Regulating the Blockchain

An in-depth look at the most pressing legal issues facing these technologies.
Presenters

- Brian Klein, Baker Marquart
- Elijah Alper, WilmerHale
- Dana Syracuse, BuckleySandler
- Patrick Murck, Pillsbury and the Berkman Center for Internet & Society
- Reuben Grinberg, Davis Polk
- Byron Rooney, Davis Polk
- Peter Van Valkenburgh, Coin Center
Agenda

- **Peter**: Multi-sig Applications and Consumer Protection.
- **Brian**: 18 USC 1960: The Most Important Criminal Statute You’ve Never Heard Of
- **Elijah**: BSA Regulation and FinCEN's Choice to Classify all Bitcoin Activities as Money Transmission.
- **Dana**: How Regulatory Issues Differ Between Consumer and Enterprise Business Models.
- **Patrick**: UCC Article 9 and Bitcoin Fungibility
- **Reuben and Byron**: Facilitating Securities Transactions with Blockchain: a Regulatory Case Study.
When does a company actually “control” virtual currency?

What are cryptocurrency transactions? And how do *multi-sig* and *n-lock* transactions work?
First, forget what you think you know about bitcoin (keys, blockchains etc.).

Here’s how a transaction actually works...
Every cryptocurrency transaction is an answer to a previous challenge and the creation of a new challenge.
These are **NOT** transactions:

Please send five bitcoin to my friend Dana.

Please send address xyA42g00 five bitcoin.

Here are the keys to these five bitcoins.
Every cryptocurrency transaction is an answer to a previous challenge and the creation of a new challenge.
This *is* a transaction:

This is my proof that I have the answer (5) to the challenge (3+2=?), which previously locked bitcoins z. 

Answer to previous challenge.

Now make bitcoins z only spendable by whoever can prove that they have answer to new challenge (2+2=?).
The Cryptocurrency Network Evaluates Answers and (if correct) Records New Challenges.

Previous Challenge: “3+2=?”
User Answers Challenge: “5”
Can set new challenge: “2+2=”

Public Blockchain
User
Public Blockchain
Now, whoever can answer the new challenge can spend the bitcoin.

New challenge: “2+2=?”

The answer is 4! Now here’s my new challenge...
Instead of a math challenge and answer:

4+4+? 8!

We can make the challenge use digital signatures (used for authentication online) with matching public-private keys.

What is digital signature of the private key matching this public key (address)?

Digital signature that could only have been made by person with private key!
This *is* also a transaction:

This is a signature made with private key $x$ that matches address $y$ which previously locked bitcoins $z$.}

Answer to previous challenge.

Now make bitcoins $z$ only spendable by person who can sign with private key $a$ that matches address $b$.}

Creation of new challenge.
If someone else tells you the address that matches their private key, you can send them bitcoins.

Previous Challenge: “Sign with Key x that Matches Address Y”

User Answers Challenge: “Signature of Key x”

Can set new challenge: “Sign with Key a that matches Address b”
Now, whoever can answer the new challenge can spend the bitcoin.

User Answers Challenge:
“Signature of Key $x$”

Can set new challenge:
“Sign with Key $a$ that matches Address $b$”

I have key $a$! That means I now control those bitcoins.
KEYS ≠ COINS
KEYS ≠ COINS

EXAMPLE: keys that had no prior transactions using them as the challenge. These are keys to nothing!
KEYS = something that *might* be needed to control coins.
What is MULTI-SIG?
This *is* a multi-sig transaction:

This is the digital signature of *key x* that matches *address y* which previously locked *bitcoins z*.

Now make *bitcoins z* only spendable by person(s) who can sign with two of the following three keys that match *address b*.

Creation of new challenge.

Answer to previous challenge.
MULTI-SIG transactions create challenges where $M$ of $N$ keys are needed to spend bitcoins.
$M$ of $N$?

15 of 15 keys needed.  
2 of 3 keys needed.  
1 of 1 key needed.  
3 of 5 keys needed.
This is a 1 of 9 in *real life!*
What is N-LOCK?
This *is* an n-lock transaction:

This is my proof that I have *key* \( x \) that matches *address* \( y \) which was previously sent *bitcoins* \( z \).

Answer to previous challenge.

Creation of new challenge.

Now make *bitcoins* \( z \) only spendable by person who can prove that they have *key* \( a \) that matches *address* \( b \) after this *date* in the future.
N-LOCK transactions create challenges where bitcoins can only be spent *after a certain amount of time.*
N-lock is like giving someone a future-dated check.
The world of possible wallets:
- Hosted
- Software
- Multi-sig
- Multi-sig with KRS
- Multi-sig with N-lock
Hosted Wallet

Bitcoins locked with simple one key challenge statement, wallet provider generates key and stores it for user in data center, user can request transactions on website.

Public Blockchain | Hosted Wallet Inc. | User
Software Wallet

Bitcoins locked with simple one key challenge statement, wallet provider writes software that user runs on her own computer, user generates key and stores it for herself.
Multi-sig Wallet

Bitcoins locked with 2 of 3 multisig challenge statement, wallet provider generates one key and stores it for user, user generates and stores other two keys.
Multi-sig Wallet Transactions

Public Blockchain -> User

Public Blockchain -> Multisig Wallet Inc.

User

Multisig Wallet Inc.

Public Blockchain

User

Multisig Wallet Inc.
Multi-sig Wallet with KRS

User

Public Blockchain

Key Recovery Service Inc.

Multisig Wallet Inc.
Multi-sig Wallet with N-lock

- User
- Public Blockchain
- N-lock transaction
- If after 10 days, then move balance to 1 key address.
- [key signatures]
So when is the user bearing the risk and when is the company?
Multi-sig Wallet (user 2 keys)

Public Blockchain → User → Multisig Wallet Inc.

RISK / CONTROL
Multi-sig Wallet
(company has 2 keys)

Public Blockchain

User

Multisig Wallet Inc.

RISK / CONTROL
Multi-sig Wallet with KRS

LEGEND

Contract

User

Public Blockchain

Key Recovery Service Inc.

Multisig Wallet Inc.

RISK / CONTROL
Multi-sig Wallet with N-lock

User

Public Blockchain

If after 10 days, then move balance to 1 key address.
[key signatures]

N-lock transaction

RISK / CONTROL
AFTER 10 DAYS

Multisig Wallet Inc.
Who are the companies in these categories?
Hosted Wallet

Bitcoin locked with simple one key challenge statement, wallet provider generates key and stores it for user.
Software Wallet

Bitcoins locked with simple one key challenge statement, wallet provider writes software that user runs on her own computer, user generates key and stores it for herself.
Multi-sig Companies

Multi-sig Wallet
Bitcoins locked with 2 of 3 or other multisig challenge statement, wallet provider retains at least one key and stores it for user, user stores other two keys or uses KRS.
Multi-sig N-lock Companies

GreenAddress

Multi-sig N-lock Wallet
Bitcoins locked with 2 of 2 multisig challenge statement, wallet provider generates and stores one key, user generates and stores second key. Additional N-Lock transaction signed by both will refund all bitcoin back to user in future.
What happens if the company is hacked?
What if hacked?

**Hosted Wallet**: Company’s keys may be stolen, if so user’s bitcoin is also stolen.

**Hosted Wallet**
Bitcoins locked with simple one key challenge statement, wallet provider generates key and stores it for user.

**Examples:**

- coinbase
- xapo
- CIRCLE
What if hacked?

**Software Wallet**: Company does not have keys on their servers, hackers have nothing to steal.

**Software Wallet**
Bitcoins locked with simple one key challenge statement, wallet provider writes software that user runs on her own computer, user generates key and stores it for herself.

Examples:
What if hacked?

**Multi-sig Wallet**: Company’s key may be stolen, but one key of three is insufficient to steal the bitcoin. User can move bitcoin to new wallet with her two keys.

---

**Multi-sig Wallet**

Bitcoins locked with 2 of 3 multisig challenge statement, wallet provider generates one key and stores it for user, user generates and stores other two keys.

**Examples:**

- BitGo
- Coinkite
- Copay
What if hacked?

**Multi-sig N-Lock Wallet:** Company’s key may be stolen, but insufficient to steal bitcoin. Hacker could block user from transacting, but user regains full control at end of n-lock.

**Multi-sig N-lock Wallet**

Bitcoins locked with 2 of 2 multisig challenge statement, wallet provider generates and stores one key, user generates and stores second key. Additional N-Lock transaction signed by both will refund all bitcoin back to user in future.

**Examples:**

- GreenAddress
What about multi-sig companies that have M of N (e.g. 2 of 3) keys? or have a partner company that along with them has sufficient keys to transact without the user?
The company or companies are effectively a hosted wallet. They can be hacked & bitcoin stolen.
The best way to draw the line between companies that do “hold” bitcoin and those that don’t is . . .
asking whether the company can unilaterally transact, or prevent transactions . . .
and if they can prevent, is there a reasonable time-limit (n-lock) that safely returns full control to the user?
Additionally, we should wonder...
Are wallets the only use case for multi-sig?
Not even close.
**Problem:** We don’t want to regulate any of these uses as money transmission. But it’s hard to draft an exemption that would cover all possible non-money transmission uses.
Solution: When properly set up, none of the providers of these tools will have the unilateral ability to execute, and those able to prevent will be reasonably time-limited.
Therefore, a definition like this:

“Control of Virtual Currency” means possession of sufficient credentials or authority on a network to execute unilaterally* or prevent indefinitely** virtual currency transactions.

* thus excluding multi-sig minority key holders  
** thus excluding key holders who offer n-lock refunds

Ensures that companies at risk and in control are included:  
And that innovative and low-risk companies are not:
Please visit coincenter.org to learn more.
18 USC 1960
The Most Important Criminal Statute You’ve Never Heard Of
18 U.S. Code § 1960 - Prohibition of unlicensed money transmitting businesses

(a) Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of a **unlicensed money transmitting business**, shall be fined in accordance with this title or imprisoned not more than 5 years, or both.

...
18 U.S. Code § 1960

(b) As used in this section—

(1) the term “unlicensed money transmitting business” means a money transmitting business which affects interstate or foreign commerce in any manner or degree and—

(A) is operated without an appropriate money transmitting license in a State where such operation is punishable as a misdemeanor or a felony under State law, whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable;

(B) fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section; or

(C) otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity;