

---

---

## **Cryptocurrency and Cyber Risk: Market Analysis and Perspectives**

---

---

### Care, Custody, & Control (CCC): Identification, quantification, and mitigation of cryptocurrency custodial risk.

Au, A., Hoffman, M., Mattingly, J., McAteer, P., Takahashi, Y.\*

Working Paper: June 2020

---

#### **Abstract**

The combination of the blockchain technology and the cryptographic protocols upon which Bitcoin and many other cryptocurrencies are founded gives rise to complex challenges in the context of asset safekeeping. The Digital Signature Scheme means that whoever holds the private key owns the asset. The immutability of the Blockchain means that transactions recorded on the distributed ledger are permanent and irreversible. This study develops a comprehensive database documenting loss events since the birth of Bitcoin. Using the empirical data, we employ an actuarial technique to estimate losses in the cryptocurrency universe. We examine the risks associated with auto-custodial solutions and offer recommendations on security hygiene for different types of wallets. We recommend multi-signature technology with protections against so-called “paralysis” where a key shareholder is unavailable or uncooperative. Finally, recognizing that trusted third party custodians will dominate the crypto landscape in the medium term, we describe a best practice framework which asset holders should observe when seeking to delegate the function of key management.

*Keywords:* Bitcoin; Cryptocurrency; Blockchain; Crypto Custody; Private Key Risk; Access-control paralysis ; Paralysis Proof Systems; Dynamic Threshold Access Structures.

---

#### **1. Introduction**

In this paper, we evaluate the inherent risks of holding cryptocurrency, investigate the safekeeping of the asset for both retail and institutional market participants and propose a best practice framework to optimize its “Care, Custody, and Control” (CCC). We define CCC as the active protection of cryptocurrency private keys from loss due to operational failure by an asset holder or trusted third-party. CCC-mitigable events include theft and negligence and exclude fraud. Our research demonstrates that loss events since the first bitcoin was mined on January 3, 2009 equate to

over \$7.3 billion. The frequency and magnitude of these failures have contributed to price volatility and negative sentiment which has impeded the broader investment in, and use of, the asset among retail and institutional market participants. Liu and Tsyvinski [1] note that the “ratio between Google searches for the phrase ‘Bitcoin hack’ and searches for the word ‘Bitcoin’...a proxy for negative investor attention...negatively and significantly predicts 1-5 week Bitcoin returns”. Our research further indicates that these loss events could have been mitigated or even prevented through a more robust custodial risk management framework. Utilizing the collected loss data, we describe the distribution of expected losses using the Loss Distribution Approach (LDA). Finally,

---

\* All authors are holders of Master of Science in Risk Management awarded by NYU Stern School of Business.

based on the qualitative and quantitative analysis, including a review of major custodians, we document the best practices asset holders should adopt or require from trusted third parties to improve Care, Custody, and Control.

## **2. Literature Review**

### *2.1. Cryptocurrency*

The intellectual heritage of Bitcoin and Blockchain is comprehensively explored by Narayan and Clark [2]. Like Nakamoto, they trace the origins of the concept of a chained, temporally ordered, and immutable ledger data structure to ideas developed in the 90's by Haber and Stornetta [3][4][5]. Their latter papers introduce the notion of using "hash pointers" to link components in the chain, aggregating the constituent elements of the distributed ledger into timestamped "blocks" and encoding the contents of the block as a Merkle tree. The concept of the Merkle tree itself was proposed by cryptographer Merkle as far back as 1980 [6]. The notion of Proof-of-Work was first seen in a paper by Dwork and Naor in 1992 [7], who proposed that proof of moderate computational work could be demanded in order to prevent email spamming. In the same context of anti-spamming, this idea was developed by Back [8][9], incorporating the idea of a Proof-of-Work into his concept of "Hashcash" which requires finding an input by random guessing that hashes into an output below a specified target value. Dai [10] and Szabo [11] seemingly independently proposed digital currency schemes called b-money and bit gold respectively. In both schemes, money is created through proof of work. In both also, users transact under their pseudonyms, which correspond to public verification keys. The Proof-of-Work (PoW)-based consensus mechanism is the driving force behind both Bitcoin and Bit gold that utilizes the computing power as a means of solving a cryptographic puzzle to establish agreement between decentralized peer-to-peer participating nodes with high Byzantine fault tolerance. In the process, both create a cryptographic hash chain linking the most recent solution to its predecessor to validate transactions.

b-money and Bitgold are the recognizable theoretical forerunners of Bitcoin. However, Nakamoto's white paper [12] addressed the previously unresolved double-spending problem and Lamport's Byzantine General's problem [13]. In a decentralized system, copies of the ledger are distributed across multiple nodes in the network. The challenge is to maintain a consistent state of the ledger, which nodes will collectively recognize as authoritative and definitive, even though data is exchanged over a network which is potentially unreliable (due to latency effects) or compromised (due to malicious actors). Collective agreement on the validity and sequencing of transactions recorded of the distributed ledger is achieved through the proof-of-work consensus mechanism. This system awards the winning miner the exclusive right to add blocks of transactions to the immutable blockchain, incentivizes them to act honestly by compensating computational expense (proven "work") with a mining reward, which the miner will be reluctant to risk by the inclusion of invalid (e.g. double-spending) transactions, resulting in the probable orphaning of the proposed block by other mining nodes.

Following the publication of Nakamoto's white paper, as the value of bitcoin increased from a few cents to thousands of dollars, primers on cryptocurrency proliferated, motivated by the piqued interest of investors and policymakers. A notable early contribution from the academic community was that of Brito and Castillo [14] which focused on the "properties [and] operations" peculiar to the Bitcoin network from a non-technical perspective before describing the risk and opportunities from an economic, societal and legal standpoint. Federal Reserve economist Velde [15] and Swedish Riksbank official Segendorf [16] both published useful primers for non-specialists which gave insight into the transactional mechanics whilst touching on systemic and regulatory implications. Legal scholar Grinberg [17] combined a high-level overview with somewhat more philosophical musings on Bitcoin's durability and upcoming legal and regulatory challenges. As the formal research content has expanded and diverged, academics have sought to impose structure on the discipline by publishing detailed texts offering varying degrees of emphasis on cryptography, computer science and finance. Pioneering contributions in this

domain include those of Franco [18], Antonopoulos [19], Narayanan et al. [20], Halaburda and Sarvary [21], Chowdhury [22] and Bashir [23].

## 2.2. *Crypto Security Risk*

The broader adoption of cryptocurrency and the exponential growth in market value, accompanied by the increasingly frequent incidence of losses through theft or negligence, has encouraged more targeted research on security issues and key management. Rauchs et al [24] highlighted key security as a primary concern among market participants, estimating that \$1.5 billion of crypto assets were stolen due to security breaches from 2011 and 2018. Krombholz et al [25] conducted a survey to evaluate user experiences with bitcoin security, discovering that 22% of coin holders had suffered losses due to “security breaches or self-induced errors”. Conti et al [26] organized and summarized the existing body of scholarly work focused on security threats and solutions. Eskandari et al [27] compare existing key management techniques from the dual perspective of usability and security. Litke and Stewart [28] document the “cryptocurrency-stealing malware landscape”. Tyler Moore collaborates with various co-authors in multiple papers to explore the vulnerabilities of crypto exchanges. In 2014 he co-authored a paper [29] focused on the Distributed Denial of Service attack on Mt Gox collapse. This analysis of DDoS attacks is broadened in a subsequent paper [30] to encompass other participants in the Bitcoin eco-system. His empirical analysis of bitcoin exchange risk [31] sought to identify the variables which have the most explanatory power vis-à-vis exchange closures. This paper was updated, and the conclusions revised, in a follow-up paper [32]. G. G. Dagher [33] proposes a privacy-preserving proof of solvency for exchanges which “demonstrates that the exchange controls sufficient reserves to settle each customer’s account” yet the “exchange does not have to disclose its Bitcoin addresses; total holdings or liabilities; or any information about its customer”. A hardware device for securing one’s cryptocurrency was proposed by Decker [34]. Gennaro et al [35] describe an efficient and optimal threshold Digital Signature Algorithm (DSA) scheme for securing private keys. The concept,

which builds on work realized by Shamir in the field of secret sharing [36], involves the private key being split into shares. More precisely, “Any subset of the shares that is equal to or greater than a predefined threshold is able to reconstruct the private key, but any subset that is smaller will gain no information about the key...the key is never revealed because the participants directly construct a signature”. Zhang et al [37] explored how secret sharing can induce paralysis which they seek to resolve with an SGX-based paralysis proof technique”.

## 2.3. *Crypto Custody*

Rauchs et al. [24] defined custodian service providers as those which control the private keys of users. According to their survey, large companies tend to offer such services. A large majority of crypto custodians also use cold storages and multi-signature schemes and have refund procedures for lost or stolen funds.

Moore G. of CoinDesk Research [38] provided the overview of crypto custody, including leading crypto custodians and key technologies, and outlined operational and regulatory challenges. For example, crypto custodians need to create an internal control mechanism to keep private keys securely and ensure that technology works well to protect crypto assets through external security audits. Compliance with Know-your-customer (KYC) and anti-money-laundering (AML) requirements is a major regulatory challenge. More fundamentally, regulatory standards for qualified custodians may need to be set.

Gemini [39], the US crypto exchange and custodian, sought to describe how institutional-grade crypto custody infrastructures look like. Key features include the use of hardware security modules (HSMs) to safeguard private keys, rule-based permissioning for custody transactions, and the maintenance of multiple storage locations and backup sites. Anchor and BlockTower [40], the US digital asset custodian and institutional investment firm, also highlights critical aspects of custodian services, such as security, usability, and crypto-native services (e.g. voting and forks). It also emphasized the importance of examining insurance coverage of custodians. Global Digital Finance [41], an industry organization to promote best practices for crypto assets in the UK,

discussed key considerations to be given in safekeeping crypto assets. It covered legal and regulatory, security, and operational issues.

Regarding the access control of private keys in cryptocurrency custody, interesting research conducted by Cornell Tech. Zhang et al. [42] proposed the use of a paralysis proof technique to avoid facing a situation where crypto assets are frozen due to the death of a person who can sign off the access. For example, suppose that a multi-signature scheme is used to manage the access and the sign-off of three persons are required. If one person is dead, one of the two remaining persons can send a challenge to the person on a block chain. If there is no reply, the sign-off of two persons can become sufficient.

Baris [43] examined legal issues on custody requirements for digital assets. He explained that under US Investment Advisors Act of 1940, registered investment advisors need to use qualified custodians if they hold directly and indirectly client funds or securities. Registered investment advisors are also required to maintain client funds or securities in segregated accounts under the names of clients and follow other requirements, such as the preparation of account statements and surprise audits. However, Baris pointed out that the current custody rule is unclear about how the rule treats digital assets and how custodians should safekeep them. For example, the impacts of losing and misusing private keys and transferring digital assets in error are significant as digital assets can be frozen and may not be recovered. The verification of the exclusive ownership of bearer assets is also challenging. These new challenges indicate that new regulatory considerations will be required.

Schaefer [44] discussed how the custody rule can be applied to cryptocurrency fund managers. He pointed out that while the custody rule requires that investment advisors hold clients' assets with qualified custodians, there are a few challenges, such as availability of qualified custodians, forks and airdrops, and security vs. convenience. In addition, there are legal debates over the applicability of the custody rules, including whether a crypto asset is a security or a client fund under applicable laws. Ultimately, Schaefer suggested as an interim solution, that the SEC provide a no action letter as long as funds meet certain conditions for now, rather than strictly

applying the existing rules by imposing fines or placing cease-and desist orders.

In fact, it is clear that the SEC intends to continue to use the Howey test to consider whether a digital asset is a security to be invested, based on the presentation of the SEC in June 2018 [45] and the related framework disclosed on its website. According to the framework, in the Howey test, an investment contract is considered to exist if one invests in a common enterprise, reasonably expecting income from the efforts of somebody else. Based on these criteria, the SEC considers that Bitcoin is not a security because of its decentralized structures (no common enterprise exists). At the same time, the SEC has taken legal actions against Initial Coin Offerings (ICOs) because digital tokens issued in ICOs were considered as securities based on the Howey test but were sold to investors without registrations required under the US securities laws.

Nevertheless, it is not entirely clear what implications the application of this test will have on crypto custody. Baris described the filing of Cipher Technologies Management LP [43] on the registration of a bitcoin fund in May 2019 and concluded, "The debate over whether cryptocurrencies are securities for the purpose of the federal securities laws is far from over, and in fact may have only just begun." Cipher tried to convince that Bitcoin is a security in its proposed Bitcoin fund. However, the SEC rejected the filing in October 2019 [45], stating that the investors of Bitcoin are not "relying on the essential managerial and entrepreneurial efforts of others to produce a profit" and the fund will not be regarded as an "investment company" under the law. The SEC also pointed out that the company has not addressed valuation, custody, and price manipulation issues sufficiently.

### **3. Contextualization of Custodial Risk**

The peculiar properties of cryptocurrency have led to significant loss events over its short history. Our research identifies 166 loss events totaling \$7.3 billion in stolen or locked cryptocurrency over approximately ten years. At least 11% of the bitcoin in circulation has been lost due to hack, negligence, Ponzi scheme, exit scam or ransom/extortion. The essential

characteristics of cryptocurrencies – control of assets with the private key, blockchain immutability, and anonymity – give rise to the potential for losses that are both total and irrevocable. Securing cryptocurrency holdings depends fundamentally on safeguarding the private key. From an ownership perspective, possession of the private key is equivalent to holding a bearer bond. Bearer bond ownership is not authenticated through any means other than possession of the certificate. The unregistered nature of bearer bonds is also analogous to the anonymity of the private key holder for cryptocurrencies such as Bitcoin and Ether. The aspect of anonymity renders cryptocurrency a particularly attractive asset for criminals and therefore more vulnerable to attacks by malicious actors. Moreover, the blockchain protocol utilized by the vast majority of cryptocurrencies, is intended to be immutable. When a transaction is recorded on the blockchain, it is permanent and irrevocable. The block that contains the transaction is locked in perpetuity. Thus, if a transaction is the manifestation of nefarious or merely negligent activity, recovering the lost asset is nearly impossible.

The tumultuous history of cryptocurrency, marked by a consistent negative association with criminal activity, encourages market participants' skepticism of the asset. Crypto's connection with illicit activity such as Silk Road, a dark web site offering drugs and other illegal goods, has led to pervasive negative sentiment and an aversion to holding the asset among retail and institutional actors. This inevitably has impeded the broader adoption of cryptocurrency as a store of value or means of exchange. Loss events, often accompanied by severe volatility, have further contributed to the negative perception of the asset. According to a study by the University of Cambridge, exchanges ranked "IT Security" and "Fraud" as 2 of the top 3 major operational risks [24]<sup>1</sup>.

By means of the anatomization of the holding risks, the empirical analysis of loss materialization, the quantification of potential losses for market participants, and the formulation of a best practice framework for the safeguarding of cryptocurrency, we hope that our research will contribute to the current

thinking and practice related to value protection and lead to a more robust cryptocurrency ecosystem.

#### 4. Technical Overview

It is helpful to preface any discussion of the security risks peculiar to cryptocurrencies with an exposition of the technical architecture and economic logic on which the assets are founded. In this section, we consider a simple Bitcoin transaction from origination to completion as an effective illustrative and pedagogical device.

Let us assume that Alice wishes to transfer 5 bitcoins to Bob. Both parties will be transacting under their pseudonyms in the network, which correspond to public verification keys,  $pk_A$  and  $pk_B$ , produced by the following algorithm, consistent with any cryptographic digital signature scheme:

$$sk, pk := generateKeys(keysize) \quad (1)$$

A digital signature protocol is the combination of a public-key algorithm with a digital signature scheme. The public-key algorithm provides the underlying asymmetric mathematical algorithm. The digital signature scheme proposes a way to use this asymmetric algorithm to arrive at a workable digital signature.

The private (secret) key,  $sk$ , is a randomly generated 256-bit number meaning that it has a value bounded by 0 and  $2^{256}$ . It is converted to a hexadecimal format. The public key,  $pk$ , is generated from the private key by using the latter as an input in an encryption function called elliptic curve multiplication<sup>2</sup>. The x co-ordinate of final point on the elliptic curve will form the compressed public key. More technically, the public key is calculated using scalar multiplication over the elliptic curve<sup>3</sup>:

$$pk = (sk \times G)_x \quad (2)$$

Elliptic curve multiplication has two properties common to all cryptographic digital signature systems. Firstly, it is a one-way "trapdoor" function meaning that it is computationally efficient in one direction

<sup>1</sup> See Sentiment Survey in Appendix

<sup>2</sup> Bitcoin uses a digital signature scheme called the Elliptic Curve Digital Signature Algorithm (ECDSA). The parameters of the particular elliptic curve of Bitcoin adhere to the standard secp256k1.

<sup>3</sup> The x subscript denotes taking the x-coordinate of an elliptic curve point

(obtaining the public key from the private key) thanks to the double-and-multiply algorithm, whilst the inverse is computationally infeasible (deriving the private key from the public key) due to the discrete logarithm problem.

The public key is also converted to a hexadecimal format. A hashed version of the public key, known as the address, is then generated by putting it through the SHA256 and RIPEMD160 hash functions<sup>4</sup>, thereby reducing it in size and providing an extra layer of security<sup>5</sup>. As a result, there is 1 private key per address. From a key management perspective, crypto holders may allocate their bitcoin to as few or many addresses as they desire<sup>6</sup>.

The so-called transaction outputs (TxOut) for the transaction between Alice and Bob,  $Tx_{AB}$ , will contain information about the use of funds, comprising the amount being sent – in our example, an integer value representing a quantity of 5 bitcoins and the recipient address,  $RIPEMD160[SHA256(pk_B)]$ . The transaction output is encumbered by a locking script, *ScriptPubKey*, which imposes conditions under which the funds can be subsequently redeemed by Bob, that is, used as inputs in future transactions. So-called transaction inputs (TxIn) for  $Tx_{AB}$  relate to the source of funds, the encumbered unspent coins, *UTXO*, which Alice has received from a previous transaction. Specifically, TxIn holds a reference to the unique identifier of the previous transaction, *TXID*, which is actually the hash of the previous transaction data<sup>8</sup>, together with a specific index number (vector), *VOUT*, within that transaction's output array. Prior to its broadcast to the network, the hash of the spending transaction must be signed with the private key of Alice to prove that she can redeem these locked unspent outputs, being the owner of the private key associated with the address at which the funds are

stored, as referenced in the locking script for this previous transaction.

$$\sigma_{SigA} := sign[sk_A, H(Tx_{AB})] \quad (3)$$

The algorithm involves first generating an ephemeral random number,  $n$ , which is multiplied by the generator point  $G$  on the elliptic curve to produce the randomized final  $x$  coordinate a point on the elliptic curve,  $r$ :

$$r = (nG)_x \text{ mod } p \quad (4)$$

The second element of the digital signature,  $s$ , is formed by multiplying this  $x$ -coordinate of an elliptic curve point by the private key, adding the hashed transaction, and then multiplying the entire term in parenthesis by the inverse of  $n$ :

$$s = n^{-1}[(r \times sk_A) + H(Tx_{AB})] \text{ mod } p \quad (5)$$

The signature therefore consists of the pair of integers  $(r, s)$ :

$$\sigma_{SigA} := (r, s) \quad (6)$$

The transaction is then “broadcast on the bitcoin network, where each Bitcoin client<sup>9</sup> validates and propagates the transaction until it reaches (almost) every node in the network. Finally, the transaction is verified by a mining node and included in a block of transactions, that is, recorded on the blockchain” [19].

The first node in the network that receives the transaction verifies that it is a valid transaction. For each input in the transaction, the validation software will first retrieve the UTXO referenced by the input by consulting the unspent transaction outputs cache to

<sup>4</sup> A hash function is defined as a function  $h: S \rightarrow [0, m]$  that maps inputs of arbitrary size of a set  $S$  to a fixed interval  $[0, m]$ . Cryptographic hash functions have several security properties (collision-resistance, pre-image resistance, and uniform distribution) which we will discuss later.

<sup>5</sup> Bitcoin addresses are almost always presented to users in an encoding called “Base58Check” which further simplifies the address to 58 characters to help human readability, avoid ambiguity, and protect against errors

<sup>6</sup> The smallest indivisible unit of the Bitcoin currency is the Satoshi.  $10^8$  satoshis = 1 bitcoin

<sup>7</sup> List unspent

<sup>8</sup> Transaction ID obtained by hashing transaction data through SHA256 twice. In our example,  $H(Tx_{AB})$  should more correctly be denoted as  $SHA256[SHA256(Tx_{AB})]$ . We opt to represent the transaction as  $H(Tx_{AB})$  for reasons of economy.

<sup>9</sup> A synonym for nodes. The Bitcoin network is composed of nodes. Nodes are computers running the Bitcoin Core (Satoshi Client) software and connected, via the internet, to other computers running the same program to form a peer-to-peer network. Every node on the network is homogeneous and equipotent, thus the network participants are described as “peers”. The nodes are also autonomous in that the decision-making is entirely dictated by the software.

confirm that the previous outputs referenced by the transaction exist and are spent. It then checks that the transaction is not spending more than the available inputs<sup>10</sup>, i.e.:

$$isValid := Verify[TxIn_{Current} \geq TxOut_{previous}] \quad (7)$$

As mentioned, the UTXO contain a locking script, *scriptPubKey*, which defines the conditions required to spend them. Bitcoin clients will validate transactions by executing the locking and unlocking scripts together. When the unlocking script, *scriptSIG*, is run, Alice's public key,  $pk_A$ , is duplicated, via the DUP operation, and then run through the SHA256 and RIPEMD160 functions, via the HASH160 operation. The EQUALVERIFY command is run to compare the hashed value with the hashed public key  $RIPEMD160[SHA256(pk_A)]$  in the original *scriptPubKey* which had locked these coins resulting from a previous transaction:

$$EQUALVERIFY(pk_A, RIPEMD160[SHA256(pk_A)]) == TRUE \quad (8)$$

If successful, the script continues and the CHECKSIG operator checks Alice's signature against the public key:

$$CHECKSIG(pk_A, \sigma_{sigA}) == TRUE \quad (9)$$

This process<sup>11</sup> supplies proof of ownership of  $pk_A$  and enables the removal of the encumbrance on the unspent outputs. The verifying algorithm takes as inputs the public key, a hash of the entire transaction data which we wish to unlock and a valid signature:

$$isValid := Verify[pk_A, \sigma_{sigA}, H(Tx_{AB})] \quad (10)$$

The equation which the signature and the hash must satisfy is:

$$P_{x,y} = [s^{-1} \times H(Tx_{AB}) \bmod p]G + [s^{-1} \times r \bmod p]pk_A \quad (11)$$

Where  $P_{x,y}$  is a point on the elliptic curve whose x coordinate,  $P_x$  must match the x co-ordinate of the original random point on the elliptic curve, that is:

$$P_x = r = (nG)_x \bmod p \quad (12)$$

This is proof that the digital signature was created using the private key connected to this public key. The intuition of this equality is best demonstrated by the algebraic reformulation of the equation, beginning with rewriting the public key:

$$\begin{aligned} P_{x,y} &= [s^{-1} \times H(Tx_{AB}) \bmod p]G + [s^{-1} \times r \bmod p]pk_A \\ &= [s^{-1} \times H(Tx_{AB}) \bmod p]G + [s^{-1} \times r \bmod p](sk_A \times G) \end{aligned} \quad (13)$$

Then factorizing:

$$P_{x,y} = \{s^{-1} [(r \times sk_A) + H(Tx_{AB})] \bmod p\} G \bmod p \quad (14)$$

Substituting  $s$  for  $n^{-1}[(r \times sk_A) + H(Tx_{AB})] \bmod p$ , yields:

$$\begin{aligned} P_{x,y} &= \{[(r \times sk_A) + H(Tx_{AB})] \bmod p\} \\ &\quad \times \{[(r \times sk_A) + H(Tx_{AB})] \bmod p\}^{-1} \\ &\quad \times [(nG) \bmod p] \end{aligned} \quad (15)$$

The multiplication of the term  $\{[(r \times sk_A) + H(Tx_{AB})] \bmod p\}$  by its inverse cancels out both these terms, simplifying to:

$$P_{x,y} = (nG) \bmod p \quad (16)$$

Taking only the x co-ordinate of this point on the elliptic curve, we can prove that the generated pair (r,s) is indeed a valid signature for the message digest  $H(Tx_{AB})$  :

<sup>10</sup> The Bitcoin protocol requires the full expenditure of outputs. Where the coin value of the output exceeds the amount which the sender wishes to pay, he creates a transaction with one input and two outputs to send the difference back to his own address. This is known as a change transaction

<sup>11</sup> This operation within the Bitcoin protocol is known as pay-to-pub-key-hash (P2PKH) transaction. It is the most common transactional operation equating to 81% of executed signature checks. Others include Pay To Pubkey (P2PK) - 0.1% of total, Pay To Multisig (P2MS) - 0.7% of total, Pay To Script Hash (P2SH) - 18% of total.

$$P_x = r = (nG)_x \text{ mod } p \quad (17)$$

If the received transaction is valid, the node updates a data structure referred to as the Unconfirmed Transactions' Memory Pool and relays it to the connected nodes. Each node independently validates each transaction. The unconfirmed transaction between Alice and Bob, involving a transfer of 5 Bitcoins is propagated in this manner through the network. Specialized mining nodes will gather this and other transactions from the memory pool to form a candidate block which they seek to append via "mining" to a chain of previously formed confirmed transaction blocks. Each candidate block is made up of a Merkle tree aggregating the new transactions and a block header. The block header contains<sup>12</sup> the Merkle root of the proposed block, the block hash of the previous block in the chain, a time stamp<sup>13</sup> and a nonce, which is a randomly generated number which miners iteratively adjust to find a valid hash of these fields in the block header, that is, a valid "block hash" for this candidate block. The first miner to resolve this puzzle of finding the valid block hash broadcasts the proposed block to the other miners along with the successful nonce. The block hash solution is trivial to verify. Once verified, the new block is timestamped and added to the chain.

As indicated above, pairs of TXID<sup>14</sup> contained within a block are recursively hashed together<sup>15</sup> and encoded into a Merkle tree to obtain a single hash, the Merkle root. A Merkle tree is a binary tree data structure allowing for the efficient verification of the integrity of large data sets. By way of example, let us suppose that a proposed transaction block contains a batch of 8 transactions (Tx1, Tx2, Tx3...), the hashes of which (H1, H2, H3...) form the leaves of the Merkle tree. The hash of each parent node is the concatenated hash of its two children. Thus:

$$\begin{aligned} \text{Parent Nodes Level 1} &>> \mathbf{H12} = H(H1||H2); \mathbf{H34} = H(H3||H4); \\ & \mathbf{H56} = H(H5||H6); \mathbf{H78} = H(H7||H8); \\ \text{Parent Nodes Level 2} &>> \mathbf{H1234} = H(H12||H34); \\ & \mathbf{H5678} = H(H56||H78); \\ \text{Merkle Root} &>> \mathbf{H12345678} = H(H1234||H5678) \end{aligned}$$

Let us now suppose that we wish to ascertain the correct inclusion of the transaction involving Alice and Bob - Tx5 - in the batch of transactions. A mining node can produce an authentication path connecting Tx5 to the Merkle root which has a length of:

$$\begin{aligned} &[\log_2 (8 \text{ Transactions})] \times \\ &32 \text{ Byte hashes} = 96 \text{ bytes total} \quad (18) \end{aligned}$$

Any corruption, modification, or exclusion of Tx5 would result in a new Merkle root revealing the change, such that:

$$\begin{aligned} \text{Original Merkle Root} &\neq \\ &H\{[H[H[H(T5) || H6] || H78] || H1234]\} \quad (19) \end{aligned}$$

One of the reasons for the widespread use of hash functions in the Bitcoin protocol is that of computational efficiency, allowing the preimage – an input message of arbitrary string length – to be stored as unique fixed-size output – for example, a digest of 256-bits in the case of SHA-256. The hash functions are also cryptographically secure. Firstly, the cryptographic hash function is preimage resistant in that it is computationally intractable to invert the hash function and compute its input(s). Secondly, the hash of the message is collision-resistant meaning that it is infeasible<sup>16</sup> to find two values,  $x$  and  $y$ , such that  $x \neq y$ , yet  $H(x) = H(y)$ . The 256-bit hash therefore serves as a unique message digest which, moreover, given its size, facilitates detection of message corruption or modification. Cryptographic hash functions should be uniformly distributed, which

<sup>12</sup> In addition to two other fields: Version of the block; Proof-of-Work difficulty target for this block

<sup>13</sup> In Unix time. It is the time elapsed since the Unix epoch. The Unix epoch begins as of 00:00:00 UTC on 1 January 1970. Time elapsed is measured in seconds excluding leap seconds.

<sup>14</sup> Transaction ID obtained by hashing valid transactions through SHA256 twice.

<sup>15</sup> The cryptographic hash algorithm used in bitcoin's merkle trees is also double-SHA256.

<sup>16</sup> Note that we use "collision resistant" rather than "collision free" and "infeasible" rather than "impossible". Given that the set of input values for a hash function can be of infinite size whilst the set of output values is of finite size, there is a non-zero probability that two different input values have the same output value. The probability of collision for a hash function with a 256-bit output size is  $1/2^{256}$  in the worst case and, on average, based on a probability phenomenon called the birthday paradox, approximately  $1/2^{128}$  which is equal to  $1/340,282,366,920,938,000,000,000,000,000,000,000,000,000$



means the function has no outputs that are more likely to occur than others.

Bitcoin uses partial hash inversion as its proof-of-work function. In this Proof-of-Work system, network participants compete to solve computationally expensive cryptographic puzzles in order to win the right to append “blocks” of aggregated transactions to the blockchain and collect the mining reward<sup>17</sup>. This puzzle-solving process is commonly referred to as “mining”. The proof of work in Bitcoin requires generating a message whose double SHA-256 hash digest – the block hash – has a value less than the hash target set by the network. The input string in the concatenation of the fields in the block header<sup>18</sup> i.e. the previous block hash, the merkle root of the new collated transactions, the timestamp and a random value, known as the nonce. The goal is to find the “golden nonce” such that the resulting block hash is less than a set target value,  $\alpha$ :

$$H(\text{Nonce} \parallel \text{Previous Block Hash} \parallel \text{Merkle Root} \parallel \text{Timestamp}) < \alpha \quad (20)$$

The SHA-256 hash algorithm generates a 64-digit hexadecimal hash value. The current Bitcoin blockchain requirement implies a nonce that creates a block hash with 18 leading zeros<sup>19</sup>. The hash function is deterministic but computationally infeasible to invert in order to analytically derive the golden nonce. The only feasible method to resolve the puzzle is to iteratively input multiple nonce values until the described condition is satisfied. This requires significant computing power.

The higher the target, the lower the difficulty. The maximum target is defined as  $2^{224}$ . Since there are  $2^{256}$  different values a SHA-256 hash can take, a random hash has a chance of about  $2^{32}$  to be lower than the max target. The current target is variable and will increase or decrease every 2016<sup>th</sup> block to maintain a block generation rate of approximately one every 10 minutes. Thus, the current target is determined by

multiplying the constant minimum difficulty threshold by a variable difficulty level,  $d$ , to define the expected number of hashes to find a valid block hash:

$$2^{32} \times d = \text{Current Required Work} \quad (21)$$

Given that a miner is expected to be successful in every 10 minutes, the implied current global computation speed – the network hash rate – in hash/second is:

$$\frac{2^{32} \times d}{10 \times 600} = \text{Current computation speed (hash/second)}$$

Miners are rewarded for expending computational effort to find a valid block by gaining the right to insert a coinbase transaction in the block, thereby minting a specified amount of currency and transferring it to an address of their choosing. Dividing this figure of the total number of hashes generated per second by the number of hashes per second generated by an individual miner will yield his expected market share. Market share and the proportional capture of total block reward is therefore is a function of a miners’ computing power relative to the total computing power dedicated to mining activity.

Having found a valid block hash, the successful mining node will broadcast the block along with the calculated hash value and nonce to its peers, who will independently validate the block and then propagate the block across the network. Each node will update its copy of the blockchain. Miners are incentivized to act honestly due to their disinclination to incur mining costs (electricity, hardware) only to jeopardize the mining reward<sup>20</sup> (transaction fee, coin award) by including invalid transactions (e.g. double spent coins) which will result in the probable orphaning of the proposed block. Mining nodes express their acceptance of the block by proceeding to work on the next block in the chain. The hash of the accepted block will serve as the previous hash. In the case of forks in the chain, the aggregate weight of CPU effort applied

<sup>17</sup> Currently 12.5 BTC. The reward halves every 210,000 blocks. Miners can also be incentivized to include certain transactions by the sender’s inclusion of a transaction fee, equivalent to the amount remaining when the value of all outputs in a transaction is subtracted from all its inputs.

<sup>18</sup> 2 fields not included here for economy are the Version of the block and Proof-of-Work difficulty target

<sup>19</sup> In the words of Satoshi Nakamoto, the objective is to “scan for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits”

<sup>20</sup> The miner can only spend his block rewards after 100 blocks have been mined on top of his mined block

to each prong will be the arbiter of acceptance or rejection and the determinant of the path of the consensus chain. Assuming either no forking or its incorporation in the winning fork, the newly appended block containing the transaction between Alice and Bob of 5 BTC, will become part of the immutable distributed ledger. The transfer of value is complete.

## 5. Risk Identification

The combination of the blockchain technology and the cryptographic protocols upon which Bitcoin and many other cryptocurrencies are founded achieved Nakamoto's vision but gave rise to two crucial challenges in the context of asset safekeeping: (1) *The Digital Signature Scheme* means that whoever holds the private key owns the asset; and (2) *The Immutability of the Blockchain* means that transactions recorded on the distributed ledger are permanent and irreversible.

Protection of the private key is therefore of paramount importance due to the risk of irrevocable (and total) loss of one's digital assets. The holder's ownership of the private key is not subject to interrogation or validation. Asset control is simply asserted by presenting a private key which corresponds to the public key, also known as the address. Any person holding the private key may authorize a transaction and spend the coins in an address. Due to the technical complexities associated with safeguarding and transacting in cryptocurrency, most market participants cede their private keys to third parties in the form of wallet providers, custodians and (custodial) exchanges. Ironically, the result of this is the centralization of an asset and the dependence on a trusted intermediary within a system originally conceived to be decentralized and trustless.

### 5.1. Asset safekeeping: The Private Key Conundrum (PKC)

As previously noted, any spending transaction must be signed with the correct private key to prove the user can legitimately redeem unspent coins. The correct private key is that which is associated with the address (public key) at which the funds are stored. The digital signature scheme requires that the cryptocurrency

protocol software validates the submitted private key. This necessitates a connection on-line with the crypto network. The asset holder is thus faced with the "Private Key Conundrum" (PKC), namely, how to store the private keys such that they are (1) Accessible by the user and the network, (2) Secured against theft by online and offline adversaries; and (3) Protected against loss through negligence or accident. The repercussions of theft or loss for the user are usually total (and catastrophic) and, due to the immutability of the blockchain, irreversible. The failure to resolve the conundrum undoubtedly presents a significant obstacle to broader adoption of crypto among retail and institutional actors as a medium of exchange and store of value.

### 5.2. Manifestations of Private Key Risk for Key-Holder

Conti et al [26] presented a systematic survey on security issues. Early users of Bitcoin initially opted to simply store keys on their device's local storage. The reference Bitcoin client software, referred to as Bitcoin Core or Satoshi Client, stores private keys in a file, referred to as a wallet, inside a preconfigured directory. Since at least 2011 adversaries exploited this naïve approach to storage by "Wallet Stealer" malware which accesses the local file, extracts the victim's keys and steals the coins by digitally signing a transaction. The private key is additionally exposed to the physical theft of the device, equipment damage or failure, accidental loss of the hardware or mistaken deletion or corruption of the file, the file folder or hard disk. As malware attacks became more prevalent, users favored encrypted wallet files, requiring a password for access. Malware authors adapted their approach, devising "Credential Stealer" malware, for example, with a keystroke logging capability to discover the victim's password and gain access to the wallet. Encrypted wallets fundamentally fail to address the risks of unencrypted wallets save, arguably, for the risk of physical theft. However, a determined adversary could blackmail or threaten the private key holder to reveal the password, in which case device theft would prove successful. As an alternative to maintaining cryptographic keys in a digital file, deterministic or "brain" wallets allow private keys to be generated by hashing a passphrase

of unrestricted length. Neither the password nor the private key need be stored in a device and the challenge of preventing access to the digital file is eliminated. However, as with encrypted wallets, the user's private key remains vulnerable to brute-force attacks and lost or forgotten passwords.

It has become increasingly common to store keys offline and only hold in online wallets the keys to unlock funds necessary for immediate operations. So-called cold storage may mean that keys are maintained on paper, USB or some other dedicated hardware device. Of course, prior to cold storage (key creation) and subsequent to cold storage (digitally signing transactions), the private key will be exposed on an internet connected device to the risk of cyber-attack. Hardware wallets seeks to address this threat by storing keys on a device that signs, and exports transactions to a second internet-enabled device for transmission onto the Bitcoin network. However, such devices remain vulnerable to malware and the underlying PKC is transformed though not resolved. For example, the threat of "Man in the Middle" malware, which alters the recipient address of a transaction before it is signed, is unsolved by such technology.

### *5.3. Delegation of Key Management: Exposure to Operational Risk*

Given the multitude of risks to which key holders are subject, a popular approach to key management is to delegate the task to trusted third parties, such as crypto exchanges or pure-play crypto custodians, who offer hosted wallet web services comprising key storage, management, and transaction functions. Transactional ease is improved, and some risks are mitigated via mechanisms such as two-factor authentication (2FA) and password recovery options. However, crucially, from the perspective of risk, the host assumes custody of the private key and, in the case of exchanges, a significant proportion of transactions occur off-chain and on-balance sheet. The key holder is thus exposed to third party operational risk. Risk materializes principally in two forms: (1) The collapse of the entity providing the custodial function; and (2) Security breaches which results in the loss of users' funds due to negligence or misconduct by the operators of the exchange. This definition

includes phishing attacks against the users of an exchange, external and internal malicious actors exploiting vulnerabilities in the exchange's software or hardware, data losses lead to unrecoverable loss of funds and insider scams.

### *5.4. Delegation of Key Management: Illustrative Cases of Risk Materialization*

This section seeks to render in more concrete form the risks faced by asset owners who place their assets under custody by drawing on illustrative examples of custodial risk materialization. We naturally consider the risk as belonging to a subset of operational risk which arises from inadequate or failed internal processes, people and systems, or from external events and includes fraud, (cyber-)security failure, human error and organizational negligence.

**Hacking:** Over the last decade, security failure attributable to cyberattacks or hacking has assumed various forms, as internal and external adversaries have sought to exploit weaknesses in the protocol and the embryonic risk processes and technology of intermediaries. According to our loss events data, out of 166 collected loss events, 67% are caused by hacking since year 2011. The most notorious hack occasioned the collapse of Mt Gox in 2014 and the loss of over \$450 million worth of BTC. This hack was detailed in papers by Decker and Wattenhofer [34] and Conti et al [26].

As previously noted, exchanges pool client assets into a small number of accounts to facilitate the aggregation of low-cost, efficient intra-platform (off-blockchain) and extra-platform (on-blockchain) trades. The keys associated with these accounts are held offline (i.e. in cold storage). A proportion of the pooled assets is held in hot storage to meet short term transactional demand (e.g. expected trades /withdrawals in a given day). In the case of Mt. Gox, malicious actors exploited a characteristic of the Bitcoin protocol known as transaction malleability by requesting withdrawals, deceiving the exchange that the ensuing trade had failed, causing the exchange to credit the account of the attacker and repeat the withdrawal trade. The technical details are beyond the scope of this paper. It is sufficient to say that the attacker creates a new additional valid transaction by altering the signature of the original transaction, which

modifies the identifying transaction hash. If the new modified (yet valid) transaction is confirmed by the Bitcoin network, the attacker can: a) receive the coins assigned in the original withdrawal trade and b) claim that the original withdrawal trade had failed. The exchange will look for the original confirmed transaction ID in the list of confirmed trades, fail to find it, classify it as failed trade, credit the account of the client and re-effectuate the attacker's initial withdrawal request. The attacker doubles his bitcoins with every supposedly "failed" transaction. A small initial holding can be used to significantly deplete the reserve of bitcoins held by the exchange over a relatively short period of time. Mt Gox publicly recognized that it had fallen victim to a transaction malleability hack on Feb 10th, 2014. On Feb 28th it announced that it would be filing for bankruptcy.

**Negligence:** An animated debate has ensued as to the extent to which the Mt Gox hack and subsequent collapse can be ascribed to the failings of the CEO or more general institutional negligence. The argument for organizational negligence in the case of QuadrigaCX was decidedly more clear-cut. The CEO purportedly died as the sole holder of passwords that could unlock customer assets equivalent to \$145 Million [46]. As Quadriga explained in their Press Release of Feb 5, 2019:

*"[W]e have worked extensively to...locate our very significant cryptocurrency reserves held in cold wallets required to satisfy customer cryptocurrency balances... Unfortunately, these efforts have not been successful... We filed for creditor protection... Gerry took sole responsibility for the handling of funds for QuadrigaCX and as such no one other than him can access the coins in the cold wallets".*

While it is obvious that Quadriga's internal operational and governance processes were deficient, it is uncertain whether this was by design, that is, to facilitate fraud.

**Fraud:** The unregulated or lightly regulated nature of crypto exchanges obviously renders them an avenue for fraudulent activity. The largest fraud to date was a Ponzi scheme totaling \$2.9 billion. PlusToken, based in China, posed as cryptocurrency wallet, encouraging its users to place their Bitcoin or Ethereum with the platform to buy high-yielding "Plus Tokens" offering a 9-18% return on investment, with larger investments generating even higher rewards. Characteristically for

classic Ponzi schemes, these subscriptions were not invested, and the returns of earlier investors were actually paid out of the subscriptions of later investors. After accumulating significant amount of funds, the owners withdrew from the hosted PlusToken customer wallet and absconded [47].

### 5.5. Implications of the Private Key Conundrum

The continued resistance of key segments of the investing community to participation in crypto markets cannot be attributed solely to concerns about operational risk. Nevertheless, the direct or indirect private key risk to which retail and institutional investors are exposed must figure in the approximation of any risk-adjusted return estimated by a rational investor. Security events undoubtedly contribute to volatility, durable drawdowns, lack of market depth and liquidity and complications in assigning an intrinsic value Liu and Tsyvinski[1]. Cryptocurrencies are justifiably perceived as highly speculative assets with extremely unpredictable price trajectories, ineffective mediums of exchange and unreliable stores of value. For many investors, it may well be that the cost of risk incurred outweighs the expected benefits. A framework to identify, quantify and mitigate private key risk, such as that proposed in this paper, will contribute to some degree of rebalancing of the broader risk-reward tradeoff.

## 6. Data Collection Methodology

We have collected loss data from multiple sources as there is no comprehensive repository of loss data on cryptocurrencies. Media outlets are the main source of information on loss events, followed by the company(s) and/or individual(s) that experienced the loss. Academic research of loss materialization is also a key source of data, documenting the entities involved, the loss type and amount, cause, country, and tokens lost. Unfortunately, details are often obscured or omitted because of limited disclosure by the parties or incomplete reporting by sources. Non-reporting poses a significant challenge for researchers in this field. The phenomenon is of less significance for major failures of exchanges, but relevant for negligence, SIM swaps and ransomware events which

may not be substantial enough to trigger media coverage. By way of example, Ciphertrace [49] reported \$4.5 billion of losses during 2019 while our research indicates only \$3.2 billion in losses over the same time frame. The Ciphertrace 2020 study examined the on-chain flows to and from illicit wallets which suggests that there is a significant amount of unreported loss events. These unreported events are theorized by Ciphertrace to be ransomware or extortion related. For these reasons, the actual number of loss events is assumed to be significantly greater. Finally, there are examples of events that have gone unreported by exchanges who actively engage in coverups of breach events. These events were subsequently uncovered or reported after a significant delay. It is impossible to estimate with any accuracy the extent of losses where coverups have proved successful.

## 7. Loss Events: Overview & Trends

Over the eleven years since the first bitcoin was mined, both the frequency of occurrence and the magnitude in dollar terms of loss events has increased. Our research indicates 166 loss events totalling over \$7 billion in lost cryptocurrency through the first quarter 2020. Media coverage of loss events publicizing the risk of complete and irrevocable loss has brought the discussion on security issues into the public domain. We have categorized loss events into the following categories; Hacks, Negligence, and Fraud as the result of Ponzi Scheme, Exit Scam, and Ransomware/Extortion. While the loss event data seeks to be comprehensive by cataloguing all loss events, the scope of our analysis and proposals are limited to events where custodial best practices could have safeguarded cryptocurrency assets. This largely implies a concentration on losses attributable to Hacks and Negligence. Nevertheless, loss events that would not have been potentially mitigated through custodial best practices are included in the Loss Event section to highlight the magnitude of losses and to provide a comprehensive taxonomy of loss events in the cryptocurrency ecosystem. This should contribute to a greater degree of precision in the dialogue on the topic.

The first recorded loss event is described as the Stone Man Loss and occurred over twenty months

after the first Bitcoin block was mined on January 3, 2009 [50]. The pseudonymous BitcoinTalk user “Stone Cold” fell victim to the first recorded loss event at his/her own hand. On August 19th, 2010, after sending one Bitcoin to him/herself, Stone Man lost 8,999 bitcoin because the wallet was not backed-up. Although backing-up a wallet after every transaction is no longer necessary due to upgrades to the Bitcoin protocol, this example served as an early warning to cryptocurrency holders of the immutability of the blockchain. Stone Man never recovered the lost Bitcoin and it is highly likely they are locked forever. In August 2010, Bitcoin was only trading at about \$0.06 per coin so the financial loss was negligible. Stone Cold’s 8,999 bitcoin can still be found at address:

167ZWTT8n6s4ya8cGjqNNQjDwDGY31vmHg [51]  
As of May 2020, Stone Man’s lost bitcoin is worth \$81.1 million

The Stone Man incident was the first of many loss events in the ten years that followed. As of March 31, 2020, our research indicates over \$7.3 billion of losses and a total of 166 unique events. Note that nearly 40% of the total losses are due to the PlusToken Ponzi scheme detected in 2019. See below for Loss Event Count by Cause and Loss Event \$ Value by Cause for the distribution of losses over the entire period.

Figure 1: Loss Event Count by Cause

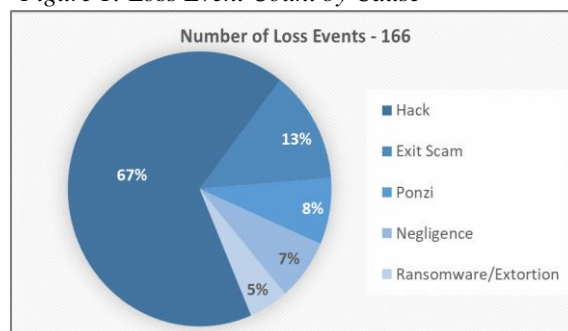
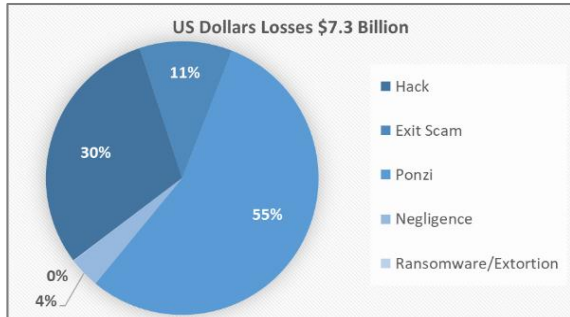
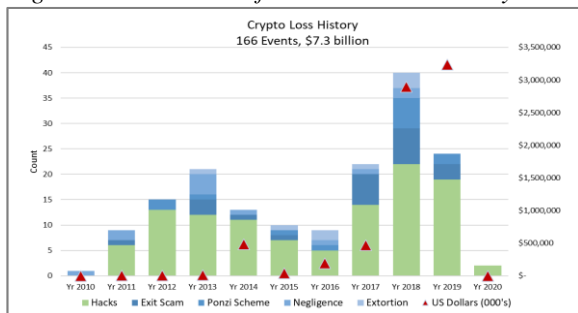


Figure 2: Loss Event Severity by Cause



Annual loss events have averaged \$1.7 billion since 2010 but are heavily weighted to the years 2017 to 2019 due to the exponential rise in cryptocurrency prices including BTC, ETH, and XRP. The average frequency of events is 16 per year or 1.4 per month, with an average dollar amount of \$44 million per event. Annual loss events have increased significantly over the past three years as compared to the prior six years. The average per year for 2017 to 2019 is 28, up from an average of 11.1 for the years 2011 to 2016. Intuition suggests that, as the value and notoriety of the asset increased in 2017, so did bad actors’ motivation to steal the asset. Focusing specifically on hacking events, the average events for the years 2017 to 2019 tripled to 18.3 from an average of 6.0 from 2011 to 2016. See Figure 3 below for the evolving distribution up of loss events.

Figure 3: Breakdown of Annual Loss Events by cause



When losses are viewed through the lens of the type of token lost or stolen, bitcoin constitutes the most in total dollars, \$1.1 billion with 83 unique events. Ether losses total \$424.9 million with 31 unique events. Unreported loss type constitutes 32% of the loss events where Other makes up 10%. The category of

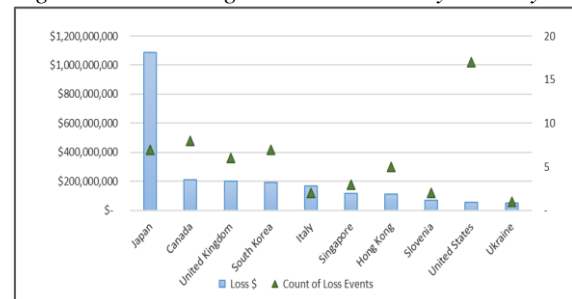
“Unreported” deserves more examination. As noted, reporting on cryptocurrency loss events is often limited regarding the type of loss. In the events where the type of loss is uncertain or undisclosed by sources, the loss type is categorized as “Unreported”. In some cases, the loss type has been described as fiat currency. In other cases, the losses have been described as “Personal Identifying Information”, or PII. In other cases, the losses have been simply described as “cryptocurrency”.

The number of bitcoins that have been stolen or lost in the 166 loss events is 2,041,714. The value of the bitcoin at the time of writing is approximately \$18 billion. The two million plus lost or stolen bitcoin accounts for 11% of the total bitcoin in circulation. Events that are within the scope of our analysis and CCC-mitigable resulted in 1.58 million lost or stolen bitcoin, or 8.7 percent of the total circulation. The same decomposition applied to Ether yields 11.3 million lost or stolen, 10.4 percent of the total circulation, and \$2.4 billion. Ether lost or stolen considered to be within the scope of CCC totals 1.3 million, 1.2 percent of the circulation, or \$1.1 billion in value at the time of the loss.

The distribution of dollar losses by country is heavily weighted to China in the amount of \$3 billion. Again, this is mainly due to the PlusToken Ponzi scheme of \$2.9 billion. The data also suggests that loss events are a global phenomenon, with at least 30 countries experiencing loss events. Average losses per event totaled \$44 million over the total 166 events.

Loss events by country that could be mitigated by custodial best practices (CCC), which excludes PlusToken, are presented is below.

Figure 4: CCC Mitigable Loss Events by Country



CCC loss events are heavily weighted by dollars to Japanese exchanges as the result of two major hacks,

Coincheck and Mt. Gox, totaling \$984 million. The remaining top 10 loss countries include Canada, the United Kingdom, and South Korea. A major outlier in the data is 17 loss events which are attributable to the United States with an average loss of \$3.4 million per event. This suggests that US loss events are a tenth of the group average of \$32.8 million, excluding the outliers Japan and US. Possible explanations are more thorough and accessible media coverage of events in the US. Of the loss events in the US, nine are related to exchanges, however, eight of these occurred in 2014 or earlier. The only other exchange loss event was in 2019 where a Kraken user's account was compromised [52]. The hacker offered the bitcoin at \$100 per coin and then filled the bid side of the transaction. The total reported lost bitcoin was 1,155.

There are 113 loss events totaling \$2.4 billion in the data set that are deemed to be events that could have been mitigated by custodial best practices (CCC). The number of events from 2010 to 2016 totaled 62 for \$579.6 million as compared to the years 2017 through the first quarter 2020 where there were 51 events and over \$1.8 billion in losses. The losses are heavily weighted toward exchanges which account for over 80 percent of the \$2.4 billion in CCC losses, and 79 of the 113 events.

Earlier, we examined one instance of loss that could have been mitigated through CCC in the Stone Man loss. While the value of the loss is much greater in today's dollars, the loss at the time was only \$544. The top ten loss events that could have been mitigated by custodial best practices range in amounts from \$50 million to \$534 million. All but one of the losses were the result of hacks. The one instance of negligence in the top 10 is the QuadrigaCX exchange failure.

The Japanese based Coincheck tops the list with a hack and loss of 523 million NEM tokens valued at a \$1 per token [53]. In January 2017, a hacker was able to breach the Coincheck system and access all on the private keys in their hot wallet. Coincheck committed the cardinal sin of cryptocurrency CCC by keeping all the crypto assets in a hot wallet. The mistake was compounded by the company not utilizing multi-sig technology. The tokens were not recovered. One could argue that the Coincheck loss was due to a combination of theft and negligence. Coincheck continues to operate as of the first quarter 2020.

The second largest, and arguably most well-known CCC failure, is Mt. Gox. The Mt. Gox failure was examined in the preceding section but notably, this was not the first time Mt. Gox was hacked. In June 2011, Mt. Gox lost 2,643 bitcoin worth \$47,123 when the administrator's credentials were compromised which caused a flash crash due to the hacker selling bitcoin for \$0.01 [54]. Mt. Gox tried to improve security after the hack by implementing solutions such as cold storage [55]. The intrigue and magnitude of the Mt. Gox story gives it the dubious honor of being both the first and most notorious cryptocurrency exchange hacked.

Hacking and negligence events in the short history of cryptocurrency have been numerous, sizeable and media worthy. Hackers have proven to be increasingly motivated and skilled, as the value of cryptocurrency and the rewards for bad actors have grown. Recently, hackers have used Google advertisements to redirect asset holders to replicated websites to gather their wallet service credentials [56]. Hackers have gained access to the cloud servers used to host cryptocurrency exchanges as a means of infiltration [57]. However, crypto holders continue to exhibit basic carelessness and negligence with reported coin losses occurring due to accidentally throwing away a hard drive prompting an attempted futile recovery attempt by sifting through landfills. Our examination of loss events supports the assertion that operational risk can be mitigated through robust custodial best practices and the application of existing technology informed by an understanding of risk indicators and loss distribution.

## 8. Risk Quantification

Based on the loss event data, we estimate the loss distribution by modelling the probability and magnitude of potential losses in the industry. To this end, we employed the Loss Distribution Approach (LDA), which convolutes the loss frequency distribution with the loss severity distribution to model an objective distribution of aggregate losses due to operational risk. While the LDA is a favored tool of large financial entities for the determination of capital adequacy for operational risk, we believe it is also eminently suitable for our objective of the

quantification of custodial risk in the cryptocurrency universe.

We focused on loss events due to hacking and negligence in this section as they are two major causes of losses and can be mitigated via prudent risk management measures. For example, exit scams and Ponzi schemes are out of the control of exchanges and custodians. Our analysis is based on loss event data over 39 quarters, from the third quarter of 2010 to the first quarter of 2020). There were 109 loss events, totaling \$2.4 billion for about 10 years. Loss events occurred on average 2.79 times every quarter, with an average loss size per event of roughly \$22 million. The number of loss events is usually 2 times or below per quarter (60% probability). However, there are several quarters in which the number of loss events is greater than 7 times (10% probability). Based on the shape of the distribution, we decided to use a Poisson mass function to describe the expected loss frequency, which is commonly used in LDA Models. We expect that each loss event will largely be independent. The size of losses tends to be below \$10 million in most of the times (70% probability); however, large losses of over \$100 million occasionally occurs (5% probability). A lognormal distribution of expected loss severity was selected to capture this characteristic.

We use the empirical data to parametrize the probability density functions of the expected loss frequency and expected loss severity of loss events. We estimate a Poisson frequency which is described by the single parameter  $\lambda$ , the expected frequency, using the mean of the empirical loss frequency distribution, 2.79. We assume a lognormal distribution for loss severity, which is described by the log mean and log variance. Under the standard assumption that frequency and severity are independent, Monte Carlo simulation is used to generate the total loss distribution as the convolution of the frequency and severity distribution.

The shape of the distribution is extremely skewed to the right and close to a lognormal distribution. Based on the simulated total annual loss distribution, we can state with an 80% confidence level that losses will be roughly \$75 million over a single quarter. However, a total loss could reach approximately \$200 million (10% probability) and \$450 million in extreme cases (5% probability).

Figure 5: Poisson Distribution - Loss Events

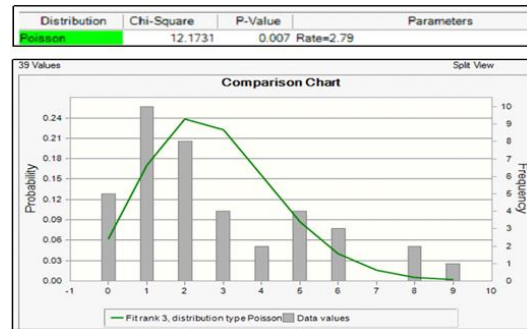


Figure 6: Lognormal Distribution – Loss Severity

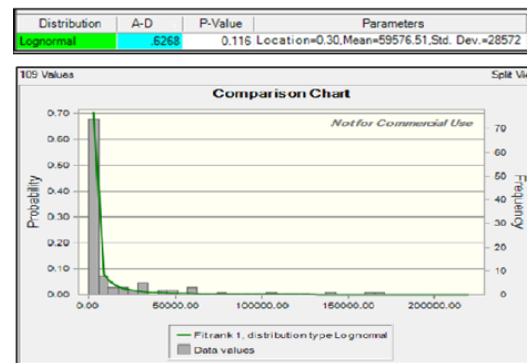
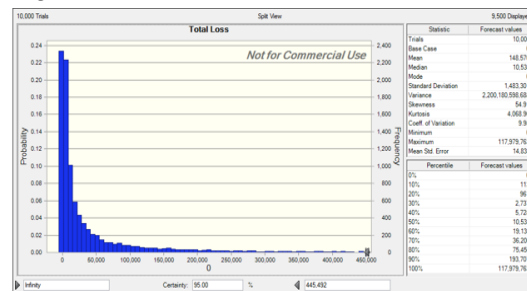


Figure 7: Simulated Loss Distribution – LDA



The model output requires careful interpretation. As shown in the chart above, the frequency of reported loss events increased for the last two to three years albeit with some recent decline. The larger amount of losses in 2018 and 2019 also reflects the higher prices of cryptocurrencies. Since 2016, the number and the size of non-BTC losses have increased significantly. Given rapid changes in the market dynamics, data in



earlier quarters may not be a good predictor of potential losses in the future.

Accordingly, we examined how the historic horizon of the sample data could affect the results. We analyzed two additional data periods, covering more recent periods: 2013 1Q – 2020 1Q and 2016 1Q – 2020 1Q. The original base case covered the last 10 years from 2010 3Q to 2020 1Q, while the new cases focus on the last 7 years and 4 years, respectively. Given the size of the samples (especially the number of the quarters), this analysis certainly has limitations. However, it does show the sensitivity of simulation results to the time horizon of the historic data.

The study examined potential quarterly losses in the industry, based on these three cases at various percentiles. At the 50th percentile, potential total quarterly losses in these three cases are estimated to be \$11 million, \$23 million, and \$52 million, respectively. At the 90th percentile, potential losses can reach about \$300 million and \$500 million in the two additional cases, vs. about \$200 million in the original case. At the 95th percentile, the potential losses can roughly range between \$500 million and \$1 billion. To provide some context, the largest quarterly loss was about \$800 million in the first quarter of 2018 when Coincheck was hacked (\$534 million), as discussed in the previous section.

We also conducted a separate analysis for bitcoin or BTC and found that the size of potential losses is much smaller. This could indicate the vulnerability of new coins, or poor risk management of less established exchanges. Typically, assets managed in hot wallets were hacked. We also excluded price impacts by using the price as of 3Q 2010. As would be expected, constant price losses are smaller.

It is noted that this loss distribution analysis has several limitations, including sampling bias, sample size, potential regime changes, the impact of outliers, and distribution assumptions. Thus, we do not intend to argue that this analysis has strong predictive power. This is rather a first step for more sophisticated research in the future. We believe that this kind of loss event analysis is essential to quantify the magnitude of risk exposure and consider risk mitigation measures, including capital reserve and insurance. Industry efforts to create a loss or near-miss event database will considerably help mitigate and price this emerging risk.

## 9. Risk Mitigation

It should be clear that cryptocurrency users remain highly vulnerable to total and irrevocable losses whether opting for self-custody or delegated custody solutions. This section begins by discussing optimal auto-custodial security practices before progressing to formulate a stylized best practice framework for (centralized, custodial) exchanges and custodians, which the asset holder would do well to bear in mind when selecting and utilizing such services. Our intention is to provide a toolkit to users which they can use to interrogate the robustness of the measures in place to safeguard their assets

### 9.1. CCC: Self-Custody and Wallet Security Hygiene

(1) **Local Storage.** *Description:* Key pairs stored in file held in device's local storage. Wallet file on a networked device is accessed by reference Bitcoin client software. *Risks:* Theft of Device / Physical Damage to Hardware / Loss of Device / Deletion of Wallet File / Corruption of File / Digital theft by malware. *Risk Mitigation:* At the very least, these wallets should be encrypted using high entropy passwords. Credential-stealing malware means private key remain extremely vulnerable to digital theft despite encryption. Risk of loss through loss/deletion/corruption of file can be mitigated with frequent automated backups, with copies of the file held on at least two different devices situated in different physical locations. Best practice would generally dictate that local storage of the wallet on a network-connected device should be avoided. In any case, the amount of funds held in this type of hot wallet should be limited to that required to meet transactional demand over a short time horizon. The remainder of the time the keys should be held offline in cold storage.

(2) **Brain Wallet.** *Description:* A memorized input which hashes to the private key meaning that no file need be stored in digital or physical format. *Risks:* Loss of memorized input due to death, injury or forgetfulness of key holder. *Risk Mitigation:* High entropy passphrases should be used. The passphrase should also be stored physically and securely in case of necessity. Ideally the password should be randomly generated by an offline device.

(3) **Paper Wallet.** *Description:* A key pair that has been committed to paper. *Risks:* Theft by visual capture or manual transcription of private key. Physical degradation or destruction. *Risk Mitigation:* High entropy passphrases should be used. Multiple copies should be held in different locations. Paper wallet should be generated without network connectivity. Paper on which keys are written should be protected against destruction due to oxygen, water and UV light. Avoid exposure to photographic/video devices.

(4) **Hardware Wallet.** *Description:* A separate electronic device stores the private key offline and receives unsigned transactions. The transaction is signed and exported to another device with network connectivity for submission to a cryptocurrency network. Hardware wallets are considered to be the gold standard for retail investors' protection of private keys. *Risks:* Hardware wallets depend on the security of the random number generator used to generate your wallet's private keys securely. User remains vulnerable to backdoor methods to access the key or modify transactional detail (Man in The Middle Attack). The connection of an offline device to a compromised online device means data remains vulnerable. *Risk Mitigation:* Hardware and software should be open source, allowing a user to validate the entire operation of the device. Hardware wallet solutions such as Ledger's Nano S and Trezor's One are best in class solutions.

## 9.2. CCC: Self-Custody with Split Control with Dynamic Threshold Access Structures

To mitigate the risk of irrevocable and total loss of assets, one proposed approach to key management is multi-sig transactions, which employ a  $k$ -of- $n$  multi-signature script, specifying  $n$  public keys and  $k$  valid signatures from these  $n$  keys in order for crypto tokens to be redeemed. A similar idea allows funds to be stored under a single public key but shares of this key can be divided among  $n$  parties using threshold cryptography. The parameters  $k$  and  $n$  remain private in this instance. However, the attempt to mitigate the security issue by split key control gives rise to another risk, termed “*access-control paralysis*”, where the cryptoasset cannot be spent by keyholders because of the failure to achieve the requisite number of digital

signatures, due to the unavailability or incapacitation of one or more private keys. The prospect of access-control paralysis has ensured that split key control has not proven to be the hoped-for panacea for private key security issues. Zhang et al [37] suggest that the novel concept of a “Paralysis Proof System” might offer a solution to the paralysis issue. If one or more parties in a static ( $k$ ,  $n$ )-threshold access structures is unable to sign transactions, the described paralysis scenario results. If the other parties provide a proof of paralysis, due to the unavailability of players or key shares, the threshold access structure is dynamically updated. This so-called *Dynamic Access Structure System* (DASS) can be achieved without a trusted third party by pre-establishing the conditions under which Paralysis is supposed to exist, and automatically updating the threshold access structure, e.g. from  $k$ -of- $n$  to  $(k-1)$ -of- $(n-1)$ , when these conditions are satisfied. The challenge is ensuring that the updating of access structures only occurs in the event of true player unavailability. The risk is that players can cheat by simulating the unavailability of a player. The authors therefore recognize the need for robust “Paralysis Proof”. One such proof is the following, described in the context of Bitcoin and  $k$ -of- $n$  threshold access structures, where  $k=n=3$ :

(1) 2 of the three shares,  $pk_1$  and  $pk_2$  claim  $pk_3$  is unavailable to sign transactions. They emit a challenge to which  $pk_3$  must respond with a *life signal* to demonstrate availability. The absence of a life signal within a predetermined period of time constitutes paralysis proof.

(2) Funds (of, for example, 5000 BTC) , held at an  $Address_A$ , are spendable either with the digital signatures of  $pk_1$  and  $pk_2$  and  $pk_3$  or by an application,  $pk_{smart}$ , which can sign transactions when presented with proof of paralysis.

(3)  $pk_{smart}$  receives the request from  $pk_1$  and  $pk_2$  to change the access structures from 3-of-3 to 2-of-2 and challenges  $pk_3$  to emit a life signal.

(4) This is achieved by  $pk_{smart}$  sending a negligible amount of bitcoin to an address,  $Address_{Test}$ , where it spendable either by  $pk_3$  at any point within a pre-defined time period or, failing that, by  $pk_{smart}$  after the time period has elapsed.

(5) The failure of  $pk_3$  to spend the negligible bitcoin amount equates to a failure to emit a life signal and constitutes proof of paralysis.

(6)  $pk_{\text{smart}}$ , now presented with proof of paralysis, can spend the 5000 BTC held at  $Address_A$  and will send them now to a new address,  $Address_B$ , where the funds are spendable with the two digital signatures of  $pk_1$  and  $pk_2$ .

(7)  $pk_{\text{smart}}$  will also send the negligible bitcoin amount used in the test to this new address.

(8) The access structure is changed from 3-of-3 to 2-of-2.

The implementation of DASS is challenging with the Bitcoin script-based system, however Zhang et al propose an off-chain solution, which utilizes Intel Software Guard Extensions (SGX), a CPU-based Trusted Execution Environment (TEE) implementation. Ethereum naturally lends itself to an on-chain solution through by specifying a smart contract stored and executed on the blockchain.

### 9.3. CCC: Delegated Custody Solutions: Lines of Defense

Should users seek to outsource the task of key management in pursuit of enhanced usability and security, they should consider the available public evidence that the custodian has mounted adequate first (pre-loss) and second (post-loss) lines of defense to safeguard client assets. As users become more informed and demanding and as the sector matures, custodians could be expected to compete on issues related to the care, custody and control of client assets. It is our hope that this and similar frameworks will contribute to a more efficient market, whereby custodians are rewarded with inflows for the implementation of the outlined basic tenets of sound and transparent risk management and penalized with outflows when they exhibit deficient and opaque policies processes and protocols.

### 9.4. Delegated Custody Solutions: First Line of Defense

(1) **Audited Proof of Solvency.** Proof of Solvency demonstrates that “an exchange controls sufficient reserves to settle each customer’s account” [33]. The process therefore requires a proof of liabilities and a proof of reserves in order to prove that reserves are equal to or greater than liabilities. These proofs are becoming increasingly standardized. Proof of

Reserves entails “determining which balances in the blockchain the exchange has access to and calculating the sum of those balances. The exchange can prove control of a Bitcoin address by providing the public key belonging to that Bitcoin address and signing transactions with the associated private key [with a pre-determined amount and target address]”. Maxwell [58] proposed a method for proving the liability of an exchange using the Merkle tree approach. Each leaf is made up of the cryptographic (SHA-256) hash of a client’s identifying data and the account balance (i.e. the exchange’s obligation). Each internal node is formed by summing the balance of its two children and concatenating the hashes of the children and then hashing the concatenation. The root node will contain the sum of all balances (the total liability) together with the root hash formed by the hashes of all nodes in the tree. The tree cannot be subsequently modified without altering the root hash. The auditor will verify all nodes were summed and hashed correctly. They publish and monitor the root hash and the root sum to ensure no balances are changed and no users are added or removed. Finally, users will be presented with the path from their leaf to the root node. Importantly, the user must verify that their identifying information hashes to the same value in the leaf node, verify that all the hashes from their leaf node up to the root node are correct and verify that the hash of the root node matches the one published by the auditor. If sufficient users perform this verification procedure, it can be concluded that the published liabilities are valid. By proving that reserves are equal to or greater than liabilities, the exchange proves solvency. See Appendix to view the described Merkle Tree and an example path from leaf node to root node used by client for verification purposes. In addition, the custodian should undergo an annual external audit by a reputable accounting firm.

(2) **Custodian Security Hygiene.** The strictest of authentication protocols should be imposed on clients, 2 factor (or more) authentication should be mandatory at least one of the factors must be extremely secure such as “iris recognition, fingerprint recognition, one-time password (token) and one-time password (software)” [59]. Group IB contends in its 2018 report that the success rate of attacks on users is attributable to a “disregard for information security and an underestimation of the capabilities of cybercriminals”

and observes “The first and main cause is that both users and exchanges omit to use two-factor authentication. The second cause is disregard for basic security rules such as the use of complex and unique passwords”. The custodian should have a dedicated specialized team in charge of cybersecurity and ensure that staff are well educated on cyber-attacks. An appropriate internal control function should be assigned to the safekeeping of assets, such as a security officer. Internal audit should also be performed to ensure all the control are properly executed.

In terms of effective exposure management, exchanges should formulate and refine models to predict transactional demand in order to minimize online storage of coin inventory and maximize the funds controlled by private keys held in cold storage or an air gapped hardware security module (HSMs). Limits and triggers on the percentage of assets held in hot storage should be set, with monitoring measures in place to ensure limits are adhered to.

**(3) SOC 2 Type II certification.** Currently held by Gemini, Coinbase Custody, BitGo, and Bakkt, the System and Operation Control (SOC) 2 Type II examination demonstrates that “an independent audit firm has examined an organization’s control objectives and activities and tested those controls to ensure that they are operating effectively” over a specified period of time. The SOC 2 reviews the custodian’s Policies, Communications, Procedures and Monitoring to evaluate the adherence to “Trust Service Principles” relating to:

*(i) Security.* The system has controls in place to protect against unauthorized access (both physical and logical);

*(ii) Availability.* The system is available for operation and use as committed or agreed;

*(iii) Processing Integrity.* System processing is complete, accurate, timely and authorized;

*(iv) Confidentiality.* Information that is designated as “confidential” by a user is protected; and

*(v) Privacy.* Personal information is collected, used, retained and disclosed in accordance with the operation’s privacy notice and principles set by the AICPA and the CICA”. [60]

**(4) Multi-signature capability with protection against custodian paralysis.** Zhang et al. extend their discussion of Paralysis Proofs to envisage a “digital asset custodian” who engages in “Denial-of-Service

(DoS)...[by failing to] respond to a user’s transaction requests” meaning “the user effectively loses her funds”. The definition of paralysis is refined in that the custodian may be “available” but “exhibits paralysis by failing to process certain legitimate transaction requests”. Supposing a user stores her funds in a (3, 3)-paralysis-proof-multisig wallet and one of the keys is held by the custodian who is responsible for authenticating the user (e.g. via 2FA) before authorizing a transaction. The custodian is eliminated from the access structure if the users emit a successful challenge to the Denial of Service, offering evidence of its illegitimacy by furnishing valid authentication information, which equates to proof of Paralysis.

#### 9.5. Delegated Custody Solutions: Second Line of Defense

The second line of defense aims to provide a safety net to cryptocurrency holders. It owes much to the financial safeguards and capital requirements, summarized as the 4 R’s, now in place for Central Clearing Parties (CCP). Ensuring *Resilience* would require Custodial Exchanges’ to ring-fence the excess capital needed to withstand significant stress events such as cyberattack or fraud and maintain continuity of operations. Stress testing similar to CCAR should be performed based on a prescribed set of market shocks. Our section on LDA could offer insight as to how capital adequacy might be assessed. Any residual losses in excess of the default fund would be distributed pro-rata among exchange members which will be compensated with some form of equity-like instruments, such as a convertible bond, which would allow exchange members to participate in an exchange’s *Recovery* after the stress event. If the combination of the Default Fund and exchange members capital were insufficient to absorb losses, we would expect the custodial exchange to be placed into *Resolution*. Resolution authorities must have the flexibility to commence resolution proceedings while the exchanges are still a going concern. Early Resolution and *Recapitalization* gives exchange members much higher likelihood of a return to profitability and some degree of recuperation of losses through the described equity-like instruments.

Insurance can also provide a backstop to provide liquidity to custodians, so they do not become

insolvent during crisis. It is important to ensure no “wrong-way-risk” from the insurers such that their performance is not correlated to custodian performance because of their own exposure to the crypto asset. There are several types of insurance policies that are available to mitigate crypto exchange and custody risks. Such insurance could help to protect investors up to a certain amount from losses incurred by the custodian as a result of hacking attempts. Insurance types include:

- **Crime insurance** covers the loss of money, securities, and other assets due to the criminal activities of employees or third parties (e.g. theft and fraud).
- **Cyber insurance** is focused more on financial costs arising from security breaches, including the third-party liability due to the loss of customer data. The latter is a relatively new area in the insurance industry, and it is expected to increase rapidly
- **Digital Asset Insurance** is to cover the loss of digital assets in cold or hot storage due to the theft and misuse of private keys. This insurance policy can be combined with crime and cyber insurance or offered independently, depending on insurance companies. The coverage of products is being expanded to hot storage (vs. cold storage) or retail investors (vs. exchanges and custodians).
- **D&O and E&O liability insurances** are also offered to crypto exchanges and custodians to protect companies, directors, officers, or employees against legal liabilities, arising from lawsuits or regulatory actions, or errors and omissions.
- Crypto exchanges and custodians hold not only digital assets but also cash for investors at banks. The US dollar deposits held at insured banks can be covered by the **Federal Deposit Insurance Corporation (FDIC) deposit insurance**

The insurance companies could even securitize the insurance premiums with catastrophe bonds. If the issuer suffered a loss exceeding a threshold, the excess loss would be funded from a reduction in principal on the CAT bond. A custodian CAT bond would need to find investors that are not already substantially exposed to cryptocurrency. With the increasing interest from both institutional and retail investors, a CAT bond could be an attractive investment for them and source of protection for the exchanges.

## 10. CCC: Retrospective Application of Best Practices

The process of compilation, classification and analysis of custodial risk undertaken for this paper should disabuse the reader of the notion that the prescribed best practices represent a panacea. Moreover, the efficacy of certain risk mitigation measures always seems self-evident in retrospect. Nevertheless, the industry’s failure to learn from its errors means that it is condemned to repeat them. Reviewing perhaps the most notorious loss event in the last 10 years, the failure of Mt Gox, we can state that a recurrent Proof of Solvency test would have detected a widening breach between exchange reserves and the clients' claims on those reserves. The CEO of the failed exchange (wrongly) blamed a failure in the Bitcoin protocol which enabled the transaction malleability attack [34]. Yet even if that were true, the incorporation of this simple best practice would have provided informed clients transparency that exchange liabilities exceeded exchange assets and they could have responded rationally with mass withdrawals. Alternatively, the exchange could have taken swifter action to address the vulnerabilities in its cybersecurity defence mechanisms before the attack proved terminal. The failure of QuadrigaCX is equally instructive. Multi-signature paralysis proof would have protected asset holders by showing that the CEO was an unresponsive key shareholder resulting in his elimination from the threshold access structures. In addition, a SOC 2 certification from a reputable auditor would have been nearly impossible given the single point of failure.

Ultimately, the rigorous application of best practices will depend on rational market participants channelling funds to where they perceive them to be the safest. This will provide the profit incentive to invest in, and boast of, a robust risk management framework. We anticipate that evidence of implementation of the described best practices, significantly conditioned by crypto's short, often painful history, will eventually be considered a basic prerequisite.

## 11. Concluding remarks and suggestions for future research

In this paper, we examined the risks associated with the safeguarding of cryptocurrency for retail and institutional users of the assets. The Care, Custody, and Control of cryptocurrency provides unique challenges because of two main attributes of blockchain: the digital signature scheme and immutability of the transaction record. The peculiar attributes of blockchain leads us to the Private Key Conundrum. The degree of protection of the private key against from theft and negligence is inversely related to the usability of the asset. Finding a point of functional equilibrium, affording both acceptable usability and value protection, is crucial to the efficacy of cryptocurrency. Contrary to principles of decentralization and “trustlessness” upon which Bitcoin and other cryptocurrencies are founded, most holders address the PKC by delegating control of their private keys to a trusted-third party.

We have identified the operational risks and described how events materialize. In documenting this materialization, we have created a comprehensive database of loss events and classified the data based on its defining attributes. The data, while limited to 10 years of history, was subjected to the Loss Distribution Approach (LDA) as a novel way to quantify expected aggregate losses, based on loss frequency and severity distributions.

We have documented a best practice framework that market participants should employ when holding the private keys or when ceding private keys to a trusted third-party. Chief among these are the first line of defense including proof of solvency, an optimal mix of hot and cold storage, robust internal controls over IT infrastructure, multi-signature technology with protection against custodian paralysis, and two-factor authentication. The second line of defense protects asset holders after losses and should include a verifiably adequate capital structure and a verifiable casualty insurance.

Our research leads to many paths of suggested additional work. As time goes on, application of LDA with additional data points will be possible and is recommended. We infer from the data that loss events for a particular coin such as BTC decrease over time. Are there variables with predictive power, such as coin

vintage, token traits or exchange characteristics which could augment existing academic and industry explanatory studies of losses? While beyond the scope of our research, the extent to which the regulatory and legal framework is informed by, and impacting on, CCC best practices merits further exploration.

## References

- [1] Liu., (2018). Risks and Returns of Cryptocurrency <https://economics.yale.edu/sites/default/files/files/Faculty/Tsyvinski/cryptoreturns%208-7-2018.pdf>.
- [2] Narayanan, A., and Clark, J., “Bitcoin’s Academic Pedigree”. 2017. [https://link.springer.com/chapter/10.1007/978-1-4613-9323-8\\_24](https://link.springer.com/chapter/10.1007/978-1-4613-9323-8_24).
- [3] Bayer, D., Haber, S. and Stornetta, W. S. “Improving the efficiency and reliability of digital time-stamping”. 1991. [https://link.springer.com/chapter/10.1007/978-1-4613-9323-8\\_24](https://link.springer.com/chapter/10.1007/978-1-4613-9323-8_24).
- [4] Haber, S. and Stornetta, W. S. “How to timestamp a digital document”. 1991. [https://link.springer.com/chapter/10.1007/3-540-38424-3\\_32](https://link.springer.com/chapter/10.1007/3-540-38424-3_32).
- [5] Haber, S., Stornetta, W. S. Secure names for bit-strings. 1997. <http://dl.acm.org/citation.cfm?id=266430>.
- [6] Merkle, R. C. “Protocols for public key cryptosystems”. 1980. <http://www.merkle.com/papers/Protocols.pdf>.
- [7] Dwork, C., Naor, M. “Pricing via processing or combatting junk mail”. 1992. <https://dl.acm.org/citation.cfm?id=705669>.
- [8] Back, A. “A partial hash collision based postage scheme”. 1997. <http://www.hashcash.org/papers/announce.txt>.
- [9] Back, A. “Hashcash—a denial of service counter measure”. 2002. <http://www.hashcash.org/papers/hashcash.pdf>.
- [10] Dai, W. 1998; <http://www.weidai.com/bmoney.txt>.
- [11] Szabo, N. “Bit gold. Unenumerated”. 2005. <https://unenumerated.blogspot.com/2005/12/bit-gold.html>.
- [12] Nakamoto, S. “Bitcoin: a peer-to-peer electronic cash system”. 2008. <https://bitcoin.org/bitcoin.pdf>.
- [13] Lamport, L., et al. “The Byzantine Generals Problem”. 1982. <https://dl.acm.org/citation.cfm?id=357176>.
- [14] Jerry Brito, Andrea Castillo. “Bitcoin: A Primer for Policymakers”. 2013. [https://www.researchgate.net/publication/269707314\\_Bitcoin\\_A\\_Primer\\_for\\_Policymakers](https://www.researchgate.net/publication/269707314_Bitcoin_A_Primer_for_Policymakers)
- [15] François Velde. “Bitcoin: A Primer”. Chicago Fed Letter. 2013. <https://www.chicagofed.org/publications/chicago-fed-letter/2013/december-317>
- [16] Björn Segendorf. “What is Bitcoin?”. Riksbank Economic Review. 2014. [https://www.researchgate.net/publication/285087430\\_What\\_is\\_bitcoin](https://www.researchgate.net/publication/285087430_What_is_bitcoin)
- [17] Reuben Grinberg. “Bitcoin: An Innovative Alternative Digital Currency”. Hastings Science & Technology Law Journal. 2011.


- [https://www.researchgate.net/publication/228199328\\_Bitcoin\\_An\\_Innovative\\_Alternative\\_Digital\\_Currency](https://www.researchgate.net/publication/228199328_Bitcoin_An_Innovative_Alternative_Digital_Currency)
- [18] Pedro Franco. "Understanding Bitcoin: Cryptography, Engineering, and Economics". 2015.
- [19] Andreas M. Antonopoulos. "Mastering Bitcoin". 2014.
- [20] Narayanan, Bonneau, Felten, Miller, Goldfeder. "Bitcoin and Cryptocurrency Technologies". 2016
- [21] Hanna Halaburda; Miklos Sarvary. "Bitcoin: The Economics of Digital Currencies". 2015.
- [22] Niaz Chowdhury. "Inside Blockchain, Bitcoin, and Cryptocurrencies" 2019.
- [23] Imran Bashir. "Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained". 2019.
- [24] Michel Rauchs, Apolline Blandin, Kristina Klein, Gina Pieters, Martino Recanatini, Bryan Zhang. "2nd Global Cryptoasset Benchmarking Study" 2018. [https://www.jbs.cam.ac.uk/fileadmin/user\\_upload/research/centres/alternative-finance/downloads/2018-12-ccaf-2nd-global-cryptoasset-benchmarking.pdf](https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-12-ccaf-2nd-global-cryptoasset-benchmarking.pdf)
- [25] Katharina Krombholz, Aljoshia Judmayer, Matthias Gusenbauer, and Edgar Weippl. "The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy" 2016. [http://fc16.ifca.ai/preproceedings/33\\_Krombholz.pdf](http://fc16.ifca.ai/preproceedings/33_Krombholz.pdf)
- [26] Mauro Conti, Sandeep Kumar, Chhagan Lal, Sushmita Ruj. "A Survey on Security and Privacy Issues of Bitcoin" 2017. <https://arxiv.org/pdf/1706.00916.pdf>
- [27] Shayan Eskandari, David Barrera, Elizabeth Stobert, and Jeremy Clark. "A First Look at the Usability of Bitcoin Key Management" 2018. <https://arxiv.org/pdf/1802.04351.pdf>
- [28] Pat Litke and Joe Stewart. "Cryptocurrency-Stealing Malware Landscape" 2014. <https://www.secureworks.com/research/cryptocurrency-stealing-malware-landscape>
- [29] Amir Feder, Neil Gandal, JT Hamrick, Tyler Moore. "The Impact of DDoS and Other Security Shocks on Bitcoin Currency Exchanges: Evidence from Mt. Gox" 2014. [https://www.researchgate.net/publication/322840689\\_The\\_impact\\_of\\_DDoS\\_and\\_other\\_security\\_shocks\\_on\\_Bitcoin\\_currency\\_exchanges\\_Evidence\\_from\\_Mt\\_Gox](https://www.researchgate.net/publication/322840689_The_impact_of_DDoS_and_other_security_shocks_on_Bitcoin_currency_exchanges_Evidence_from_Mt_Gox)
- [30] Marie Vasek, Micah Thornton, Tyler Moore. "Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem" 2014. [https://fc14.ifca.ai/bitcoin/papers/bitcoin14\\_submission\\_17.pdf](https://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_17.pdf)
- [31] Tyler Moore and Nicolas Christin. "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk" 2013. [https://www.researchgate.net/publication/286267694\\_Beware\\_the\\_Middleman\\_Empirical\\_Analysis\\_of\\_Bitcoin-Exchange\\_Risk](https://www.researchgate.net/publication/286267694_Beware_the_Middleman_Empirical_Analysis_of_Bitcoin-Exchange_Risk)
- [32] Tyler Moore and Nicolas Christin. "Revisiting the Risks of Bitcoin Currency Exchange Closure" 2018. <https://dl.acm.org/doi/10.1145/3155808>
- [33] Gaby G. Dagher, Benedikt Bünz, Joseph Bonneau, Jeremy Clark, Dan Boneh. "Provisions: Privacy-preserving proofs of solvency for bitcoin exchanges" 2015. <https://nyuscholars.nyu.edu/en/publications/provisions-privacy-preserving-proofs-of-solvency-for-bitcoin-exch>
- [34] Christian Decker. "BlueWallet: The Secure Bitcoin Wallet" 2014. [https://www.researchgate.net/publication/278010213\\_BlueWallet\\_The\\_Secure\\_Bitcoin\\_Wallet](https://www.researchgate.net/publication/278010213_BlueWallet_The_Secure_Bitcoin_Wallet)
- [35] Rosario Gennaro, Steven Goldfeder, Arvind Narayanan "Threshold-Optimal DSA/ECDSA Signatures and an Application to Bitcoin Wallet Security" 2016. [https://www.researchgate.net/publication/303860501\\_Threshold-Optimal\\_DSAECDSA\\_Signatures\\_and\\_an\\_Application\\_to\\_Bitcoin\\_Wallet\\_Security](https://www.researchgate.net/publication/303860501_Threshold-Optimal_DSAECDSA_Signatures_and_an_Application_to_Bitcoin_Wallet_Security)
- [36] Shamir, A. "How to share a secret" 1979. <https://dl.acm.org/doi/10.1145/359168.359176>
- [37] Fan Zhang, Philip Daian, Iddo Bentov, Ari Juels. "Paralysis Proofs: Safe Access-Structure Updates for Cryptocurrencies and More" 2018. <https://www.initec3.org/files/pp.pdf>
- [38] Moore, G. (2019). Custody: Crypto Assets' Unique Challenge and Opportunity. CoinDesk. <https://downloads.coindesk.com/crypto-investing/custody-report.pdf>
- [39] Gemini Trust Company, LLC (2019). A Guide to Crypto Custody. Gemini. <https://gemini.com/static/documents/guide-to-crypto-custody.pdf>
- [40] Anchor Labs and BlockTower Advisors LP. (Sep 2019). Institutional Digital Asset Custody. Anchorage. <https://medium.com/anchorage/institutional-digital-asset-custody-a-guide-for-crypto-investors-17c8eb3e12f>
- [41] Global Digital Finance. (Apr 2019). Crypto Asset Safekeeping and Custody: Key Considerations and Takeaways. Global Digital Finance. [https://www.gdf.io/wp-content/uploads/2019/02/2\\_2\\_2019-Crypto-Asset-Safekeeping-draft-for-mini-summit.pdf](https://www.gdf.io/wp-content/uploads/2019/02/2_2_2019-Crypto-Asset-Safekeeping-draft-for-mini-summit.pdf)
- [42] Zhang, F., Daian, P., Bentov, I., Miers, I., Juels, A. (2018). Paralysis Proofs: Secure Dynamic Access Structures for Cryptocurrency Custody and More. In ACM Conference on Advances in Financial Technologies, 2018. <https://eprint.iacr.org/2018/096.pdf>
- [43] Baris, J. (2020). Blockchain & Cryptocurrency Regulation 2020: The Custody of Digital Assets. Global Legal Insights. <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/06-the-custody-of-digital-assets-2020>
- [44] Schaefer, C. (Sep 2019). Applying the SEC Custody Rule to Cryptocurrency Hedge Fund Managers. California Law Review, 107(4), 1381-[vi]. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3461029](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3461029)
- [45] SEC (2018). Digital Asset Transactions: When Howey Met Gary (Plastic). Remarks at the Yahoo Finance All Markets Summit: Crypto by William Hinman, Director, Division of Corporation Finance, SEC on June 14, 2018. Retrieved from <https://www.sec.gov/news/speech/speech-hinman-061418>
- [46] SEC (2019). Framework for "Investment Contract" Analysis of Digital Assets. Retrieved from <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets>

- [47] CipherTrace Cryptocurrency Alexander, D. (Feb 2019). Technology: Crypto CEO dies Holding Only Password that can unlock Millions in Customer Coins. Bloomberg. <https://www.bloomberg.com/news/articles/2019-02-04/crypto-exchange-founder-dies-leaves-behind-200-million-problem>
- [48] Bryanov, K. (Dec 2019). PlusToken Effect: Alleged Asian Exit Scam to Blame for Market Decline? Cointelegraph. <https://cointelegraph.com/news/plustoken-effect-alleged-asian-exit-scam-to-blame-for-market-decline>
- [49] Intelligence (Feb 2020). Q4 2019 Cryptocurrency Anti-Money Laundering Report. CipherTrace.
- [50] Bitcointalk.org. Bitcoin Forum: Bitcoin: Bitcoin Discussion: List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses. Retrieved May 22, 2020. [https://bitcointalk.org/index.php?topic=576337#post\\_toc\\_18](https://bitcointalk.org/index.php?topic=576337#post_toc_18)
- [51] Sedgwick, K. (Apr 2019). Bitcoin History Part 11: The First Major Loss of Coins: Featured Bitcoin News. Bitcoin News. Bitcoin.com <https://news.bitcoin.com/bitcoin-history-part-11-the-first-major-loss-of-coins/>
- [52] Spilotro, Tony. (Jun 2019). Bitcoin Price 99% Flash Crash May Have Been Work of Clever Crypto Hacker NewsBTC. [www.newsbtc.com/2019/06/03/bitcoin-price-99-flash-crash-may-have-been-work-of-clever-crypto-hacker/](http://www.newsbtc.com/2019/06/03/bitcoin-price-99-flash-crash-may-have-been-work-of-clever-crypto-hacker/)
- [53] Bloomberg. (Jan 2018). How Hackers Stole \$500 Million in Digital Currency. Fortune.com <https://fortune.com/2018/01/31/coincheck-hack-how/>
- [54] Sedgwick, K. (Aug 2019). Bitcoin History Part 16: The First Mt. Gox Hack. Bitcoin.com. <https://news.bitcoin.com/bitcoin-history-part-16-the-first-mt-gox-hack/>
- [55] Roy, L. (Oct 2019). Mt Gox Hack Explained: Full History & Information Guide. TotalCrypto. <https://totalcrypto.io/mt-gox/>
- [56] Newsbtc (Mar 2018). CoinHoarder Steals Over \$50M in Crypto Using Google Ads. NewsBTC. [www.newsbtc.com/2018/02/15/hackers-coinhoarder-steal-more-than-50-million-in-cryptocurrencies-using-google-ads/](http://www.newsbtc.com/2018/02/15/hackers-coinhoarder-steal-more-than-50-million-in-cryptocurrencies-using-google-ads/)
- [57] Dotson, KYT (Jan 2014). Linode Breach Leads to Massive Heist of 46,000 BTC from Bitcoinica, Faucet. SiliconANGLE. <https://siliconangle.com/2012/03/02/linode-breach-leads-to-massive-heist-of-46000-btc-from-bitcoinica-faucet/>
- [58] Z. Wilcox. Proving Your Bitcoin Reserves. <https://bitcointalk.org/index.php?topic=595180.0>
- [59] Braam, T.B., (2019). A Security Assessment Model for Crypto Asset Safekeeping. <https://dspace.library.uu.nl/handle/1874/393359>
- [60] Monahan, G. (2014), What SOC 2 Type II Certification Means, Law Technology Today, <https://www.lawtechnologytoday.org/2014/07/soc-2-type-ii-certification-means/>



## Appendices

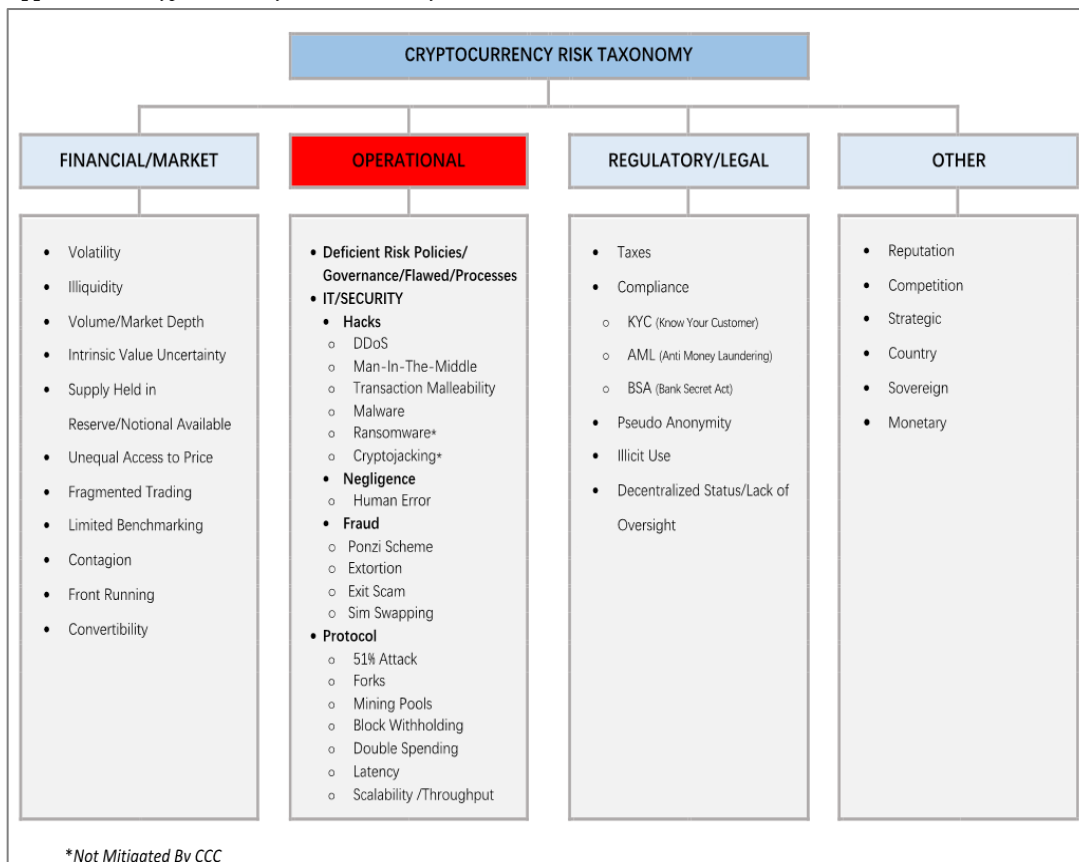
### Appendix 1: University of Cambridge Benchmarking Study

Respondents scored these categories on a 1-5 scale:  
 1: Completely disagree 2: Disagree 3: Neutral 4: Somewhat agree 5: Completely agree  
 Lowest average score  Highest average score

		IT Security	Fraud	AML/KYC Enforcement	Regulatory Burden	Risks Competition	Negative Publicity	Bank Relationship	Entering Bank Relationship	Lack of Talent
Large	2018	4.20	3.83	3.40	3.84	3.29	3.52	3.54	3.63	3.83
	2017	3.17	2.08	2.75	3.50	2.58	2.75	2.67	2.67	2.33
Small	2018	3.81	3.48	3.17	3.78	3.21	3.30	3.48	3.69	3.48
	2017	3.93	3.50	2.64	2.89	3.00	2.93	3.79	3.79	2.52

Source: 2nd Global Cryptoasset Benchmarking Study (2018).  
 Centre for Alternative Finance, University of Cambridge

### Appendix 2: Cryptocurrency Risk Taxonomy

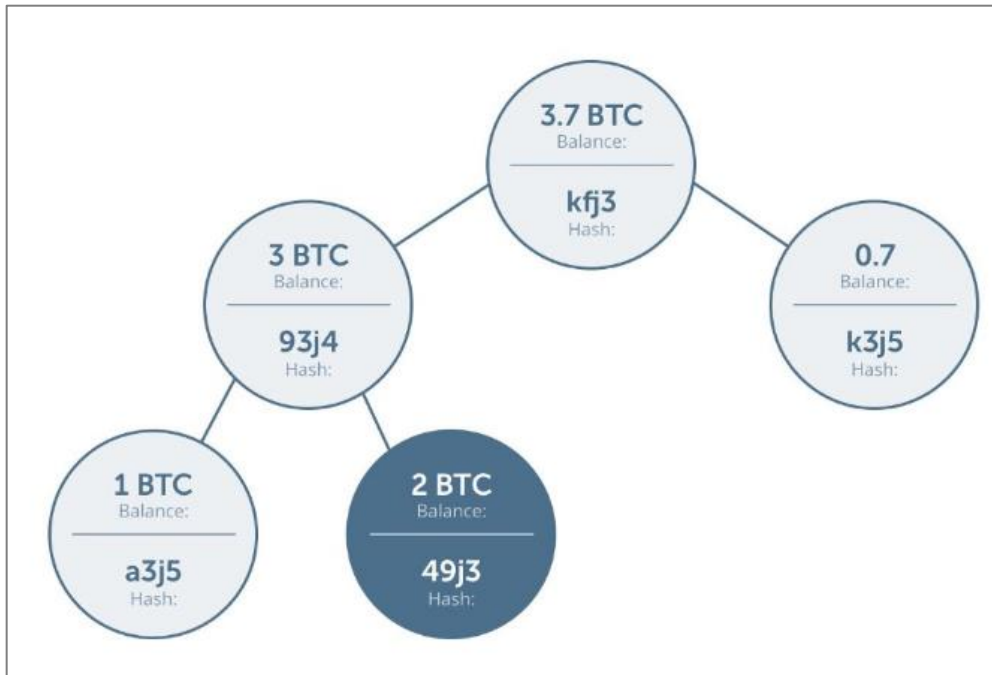


**Appendix 3: CCC-Mitigable Top 10 Loss Events**

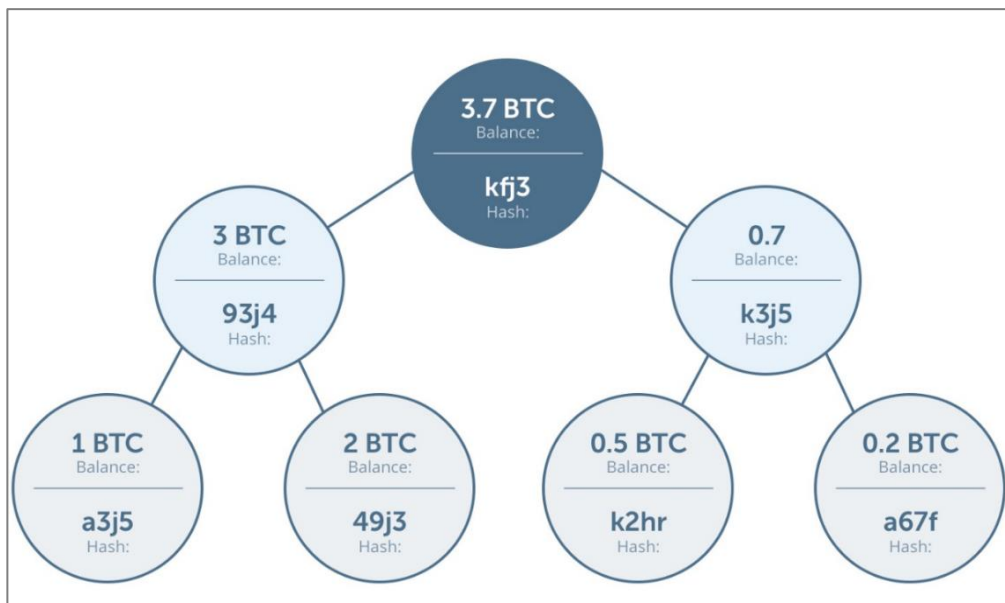
Event	Date	\$Losses	Type of Loss	Location	Source
Coincheck	January-18	\$534,000,000	523,000,000 NEM	Japan	<a href="http://www.cointelegraph.com/news/report-record-breaking-coincheck-hack-perpetrated-by-virus-tied-to-russian-hackers">www.cointelegraph.com/news/report-record-breaking-coincheck-hack-perpetrated-by-virus-tied-to-russian-hackers</a>
Mt Gox	February-14	\$450,000,000	850,000 BTC	Japan	<a href="http://www.coindesk.com/mt-gox-the-history-of-a-failed-bitcoin-exchange">www.coindesk.com/mt-gox-the-history-of-a-failed-bitcoin-exchange</a>
BitGrail	February-18	\$170,000,000	17,000,000 NANO	Italy	<a href="http://www.bitcoinist.com/bitgrail-cryptocurrency-exchange-hacked-170-million-nano-allegedly-stolen/">www.bitcoinist.com/bitgrail-cryptocurrency-exchange-hacked-170-million-nano-allegedly-stolen/</a>
Parity Wallet	November-17	\$160,000,000	513,774 ETH	United Kingdom	<a href="http://www.parity.io/parity-technologies-multi-sig-wallet-issue-update/">www.parity.io/parity-technologies-multi-sig-wallet-issue-update/</a>
QuadrigaCX	December-18	\$140,000,000	26,350 BTC	Canada	<a href="http://www.coindesk.com/quadrigacx-explainer">www.coindesk.com/quadrigacx-explainer</a>
CoinBene	March-19	\$105,000,000	ERC-20 Tokens	Singapore	<a href="http://www.cointelegraph.com/news/most-significant-hacks-of-2019-new-record-of-twelve-in-one-year">www.cointelegraph.com/news/most-significant-hacks-of-2019-new-record-of-twelve-in-one-year</a>
Bitfinex	August-16	\$77,000,000	120,000 BTC	Hong Kong	<a href="http://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know">www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know</a>
NiceHash	December-17	\$62,000,000	4,736 BTC	Slovenia	<a href="http://www.coindesk.com/62-million-gone-cryptocurrency-mining-market-nicehash-hacked">www.coindesk.com/62-million-gone-cryptocurrency-mining-market-nicehash-hacked</a>
Zaif	September-18	\$60,000,000	5,966 BTC	Japan	<a href="http://www.selfkey.org/list-of-cryptocurrency-exchange-hacks/">www.selfkey.org/list-of-cryptocurrency-exchange-hacks/</a>
Coinhoarder/ Blockchain.info	February-18	\$50,000,000	Unknown	Ukraine/Luxembourg	<a href="http://www.newsbtc.com/2018/02/15/hackers-coinhoarder-steal-more-than-50-million-in-cryptocurrencies-using-google-ads/">www.newsbtc.com/2018/02/15/hackers-coinhoarder-steal-more-than-50-million-in-cryptocurrencies-using-google-ads/</a>

**Appendix 4: Proof of Liabilities-The Merkle Tree Approach**

**i) Merkle Tree for Proof of Liabilities**

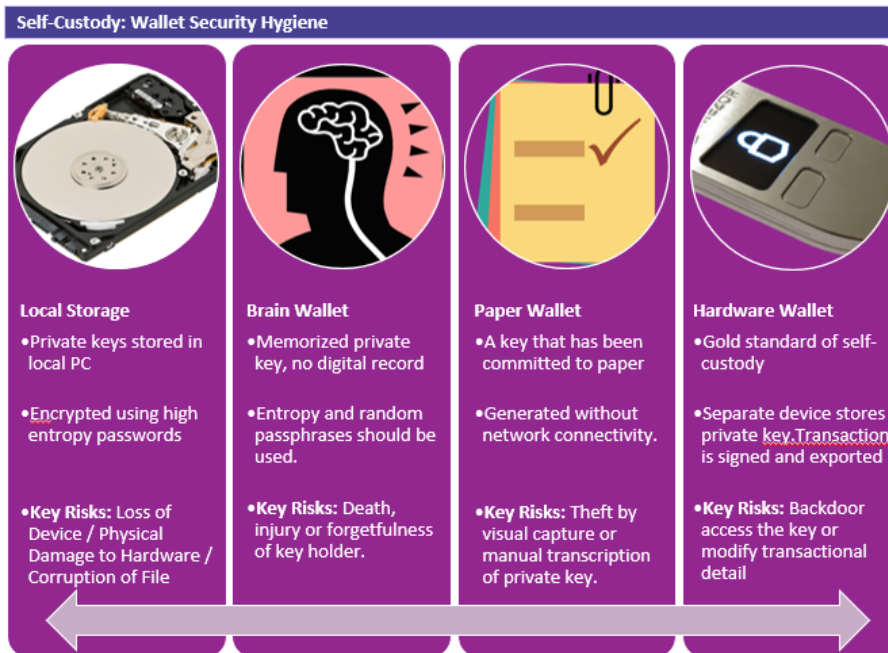


**ii) Partial Path from Leaf to Root**



### Appendix 5: Best Practices: Self-Custody

#### (i) Self-Custody: Wallet Security Hygiene



#### (ii) Self-Custody: Split Control with Dynamic Threshold Access Structure

- **Multi-sig Transactions:** Funds to be stored under a single private key but share this key and divided among n parties using threshold cryptography
- Split key control gives rise to “access-control paralysis”, where the cryptoasset cannot be spent by keyholders because of the failure to achieve the requisite number of digital signatures
- **Dynamic Access Structure System (DASS)**, can be achieved without a trusted third party by pre-establishing the conditions under which Paralysis is supposed to exist, and automatically updating the threshold access structure. Zhang et al (2019)
- The risk is that players can cheat by simulating the unavailability of a player. The authors therefore recognize the need for robust “Paralysis Proof”.
- The implementation of DASS is challenging with the Bitcoin script-based system. Off-chain solution was provided which utilizes Intel Software Guard Extensions (SGX).
- Ethereum naturally lends itself to an on-chain solution through by specifying a smart contract stored and executed on the blockchain

**Appendix 6: Best Practices: Delegated Custody Solution**

