July 2019

ANDERSON KILL
POLICYHOLDER
ALERT

Insurance Coverage for Cryptocurrency and Blockchain Risks

By Stephen D. Palley

Insurance coverage for blockchain-related risks can be divided into several categories. The first and most familiar is risk associated with cryptocurrencies like bitcoin. The type of applicable coverage depends largely on how the cryptocurrency is being used and stored.

To date, the most commonly triggered risk has been associated with loss due to exchange hacks. According to a recent report by industry trade publication The Block Crypto[1], the total amount stolen from cryptocurrency exchanges exceeds $1.3 billion in value as of April 1, 2019. Of that amount, "approximately 61% of the thefts were in 2018 alone."

In practice, cryptocurrency is stolen via theft of private keys, which are kept either in "hot wallets" or "cold storage." A hot wallet provides storage that can be accessed from a network. Cold storage is offline, and inaccessible by other computers **via the internet**. While cold storage is more resistant to theft by hacking, it is less convenient and remains susceptible to loss or damage from a variety of perils.

Cryptocurrency is built on an append-only database structure, which can be changed only by adding new data. There is no "help desk," and transactions cannot be reversed.

Coverage for Hot Wallet and Cold Storage Theft

Cold storage risk is typically covered under a specie policy[2], a policy type that has historically been used to cover "high value portable items — such as precious metal, gems, securities, cash."

Coverage for theft from hot wallets may be available under a crime policy. In 2015, ISO amended the commercial crime coverage form to include a specific exclusion for "virtual currencies" applicable to "loss involving virtual currency of any kind, by whatever name known, whether actual or fictitious including, but not limited to, digital currency, crypto currency or any other type of electronic currency." When a version of the 2015 form is used, coverage can be added back for scheduled virtual currencies by using ISO endorsements issued at the same time.

Coinbase, a leading cryptocurrency exchange, recently disclosed in a blog post[3] that it has hot wallet crime coverage with a $255 million limit of liability through Lloyd's syndicates. Specie coverage limits have not been

ANDERSON KILL
1251 Avenue of the Americas
New York, NY 10020
(212) 278-1000

ANDERSON KILL
1760 Market Street, Suite 600
Philadelphia, PA 19103
(267) 216-2700

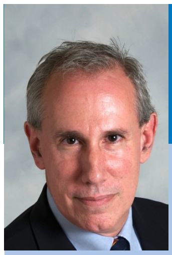
ANDERSON KILL
1055 Washington Boulevard, Suite 510
Stamford, CT 06901
(203) 388-7950

ANDERSON KILL
1717 Pennsylvania Avenue, Suite 200
Washington, DC 20006
(202) 416-6500

ANDERSON KILL
One Gateway Center, Suite 1510
Newark, NJ 07102
(973) 642-5858

ANDERSON KILL
Wells Fargo Building
355 South Grand Avenue, Suite 2450
Los Angeles, CA 90071
(213) 943-144

www.andersonkill.com



who's who

Stephen D. Palley is a partner in the Washington D.C. office of Anderson Kill. Mr. Palley is a seasoned litigator with deep experience in software design and development well-known in the cryptocurrency community. He is co-chair of Anderson Kill's recently launched Blockchain and Virtual Currency group, a cross-disciplinary team of lawyers with experience across a wide range of legal practice areas. The group provides legal advice in areas as diverse as litigation, trial practice, insurance coverage, tax, intellectual property, corporate/transactional and employment law.

spalley@andersonkill.com
(202) 416-6552

Anderson Kill
Newsletters & Alerts

TO SUBSCRIBE PLEASE VISIT:
andersonkill.com/Publication-Subscription.aspx

TO UNSUBSCRIBE PLEASE EMAIL:
unsubscribe@andersonkill.com

disclosed but would in theory cover "physical damage or loss of private keys (including employee misuse or theft) in cold storage."

Valuation Issues

What about insurance coverage for cryptocurrency held by an individual or business that does not carry specialized specie coverage? At the moment, only one case has considered this issue. *Kimmelman v. Wayne Insurance*[4] dealt with coverage for $16,000 in stolen bitcoins under a homeowner's insurance policy. The insurance company investigated the claim and paid the plaintiff $200, after applying a sublimit for "money." The plaintiff sued, alleging that the sublimit should not apply. The court denied the insurance company's motion to dismiss, reasoning that under IRS guidance, for federal tax purposes, "virtual currency is treated as property" and is therefore not money.

Another recent lawsuit has not yet resulted in a ruling on the merits of the underlying coverage dispute, but still illustrates an insurance quandary that the technology might engender. Plaintiffs in *818Computer, Inc. v. Sentinel Insurance Company Ltd.*[5], allege that prior to September 2017, their "business model was to design and build high-powered computers that 'mine' cryptocurrency full time" and depended on their ability to provide a warranty, only offered after three months of continuous operation. They further allege,

> [...] at the time of the burglary, Plaintiff had purchased the component parts for their machines on credit, with the intent of repaying those loans once the machines were sold. At the time of the burglary, the global cryptocurrency market was very favorable, and demand for the "rigs" was very high.

In short, an element of the damages that they seek in this case arises out hardware and software with highly volatile value. Whatever the ultimate outcome of this case, those seeking coverage for crypto losses should be mindful of this volatility when selecting limits.

"Smart Contract" Coverage

Finally, errors in "smart contract" code execution present another area of emerging technological risk where on-point precedent may not be obvious. The term smart contract refers generically to code stored using blockchain technology (they aren't actually legal contracts or necessarily "smart"). One of the stated benefits of smart contract code is that it cannot be changed, because of the nature of blockchains. Thus, if a smart contract-based flight insurance policy promises to pay a claim when a flight is late, the code cannot be changed after payment is made. At the same time, unchangeability presents a new and unique risk factor.

In one case involving cryptocurrency wallet software provided by an organization called Parity, more than $100 million in cryptocurrency was permanently locked and made inaccessible to wallet users.

Given the nature of open-source software creations, it is questionable whether professional liability or other insurance would be available to cover such losses. Smart contract-specific cover has begun to develop, however, with at least one company offering protection in the form of "discretionary cover" via a U.K.-based mutual insurer:

> The product will cover "unintended code usage" where someone, not necessarily the cover purchaser, has suffered a financial loss on the smart contract. As an example, the cover would pay out on the DAO hack, and the two Parity multi-sig wallet issues. It is not intended to pay-out on loss/misuse/phishing of private keys as this cannot be verified.

Insurance for cryptocurrency risks is still emerging as an industry-specific product, and case law remains limited. If the technology continues to scale, it is reasonable to assume that insurance will scale and grow with it.

ENDNOTES

[1] *https://www.theblockcrypto.com/2019/04/01/research-cryptocurrency-exchange-hacks-surpass-1-3-billion-all-time-61-coming from-2018/*

[2] *https://axaxl.com/fast-fast-forward/articles/specie-insurance_a-valuable-form-of-coverage*

[3] *https://blog.coinbase.com/on-insurance-and-cryptocurrency-d6db86ba40bd*

[4] *2018 Ohio Misc. LEXIS 1953 (Oh. Ct. of Common Pleas, Franklin County, 18 CV 1041, 9/25/2018)*

[5] *Cal. Superior Court, Los Angeles County, 18STSVO7218 (12/5/2018)*

[6] *https://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf*

This was prepared by Anderson Kill PC to provide information of interest to readers. Distribution of this publication does not establish an attorney-client relationship or provide legal advice. Prior results do not guarantee a similar outcome. Future developments may supersede this information. We invite you to contact the editor, Mark Garbowski at mgarbowski@andersonkill.com or (212) 278-1169, with any questions.