope to be insured. Rather than regulators mandating such standards, insurers can incentivize companies to meet security benchmarks on their own. Companies that do not meet these guidelines would be deemed uninsurable and have less credibility with security-conscious consumers.

[210] William B. Barker, *Federal Income Taxation and Captive Insurance*, 6 VA. TAX REV. 267, 269 (1986).

A. Insurance Captives

In a traditional commercial insurance agreement, a company pays one or more third-party insurers a premium to transfer a risk or set of risks. For any number of reasons, a company may instead choose to retain such risks internally rather than transfer them to a third-party. There are a variety of strategies for doing so. *Self-insurance*, the simplest approach, is essentially a rainy-day fund that companies can use to cover losses that could otherwise be formally insured.[211] Self-insurance usually refers to an informal arrangement or promise by the company that carries with it no legal obligations to segregate funds, maintain minimum reserves, or any of the other requirements imposed on a legally designated insurer.[212] The informality of self-insurance is attractive because of the ease and lack of administrative costs of starting and operating such a program.[213] For these same reasons, however, the protection to consumers of self-insurance is less substantial than a traditional, fully-regulated third-party insurer.

A second option for retaining risk internally is to establish a trust. A trust, also relatively inexpensive, is legally designated for a particular use, but it is also not an insurance company.[214] A company may establish a trust designed to settle claims arising from a clearly identifiable group of claimants where the expense and requirements of a formal insurance subsidiary (a captive) is overly burdensome.[215] There are particular bodies of laws that govern trusts, but they are also not required to comply with all the requirements imposed on an insurer.[216]

Third, a *captive* offers a more formalized option for retaining risk. A captive is defined as "a wholly-owned insurance subsidiary with a primary function of insuring the outstanding exposures of the parent organization."[217] Captives can have many different structures and purposes, some that render this definition somewhat inadequate, but it is more or less the "formalization of the self-insurance concept."[218] A captive is an insurance company. It must therefore abide by the same rules and regulations that govern traditional insurers.[219] This includes maintaining sufficient capital reserves, setting premiums with a profit-making motive, undergoing certain risk mitigation measures for its clients, and being a legally distinct entity with its own management that must operate at arm's length with the parent.[220]

---

[211] Will Kenton, *Self Insure*, INVESTOPEDIA (Nov. 12, 2019), https://www.investopedia.com/terms/s/self-insure.asp.
[212] *See* Denning, *supra* note 145, at 786 (discussing how companies who select to self- insure "should…[create] an explicit policy of the company to assume an amount of risk in predefined areas," but there is no legal obligation for the company to do so).
[213] *Id.*
[214] *Id.* at 787.
[215] *Id.*
[216] *Id.*
[217] Barker, *supra* note 210.
[218] Denning, *supra* note 145, at 787.
[219] *Id.*
[220] *Id.*

Establishing a captive rather than securing traditional third-party insurance has two primary benefits: potential cost savings and access to reinsurance. Rather than paying premiums to a third-party, establishing a captive allows a company to pay those premiums to its own corporate subsidiary.[221] Premium prices paid to one's own captive must be justifiable to a regulator as high enough to generate profit, but any profit that would otherwise go to a third-party insurer is retained within the corporate family.[222] Additionally, insurance companies are afforded some advantageous tax treatment that may justify a captive because of the significant tax savings to the parent.[223]

The second major benefit of creating a captive is improving access to and reducing the cost of reinsurance.[224] Reinsurance typically refers to an insurer (called the primary insurer in this context) selling some of its underwritten risk to another insurer (called the reinsurer) to spread the risk.[225] Because the captive is an insurance company itself, it can transfer risk directly to a reinsurer, rather than needing to go through a direct insurer as would be the case in a traditional insurance arrangement. Captives can reduce the cost of reinsurance because it cuts out the need for an intermediary – the third-party primary insurer. Or, if the parent company is unable to secure direct insurance for any number of reasons, a captive may present the only path to accessing the capital in the traditional insurance market through reinsurance.

Establishing a captive, however, is not without considerable drawbacks. First and foremost, captives traditionally have limited risk diversity.[226] The theory of insurance is typically that an insurer will pool a number of largely uncorrelated risks. As long as only a portion of the risks manifest at the same time, the premiums from the other unclaimed risks should cover the losses.[227] As captives only support the parent company, they often have a very narrow or even singular portfolio of risk, so a large claim could bankrupt the entire insurance captive.

Additionally, creating a captive insurance company can be costly. Insurance is a heavily regulated industry, so setting up an insurance company can be timely and expensive.[228] Furthermore, in order to account for the lack of risk pooling, captive insurers must maintain higher capital reserves.[229] For these reasons, initiating a captive insurance company is often prohibitively pricey for smaller companies and

---

[221] *Id.* at 811.
[222] *Id.* at 787.
[223] *Id.* at 811.
[224] *Id.*
[225] Caroline Banton, *Reinsurance*, INVESTOPEDIA (July 20, 2020), https://www.investopedia.com/terms/r/reinsurance.asp.
[226] Constance A. Anastopoulo, *Taking No Prisoners: Captive Insurance as an Alternative to Traditional or Commercial Insurance*, 8 ENTREPEN. BUS. L.J. 209, 217 (2013).
[227] *Id.* at 218.
[228] *Id.* at 217.
[229] Joseph W. Tucciarone & Louis Biscotti, *Captive Insurance Companies: A Common Sense Approach to Improved Risk Management*, THE CPA J. (Dec. 2018), https://www.cpajournal.com/2018/12/19/captive-insurance-companies/.

only economically worthwhile for larger institutions.[230]

Nonetheless, where these impediments do not make captives out of the question, the digital asset storage industry could use captives to dramatically increase the amount of assets under some insurance coverage. Digital asset custodians are not the typical Fortune 500 company for which a captive is appealing, but the industry could benefit from the broader use of captives for a number of reasons.

First, for many companies, a captive may be the only available option for securing formal insurance because the supply of digital asset insurance is still constrained by limited insurers, high premiums, and skepticism about insuring digital asset companies. Insurers, seeking to limit their exposure with such an unknown risk, are being highly selective about what companies to insure.[231] Thus, many companies have been locked out of the traditional insurance market leaving a captive as the only viable option for insurance.[232] A captive, which is legally an insurance company, offers far more protection to consumers than self-insurance, which does not have to comply with regulations such as segregated funds or mandated capital reserves. Because hacks have been so prevalent in the industry, consumers should care greatly about how their assets are insured, and therefore captives may be a worthwhile investment to attract and retain clients.[233]

Second, digital asset insurance is a new product with a very difficult to assess risk. Insurers, therefore, must set relatively high premiums to provide a buffer for potential underwriting miscalculations. A captive provides the opportunity for the parent company to "evaluate and assess the risk based on its own experiences as opposed to industry-wide calculations" that will likely include a pricing premium to account for the lack of underwriting precision in the new product.[234] There are also not many experts on digital asset storage security, few, if any, of whom work in the insurance industry. If the parent company employs or has better access to those industry experts, it may be better placed than any insurer to evaluate the risks associated with its storage solution and can therefore price premiums more accurately.[235] Of course, there is potential for bias in this scenario that must be addressed by ensuring that the captive has sufficient autonomy and independence to appropriately assess risk and set premiums.

Third, a captive provides digital asset companies an alternative path to the reinsurance market. As with any captive, this allows a back-door method of securing insurance from large, traditional reinsurers for companies that could not access the primary insurance market. Digital asset custodians that could not secure name-brand insurance may be able to do so through reinsurance. And those that are otherwise able to secure insurance may be able to access the reinsurance market more cheaply by

---

[230] *Id.*
[231] Downey, *supra* note 103.
[232] Denning, *supra* note 145, at 785.
[233] *A Comprehensive List, supra* note 3.
[234] Anastopoulo, *supra* note 226, at 216.
[235] *Id.*

first establishing a captive.

Finally, captives for digital asset companies have interests better aligned with consumers. The traditional insureds-insurer relationship is inherently adversarial in the claims process.[236] A company that makes a claim on its digital asset insurance policy is seeking payment from an insurer. The individual claim is a net-zero equation between the insurer and insured.[237] With a captive, however, "the parent and captive have the same incentive to pay the claim from the captive's reserves."[238] To date, there have been no, or very few, insured claims in the digital asset insurance industry, so there is no direct precedent as to what types of claims are typically paid out by insurers.[239] The coverage provided by a captive may actually be more valuable to consumers than third-party insurance because of the lack of claims precedent in the industry and the better aligned incentives of a captive.

In January 2020, Gemini, a large US crypto exchange, was the first in the digital asset space to publicly introduce a captive insurance company to insure crypto custody.[240] Gemini cited the low available coverage limits and the access to the reinsurance market as primary reasons it established a captive.[241] Its policy is structured such that the insurance captive is responsible for the first tranche of losses, and the excess insurers would be responsible for all or part of the liability after the first tranche for a total of up to $200 million in coverage.[242] This allows Gemini to demonstrate to insurers and reinsurers that it has skin in the game and limits claims to the excess insurers to only very large incidents, and thereby secures a large policy limit at a more affordable price. Because the primary risk is taken on by Gemini itself in the captive model, insurers are willing to provide excess coverage and reinsurers are willing to insure a captive where the company otherwise may not have been able to secure direct coverage or the policy limit would have been much smaller.

This structure also helps solve both the moral hazard and adverse selection problems that insurers may face in covering digital asset-based companies. Companies with traditional insurance may be less incentivized to prevent a hack if they have strong third-party insurance coverage, whereas those with a captive are still financially responsible at least in part for any losses. Additionally, third-party insurers can use the structure and premiums of the captive in their reinsurance or excess coverage policy, which helps limit the information asymmetry as to the company's security and therefore adverse selection risk.

---

[236] *Id.* at 216-7.
[237] Insurance companies are incentivized on a macro level to pay claims because a reputation for avoiding claims payments will make other companies reluctant to seek their insurance services.
[238] *Id.* at 216.
[239] Kharif et al., *supra* note 74.
[240] Yusuf Hussain, *Gemini Launches Captive Insurance Company- Now Has the Most Custody Insurance Coverage in the Crypto Market*, GEMINI (Jan. 16, 2020), https://gemini.com/blog/gemini-launches-captive-insurance-company-now-has-the-most-custody.
[241] Ian Allison, *Winklevoss-Led Gemini Exchange Now Has Its Own Insurance Company*, COINDESK (Jan. 16, 2020, 4:33 PM), https://www.coindesk.com/winklevoss-led-gemini-exchange-now-has-its-own-insurance-company.
[242] *Id.*

If the lower price and autonomy of insuring digital assets using captives expands coverage to more companies, this should have the secondary benefit of increasing the speed at which there will be claims in the industry. These claims are essential to the maturation of the digital asset insurance industry, as they provide valuable data and insight that insurers can use to refine their underwriting techniques. A meaningful number of claims more quickly allows insurers to test their policies, improve their models, and gain valuable experience in the industry allowing them to expand their coverage supply.

Despite the potential benefits, captives are not a perfect solution for the digital asset industry. They are expensive to set up and operate, and third-party insurance providers, which have a diverse line of products, deeper reserves, and better access to reinsurance, are still far better positioned to handle large losses.[243] The high set-up and operating costs can be particularly limiting because the digital asset industry is itself new, so most companies in the space are still start-ups that may lack sufficient time or capital to establish a captive. A "core-cell" captive, also referred to as a "rent-a-captive,"[244] is an alternative model that may provide the benefits of a captive at a fraction of the cost.[245] A core-cell captive is a captive insurance company with a core operated by a third-party with associated cells that have legally distinct entities that assigns shares to the company seeking captive insurance.[246] The cells function as a captive insurer, while the costs of creating and maintaining the core can be split among all the different companies that have been assigned a cell.[247] The core-cell captive harnesses most of the benefits of a traditional captive while dispersing the costs.

In such a limited market for digital asset insurance, captives can be an excellent alternative to traditional third-party coverage. Very few companies that hold significant digital assets have insurance, leaving billions of dollars' worth of digital assets vulnerable. For digital asset companies who have third-party insurance, a captive can be a means of cutting costs or expanding coverage. For smaller companies or those otherwise unable to obtain third-party insurance, captives can be an intermediary solution until digital asset insurance becomes more widely available.[248] Captives can provide additional protection to consumers' assets for an industry that is badly in need of expanded coverage.

B. Insurance as a De Facto Regulator

A fundamental role of a government is to enact laws that create order in a society.

---

[243] Anastopoulo, *supra* note 226, at 217-219
[244] *See* David White, *Growing Interest in Captive Cells: Who and Why?*, 47 CAPTIVE INS. TIMES 1 (2014) ("For all of the varieties, the industry often refers to these types of facilities as 'rent-a-captive' structures. I like to use the term 'captive cell' when referring to a rented segregated account.").
[245] Anastopoulo, *supra* note 226, at 225.
[246] *Id.*
[247] *Id.*
[248] *Id.* at 209.

As the only body sanctioned to use force, the State has the power to enforce the laws by punishing those that break them. Ideally, the laws that the State imposes should be designed to improve the welfare of its people, as every law comes at the cost of some restriction of personal freedom. While the State is the only entity that can legitimately govern through the use or threat of force, other bodies can still indirectly contribute to the regulation of a society. A number of scholars have persuasively reasoned that insurance is *the* primary method of societal governance outside of the State because it has such power to influence industries at a systemic level.[249]

Insurers frequently function as de facto regulator because the insurer, the State, and consumers often have aligned incentives.[250] Insurance is generally purchased to compensate the insured for a loss. A loss such as a fire in one's home, a car crash, or an online hack may trigger property insurance, auto insurance, or cyber insurance respectively. In each instance, it is in all parties' (the insured, the insurer, and the government) interests to prevent or mitigate the damage from the fire, car crash, or hack. Taking preventative or mitigative measures is frequently a profit-maximizing strategy for the insurer that also benefits the government and consumer. Notable contracts and insurance scholars Omri Ben-Shahar and Kyle Logue argue that the insurer is in fact often a more effective regulator than the government because insurers tend to have better information and have profit as a motivator.[251]

For example, the first fire departments in history were established by insurers after suffering heavy claims from the Great Fire of London in 1666.[252] Later, insurers were responsible for the widespread adoption of sprinkler systems that are now legally required in most commercial buildings.[253] Similarly, the insurance industry has had immeasurable impact on automobile safety over the last century. Insurers have encouraged legislation to mandate airbags, heavily promoted the use of seatbelts, and helped improve road safety.[254] These were not altruistic gestures from socially conscious insurance companies concerned about injuries from fires and car crashes. These were calculated maneuvers that the insurers deemed would help their bottom

[249] *See* ERICSON, ET AL., *supra* note 62, at 14 (arguing that "Insurance is the institution of governance beyond the state" and explaining the governance mechanisms of insurance and how it is the most powerful form of governance after the state itself); Talesh, *supra* note 72, at 471 (explaining the ways in which insurers are effective regulators and even make the argument that insurers can be more effective than the state).
[250] ERICSON, ET AL., *supra* note 62, at 45.
[251] Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197, 198-9 (2012).
[252] Camillo, *supra* note 70, at 60.
[253] *Id.*
[254] ERICSON, ET AL., *supra* note 62 (commenting on how insurance companies also employ far more subtle techniques such as campaigning to replace the word "accident" with "crash" in our lexicon and explaining that insurers reason that "crash" denotes a cause whereas "accident" implies mere misfortune because they believe that suggesting that human's cause crashes (which is believed to be true approximately 93% of the time) will encourage people to drive more safely to reduce such incidents). Insurers also use more concrete approaches to reduce crashes. *Id*. In Canada an insurance association went so far as to actually pay for the engineering of safer roads and found that this saved the insurer twenty-two times what they paid for the construction. *Id*.

line – which had a secondary benefit of saving lives as well as money for both consumers and the government.

The same trend is now occurring in the cyber industry. Cyber insurers are playing an ever-expanding regulatory role in the cyber security industry. For example, insurers are attempting to improve cyber security by requiring that companies seeking insurance comply with cyber security standards such as ISO 27001, a global information security management standard.[255] Those that do not comply with this or a comparable standard often will have difficulty obtaining cyber insurance or will have higher premiums. This, in theory, should encourage the adoption of global cyber security standards and improve cyber security generally.

How effective insurance is at regulating an industry is dependent on a variety of factors and is often a subject of considerable scholarly debate. Some recent evidence suggests that insurers may be less impactful in improving cyber security and preventing cyber incidents than previously thought.[256] A recent report by Cyberspace Solarium Commission (CSC), a group established by the US Congress to investigate cyber threats and develop a strategy to protect the US against significant cyber-attacks, argues that risk mitigation in the cyber insurance industry has little impact on hack prevention.[257] The CSC suggests that the relatively small market size of the cyber insurance industry and the ability to offload risk to reinsurers (both characteristics of the digital asset insurance industry) dampens the incentive of insurers to take risk mitigation seriously.[258] Scholars such as law professor Shauhin Talesh, however, have found that risk mitigation in the cyber industry can add value, though much of the benefit comes from services provided after a hack rather than preventing the cyber intrusion in the first place.[259]

Insurers have acted as de facto regulators across a variety of industries for centuries,[260] and they can and should do the same in the digital asset industry. Insurers should work together to adopt an industry-wide digital asset security standard. The Cryptocurrency Security Standard (CCSS), for example, is an independent organization that created a "set of requirements for all information systems that make use of cryptocurrencies, including exchanges, web applications, and cryptocurrency storage solutions."[261] Major insurers could adopt the CCSS (or any other mutually

---

[255] Camillo, *supra* note 70, at 60.
[256] CYBERSPACE SOLARIUM COMM'N., 2020 CYBERSPACE SOLARIUM COMMISSION REPORT, 81 (2020) ("A robust and functioning market for cyber insurance could play a similar role in identifying and regulating behavior to improve cyber risk management. Today, the market for cyber insurance is failing to deliver on this potential.").
[257] *Id.*
[258] *Id.* ("Because insurers can either assume their inherited cyber risk with little threat to their overall solvency or pass this risk along to reinsurers in the form of derivatives, they have little incentive to push the entities they insure to manage that risk.").
[259] Talesh, *supra* note 72, at 475; *see also* Camillo, *supra* note 70, at 60-61 (discussing how conducting simulated attacks and war games helps prepare companies to respond to hacks thus reducing the damage when a hack does occur).
[260] Talesh, *supra* note 72, at 472-3.
[261] *Cryptocurrency Security Standard*, CRYPTOCONSORTIUM,

agreed upon standard) as a minimum security threshold for crypto businesses hoping to obtain insurance. Insurers have a financial stake in the security of these storage solutions, so they are incentivized to adopt strong, dynamic standards and make improvements to such standards when the industry necessitates it.

Insurers acting as a de facto regulator by instituting industry-wide security standards would have a number of benefits. First, industry-wide security standards would improve the security of digital assets. If insurers were to institute such a standard, any company who wants to be viewed as a safe storage option would need to meet "certain cyber hygiene and pre-loss standards."[262] If insurers' standards are not met, the company would have difficulty obtaining insurance serving as a red flag to security-conscious consumers. While the most secure storage solutions available already likely surpass such proposed standards and therefore require little modification to their security infrastructure, those companies most susceptible to a hack would be forced to improve their security if they hope to obtain insurance. Otherwise, they risk losing customers to those competitors that do have insurance.

Collective security standards or rating systems would not be new to the insurance industry. Insurers in Canada, for example, fund the Vehicle Information Centre of Canada, which uses the CLEAR vehicle rating system to assess "the crashability, damagibility, and theft vulnerability of each type of manufactured vehicle, as well as the protection of individuals in them."[263] The CLEAR rating system indirectly improves the safety of automobiles in Canada. Rather than the government mandating a certain safety level, insurers indirectly improve automobile safety by charging higher premiums for models with lower CLEAR ratings. This unbiased safety information sponsored by CLEAR – and funded by insurers – allows consumers to pick safer cars both because they value their own safety, but also because their insurance premiums are lower.[264] Thus, car companies compete to make safer and safer cars not because they are legally required to but because consumers can see which cars are safest. Similarly, a common standard among insurers for digital asset storage solutions would allow consumers to recognize which companies provide suitable security.

Adopting a ubiquitous security standard such as CCSS or funding an independent security trade association focused on digital asset storage would also allow insurers to become familiar with that particular standard or rating system. The insurers would benefit from the consistency of applying the same model because they or their partners could quickly become experts in assessing compliant security architectures. Today, companies must spend hours educating the insurers about the digital asset industry and their security infrastructure, so insurers can make a one-off judgment about the risk. Adopting one framework for assessing security would save all parties time and

https://cryptoconsortium.github.io/CCSS/ (last visited Apr. 4, 2020).
[262] Camillo, *supra* note 70, at 60.
[263] ERICSON, ET AL., *supra* note 62, at 277.
[264] *Id.*

money and encourage industry conformity towards best practices. It may also make the development of risk mitigation tools economically viable. Methods such as simulated hacks to test security may not be feasible for one company to develop but could be worthwhile for an insurer to develop and deploy to all of its clients.[265]

Companies could also be confident that once they met the transparent and rigorous standards set by insurers or an independent organization, they would be able to obtain coverage. Today, many companies hoping to obtain insurance are denied because they are deemed too risky.[266] Setting one standard will help improve the clarity and transparency around what insurers expect in order to underwrite a digital asset storage policy. If there is one uniformly approved standard, companies will better understand what is expected of them and their security infrastructure to be deemed insurable. Insurers then benefit from increased demand of more attractive insureds rather than being forced to sift through the deluge of overly risky companies from whom they receive requests today.[267]

Finally, insurers stepping into this regulatory role alleviates pressure on the government to issue clearer rules and regulations surrounding asset security that could quickly become ineffective or outdated. In many ways, insurers are better placed than the government to be the regulatory force in the digital asset storage industry. Insurers tend to have far better access to information and more sophisticated tools for information aggregation and prediction.[268] Additionally, insurers are financially incentivized to limit digital asset security vulnerabilities. Nobody on a government payroll has any salary motivation to reduce digital asset risk.[269] A uniform approach by insurers can also create a national system rather than forcing digital asset companies to try to comply with a patchwork of state regulations. As the industry inevitably evolves, insurers can stay flexible and dynamic with their standards, which permits the government to take a more measured approach to creating new rules and laws and avoid implementing premature regulations.

CONCLUSION

[265] Camillo, *supra* note 70, at 60-61 (discussing how simulated hacks are typically sophisticated and best performed by a third-party so as to be the most realistic test of the security infrastructure, and that insurers are far better placed to assume this role than the company itself).
[266] *See* BITGO, *Insurance for Digital Currencies*, *supra* note 39, at 2-4 ("Shortage of quality institutional buyers with the attributes necessary to build a pool of similar risk and thus spread and mitigate aggregation of risk."). Additionally, a "high volume of submissions from cryptocurrency companies not able to pay the requisite premiums in order to fund significant losses." *Id*. As such, insurers are receiving significant requests for coverage, but most requests are coming from parties they deem too risky to insure. *Id*. Thus, they are unable to build a pool of companies the insurers' perceive as similarly less risky. *Id*.
[267] Johnathan McGoran, *Cryptocurrency is a Massive Uninsurable Risk: Here's How to Protect Your Assets*, RISK & INSURANCE J. (Mar. 18, 2020), https://riskandinsurance.com/cryptocurrency-is-a-massive-uninsurable-risk-heres-how-to-protect-your-assets/.
[268] Talesh, *supra* note 72, at 472.
[269] *Id.* at 471.

In the 1930s the Great Depression caused over 9,000 banks to fail in the US resulting in the worst economic depression in modern history.[270] In response Franklin D. Roosevelt signed the Banking Act of 1933, which among other initiatives created the FDIC, which provides government-backed insurance of deposited funds up to $250,000 per account. The FDIC restored faith in banks, dramatically increased deposits and lending, and is foundational to modern banking.[271] Until individuals can be guaranteed a similar level of security with their crypto assets as that in modern banks, it is unlikely that the industry will achieve the broad adoption that many enthusiasts desire.

Private insurance is currently the best and only realistic solution to guaranteeing the security of crypto assets. Institutional storage solutions have emerged that offer security-focused custody of digital assets that dramatically improve the security of assets. And a recent announcement by the Office of the Comptroller also confirmed that federally chartered banks could provide custody services for crypto assets.[272] Historically, however, no solution is one hundred percent bullet-proof. At the very least, nobody should consider digital asset storage solutions impenetrable until we have far more history and data.[273]

In the absence of perfect security, insurance is the only means of guaranteeing the value of the asset does not disappear overnight. Given the prevalence of hacks and the nascency of both the cryptocurrencies themselves and the available custody solutions, institutional investors are unlikely to be comfortable investing in digital assets without strong insurance coverage.[274] This backstop is likely a necessity for broad institutional adoption of crypto assets.[275] Even if custody solutions could guarantee security, insurance coverage may still be a legal or regulatory requirement for investment.[276]

Demand for insurance has skyrocketed in part because investors are chomping at the bit to be able to safely invest in this new asset class.[277] Over 70% of institutional finance executives believe that digital assets will have a place in the future of investing.[278] Without quality insurance coverage that can make holding digital assets functionally as safe as traditional asset classes, institutional investors will largely remain on the sidelines. At a bare minimum, investors need to be able to quantify the risk of holding digital assets. Insurance allows investors to convert an unknown risk

---

[270] Robert Stammers, *The History of the FDIC*, INVESTOPEDIA (Aug. 11, 2019), https://www.investopedia.com/articles/economics/09/fdic-history.asp
[271] *Id.*
[272] *Federally Chartered Banks and Thrifts May Provide Custody Services for Crypto Assets*, OFFICE OF THE COMPTROLLER OF THE CURRENCY (July 22, 2020), https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-98.html.
[273] Newman, *supra* note 98.
[274] *Id.*
[275] *Id.*
[276] *Id.*; Downey, *supra* note 103.
[277] Kathryn Tully, *Crypto's Next Act*, BNY MELLON (June 24, 2019), https://www.bnymellon.com/us/en/insights/aerial-view-magazine/cryptos-next-act.html.
[278] *Id.*

of catastrophic loss from a hack into a quantifiable monthly cost, which makes assessing the value of a digital asset investment far easier.

Retail users that would like to adopt cryptocurrencies and digital assets as daily forms of payment are also eagerly awaiting insurance. When cryptocurrencies gained prominence in 2017, many believed that it would be just months until bitcoin and other cryptocurrencies were a widely accepted retail payment option. Three years later (and over ten since the invention of Bitcoin), only an infinitesimal number of retailers accept payment in cryptocurrency. Lack of security is partially to blame. Users and retailers are not willing to hold a significant amount of money in digital assets until they can be confident that those assets will not disappear at the hands of a hacker. Those that do allow payment with crypto assets generally convert it back into fiat at the point of sale which is both expensive and clunky for the retailer.

Projects such as Libra[279] or the emerging interest in Central Bank Digital Currencies[280] could transform cryptocurrencies from a mainstream interest into a foundation of our everyday life, but they risk doing so before the problem of asset security is solved. If crypto assets are broadly adopted before we find a solution to improve or even guarantee the security of those assets, we will likely experience a digital repeat of the 1930s. Without broad insurance coverage and with new, untested custody solutions, the same systemic risks face the digital asset industry as those that caused banks to fail and millions to lose their assets during the Great Depression.

[279] LIBRA, https://libra.org/en-US/ (last visited Oct. 19, 2020).
[280] Raphael Auer, Giulio Cornelli and Jon Frost, *Rise of the central bank digital currencies: drivers, approaches and technologies* 1 (Monetary & Econ. Dept. Bank for Int'l Settlements, Working Paper No. 880, 2020), available at https://www.bis.org/publ/work880.pdf.