Michigan Business & Entrepreneurial Law Review

Volume 6 | Issue 2

2017

# Bitcoin's Growing Pains: Intermediation and the Need for an Effective Loss Allocation Mechanism

Andrew Kang
*University of Michigan Law School*



https://doi.org/10.36639/mbelr.6.2.bitcoins

# BITCOIN'S GROWING PAINS: INTERMEDIATION AND THE NEED FOR AN EFFECTIVE LOSS ALLOCATION MECHANISM

*Andrew Kang**



* J.D., University of Michigan Law School, 2017. B.A. Cornell University, 2010. Special thanks to Professor J.J. White for his thoughtful feedback and the members of Michigan Business & Entrepreneurial Law Review for their helpful comments.

## INTRODUCTION

Traditional non-cash payment systems are built around a complex system of financial intermediaries. In these systems, payments require both the payer and payee to have deposit accounts with an intermediary (such as a bank). The movement of money from the payer to the payee involves a process called settlement[1] that results in the payment amount being debited from the payer's balance and that same amount being credited to the payee's balance. On an operational level, settlement requires intermediaries to communicate with each other to adjust the balances of their internal ledgers and decide on a set of rules and procedures that dictate when payments are final and how disputes will be resolved. In essence, traditional payment systems require users to trust third party intermediaries to manage a complex, centralized settlement process.[2]

It was in this context that Bitcoin, a revolutionary new consumer payment system[3] based on disintermediation, was invented. Bitcoin sought to exclude banks and other financial intermediaries from the settlement pro-

1. Settlement, the conceptual engine that drives all payments, is "an act that discharges obligations . . . between two or more parties." COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS, *A Glossary of Terms Used in Payments and Settlement Systems*, BANK FOR INTERNATIONAL SETTLEMENTS, 45, (Mar. 2003) http://www.bis.org/cpmi/glossary_030301.pdf. The fundamental purpose of all payment systems, regardless of the method, is to facilitate settlement between parties. Indeed, the historical development of payment instruments and systems can be traced to innovations in the conceptual, operational, and legal frameworks that allowed settlement to become more efficient, secure, and/or accessible over time. In early payment methods like gold or cash, settlement was achieved through the physical transfer of money from the payer to the payee. Ina cash transaction, for example, the payer's payment obligation to the payee is discharged upon the payee's physical possession of the currency. The problems involved in moving large amounts of physical money, however, spurred the development of a new conceptual model of settlement through deposit banking. In this model, obligations between parties could be settled by adjusting the parties' bank deposit balances, rather than requiring the physical movement of money. From this conceptual framework flowed operational and legal innovation that allowed such deposit-oriented payment instruments and systems to evolve from the humble paper check to electronic funds transfers (e.g. ACH, Fedwire), payment cards, and modern peer-to-peer applications (e.g. PayPal, Venmo).

2. *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG, 1 (2008), https://bitcoin.org/bitcoin.pdf.

3. Bitcoin has another important use that its creator did not anticipate—an alternative investment vehicle. As bitcoin prices continue to rise, bitcoin has become an alternative asset class. While the rise of bitcoin as a new investment vehicle raises many important issues, they are beyond the scope of this paper as it focuses only on Bitcoin's use as a consumer payment system.

cess.[4] Bitcoin's founder envisioned a new paradigm of decentralized settlement in which transactions were settled collectively by the users themselves on a publicly distributed ledger, rather than unilaterally by intermediaries on their own private ledgers. Instead of having a deposit account with an intermediary, a Bitcoin user could create and manage her own "personal wallet." This wallet would serve as her own personal bitcoin "bank" through which she can create her own accounts to receive and send bitcoins. Bitcoin's founder reasoned that, by excluding intermediaries, Bitcoin would function purely as a peer-to-peer digital analogue of physical cash and would obviate the need to deal with tricky loss allocation or dispute mediation issues involving intermediaries. Ultimately, this exclusion would lower transaction costs for all of the users on the Bitcoin network.[5]

An interesting development, however, has occurred over the past few years. As Bitcoin started to witness an explosive growth in mainstream and casual adoption, more and more users—consumers and merchants alike—moved away from personal wallets and have begun using "hosted wallet services" provided by third-party intermediaries. Through these hosted wallet services, intermediaries manage their users' bitcoin wallets and facilitate transactions on their behalf. These services appeal to new and mainstream users because the services greatly lower the learning curve for using Bitcoin and reduce the time and energy involved in conducting routine transactions with bitcoin. These intermediaries not only streamlined the Bitcoin experience, but also fundamentally altered both the underlying transaction mechanics and the way risk of loss is spread throughout the participants of the system.

This paper examines a phenomenon largely overlooked in existing literature: as Bitcoin matures into a mainstream consumer payments system with the rise of intermediation and hosted wallet services, it is slowly transforming from a purely decentralized peer-to-peer currency into something that (ironically) more closely resembles the bank-intermediated payment systems of the past. This paper explains how this transformation creates complicated issues of loss allocation not anticipated by Bitcoin's founder. Further, it argues for the need of an effective legal mechanism to efficiently and fairly allocate losses between intermediaries and users. The first section of this paper will explain how Bitcoin transactions work when users manage their own personal wallets, describing both the transaction mechanics and risks of loss. Then, it will explain how hosted wallet services have changed these mechanics and risks, as well as why a set of loss allocation rules is necessary. Finally, the paper will recommend a set of loss allocation rules based on the policy rationales that drive rules under other existing payment systems law.

---

4. Nakamoto, *supra* note 3.

5. *Id*.

## I. Bitcoin's Beginnings: Personal Wallets And Purely Peer-To-Peer Transactions

Bitcoin was created by Satoshi Nakamoto to offer the first digital analogue of physical cash that truly did not require the involvement of any intermediaries.[6] As such, Nakamoto envisioned that each user could create and manage her own personal wallet, as well as conduct transactions using Bitcoin's decentralized settlement process. This section will explain the mechanics of transactions conducted with personal wallets—that is, without the presence of any intermediaries.

### A. *Transaction Mechanics*

In most of the legal scholarship devoted to Bitcoin, it is common for authors to engage in a cursory discussion about how bitcoin transactions generally work before addressing the legal issues. Such an approach will not work here. A deeper understanding of the specific nuts and bolts of bitcoin transactions is necessary to engage in a meaningful discussion about the risks of loss and how they should be allocated. To do so without resorting to overly abstract or technical language, the following subsections will walk the reader through the experiences of a fictional new Bitcoin user, Adam, who decides to create a personal wallet, buy bitcoins from a broker (also sometimes called simply a seller) named Beth, and use those bitcoins to purchase a product from Charlie.

#### 1. Getting Started: Adam Creates A Personal Wallet

When Adam decides he wants to start using Bitcoin, he creates a "personal wallet," or a digital file that essentially serves as Adam's own personal Bitcoin bank. This file is either stored on his own computer offline (a "cold" wallet) or online (a "hot" wallet). Adam uses this wallet to generate *addresses*, or the destinations to which bitcoins can be sent. Addresses are akin to bank accounts. Just as banks can create a number of different accounts, Adam's wallet can create a number of different addresses to receive bitcoin. For this example, suppose that Adam decides to create an address for the bitcoins he is about to buy from Beth. To do so, he does the following:

1. Adam starts by generating a "private key," which is a random string of numbers and characters only he knows (here, it is "ADAMKEY1").
2. Adam then uses ADAMKEY1 to generate the address, which is essentially another string of numbers and characters (here, "ADAMADDRESS1").

As will be illustrated later, the private key and the address are inherently linked together. Only someone who holds the private key corresponding with a particular address can access the bitcoins in that address. In a way, the private key is like the pin number to a bank account.

6. *See generally id.*

2. Buying Bitcoin With Dollars: Adam Buys Bitcoin From Broker, Beth

In order to start conducting bitcoin transactions, Adam needs to first buy some bitcoins with US dollars. He finds a seller, Beth, who agrees to sell him 100 bitcoins for $100. Adam provides Beth the address, ADAMADDRESS1, which he generated with ADAMKEY1 earlier. Beth must now go online and run the Bitcoin software to initiate a transaction—a set of instructions transmitted throughout the Bitcoin network for the purpose of sending 100 bitcoins to ADAMADDRESS1. The word "send," however, is misleading, as Beth does not actually send Adam anything. Rather, she reassigns to Adam a set of 100 bitcoins she received in a previously confirmed transaction or sets of transactions,[7] as will be explained shortly.

a. *Transaction initiation and transmission by Beth*

The transaction (or set of instructions) that Beth initiates will have a unique transaction ID—in this case, "BETHADAMTRANSACTION"—and consists of an input, a digital signature, and an output.

1. Input:

   For the input, Beth will reference the ID of a previously confirmed transaction in which someone else had routed 100 bitcoins to an address of her own. Here, imagine that in the previous month her friend Joe sent her 100 bitcoins to an address named "BETHADDRESS" in a transaction known as "JOEBETHTRANSACTION." Beth will use JOEBETHTRANSACTION as the input in her transaction with Adam.[8] In plain English, Beth is telling the network, "Here is an address where you will find 100 bitcoins received from a previous transaction."

2. Digital signature:

   With her input, Beth includes a digital signature (call it "BETHSIG") that she generates with the same private key that generated BETHADDRESS to prove she is the owner of that address. In plain English, Beth is saying, "I own the address I just referenced in the input, and so, I own these 100 bitcoins."

3. Output:

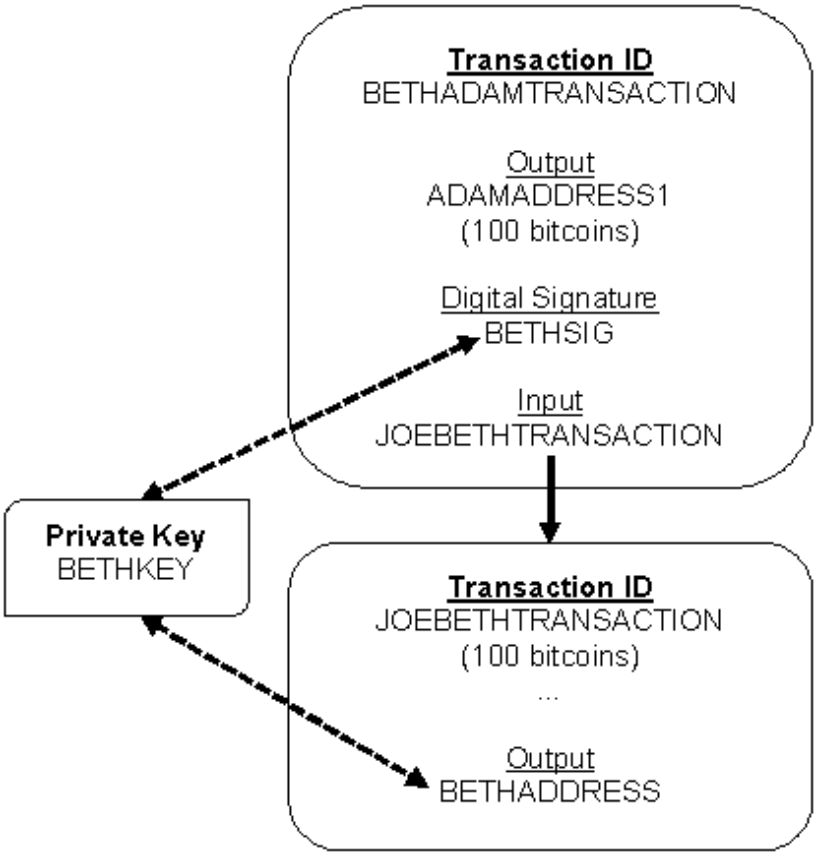
   For her output, Beth will use Adam's address, ADAMADDRESS. She will also specify an amount to be transferred, here, the full

7. Jeff Preshing, *What Is a Bitcoin, Really?*, PRESHING ON PROGRAMMING (Jan. 27, 2014), http://preshing.com/20140127/what-is-a-bitcoin-really/.

8. Note that it is not always this simple. There may be no previous transaction with the exact amount that Beth might be looking for. In that case, she would need to include multiple inputs referencing different previous transactions that add up to the correct amount. For example, she might include as her inputs one transaction in which one of her addresses was sent 20 bitcoins, as well as another transaction in which another one of her addresses was sent 80 bitcoins.

> amount of 100 bitcoins. In plain English, Beth is telling the network, "I would like to send all of those 100 bitcoins, I just referenced, to Adam's address."

After Beth initiates BETHADAMTRANSACTION with the input, output, and digital signature, she transmits the transaction to the Bitcoin network online for validation. The following diagram illustrates the mechanics of the transaction.




b. *Transaction validation by a miner*

After being transmitted through the network by Beth, the transaction, known as BETHADAMTRANSACTION, must be "validated." Validation involves a two-step process conducted voluntarily by a user in the Bitcoin network known as a "miner." Any user can be a miner and can connect to the Bitcoin network like a telephone operator, using her computer to listen for transaction requests across the entire network.[9] Validation involves a two-step process:

9. Peter Van Valkenburgh, *What Is Bitcoin Mining, and Why Is it Necessary?*, COIN CENTER (December 15, 2014), https://coincenter.org/entry/what-is-bitcoin-mining-and-why-is-it-necessary.

1. First, the miner checks the authenticity of Beth's digital signature, BETHSIG, to ensure that BETHADDRESS belongs to Beth and that she was the intended beneficiary in JOEBETHTRANSACTION. Simply put, BETHSIG will only be authentic if a specific mathematical equation is satisfied by BETHADDRESS, JOEBETHTRANSACTION and BETHSIG.[10] The miner uses her computer's processing power to solve these equations and verify BETHSIG.
2. Second, the miner checks to make sure that the 100 bitcoins from the previous transaction Beth is referencing have not already been spent. The miner does this authentication by examining the public blockchain ledger[11] and making sure that JOEBETHTRANSACTION has not already been used as an input in another confirmed transaction (if it has, then those particular 100 bitcoins have already been "spent").[12]

Once these two steps have been completed and the miner deems the transaction valid, the miner then proposes that BETHADAMTRANSACTION should be published as a new entry, or a "transaction block," in the public blockchain ledger. In a way, miners play the role of bank tellers: inspecting checks, making sure all the appropriate signatures and account numbers are there, checking the customer's ID, and looking for proof that the customer has enough cash-on-hand to fund the transaction.[13]

### c. *Confirmation of validation by the entire network*

Of course, to stop there and publish/finalize the transaction upon a single miner's determination that it is valid would leave the opportunity for miners to fraudulently publish blocks. For example, a fraudster can initiate a fraudulent transaction and simply rush to mine and validate such transaction herself. To prevent fraud, Nakamoto designed Bitcoin so that a miner's proposed validated block will only become part of the chain when it is confirmed by a majority of the miners in the network.

A miner's block will only be confirmed and become a part of the chain when a majority of the miners agree: (1) the transactions listed by the miner are valid (in other words, no signatures from impersonators and no double spending occurred) and (2) the miner correctly guessed a special number that solves a particular math problem.[14] Miners perform this check by looking at the proposed block's particular digital signature. This signature is a computer-generated product of three inputs: (1) the signature of the predecessor block, (2) a list of valid transactions from that predecessor, and (3) a particular random number.[15]

---

10. Preshing, *supra* note 8.

11. The "blockchain" is a shared public ledger on which the entire Bitcoin network relies. All confirmed transactions are included in the block chain. *See* BITCOIN.ORG, *How Does Bitcoin Work?*, https://bitcoin.org/en/how-it-works.

12. Valkenburgh, *supra* note 10.

13. *Id.*

14. *Id.*

15. *Id.*

All of these activities require a substantial amount of computer processing power and electricity, so why would anyone volunteer to become a miner? The answer is that any miner who confirms a transaction and publishes a new block on the blockchain ledger is rewarded with bitcoins.[16] In fact, the Bitcoin protocol gives this miner permission to reward herself brand new bitcoins.[17] Additionally, she may also receive voluntary transaction fees from the initiator of the transaction (from the initiator's point of view, these fees will incentivize more miners to confirm the transaction and conduct settlement more quickly).[18]

### 3. Adam's First Commercial Transaction With Bitcoin: Buying A Product From Charlie

With the 100 new bitcoins he just bought from Beth, Adam is ready to conduct his first commercial transaction: buying a product from Charlie. Charlie quotes a price of 50 bitcoins for his product, and provides Adam with his own address, "CHARLIEADDRESS".

#### a. *Transaction initiation and transmission by Adam*

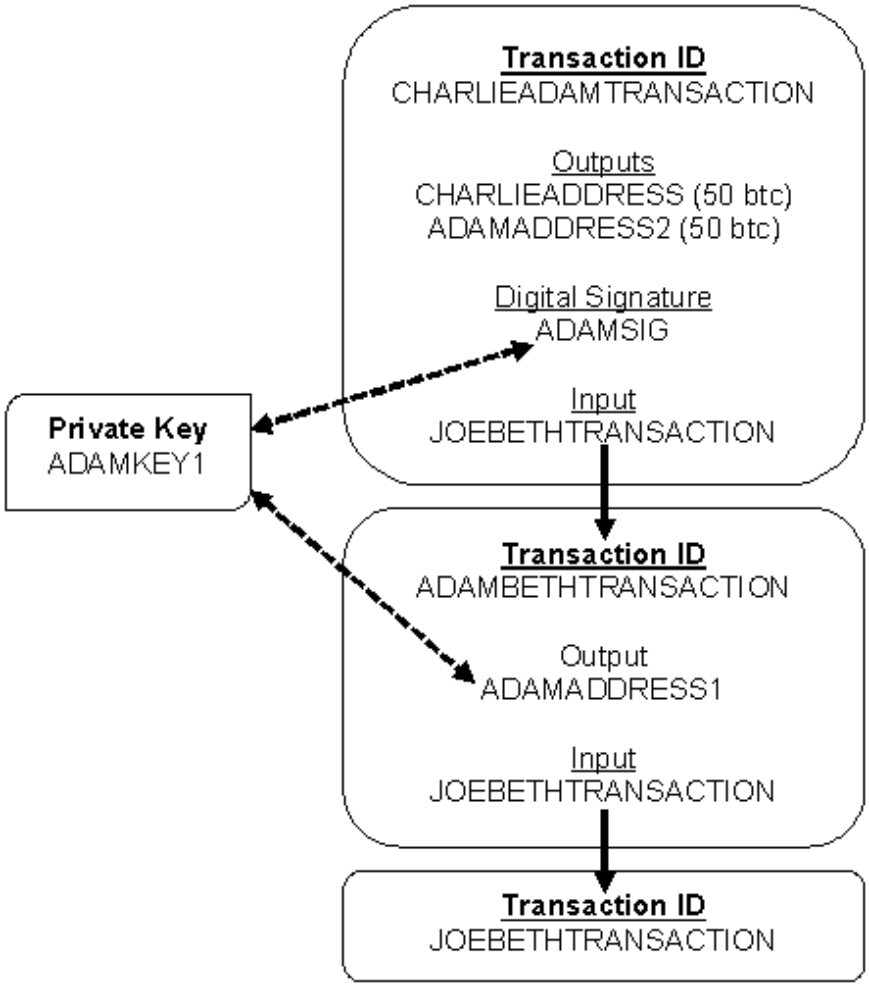
Adam initiates another transaction for his purchase of Charlie's product, known as ADAMCHARLIETRANSACTION, with the following:

1. Input:
   For the input, Adam references BETHADAMTRANSACTION and the underlying address, ADAMADDRESS1. Here, Adam is essentially telling the network, "Here is an address where you will find 100 bitcoins received from a previous transaction."
2. Digital signature:
   With his input, Adam includes a digital signature (here, ADAMSIG) that he generates with ADAMKEY1. Here, Adam is saying, "I own the address I just referenced, and so, I own these 100 bitcoins."
3. Output:
   Here, Adam runs into a slight issue. The transaction he references in the input was for 100 bitcoins, but the product he is buying only costs 50 bitcoins—he needs change! To do this, Adam simply uses his wallet to create another private key to generate another address, ADAMADDRESS2, which he will use to send himself back 50 bitcoins in change for the product. Thus, in the transaction Adam will have two outputs, CHARLIEADDRESS for an amount of 50 bitcoins, and ADAMADDRESS2 in the amount of 50 bitcoins. Here, Adam is saying, "From the 100 bitcoins I just referenced, I would like to send 50 bitcoins to Charlie's address and 50 bitcoins to one of my own addresses."

After Adam initiates BETHADAMTRANSACTION with the input, outputs, and digital signature, he transmits it to the Bitcoin network online for confirmation. The following diagram illustrates the transaction mechanics.

---

16. *Id.*
17. *Id.*
18. *Id.*




b. *Transaction validation and update of the blockchain ledger by miners*

As in ADAMBETHTRANSACTION, after being transmitted through the network by Adam, the transaction known as ADAMCHARLIE-TRANSACTION must be confirmed for it to be published on the blockchain ledger and for final settlement between Adam and Charlie to occur. A miner or group of miners confirm the following:

1. First, the miner(s) checks the validity of ADAMSIG to ensure that Adam owned ADAMADDRESS1 and to ensure that Adam was the intended beneficiary in BETHADAMTRANSACTION.
2. Second, the miner(s) checks to make sure the 100 bitcoins in BETHADAMTRANSACTION, referenced by Adam, have not already been spent. The miner(s) complete this check by examining the public blockchain ledger and making sure BETHADAMTRANSACTION has not already been used as an input in another confirmed transaction.

Once these two steps have been completed, the miner publishes ADAMCHARLIETRANSACTION as a new "block" on the public blockchain ledger, and settlement between Adam and Charlie is complete. Charlie can now spend the bitcoins by creating a new transaction using ADAMCHARLIETRANSACTION as the input, and so on.

### B. *Losses From Purely Peer-To-Peer Transactions*

With transactions conducted with personal wallets, losses can occur through a number of different scenarios as described below.

#### 1. Risks Of Loss

##### a. *User's misplacement of private keys*

A user will lose a set of bitcoins if she misplaces the private key corresponding to the address holding such bitcoins. As described in the previous section, a transaction must be signed with the right digital signature in order to be deemed valid and to eventually get published in the blockchain. Once a user loses the private key, she can no longer spend the bitcoins because she loses her ability to generate the right digital signature with which to sign transactions. Indeed, as long as nobody finds the private key, these bitcoins are probably lost forever. To use the previous example, if Adam lost or forgot that the key to ADAMADDRESS1 is ADAMKEY1, he will forever lose the 100 bitcoins he received in BETHADAMTRANSACTION because he will no longer be able to correctly sign any transaction using BETHADAMTRANSACTION as the input.

##### b. *Unauthorized transactions resulting from the theft of user's private keys*

Another possible way for a user to lose bitcoins is if a thief steals the private key associated with the address where those bitcoins are held. The thief can do this a number of ways depending on whether a wallet is a cold or hot wallet and on the types of security procedures the user employs to protect her wallet. If a user's wallet exists offline as a file on her computer, the thief can steal the private key by stealing the entire computer itself or seeing the key and recording it while the user is unaware. If the user's wallet exists online, the thief can employ a variety of hacking methods to access her key. In any case, once the thief controls the private key, she can sign any number of unauthorized transactions to spend the bitcoins held in the address or she can transfer the bitcoins to an address of her own. To use the previous example, suppose a thief, Tom, stole Adam's computer and found the contents of his wallet, including ADAMKEY. Tom can now sign any number of unauthorized transactions with the digital signature generated by ADAMKEY, including sending the bitcoins to his own address or spending them.

c. *"Double push" transaction by a fraudulent payer (rare)*

Although extremely rare, a fraudulent payer can trick the payee into providing a product or service for free by conducting a fraudulent "double push" transaction. In a "double push" transaction, the fraudulent payer initiates and transmits two transactions simultaneously using the same input bitcoins: one legitimate transaction where the output is the payee's address and another fraudulent transaction where the output is another address owned by the payer.[19] For the fraudulent transaction, the payer includes an extremely high transaction fee to incentivize miners to validate the fraudulent transaction more quickly than the, legitimate transaction.[20] Thus, the legitimate transaction may be validated, but will eventually fail to be confirmed because the fraudulent transaction will be confirmed and published first.[21] If the payee chooses not to wait for the legitimate transaction to be confirmed, she will provide the product or service before she realizes that she did not actually get paid.[22] By the time she realizes her mistake, the fraudulent payer is nowhere in sight, having availed herself of the payee's product or service for free.

To use the previous example, suppose Adam wishes to defraud Charlie. Adam initiates two transactions simultaneously—the legitimate transaction in which he pays Charlie, ADAMCHARLIETRANSACTION, and an additional fraudulent transaction, ADAMFRAUDTRANS, in which he uses one of his own addresses as the output to send the money back to himself. For ADAMFRAUDTRANS, Adam includes an extremely large transaction fee so that miners will verify it quickly. He then shows Charlie that the transaction is verified and convinces him not to wait for confirmation (in fact, many merchants choose not to wait for confirmation since it can take hours and slow down the pace of business). If Charlie decides not to wait for confirmation before giving Adam the product, Adam's fraudulent transaction will eventually be confirmed, and Charlie will have received nothing for his product.

d. *"Double pull" transaction by a fraudulent payee (rare)*

Finally, a fraudulent payee can trick the payer into paying twice by conducting a "double pull" transaction. In a double pull transaction, the payee intercepts the payer's transaction and slightly modifies the transaction's data structure so that the inputs and outputs remain the same, but the transaction ID is slightly tweaked.[23] If all the right conditions are in

19. *See* Christian Decker & Roger Wattenhofer, *Bitcoin Transaction Malleability and Mt. Gox*, ARXIV (Mar. 26, 2014), https://arxiv.org/abs/1403.6676; *See also* Michael Nielson, *How the Bitcoin Protocol Actually Works*, (Dec. 6, 2013), http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/.

20. *Id*.

21. *Id*.

22. *Id*.

23. *Id*.

place, miners will confirm the tweaked transaction, while allowing the fraudulent payee to claim that the intended transaction did not go through based on the transaction ID.[24] When that happens, the payee might convince the payer to initiate another transaction using a different input. If she does, the fraudulent payee will have received two payments.

To use the previous example, suppose that Charlie wishes to defraud Adam into paying him twice for the same product. After Adam transmits the transaction known as ADAMCHARLIETRANSACTION to the network, Charlie intercepts it and modifies the ID ever so slightly without changing its inputs or outputs. For example, Charlie changes it to ADCHARTRANS. After ADCHARTRANS transaction is confirmed, Charlie would point out to Adam that no transaction named ADAMCHARLIETRANSACTION was ever confirmed, and he would ask Adam to try another payment using a different input. Adam would then create another transaction for the same amount. When that second transaction is confirmed, Charlie would have been paid twice.

### 2. Allocating Losses

In each of the four scenarios, it should have been abundantly clear as to which parties should and which parties will sustain the entirety of the loss. In each scenario, there are at most two parties (the victim and the fraudster). The victim is the only party who bears the risk of loss and is the only party in a position to manage such risk through adequate precautions. There is no other party to whom the loss can be shifted.

In the first two scenarios, the user is the only one who can protect her own private keys, either from misplacement or from theft. In the third scenario, it is entirely up to the payee to make sure that the intended transaction was confirmed before rendering the product or service. In the fourth scenario, it is entirely up to the payer to make sure that the intended transaction had not already been confirmed with a different ID before paying the same amount twice in a separate transaction.

In a way, basic bitcoin transactions resemble transactions made with hard cash because they are almost entirely peer-to-peer in nature. This illustrates why Bitcoin's founder envisioned a system that obviated the need for a set of rules of loss allocation or dispute mediation, lowering the transaction costs across the system.[25]

## II. Bitcoin's Maturation: The Rise Of Hosted Wallet Services And Intermediated Transactions

While personal wallets provide the user with total control over the management of risks and security procedures (for better or for worse),

24. Danny Bradbury, *What the 'Bitcoin Bug' Means: A Guide to Transaction Malleability*, CoinDesk (Feb. 12, 2014, 7:26 PM), http://www.coindesk.com/bitcoin-bug-guide-transaction-malleability/.

25. *See* Nakamoto, *supra* note 3.

they also generate a degree of inconvenience. Managing a personal wallet involves a steep learning curve, especially for the less technologically savvy users. Running the Bitcoin software and conducting transactions is not a user-friendly process. For example, there is no slick visual interface that tells users how many bitcoins they own. Instead, users must (themselves or with the help of a service) go through the blockchain ledger and add up the different unspent transaction outputs in all of their addresses.

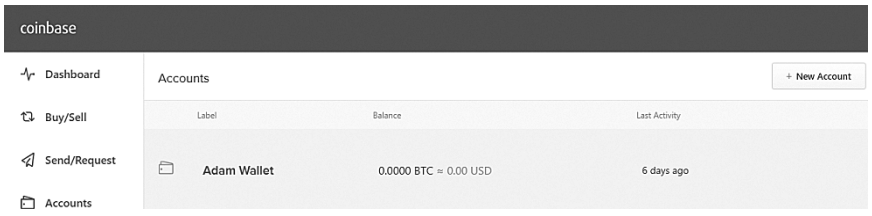
This inconvenience has spawned opportunities for third-party intermediaries to offer hosted wallet services with such friendly interfaces, through which providers manage wallets for their users and help conduct transactions on users' behalf. These wallets are stored in the cloud for use online and through mobile devices. Additionally, the wallets reduce the friction of conducting basic transactions, such as buying bitcoins and using them for commercial transactions. While users who use these hosted wallet services enjoy a much more user-friendly and convenient bitcoin experience, they also must entrust a third-party intermediary to safeguard their bitcoin holdings and to manage security issues. This reliance on a third-party intermediary fundamentally alters the mechanics of the underlying transactions and the way the risk of loss is spread throughout the system.

### A. *Transaction Mechanics*

To illustrate the differences in transaction mechanics between personal wallets and hosted wallet services, this Section will revisit the previous example involving Adam. This Section, however, will walk through the example as if Adam used the hosted wallet services of Coinbase, a leading hosted wallet service intermediary that currently boasts over 5 million users and 45,000 merchants.[26]

#### 1. Getting Started: Adam Creates A Hosted Wallet

Adam decides to create a hosted wallet through an account with Coinbase. In addition to asking him to create his account credentials (user name and password), Coinbase also asks Adam to link a source of funds, such as a bank account or his debit or credit card. When his setup is complete, Adam can go to his accounts page on Coinbase and see a streamlined interface in which he can create hosted wallets. Adam creates a hosted wallet called AdamWallet.




26. COINBASE, INC., *About Coinbase*, COINBASE.COM https://www.coinbase.com/about?locale=en (last visited Apr. 10, 2017).

After Adam creates his hosted wallet, he notices that the interface lets him see his Bitcoin address without showing him his private key. Indeed, upon looking through the user guides, he realizes that he does not have access to the private keys of individual hosted wallets; instead, the private keys are completely controlled by Coinbase.[27] This is fundamentally different from the scenario in which Adam creates a personal wallet. In that case, Adam alone would create and manage the private keys that generate the addresses for his transactions.

This brings up an extremely important question of bitcoin custody and ownership. Recall that the only way to prove ownership of the bitcoins in a certain address is to sign the transaction using the digital signature generated with the private key linked to the address. Since Adam does not control the private key, does he not actually own the bitcoins in his wallet?

Coinbase holds most of its bitcoins (Adam's and all of its users') offline in a consolidated virtual vault.[28] In a way, Adam's relationship with Coinbase resembles the kind of relationship he would have with his bank when he deposits cash—the bank holds on to the cash and issues a claim for the amount of Adam's deposit. This exposes users to counterparty risk they otherwise would not face with personal wallets, discussed later.

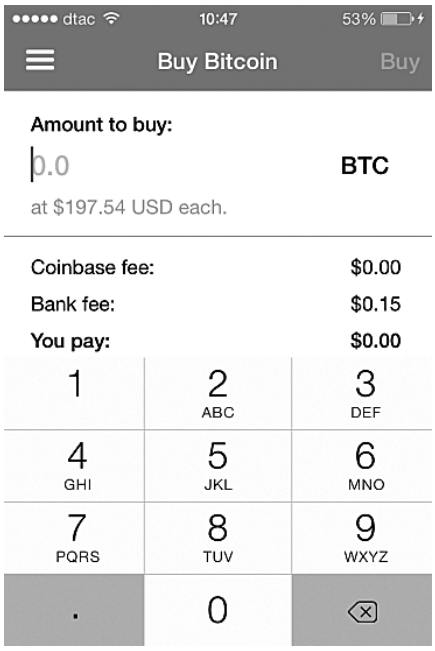
### 2. Buying Bitcoin With Dollars: Adam Buys Bitcoin From The Intermediary

Just like before, Adam needs to first buy some bitcoins with U.S. dollars before he can conduct any commercial transactions. Rather than having to find a private seller such as Beth, however, Adam can simply use Coinbase's buy/sell feature to buy bitcoins from the intermediary's bitcoin stores. In essence, Coinbase serves as a foreign exchange trader, allowing Adam to buy and sell bitcoins with U.S. dollars at up-to-date market prices rather than having to privately negotiate prices and terms with a bitcoin seller like Beth. Adam decides to buy 100 bitcoins using this buy/sell feature.

---

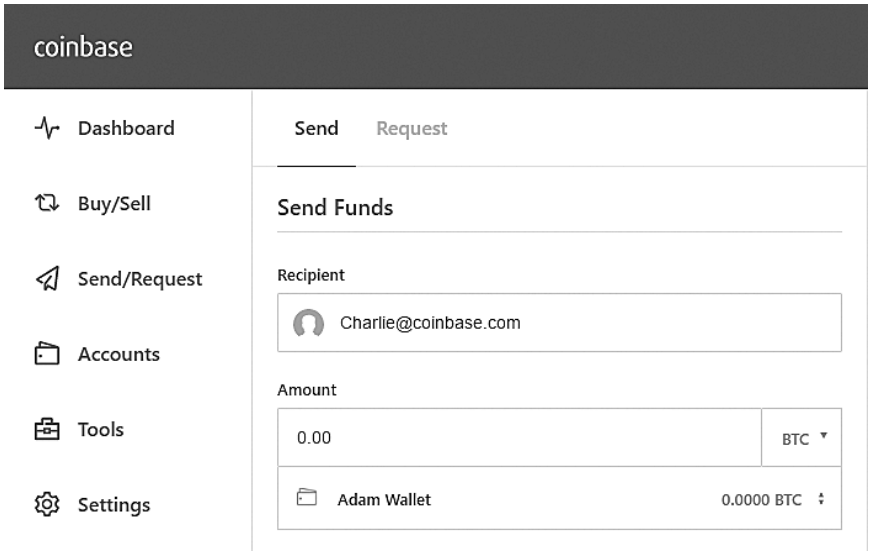
27. *See* COINBASE, INC., *Frequently Asked Questions*, COINBASE.COM https://support.coinbase.com/customer/portal/articles/1526452-where-can-i-find-the-private-keys-for-my-wallet- (last visited Apr. 10, 2017)

28. *See* COINBASE, INC., COINBASE.COM, https://www.coinbase.com/ (last visited Apr. 10, 2017).




### 3. Adam's First Commercial Transaction With Bitcoin: Buying A Product From Charlie

With the 100 bitcoins that he just bought from Coinbase, Adam is ready to conduct his first commercial transaction: buying a product from Charlie that costs 50 bitcoins. Unlike in the previous example, however, Adam can use a streamlined send/request interface instead of having to initiate a transaction and deal with inputs and outputs. All he needs to do is enter Charlie's Bitcoin address or e-mail address.



As Coinbase makes clear in its user agreement, however, Charlie *must* have a Coinbase account in order for the transaction to work.[29] If Coinbase cannot find any account linked to the address that Adam provides, it will prompt Charlie to set up his own Coinbase account or else void the transaction.[30] Why would Coinbase impose this requirement?

The reason for this requirement is that Coinbase does not conduct this transaction using Bitcoin network or the blockchain at all! Rather, all Coinbase does to effect a payment from Adam to Charlie is adjust the bitcoin balances in both accounts to debit 50 bitcoins from Adam and credit that same amount to Charlie (this is called an off-blockchain transaction).[31] By conducting settlement between its users in house, Coinbase can save on the fees that normally would have been paid to miners.

This example illustrates the fundamental differences in mechanics between a transaction conducted with a personal wallet and one conducted with a hosted wallet. In the former, a transaction is truly a peer-to-peer process between Adam and Charlie: it involves collective settlement by the users of the network without the involvement of any intermediaries. In the latter, settlement involves a unilateral act by an intermediary—in this case, Coinbase—where Coinbase updates its own internal ledger.

### B. *Losses From Intermediated Transactions*

The types of losses that can occur with transactions made with hosted wallet services are different than the losses that can occur with personal wallets. Furthermore, unlike the losses incurred with personal wallets, those incurred with hosted wallet services raise some significant issues of loss allocation.

#### 1. Risks Of Loss

##### a. *Scenario 1: Unauthorized transactions resulting from theft of user's account credentials*

An attacker who steals a user's account credentials with a hosted wallet services provider (i.e. the username and password) can conduct unauthorized transactions with that account. This is a much more serious attack than the theft of a private key in a personal wallet. Not only does the attacker have free reign to spend the bitcoin in *all* of the victim's addresses (and not just the one linked to a private key), but she can also steal

29. *See* COINBASE, INC., *Coinbase User Agreement*, COINBASE.COM https://www.coinbase.com/legal/user_agreement?locale=en (last visited Apr. 10, 2017).

30. *See Id.*

31. COINBASE, INC., *Why Can't I See My Transaction in the Blockchain?*, COINBASE.COM (July 21, 2016), https://support.coinbase.com/customer/en/portal/articles/1392055-why-can-t-i-see-my-transaction-in-the-blockchain-?b_id=13521.

funds from the bank accounts that are linked to the hosted wallets.[32] When such an attack occurs, significant issues must be resolved.

First, as a factual matter, it might not be clear who was at fault for the stolen credentials. Did the user fail to properly protect her credentials, either by choosing a password that was too simple or by leaving the password unattended? Were the stolen credentials the result of some sort of attack orchestrated on the hosted wallet service provider? Or did a fraudulent employee of the hosted wallet service provider conduct the attacks? Resolving this factual issue might take a great deal of fact-finding and due diligence.

Moving past the factual issues of fault, who should bear the loss of these unauthorized transactions? With a traditional bank account or payment card, the bank or payment card company will generally return the funds or reverse the charges resulting from an unauthorized transfer.[33] In contrast, hosted wallet intermediaries may disclaim responsibility for reimbursing users for the bitcoins that are stolen on their watch. Is this fair?

Finally, there is an additional issue as to who should be responsible for stopping the bleeding when credentials are compromised. Unlike the theft of a single private key, access to a user's credentials gives the attacker free reign to all the bitcoins in the user's wallet . Thus, it is imperative for the account to be shut down or frozen as soon as possible when an attack is recognized. Who should be responsible for recognizing the attack so that the account can be frozen: the user or the service provider?

]b. *Scenario 2: Large-scale theft of the intermediary's private keys*

Rather than target an individual user account, an attacker might find that it makes much more sense to go after an intermediary's entire bitcoin store. To do so, the attacker might try to breach the intermediary's security measures to steal a large number of the private keys held by the intermediaries. There have been many documented cases of such large scale breaches . For example, hackers stole roughly $350 million in bitcoins from a hosted wallet intermediary, Mt. Gox, in early 2014 and around $70 million from another intermediary called Bitfinex in 2016.[34]

Recall that users of hosted wallet services do not own the bitcoins in their wallets, but rather the claim against the intermediary for the amount of such bitcoins. Thus, the users face massive counterparty risk when such large scale losses occur; if the attack leaves the intermediary insolvent, the user will walk away with nothing. In these cases, users suffer losses even if the breach occurred through no fault of their own (recall that the users

32. U.S. Consumer Fin. Prot. Bureau, Consumer Advisory: Risks to Consumers Posed by Virtual Currencies, 5 (Aug. 2014), files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual–currencies.pdf.

33. *Id.*

34. Stan Higgins, *The Bitfinex Bitcoin Hack: What We Know (And Don't Know)*, Coindesk (Aug. 3, 2016 6:49 PM) http://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know/.

have no access to the private keys and no responsibility over their safekeeping). This fact raises the issue of fairness and consumer protection.

### 2. Allocating Losses

The tricky loss allocation issues raised above are currently resolved contractually through the agreement that each user enters with the intermediary. In most cases, the intermediary disclaims liability for unauthorized transactions or places the burden on the user to prove that the intermediary was at fault. For example, with respect to Scenario 1, Coinbase states that they "assume no responsibility for any loss that [a user] may sustain due to compromise of account login credentials due to no fault of Coinbase and/or failure to follow or act on any notices or alerts that we may send to [the user]."[35] In other words, Coinbase places the burden of proving fault on the user—a very difficult task. As discussed in the previous subsection, pinpointing the cause of unauthorized transactions requires a good deal of fact finding and diligence that cannot be reasonably expected of the user. Users of Coinbase who noticed unauthorized transactions depleting their bitcoin holdings have often been left without any recourse.[36]

Resolution of loss allocation issued solely through such private agreements is problematic. First, such private agreements may lead to economically inefficient outcomes. In the context of Bitcoin intermediaries, such market failure necessitate legal intervention. Leaving the effects of market structure aside, it is unrealistic to believe that customers will negotiate any of the loss allocation provisions to which they agree, since the cost of negotiating such provisions typically exceeds the potential benefit to them.[37] To the extent that customers might "shop" around for better user agreements rather than negotiate, negotiation costs are replaced with search costs. Asymmetric information, furthermore, limits the effectiveness of consumer shopping as users are unlikely to think about the liability terms when opening an account. Those that do will encounter largely incomprehensible legal jargon. Second, the intermediaries are not bound by consumer protection norms when they unilaterally decide on the loss allocation terms in the user agreement that they enter into with their user.

## III. Policy Recommendations: Building An Effective Loss Allocation Mechanism For Bitcoin Transactions

As the previous section indicated, the rise of intermediation and hosted wallet services creates a real need for an effective legal mechanism

35. *See* Coinbase, Inc., *Coinbase User Agreement*, Coinbase.com https://www.coinbase.com/legal/user_agreement?locale=en (last visited Mar. 9, 2017).

36. Russell Brandom, *A String of Thefts Hits Bitcoin's Most Reputable Wallet Service*, The Verge, (Feb. 7, 2014, 9:01 AM), http://www.theverge.com/2014/2/7/5386222/a-string-of-thefts-hit-coinbase-bitcoins-most-reputable-wallet-service.

37. Robert D. Cooter, *A Theory of Loss Allocation for Consumer Payments*, 66 Tex. L. Rev. 63 (1987).

for allocating losses from fraud, forgery, or error. Even if losses can subsequently be shifted through private contractual arrangements, this mechanism would serve as an important foundation for efficient and fair dispute resolution.[38] This section will attempt to define the contours of this mechanism, opting not to dwell on the specifics of how they should be drafted and implemented into law.[39] In doing so, the discussion will draw upon the functions and policy purposes of the loss allocation mechanisms found in existing payment system laws, namely Articles 3 and 4 of the U.C.C. under state law and the Electronic Funds Transfer Act under federal law.

### A. *Overview Of Important Policy Considerations*

Rather than using a single set of laws that covers all payment systems, Congress and regulators have decided to tailor a different set of laws for each major consumer payment system, even if such systems may serve similar functions (for example, loss allocation rules for debit card transactions differ from those for credit cards).[40] The divergence of these laws reflect the different choices made with respect to certain important policy questions. Should the resolution method be based on flexible standards, rigid rules, or both? Upon what norms should the mechanism be based—economic efficiency, consumer protection, or a balance of both?

#### 1. Resolution Method: Standards, Rules, Or Both?

The laws of each major payment system vary as to whether loss allocation issues should be resolved with a mechanism based on flexible standards, rigid rules, or a mix of both. For checks on one hand, UCC Articles 3 and 4 employ a relatively complex negligence standard that requires ad hoc investigation into the reasonableness of each party's conduct. Different transactions require different levels of care to meet the reasonableness standard, and insofar as negligence depends on the size of the potential loss, the law of checks implicitly considers the amount at issue in determining the liability of the parties.[41] For cards, on the other hand, the Electronic Funds Transfer Act and the Truth in Lending Act employ highly tailored rules such as caps on customer liability. These provisions do not take into consideration the circumstances of the individual transaction, the level of care practiced by transaction parties, or the amount at issue.[42]

Clayton Gillette notes in his study of the divergence between the laws of different payment systems that policy decision whether to resolve loss

38. Andrew P. Morriss & Jason Korosec, *Private Dispute Resolution in the Card Context: Structure, Reputation, and Incentives*, 1 J.L. ECON. & POL'Y 393 (2005).

39. After all, any regulation may disserve the objectives that it purportedly addresses due to external factors, such as politics or historical accident, affecting the process, and hence, the substance of formulation. *See* Clayton P. Gillette, *Rules, Standards and Precautions in Payment Systems,* 82 VA. L. REV. 181 (1996).

40. *Id.* at 184.

41. *Id*.

42. *Id*.

allocation issues based on flexible standards, rigid rules, or a mix of both should depend on the capacity to strike a balance among the costs of drafting, implementing, and enforcing the alternative formulations.[43] As Gillette notes:

> "[P]recise directives are more appropriate when we have the greatest confidence in our capacity to inform target actors (those at whom legal directives are aimed), to describe antisocial forms of behavior (so that target actors know the scope of permitted and prohibited activity), and to recognize the occurrence of such behavior (for purposes of enforcement). Uncertainty about any of these factors warrants the use of less precise formulations. For instance, if the conditions under which antisocial behavior might arise are too varied to be described ex ante, a precise rule that proscribes specific activities will be less effective than a flexible standard in addressing the full range of undesirable conduct. Finally, we might seek a middle ground and include precise immunities or safe harbors if we believed that a vague legal standard might over-deter desirable activity as people shy away from the boundaries of potential liability.[44]

The choice of how precise to make loss allocation rules for commercial transactions, thus, depends on the ability of those who make and apply the law, as well as the ability of the targets of legal directives to define and identify desirable and undesirable behavior.

### 2. Norms: Economic Efficiency And Consumer Protection

A related but equally important policy consideration is the choice of norms upon which the loss allocation mechanism should be based. On one hand, the mechanism can aim for economic efficiency. The goal of economic efficiency provides that any loss allocation mechanism should provide incentives to the party best able to prevent the unauthorized payment transaction at the lowest cost.[45] On the other hand, the loss allocation mechanism can be based on the norms of consumer protection, seeking to protect consumers by limiting the liability they can incur.

These two norms are sometimes, but not always, in tension. For example, laws governing debit and credit card payments impose an arbitrary $50 cap on the liability that can be incurred by a consumer, regardless of the consumer's level of care (for debit cards but not credit cards, liability can increase depending on the consumer's failure to report an unauthorized transaction after a specified period of time).[46] But as Cooter points out, holding the financial intermediary strictly liable for any loss beyond the cap erodes the consumer's incentive to take precaution and to refrain

---

43. *Id.* at 185.

44. *Id.* at 185-86.

45. *Id.* at 184. Gillette states that "[w]here multiple parties (i.e., either customers or financial institutions) could take such precautions [against loss], regulations should, therefore, place the obligation on the party who can avoid the loss at the lowest cost."

46. *See* Linda J. Rusch, *Reimagining Payment Systems: Allocating Risk for Unauthorized Payment Inception*, 83 CHI. KENT L. REV. 561, 581-83 (2008).

from any action that would increase the loss, reducing economic efficiency.[47]

### B. *Suggested Loss Allocation Mechanism For Intermediated Bitcoin Transactions*

Having described the important policy choices to consider when designing a loss allocation mechanism, the discussion will now revisit the loss allocation issues described in Section III.B and propose a legal mechanism to resolve such issues.

#### 1. Unauthorized Transactions Resulting From Theft Of User's Account Credentials

In situations where a malicious attacker steals the user's account credentials to conduct unauthorized transactions, the intermediary should bear all of the losses *up to* a certain small amount (say $200). This should be a strict liability rule that does not take into account the level of care exercised by the user.

##### a. *Strict liability rule placing liability on intermediary up to a certain threshold*

The burden of loss, at least up to a certain amount, should fall on the intermediary rather than the user. Consumer protection reasons aside, this strict liability rule is justified under several principles of economic efficiency identified by Cooter. First, the principle of loss spreading dictates that liability for a loss should be assigned to the intermediary because the intermediary has greater economic resources and is in a better position to predict the total volume of its losses, as well as spread these losses over a large group of consumers. In contrast, the user would have no ability to spread a loss.[48] Second, the principle of loss imposition dictates that the loss allocation mechanism should be a strict liability rule rather than a flexible standard based on fault, as decisive rules that clearly impose liability would lower enforcement costs, which are deadweight costs to the system.[49] This is especially true because, as indicated earlier, many factual issues must be resolved to determine fault in a particular occurrence of loss. It will not always be clear *how* an attacker got access to a user's credentials. Opting for a flexible standard will most likely increase enforcement costs.

##### b. *Strict liability rule placing liability on the user for any losses beyond the threshold*

Strict liability should fall on the user for any losses beyond the threshold. Such a liability rule will create an incentive for users to hold only as

47. Cooter, *supra* note 38 at 74.

48. *Id.* at 72.

49. *Id.* at 78.

much bitcoins with the intermediary as they need for their immediate transactions, while keeping the rest of their bitcoins in their own personal wallet. This aligns with Bitcoin security best practices, which dictate that due to the irreversibility of bitcoin transactions and the potential for loss, users should hold as much of their bitcoin in "cold" wallets offline.[50]

### 2. Large-Scale Theft Of The Intermediary's Private Keys

Where loss occurs from a large-scale theft of the intermediary's private keys from a major security breach, the intermediary should bear *all* of the loss. Having exclusive control of the keys, the intermediary is the only entity that can prevent the loss. Fairness considerations dictate that the user should not bear any loss for which she is not responsible. Finally, regulators should consider mandating insurance for intermediaries to mitigate users' counterparty risk. As incidents such as the Mt. Gox breach showed, even a single large-scale theft of bitcoin can wipe out an intermediary's reserves and make it insolvent, leaving users with no way to get their money back.

## IV. Conclusion

Every year, Bitcoin's naysayers claim that the end of the virtual currency is near. It is true that going forward, Bitcoin will face a number of growing pains that its creator probably did not anticipate. With the explosive growth in transaction volume, there are concerns that the network will become oversaturated and future transactions will take too long or become too costly to process.[51] Mining pools in China, formed by groups of miners looking to consolidate computing power in order to exploit economies of scale, threaten to "control" the blockchain and compromise its integrity.[52] Other "coins" and virtual currencies modeled off Bitcoin threaten to divide Bitcoin's user base and weaken its impact. Bitcoin, nonetheless, has shown remarkable resilience and does not show signs of slowing down, especially in its capacity as an alternative consumer payments system.

Still, as Bitcoin matures from a tech experiment into a bona fide consumer payments system, the rise of intermediation and hosted wallet services creates issues that Bitcoin's founder did not anticipate. In essence, Bitcoin is slowly transforming from a purely peer-to-peer digital analogue of cash into something that more closely resembles the intermediated systems of the past. On one hand, the presence of intermediaries is necessary to attract new users, especially those less technologically savvy, and to

50. *See* Bitcoin.org, *Securing Your Wallet*, https://bitcoin.org/en/secure-your-wallet.

51. Chris Baranuik, *Bitcoin: Is the crypto-currency doomed?*, BBC News (Jan. 19, 2016), http://www.bbc.com/news/technology-35343561.

52. Nathaniel Popper, *How China Took Center Stage in Bitcoin's Civil War*, NY Times (July 3, 2016), http://www.nytimes.com/2016/07/03/business/dealbook/bitcoin-china.html?_r=0.

Bitcoin's mainstream growth. On the other hand, such intermediation can fundamentally alter the nature of bitcoin transactions in a way that raises new issues of loss allocation and dispute mediation. Policymakers should heed this changing dynamic and put in place a legal mechanism to resolve these issues efficiently and fairly.