Lessons Learned From Recent Virtual Currency Cases
• The web seminar has not yet started:
• A sound check will be performed 5 minutes before the start time.

• COPYRIGHT NOTICE – USE OF WEBEX LOGIN/PASSWORD FOR ACAMS WEB SEMINARS

Each site license entitles registrant to **one login: one** phone connection (if accessing audio via teleconference) and **one** Internet connection for simultaneous Webcast, in **one room** where an unlimited number of listeners may participate.

Providing your login instructions and password to another for their use, using your login ID/password more than once, or any simultaneous or delayed transmission, broadcast, re-transmission or re-broadcast of this event to additional sites/rooms by any means (including but not limited to the use of telephone conferencing services or a conference bridge, whether external or owned by the registrant) or recording is a violation of U.S. copyright law and is strictly prohibited.
Speakers:

Juan Llanos, CAMS  
Executive Vice President  
Bitserve.org

Brian Stoeckert, JD, CAMS, CFE  
Managing Partner  
Stratis Advisory

John Bandler, CAMS, CISSP, CFE  
Assistant District Attorney  
New York Country District Attorney’s Office
Juan Llanos, CAMS
Executive Vice President
Bitserve.org
WHAT DIGITAL ASSETS ARE
Digital Assets tend to be global, open, nodal and evolutionary in nature. They live on the Internet and vary widely in scope and use.
Features
Digital Assets vary widely in scope and capability.

Type
- Cryptographic
- Mathematical
- Centralized
- Distributed
- Public/Private Ledger

Source
- Asset, Reputation or Demand Backing
- Mined, Earned or Issued
- Volume Fixed or Variable Supply

Fungibility
- Open, Federated or Closed Loops
- FX/Equity or Digital Asset Exchanges

Network
- Rails
- Identity
- Personalization
- Social Accounts
- Distributed Accounts
WHAT BITCOIN IS
“A Peer-to-Peer Electronic Cash System.”
Satoshi Nakamoto

“A peer-to-peer network that allows for the proof and transfer of ownership without the need of a trusted third party.”
Goldman Sachs

“The world’s pre-eminent internet-scale open platform for value exchange.”
Richard Brown (IBM)
AN ACCOUNTING SYSTEM
WHY BITCOIN IS REVOLUTIONARY
Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.
Revolutionary

NO financial institution or central authority in control

DISTRIBUTED CONSENSUS

MATH-ENFORCED TRUST

DOUBLE-SPEND → SOLVED
Revolutionary TRANSPARENT LEDGER

Every transaction that has ever occurred in the history of the bitcoin economy is publicly viewable in the BLOCK CHAIN.

Privacy without anonymity → pseudonymity
Revolutionary
PAYMENT & IDENTITY SEPARATED
CONSUMER ➔ PRIVACY PROTECTED
MERCHANT ➔ NO CHARGEBACKS / FRAUD

Payment only
HOW BITCOIN WORKS

Less technical video [5 mts]
https://www.youtube.com/watch?v=l9jOJk30eQs&src_vid=Lx9zgZCMqXE&feature=iv&annotation_id=annotation_1458036875

More technical video [22 mts]
https://www.youtube.com/watch?v=Lx9zgZCMqXE
Bob owes Alice money for lunch, so he picks up his smartphone and opens his Bitcoin smartphone app.

To pay her, he needs two pieces of information: his private key, and her public key.

Bob gets Alice’s public key by scanning a QR code from her phone, or by having her email him the payment address, a string of seemingly random numbers and letters.

Anyone who has a public key can send money to a Bitcoin address, but only a signature generated by the private key can release money from it.

The app alerts Bitcoin “miners” around the world of the impending transaction.

The miners verify that Bob has enough bitcoin to make the payment.

Miners race to bundle data from the pending transaction with other unrecorded transactions, plus the last block of transactions recorded in the public ledger, as well as a random number known as a nonce.

Then the miner applies a mathematical function known as a hash, which produces a unique cryptographic “fingerprint” that makes transactions verifiable.

The hashed block must have a certain, but arbitrary, number of zeroes at the beginning. It’s unpredictable which nonce will produce a hash with the correct number of zeroes, so the miner has to keep trying different nonces to find the right value.

When a miner finds a hash with the correct number of zeroes, the discovery is announced to the rest of the network. Other miners communicate their acceptance when they turn their attention to finding the next block, with the newly made block as a component.

The algorithm rewards the winning miner with 25 newly created bitcoins, and the hashed block is published in the public ledger.

Within 10 minutes of Bob initiating the transaction, he and Alice each receive the first confirmation that the bitcoin was signed over to her.

The parties receive several more confirmations as the block that recorded their transaction is embedded into subsequent blocks.
“Virtual currencies promise to benefit commerce on many levels, from serving the unbanked to new financial products. I challenge our innovators: devise creative solutions to prevent virtual currency abuse.”

FinCEN Director Jennifer Shasky Calvery
BITCOIN & FINANCIAL CRIME
Before March 18, 2013

The Criminal Precedent that Could Curb Bitcoin’s Enthusiasm
• ISSUER OF DIGITAL CURRENCY
  • a medium of exchange offered over the Internet
  • Global acceptance without the need for conversion between national currencies

• USED FOR ONLINE COMMERCE AND FOR FUNDS TRANSFERS BETWEEN INDIVIDUALS

• FOUR PRIMARY STEPS
  1. Opening a digital currency account
  2. Converting national currency into “e-gold” to fund the account
  3. Using “e-gold” to buy a good or service or transfer funds to another person
  4. Exchanging “e-gold” back into national currency

• PARTIES NEEDED:
  • Digital currency exchanges
  • Merchants or individuals that accepted “e-gold”

• ABILITY TO OPERATE ACCOUNTS ANONYMOUSLY
  • Highly-favored method of payment by operators of “get-rich-quick” scams

• ALL TRANSFERS OF “E-GOLD” WERE IRREVOCABLE AND IRREVERSIBLE
E-Gold

2008-07 Guilty Plea

- Conspiracy To Launder Monetary Instruments (federal)
- Conspiracy To Commit The Offense Against The United States (federal)
- Operating Of Unlicensed Money Transmitting Business (federal)
- Transmitting Money Without A License (District of Columbia)

“The root causes of E-Gold’s failure were design flaws in the account creation and provisioning logic that led to the unfortunate consequence of vulnerability to criminal abuse.”

“We acknowledge that E-Gold is indeed a financial institution or agency as defined in US law and should be regulated as a financial institution.”

Douglas Jackson, E-Gold Founder
FinCEN Guidance FIN-2013-G001

• “Interpretive Guidance” → not new rule-making
• Centralized vs. Decentralized virtual currencies
• Virtual Currency Actors:
  • **USER** → a person that obtains virtual currency to purchase goods or services.
  • **EXCHANGER** → a person engaged *as a business* in the exchange of virtual currency for real currency, funds, or other virtual currency.
  • **ADMINISTRATOR** → a person engaged *as a business* in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.
FinCEN Guidance FIN-2013-G001

• “An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN’s regulations […].”

• “Under FinCEN’s regulations, sending “value that substitutes for currency” to another person or to another location constitutes money transmission, unless a limitation to or exemption from the definition applies. This circumstance constitutes transmission to another location, namely from the user’s account at one location (e.g., a user’s real currency account at a bank) to the user’s convertible virtual currency account with the administrator.”

• “[…] a person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter.
After May 28, 2013

The *End of Bitcoin* as We Know It
Liberty Reserve

• alternative digital payment network
• “Closed loop” → centralized virtual currency (LR dollars)
• shut down and its management indicted and arrested in May 2013.
• “the largest money laundering case in U.S. history”
• a convenient tool for foreign currency brokers, as it allowed them to bypass local legislation and avoid exchange rate fluctuations
• “a shadowy netherworld of cyber-finance”
• its realm of anonymity made it a popular hub for fraudsters, hackers and traffickers
Liberty Reserve Indictment

[x] ANONYMITY ➔ product has to dissuade the bad element, never attract it.

- “deliberately attracting, and maintaining a customer base of criminals by making financial activity on LR anonymous and untraceable.”
- “designed so that criminals could effect financial transactions under multiple layers of anonymity and thereby avoid apprehension by law enforcement.”

[y] COMPLIANCE ➔ product and operations cannot be in violation of any applicable laws and regulations (the “form” or “paper” side of compliance).

- “was not registered as a money transmitting business with FinCEN”
- “operated an unlicensed money transmitting business.”

[z] SUBSTANCE ➔ what is written in a policy must actually be implemented. Businesses must be run with integrity, responsibility and control.

- “intentionally creating, structuring, and operating LR as a criminal business venture, one designed to help criminals conduct illegal transactions and launder the proceeds of their crimes.”
- “lying to anti-money laundering authorities in Costa Rica, pretending to shut down LR after learning the company was being investigated by US law enforcement (only to continue operating the business through a set of shell companies)”
- “created a system to feign compliance with anti-money laundering procedures, [...] including a ‘fake’ portal that was manipulated to hide data that LR did not want regulators to see.”
Convertible virtual currencies
- are potentially vulnerable to money laundering and terrorist financing abuse
- may allow greater anonymity than traditional non-cash payment methods

Virtual currency systems
- can be traded on the Internet (global reach)
- generally characterized by non-face-to-face customer relationships
- may permit anonymous funding
- may permit anonymous transfers
- may operate in jurisdictions with inadequate controls

Decentralized systems
- are vulnerable to anonymity risks. E.g., Bitcoin...
  - addresses have no names or other customer identification attached
  - has no central server or service provider
  - does not require or provide identification and verification of participants
  - does not generate historical records of transactions associated with real world identity
  - has no central oversight body
- no AML software is currently available to monitor and identify suspicious transaction patterns
- law enforcement cannot target one central location or entity for investigative or asset forfeiture purposes
<table>
<thead>
<tr>
<th>Convertible (open)</th>
<th>Decentralized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator;</td>
<td>No administrator</td>
</tr>
<tr>
<td>Exchangers;</td>
<td>Exchangers;</td>
</tr>
<tr>
<td>3rd-party ledger;</td>
<td>Users;</td>
</tr>
<tr>
<td>Can be exchanged for fiat currency</td>
<td>No 3rd-party ledger;</td>
</tr>
<tr>
<td>E.g.: WebMoney, LR dollars, e-Gold, Second Life Linden Dollars</td>
<td>Can be exchanged for fiat currency</td>
</tr>
<tr>
<td></td>
<td>E.g.: bitcoin, Litecoin</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Non-Convertible (closed)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator;</td>
<td>??</td>
</tr>
<tr>
<td>Exchangers;</td>
<td></td>
</tr>
<tr>
<td>3rd-party ledger;</td>
<td></td>
</tr>
<tr>
<td>Cannot be exchanged for fiat currency</td>
<td></td>
</tr>
<tr>
<td>E.g.: World of Warcraft Gold, Reddit Gold, Q Coins, Microsoft Points, Amazon Coins; online gaming credits</td>
<td></td>
</tr>
</tbody>
</table>
2014 EBA Opinion

European Banking Authority Opinion on Virtual Currency

RISK DRIVERS

- t. No stabilising authority
- s. Not legal tender
- r. Interconnectedness to FC
- q. No reporting
- p. Lack of corporate capacity and governance
- o. Lack of access to redress
- n. No complaint process
- m. No separation of accounts
- l. Insufficient funds or VC units
- k. Information is neither objective nor equally distributed
- a. VC schemes can be created (and their functioning subsequently changed) by anyone, anonymously
- b. Payer and payee are anonymous
- c. Global reach
- d. Lack of probity
- e. Not a legal person
- f. Opaque price formation
- g. No refunds or payment guarantee
- h. Unclear regulation
- i. Lack of definitions and standards
- j. Inadequate IT safety

Price formation on exchanges is subject to reliable standard significantly between manipulation of exchange.

Market participants are not as entities that could be subject to reliable standard.

The regulatory treatment is creates uncertainty for many participants.

The feature misrepresentation definitions

The IT systems, infrastructure, encryption are either insecure and, in the case of the process miners...
Bitcoin

Anonymous
Untraceable

“Invisible to law enforcement and the taxman”
An Analysis of Anonymity in the Bitcoin System –

*Bitcoin is Not Anonymous*

by Fergal Reid and Martin Harrigan (2011)


- The entire history of Bitcoin transactions is publicly available.
- “Using an appropriate network representation, it is possible to associate many public-keys with each other, and with external identifying information.”
- “Large centralized services such as the exchanges and wallet services are capable of identifying and tracking considerable portions of user activity.”
A Fistful of Bitcoins
by Sarah Meiklejohn et al (2013)


• The demonstrated centrality of these services makes it difficult for even highly motivated individuals—e.g., thieves or others attracted to the anonymity properties of Bitcoin—to stay completely anonymous, provided they are interested in cashing out by converting to fiat money (or even other virtual currencies).

• The increasing dominance of a small number of Bitcoin institutions (most notably services that perform currency exchange), coupled with the public nature of transactions and our ability to label monetary flows to major institutions, ultimately makes Bitcoin unattractive today for high-volume illicit use such as money laundering.

• A well and fairly regulated virtual currency industry makes it exceedingly difficult for bad actors to use the system for illicit activities.
Bitcoin Myths

Anonymous
Untraceable
“Invisible to law enforcement and the taxman”

Opportunities for enhanced surveillance and control
**Key AML Challenges**

"Know Your Counterparty"

No effective way to *know the identity of their customers’ counterparties* for digital currency to digital currency transactions. This hinders ability to:

- Conduct fully-effective sanctions screening
- Implement transaction monitoring rules based on counterparties (e.g., by country risk of counterparties)
- Comply with the Travel Rule

**AML Transaction Monitoring**

Automated transaction monitoring service providers don’t (yet) integrate well into a digital currency environment

Compliance software: stronger on identity than on transaction monitoring

Blockchain analysis: highly manual/unscalable

Significant resource constraints
Brian Stoeckert, JD, CAMS, CFE
Managing Partner
Stratis Advisory
Themes of Enforcement Actions

- Unlicensed Money Transmission
- Fraud
- Narcotics Trafficking
- Money Laundering
UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

ROSS WILLIAM ULBRICHT,
a/k/a “Dread Pirate Roberts,”
a/k/a “DPR,”
a/k/a “Silk Road,”
Defendant.

SOUTHERN DISTRICT OF NEW YORK, ss.: 

UNITED STATES OF AMERICA

- v. -

BLAKE BENTHALL,
a/k/a “Defcon,”
Defendant.

SOUTHERN DISTRICT OF NEW YORK, ss.:
Silk Road Fallout Continues
## Transactions Relayed By 217.69.224.209

Transactions that were relayed first by the ip 217.69.224.209

<table>
<thead>
<tr>
<th>Transaction Hash</th>
<th>Output Address</th>
<th>Amount (Satoshis)</th>
<th>(SatoshiBONES Percentage)</th>
<th>(Spent) Address</th>
<th>Amount (Satoshis)</th>
<th>(SatoshiBONES Percentage)</th>
<th>Fee (BTC)</th>
<th>Size (Bytes)</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>27340427c4fc8d85a6c4ce4b21eed82e97a3a653e551de8c95cb923e5efb4a5</td>
<td>1bosenVHLNM...</td>
<td>31.64</td>
<td>12.5pct</td>
<td>(Spent) 1JWAK4UNjihZRG6NvM1WeGmqDvvrHJBB3</td>
<td>140.56</td>
<td>(Spent)</td>
<td>$0.02</td>
<td>225</td>
<td>2015-01-18 08:16:05</td>
</tr>
<tr>
<td>89de357a90b4e312d65a644c587da8c853dd33f4f543c401dd7d9ebca676dcb</td>
<td>1bonesUzxUKp...</td>
<td>102.06</td>
<td>87.5pct</td>
<td>(Spent)</td>
<td>$0.02</td>
<td>191</td>
<td>2015-01-18 05:58:30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>82a55ce915fa2956406325e4983f1d151a503e471e0eb269e75ade4f753790d</td>
<td>1Hfmwx2kddR...</td>
<td>30.26</td>
<td>(Spent) 1454SN5zrgsk7yaWBzlUm2zcERu55aybD</td>
<td>2.10</td>
<td>(Unspent) 1Hs4BxrmsJwQDcyKSo4YNN1y3jnGh</td>
<td>$0.02</td>
<td>228</td>
<td>2015-01-18 04:14:32</td>
<td></td>
</tr>
</tbody>
</table>
John Bandler, CAMS, CISSP, CFE
Assistant District Attorney
New York Country District Attorney’s Office
• Perspective from a cybercrime investigator & prosecutor
• Time spent looking at how criminals use digital currency
  • To buy stolen data
  • To launder cybercrime proceeds
  • To remain anonymous
Caveat:

- My time has been focused on digital currency’s **illegitimate** uses
- Have not spent time analyzing how digital currency is used for legitimate purposes
- A view from a narrower perspective
• Investigated and prosecuted a case involving digital currency money laundering, and global trafficking in stolen data
• People v. Western Express International, Inc., et al.
• Cybercriminals and money launderers using digital currency, during the early periods of digital currency, 2002-2008
The Western Express case involved:

- A corrupt digital currency exchanger in Manhattan
- Illegal money transmitting
- Money laundering of digital currency (Egold, Webmoney)
- Use of digital currency to make instant, anonymous, irreversible payments in order to buy and sell hacked data
- Stolen data Vendors who sold hacked credit card information (DANY extradited one such vendor from overseas, who was later convicted at trial)
- Identity thieves (Buyers) who bought hacked credit card information and used it to forge credit cards and go shopping
Western Express, the corrupt digital currency exchanger, facilitated cybercrime on both an individual level and a global level:

- **Individual level:**
  - Allowed customers to obtain digital currency in order to purchase stolen data
  - Allowed customers to launder digital currency criminal proceeds

- **Global level:**
  - Balancing the global flow of digital currency with transfer of US funds
  - Balance the digital currency “trade deficit” caused by sophisticated cybercriminals in Eastern Europe
• Cybercrime is global
• Cybercriminals, wherever they are, target the United States (individuals, corporations, financial institutions)
• They can earn cybercrime profits without ever stepping foot in the US
• They need to get the illegal profits out
• Criminals are resourceful at finding ways to transfer and launder funds
• Digital currencies are perfect for cybercriminals

• Cybercriminals can pay each other across international borders, instantly, irreversibly, anonymously

• Street drug dealers use cash, cybercriminals use digital currency. Same concept, different medium.

• Cybercriminals need to get the illegal profits out of the US
• Digital currencies rely upon the conventional financial system, so the two systems will intersect
• Especially where there is a cybercrime related digital currency “trade surplus”
• If international cybercriminals are paid in digital currency from US sources, ultimately, that digital currency needs to be “repatriated” back to the US
• Repatriation” of digital currency across international borders would be accompanied by corresponding international bank wires (from the US)
Next, an illustration of how a digital currency and the conventional financial system, together can be used by cybercriminals who are located outside of the US, in order to earn cybercrime profits from inside the US.
Identity Thieves
Buyers of stolen credit card data

United States

Outside of the United States

Hackers and Vendors of Stolen Data

United States

Outside of the United States
Identity Thieves
Buyers of stolen credit card data

Use of stolen credit card data to buy merchandise

RETAIL STORES
shopping with forged credit card data

RETAILER
or other repository of credit card data or other valuable data

United States

Digital Currency

Hacking and stealing of data

Outside of the United States

Hackers and Vendors of Stolen Data

ACAMS WEB SEMINARS

www2.acams.org/webinars
Digital currencies that criminals use today include:

- Bitcoin
- Webmoney
- Perfect Money

Ways criminals can conceal & disguise funds:

- Anonymous accounts and no KYC
- “Tumblers” – disguise true recipient
- Layering within a currency
- Exchange between digital currencies