Managing the Risk of Bitcoin & Virtual currencies

by Juan Llanos, CAMS

Money Transmitter Regulators Association
Boston, November 6, 2014
Agenda

1. WHAT DIGITAL ASSETS ARE
2. WHAT BITCOIN IS
3. WHY BITCOIN IS REVOLUTIONARY
4. HOW BITCOIN WORKS
5. BITCOIN’S CHALLENGES
6. BITCOIN & FINANCIAL CRIME
7. MANAGING BITCOIN’S RISKS
WHAT DIGITAL ASSETS ARE
“Digital assets include digital, asset-backed, and cryptographic currencies along with the emerging ecosystem of payment innovations, fiscal tools, and P2P products enabled by these new Internet technologies.”

DATAAuthority.org
Digital Assets tend to be global, open, nodal and evolutionary in nature. They live on the Internet and vary widely in scope and use.
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

© 2014 Hub Culture for DATA
WHAT BITCOIN IS
“Think of Bitcoin as a numbered Swiss bank account living on your smartphone. [...] retail and online purchases can be made with virtually no transaction fees. It's the ultimate bank debit card, except there's no card — or bank for that matter.”

Robert Berry
“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)*
DIGITAL PAYMENTS NETWORK (B)

DIGITAL TOKEN (b)

PROTOCOL (B)
DIGITAL PAYMENTS NETWORK

INSTANTANEOUS, SECURE
LOW COST, GLOBAL
TRANSFER OF VALUE
DIGITAL TOKEN → MONEY

UNIT OF TRANSACTION → “BITCOIN”
DOLLAR VALUE → OPEN MARKET
COUNTERFEIT-PROOF “ONLINE CASH”
TOTAL CAPPED → INFLATION-PROOF

© 2014 Juan Llanos
TOKEN
Tangible representation of something of value

MONEY | COMMODITY | PROPERTY
"bitcoins" (tokens)

SCARCE → Central Banks can’t inflate them
DURABLE → they don’t degrade
PORTABLE → can be carried and transmitted electronically or as numbers in your head
DIVISIBLE → into trillionths
VERIFIABLE → through everyone’s block chain
EASY TO STORE → paper or electronic
FUNGIBLE → each bitcoin is equal
DIFFICULT TO COUNTERFEIT → cryptographically impossible

Naval Ravikant

© 2014 Juan Llanos
PROTOCOL

APPLICATIONS BEYOND PAYMENTS ➔
SECURE CONTRACTS, ESCROW, TAMPER-
PROOF VOTING, NOTARY SERVICES, ETC.

PLATFORM FOR INNOVATION

© 2014 Juan Llanos
• *The Shadow Superpower* (Robert Neuwirth, Foreign Policy) \( \rightarrow \) System D (“Debruillards”)

• Informal (“extra legal,” “black”) economies \( \rightarrow \) $10\ trillion in aggregate

• *The Mystery of Capital* (Hernando de Soto, 2000)

• Mystery \( \rightarrow \) failure of assets to serve as capital

• Problem \( \rightarrow \) credibility of rights transfer at a distance (i.e., ability to engage in binding contracts)

• Smart contracts \( \rightarrow \) jurisdiction-free contracting mechanism

• Distributed asset ledger for everyone, **EVERYONE**, around the globe
AN ACCOUNTING SYSTEM

© 2014 Juan Llanos
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

© 2014 Juan Llanos
Revolutionary

TRANSPARENT LEDGER

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

Privacy without anonymity → pseudonymity
Revolutionary

**PAYMENT & IDENTITY SEPARATED**

**CONSUMER ➔ PRIVACY PROTECTED**

**MERCHANT ➔ NO CHARGEBACKS / FRAUD**

Payment *only*
Revolutionary

OPEN SOURCE SOFTWARE

• Cathedral (restricted) vs. bazaar (internet)
• Public source code
• Users = co-developers
• Highly modular
• Dynamic decision-making
Revolutionary

INCENTIVES FOR ALL

• Miners $\rightarrow$ ‘bitcoins’ + fees
• Users $\rightarrow$ speed, security, privacy
• Developers $\rightarrow$ global experiment
• Society $\rightarrow$ transparency, financial inclusion, freedom

© 2014 Juan Llanos
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
Marc Hochstein, “Why Bitcoin Matters for Bankers”
BITCOIN’S CHALLENGES
CHALLENGES

REGULATION
PRIVACY
SPECULATION
SECURITY
COMPLEXITY
DISRUPTION POTENTIAL

© 2014 Juan Llanos
“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

Financial Action Task Force
Groupe d’Action Financière Internationale
(FATF-GAFI)
Financial Action Task Force
Groupe d’Action Financière Internationale
(FATF-GAFI)

Special Recommendation VI

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions.
Anonymity = Anathema

- Anonymous identification
- No value limits
- Anonymous funding
- No transaction records
- Wide geographical use
- No usage limits

Cash features

<table>
<thead>
<tr>
<th>CRITERIA</th>
<th>HIGHER RISK</th>
<th>LOWER RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Due Diligence</td>
<td>anonymous</td>
<td>identified/verified</td>
</tr>
<tr>
<td>Record-Keeping</td>
<td>not retained/accessible</td>
<td>retained/accessible</td>
</tr>
<tr>
<td>Value Limits</td>
<td>no limits</td>
<td>amount/transaction limits</td>
</tr>
<tr>
<td>Methods of Funding</td>
<td>via anonymous/multiple sources</td>
<td>via identified sources subject to oversight</td>
</tr>
<tr>
<td>Geographical Limits</td>
<td>wide</td>
<td>narrow</td>
</tr>
<tr>
<td>Usage Limits</td>
<td>anonymous/varied acceptance/unlimited</td>
<td>Identified/limited acceptance/restricted</td>
</tr>
<tr>
<td>Segmentation of Services</td>
<td>dispersed/outsourced</td>
<td>single provider</td>
</tr>
</tbody>
</table>

Before March 18, 2013

The Criminal Precedent that Could Curb Bitcoin's Enthusiasm
E-Gold

• 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

© 2014 Juan Llanos
March 18, 2013

FinCEN Guidance FIN-2013-G001
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 and sells units of convertible virtual currency those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter.”
Who is **a money transmitter** in the USA?

<table>
<thead>
<tr>
<th><strong>IS</strong></th>
<th><strong>IS NOT</strong></th>
</tr>
</thead>
</table>
| **...whoever *as a business***:  
  • Exchanges virtual currency for government currency, and one virtual currency for another (e.g., exchanges)  
  • Mines and makes a payment to a third party on behalf of a customer (e.g., for-profit miners)  
  • Accepts value from A and delivers it to B (e.g., some wallets)  
  • Accepts value from A and delivers it to A at a different time or place (e.g., vaults) | **...whoever**  
  • Mines, uses or invests virtual currency for own benefit  
  • Provides network access services to money transmitters  
  • Acts as a payment processor by agreement with a seller or creditor  
  • Acts as intermediary between BSA-regulated institutions |
Money Transmitter Regulation (US)

<table>
<thead>
<tr>
<th>Main Risk Areas</th>
<th>Main Statutes and Regs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Money Laundering</td>
<td>BSA, USA PATRIOT Act, Money Laundering Acts</td>
</tr>
<tr>
<td>Anti-Terrorism Financing (CFT)</td>
<td>USA PATRIOT Act, OFAC</td>
</tr>
<tr>
<td>Privacy and Information Security</td>
<td>Gramm-Leach-Bliley</td>
</tr>
<tr>
<td>Safety and soundness</td>
<td>State (via licensing)</td>
</tr>
<tr>
<td>Consumer protection</td>
<td>State (via licensing) + Dodd-Frank / Regulation E (CFPB)</td>
</tr>
</tbody>
</table>

Two regulation layers → Federal + State
AML Program Pillars*

1. A designated compliance officer + professional team

2. Written policies and procedures + operational controls:
   - Licensing, renewal and reporting procedures (S)
   - Registration, record-keeping and report-filing procedures (F)
   - KY (Know Your...) Subprograms: Acceptance, monitoring, correction and termination
     - KY...Customer
     - KY...Agent
     - KY...Foreign Counterparty
     - KY...Employee
     - KY...Vendor
   - Monitoring, analysis and investigating procedures
   - OFAC compliance program
   - Response to official information requests
   - Privacy and information security protection protocols

3. An on-going training program
   - Risk & Compliance Committee

4. An independent compliance auditing function

* AML Program Elements (Section 352 of the USA PATRIOT Act)
Foreign-Located MSBs

(September 19, 2011)

Foreign-located MSBs are financial institutions under the BSA (Bank Secrecy Act). With respect to their activities in the United States, foreign-located MSBs must comply with recordkeeping, reporting, and anti-money laundering (AML) program requirements under the BSA. They must also register with FinCEN.”

Foreign-located MSBs are subject to the same civil and criminal penalties for violations of the BSA and its implementing regulations as MSBs with a physical presence in the United States.
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>Centralized</th>
<th>Decentralized</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Administrator; Exchangers; 3rd-party ledger; Can be exchanged for fiat currency; E.g.: WebMoney, LR dollars, e-Gold, Second Life Linden Dollars</td>
<td>No administrator; Exchangers; Users; No 3rd-party ledger; Can be exchanged for fiat currency; E.g.: bitcoin, Litecoin</td>
</tr>
</tbody>
</table>

| Non-Convertible (closed) | Administrator; Exchangers; 3rd-party ledger; Cannot be exchanged for fiat currency; E.g.: World of Warcraft Gold, Reddit Gold, Q Coins, Microsoft Points, Amazon Coins; online gaming credits | ?? |

© 2014 Juan Llanos
2014 EBA Opinion

European Banking Authority Opinion on Virtual Currency RISK DRIVERS

- 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
- k. Information is neither objective nor equally distributed
- l. Insufficient funds or VC units
- m. No separation of accounts
- n. No complaint process
- o. Lack of access to redress
- p. Lack of corporate capacity and governance
- q. No reporting
- r. Interconnectedness to FC
- s. Not legal tender
- t. No stabilising authority

© 2014 Juan Llanos
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

© 2014 Juan Llanos
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

© 2014 Juan Llanos
MANAGING BITCOIN’S RISKS
Machine Learning (AI) Methods

SUPERVISED LEARNING: relies on two labeled classes (good vs. bad)

Goal → Detect known suspicious patterns

1. Training set:
   a. Select dataset with clean and dirty cases.
   b. Classification algorithm to discriminate between the two classes (*finds the rules or conditions*)
   c. Probabilities of class 1 and class 2 assignment

2. Run discrimination method on all future purchases.

UNSUPERVISED LEARNING: no class labels

Goal → Detect anomalies

1. Takes recent purchase history and summarize in descriptive statistics.
2. Measure whether selected variables exceed a certain threshold. (*deviations from the norm*)
3. Sounds alarm and records a high score.
“What customers do speaks so loudly that I cannot hear what they’re saying.”

(Paraphrasing Ralph Waldo Emerson)

Customer identification vs. customer knowledge

BEHAVIORAL ANALYTICS
“Risk management is not only about reducing downside potential (the probability of pain), but also about increasing upside opportunity (the prospects for gain).”

James Lam
Thank you!

Juan Llanos
EVP, Strategic Partnerships & Chief Compliance Officer
Bitreserve, Inc.
New York, NY
Mobile: (917) 684-0560
Email: juanbllanos@gmail.com

LinkedIn: www.linkedin.com/in/in/Juan Llanos
Twitter: @JuanLlanos
Blog: ContrarianCompliance.com
Resources 1/3

• Bitcoin Educational Resources: http://www.forbes.com/sites/jonmatonis/2013/05/13/6-new-bitcoin-educational-resources/

• Bitcoin Education Project (Udemy): https://www.udemy.com/bitcoin-or-how-i-learned-to-stop-worrying-and-love-crypto/

• Bitcoin Primer for Policymakers: http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_embargoed.pdf

• Bitcoin Wiki: https://en.bitcoin.it/wiki/Main_Page


• CoinDesk: http://www.coindesk.com/

• Contrarian Compliance: http://contrariancompliance.com/

• Let’s Talk Bitcoin: http://letstalkbitcoin.com/

Resources 2/3

• We Use Coins: https://www.weusecoins.com/en/
• Why Bitcoin Matters (Marc Andreessen): http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/?_php=true&_type=blogs&_r=0
• Smart Property, Colored Coins and Mastercoin: http://www.coindesk.com/smart-property-colored-coins-mastercoin/
• Anything by Vitalik Buterin, the creator of Ethereum: https://www.ethereum.org/
Resources 3/3

- Ettay Eyal & Emin Gun Sirer: http://hackingdistributed.com/2014/06/13/time-for-a-hard-bitcoin-fork/
- Tim Swanson: http://www.ofnumbers.com/author/timswanson/