Cryptocurrency Insurance. Who Cares?

In 2021 a record $14 Billion was lost due to cryptocurrency related crime.[1] This number is up 79% from 2020 and will likely be dwarfed in 2022 due to the recent hacking and subsequent bankruptcy of $32 billion-dollar cryptocurrency exchange FTX.[2] In response insurance companies have begun selling 'digital asset insurance' to provide coverage for entities with significant amounts of cryptocurrencies. This report will explore the basic building blocks of cryptocurrencies, current digital asset insurance options, legal challenges surrounding coverage, and regulatory legal questions hampering the digital asset insurance industry.

A. Basic Building Blocks of Cryptocurrencies.

What are cryptocurrencies? Cryptocurrencies are digital currencies with no physical presence that operate on code called blockchain. A blockchain is a database stored and shared across multiple computers typically referred to as nodes.[3] These nodes perform cryptographic computations that validate transactions on the blockchain.[4] The result is a decentralized network of computers that allow the blockchain code to operate without a single party having the authority to control or modify it.[5] This novel way of computing allows users to trust the code without trusting any individual or organization.

---

[1] MacKenzie Sigalos, Crypto scammers took a record $14 billion in 2021, CNBC (Jan. 6, 2022, 4:00 AM), https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html.
[2] Joe Light, Crypto Self-Destructs Yet Again. Inside FTX's Failure, Barrons (Nov. 11, 2022), https://www.barrons.com/articles/ftx-binance-sam-bankman-fried-crypto-bitcoin-solana-price-crash-51668135110.
[3] Adam Hayes, Blockchain Facts, Investopedia (Sept. 27, 2022), https://www.investopedia.com/terms/b/blockchain.asp.
[4] Brooke Becher, What Are Blockchain Nodes and How Do They Work, Built In (Sep. 29, 2022) https://builtin.com/blockchain/blockchain-node.
[5] Anshika Bhalla, What Is Decentralization in Blockchain, Blockchain Council (Dec. 13, 2022) https://www.blockchain-council.org/blockchain/what-is-decentralization-in-blockchain/.

There are many different cryptocurrencies that utilize the blockchain uniquely. One common issue among all cryptocurrencies is storage. Users can store their currencies in wallets that can either be self-hosted or custodied by another entity. In either case, the wallet is accessed, and password protected via a private key. Whoever controls the private key controls the cryptocurrency and if the private key is lost then the assets are locked inside of the wallet forever.[6] Similarly, if the private key is stolen then the cryptocurrency inside of the wallet can also be stolen.[7]

B. Current Digital Asset Insurance Options.

Digital asset insurance operates like a standard insurance policy. An insurance provider agrees to indemnify another party against an unknown future loss in return for payments known as premiums.[8] The premiums are based on the assessed risk to the party providing the indemnification. Given how complexed the underlying blockchain technology is and the general nascency of the industry, calculating risk can be difficult.

There are three major areas that digital asset insurance attempts to remedy: (1) theft of cryptocurrencies from exchanges and wallets; (2) loss of private key access due to fire, natural disaster, or an act of God; and of course, an age-old problem, (3) scammers using fake emails or identities to steal cryptocurrencies. Digital asset insurance attempts to remedy these three major issues with three major policy benefits. First, digital asset insurance provides risk mitigation for

---

[6] Kirsty Moreland, What Are Public Keys and Private Keys, Ledger (Oct. 27, 2022), https://www.ledger.com/academy/blockchain/what-are-public-keys-and-private-keys.
[7] Benedict George, A Crypto Must-Know: Public vs. Private Keys, Coin Desk (Aug. 5, 2022), https://www.coindesk.com/learn/a-crypto-must-know-public-vs-private-keys/.
[8] Julia Kagan, Insurance Premium Defined, Investopedia (Mar. 3, 2022), https://www.investopedia.com/terms/i/insurance-premium.asp.

cryptocurrency holders (although the insurance companies will want to limit their downside by requiring technology infrastructure audits and extensive background checks for their insureds' employees). Second, the insurance provides a risk transfer benefit, in which cryptocurrency companies or exchanges can pay a predictable monthly premium which allows them to shift the risk of their assets being lost or stolen. Third, and potentially most important to policyholders is the marketing benefit. By having a digital asset insurance policy in place, cryptocurrency companies can use the veil of safety and security to advertise to potential customers.

In 2018 there was only a small number of digital asset policies available.[9] No major insurers had publicly announced any involvement in the industry. However, by 2020 the digital asset insurance market became a billion-dollar industry.[10] Many experts predict growth in the digital asset insurance market will outpace the general cyber security insurance market that has become a mainstay for many major insurers.[11] At the onset, insurance companies tried to apply existing policy forms to crypto currency. Crime insurance was seemingly the most relevant policy category. Many insurers felt that like real fiat currency, gold, or diamonds, cryptocurrency simply needed to be protected against theft with vaults and security. However, unlike fiat currency, gold, or diamonds, billions of dollars' worth of cryptocurrencies can be held on a device as small as a USB flash drive. This makes cryptocurrency exceptionally easy to steal. Issues like these also make risk hard to calculate because of misinformation surrounding hackings and in some cases the FBI won't give details.[12]

---

[9] Olga Kharif, Interest in Crypto Insurance Grows, Insurance Journal (July 23, 2018), https://www.insurancejournal.com/news/national/2018/07/23/495680.htm.
[10] Mengqi Sun, Insurance Providers Rethink Their Approach to Crypto, The Wall Street Journal (May 25, 2022),
[11] Ana Alexandre, Crypto Insurance Market to Grow, Coin Telegraph (Sept. 5, 2019), https://cointelegraph.com/news/crypto-insurance-market-to-grow-lloyds-of-london-and-aon-to-lead.
[12] MacKenzie Sigalos, The FBI Likely Exploited Sloppy Password Storage, CNBC (Jun. 9, 2021, 7:09 AM), https://www.cnbc.com/2021/06/08/fbi-likely-exploited-sloppy-password-storage-to-seize-colonial-ransom.html.

Like nearly all insurance policies, there are limitations to cryptocurrency coverage. For many reasons a cryptocurrency company may want to carve out parts of a policy or add liability caps that significantly weaken the value of a digital asset insurance policy to customers. Insuring all the cryptocurrency in an exchange may be an unnecessary cost if only a small portion of the currency is vulnerable to internet-based attacks. These limitations explain why only 2% of crypto related risks are currently insured.[13]

C. Legal Challenges Surrounding Coverage.

Without defined terms the legal world would fall into chaos. A similar issue exists when drafting insurance policies for cryptocurrency insurance. Vagueness presents big legal challenges for coverage and is evidenced by multiple cryptocurrency companies. As an example, Coinbase (one of the world's largest cryptocurrency exchanges) has on its website that its insurance policy "protects a portion of digital currencies held across our storage systems against losses from theft, including cybersecurity breaches."[14] This defined policy is much too vague to provide a framework for what incidents will or will not be covered because most events will probably not fall neatly under 'covered' and 'not covered' categories. To make matters worse there are many terms used in the cryptocurrency field that are not recognized in the Black's Law Dictionary such as "hash power" and "DeFi".[15] This can make even the most well written insurance policies null because the courts would have to hold trials just to have these words defined.

---

[13] Daphne Zhang, Crypto Insurance Policies 'Popping Up' to Meet Frenetic Demand, Bloomberg Law (Aug. 12, 2022), https://news.bloomberglaw.com/insurance/crypto-insurance-policies-popping-up-to-meet-frenetic-demand.
[14] Coin Base, Insurance - Legal, Coin Base (Dec. 12, 2022), https://www.coinbase.com/legal/insurance.
[15] Kara Pederson, Black's Law Dictionary 11th Edition, Featured New Terms, Thomson Reuters (July 30, 2018), https://www.legalcurrent.com/blacks-law-dictionary-11th-edition-featured-new-terms/#:~:text=cryptocurrency.,dark%20money.

This vagueness in the legal framework is also extended to the public purview. Many companies do not have their insurance policies available for public viewing so there is no way for consumers to evaluate the policies against one another. Even when the policies are public, they frequently fail to give the full story. Another large cryptocurrency company BitGo advertises that their insurance policy protects against "Third-party hacks, or theft of private keys. Insider theft or dishonest acts by BitGo employees or executives and loss of private keys."[16] But do vulnerabilities in the blockchain code that are exploited by nefarious users qualify as "third-party hacks" if they are not attacking BitGo directly? Does employee negligence fall under dishonest acts or would a different standard such as recklessness or intent apply? These are legal questions that make coverage challenging.

Another legal challenge surrounding coverage is decentralization. Earlier we discussed how the blockchain code is processed by multiple computers around the world creating a decentralized network. While this is a breakthrough in computer processing capabilities it also opens a can of worms for who is to blame when problems arise. Many cryptocurrencies have no central authority so where do you send a subpoena to? Who do you list on court filings when there is a claim? The answers are not clear and detract from recourse that insurers need to operate cryptocurrency policies effectively when claims are made.

Worse yet is when the decentralization concept is undermined with a 51% attack. When this occurs, 51% of the computers running the blockchain become compromised by an anonymous

[16] BitGo, Backed by up to $250M in Insurance, BitGo (Dec. 12, 2022), https://www.bitgo.com/resources/digital-asset-insurance.

individual who forces the blockchain to make changes to its code. Sometimes resulting in the exploitation of millions of dollars' worth of cryptocurrencies from the blockchain code. Since the attacker is anonymous and the hack is an exploitation of the code and not of a particular company who is to blame? How is an insurance provider to recover when no one party is at fault?

These types of attacks are only further complicated with the recent invention of decentralized finance. Decentralized finance, or DeFi for short, is essentially a banking system run on blockchain code. It eliminates intermediaries by allowing individuals to transact through peer-to-peer financial networks utilizing, security protocols and blockchain software. Once connected to a DeFi network, people can lend, trade, and borrow cryptocurrency with no centralized authority. However, while this new technology based on the blockchain is revolutionary, it is susceptible to abuse. Theft and money laundering plague the DeFi segment of the blockchain world but the question remains, are those responsible for writing the code also responsible for the abuse of that code?[17] Different policies vary in their stance on DeFi but many carriers refuse to engage in this segment because of the inherent issues it presents.

D. Regulatory Legal Questions Hampering the Digital Asset Insurance Industry.

Another issue to consider is whether federal law applies to cryptocurrencies and if so, can the insurance providers utilize the federal law to enforce their policies? The answer is it depends. Currently the SEC has been trying to apply federal securities laws to cryptocurrencies but is unable

[17] Mengqi Sun, DeFi Increasingly Popular Tool for Laundering Money, The Wall Street Journal (Jan. 26, 2022), https://www.wsj.com/articles/defi-increasingly-popular-tool-for-laundering-money-study-finds-11643202002.

to because of lawsuits against the SEC.[18] Many cryptocurrency companies are voluntarily complying with existing Know Your Customer (KYC) and Anti-Money Laundering (AML) laws, but the SEC still has not been able to define cryptocurrencies in a regulatory manner that applies. Attempts to create legal regulatory terms have been thwarted by cryptocurrency actors who believe the underlying technology that creates the cryptocurrency ecosystem is completely different than securities.

Current proposals for the future of regulation are coming from both sides of the isle. Some people say that the government has no place in the regulation of crypto currency, but that position would make insurance policies nearly impossible to underwrite. Others say that the government should purchase large amounts of the most popular cryptocurrencies so that they may become a market participant and regulate that way. Still others say that insurance carriers should operate as de facto regulators. The case for insurance carriers acting as de facto regulators is a strong one. In 1666, the first fire departments in history were established by insurers after suffering huge losses from the Great Fire of London.[19]

Later the insurance companies were responsible for the adoption of ceiling sprinklers and fire suppression systems that are now legally required in most modern buildings.[20] Insurance carriers also had a major impact on the auto industry by encouraging mandates for airbags and use

[18] Daily Hodl Staff, Pro-XRP Lawyer Forecasts End of Ripple Lawsuit as Rumors of Settlement Swirl, The Daily Hodl (Dec. 14, 2022), https://dailyhodl.com/2022/12/14/pro-xrp-lawyer-forecasts-end-of-ripple-lawsuit-as-rumors-of-settlement-swirl/.
[19] Mark Camillo, Cyber Risk and the Changing Role of Insurance, Taylor & Francis (Mar. 27, 2017), https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1296878.
[20] *Id.*

of seatbelts.[21] It seems insurance companies have a close nexus with the results of regulation and therefore are in the best position to propose regulations.

Even if all issues with crypto insurance are resolved will it matter? Many individuals want to keep their cryptocurrency holdings anonymous. Whether for tax purposes or personal privacy reasons sometimes there are no names associates with cryptocurrency wallets. Will someone with an anonymous wallet be allowed to purchase and pay for cryptocurrency insurance or will the government step in and disallow the practice?

E. Conclusion, a Lack of Consensus.

Like most of evolution, cryptocurrency insurance products will likely be a succession of failures that eventually brings us to something that works. There are numerous lawsuits pending surrounding the issues discussed in the paper. Thus, in the wise words of Roman statesman Lucius Annaeus Seneca, 'time will tell'.

[21] Richard Ericson, Insurance as Governance, Scholars Portal Journal (July 22, 2015), https://journals.scholarsportal.info/details/00029602/v111i0001/316_iagbrvotp2pv.xml&sub=all.