

Regulation of Bitcoin

Jerry Brito
Coin Center
coincenter.org

Is Bitcoin regulated?

Is Bitcoin regulated?

“The so far unregulated digital currency has courted controversy because of its volatile value and its popularity among cybercriminals.”

–BBC News, August 15, 2014

Is Bitcoin regulated?

“The value in the decentralized and unregulated digital currency has plummeted since hitting a high of more than \$1,130 in December 2013.”

–USA Today, October 22, 2014

Is Bitcoin regulated?

“A Texas man was charged with fraud in New York on Thursday, in what federal authorities claim is the first-ever Ponzi scheme involving the unregulated digital currency Bitcoin.”

–TIME, Nov. 6, 2014

Is Bitcoin regulated?

- Confusion stems from what we mean by “Bitcoin”
 - Technology, protocol, network cannot be regulated
 - Software is typically protected speech (certainly in U.S.)
 - P2P network almost impossible to regulate because too many users to police efficiently
 - Also, it may be accurate to say that Bitcoin is **never** unregulated because Bitcoin is a protocol — a set of rules — and the P2P network enforces those rules.
 - Indeed, at its core Bitcoin is an attempt at regulation through technology and incentives rather than human institutions.

Is Bitcoin regulated?

- The technology and the network cannot be efficiently regulated by governments, but actors certainly can
 - Bitcoin businesses and users have always been subject to regulation.
 - Another reason there's confusion: notion that because governments have not acted (issued regs) Bitcoin is not regulated
 - In fact, existing law and regulation covers activity no matter what tech is employed
 - Regulation vs guidance - how, not if
 - Bitcoin businesses have been subject to reg since 2009

Bitcoin regulations

We the People



Major areas of regulation

- Consumer Protection
- Financial Surveillance
- Sanctions Enforcement
- Securities Regulation
- Taxation

Consumer Protection Regulation

Rationale for Consumer Regulation

- Centralized systems are subject to
 - Going offline
 - Blacklisting
 - Hacking
 - Double spending
- We saw this in Mt Gox - Jan. 2014 - \$600M lost

Rationale for Consumer Regulation

- CSBS Model Regulatory Framework - Feb. 2015
 - [M]any virtual currency services are clearly focused on consumer financial services. Such virtual currency service providers are in a position of trust with the consumer, which creates a public interest to ensure activities are performed as advertised with appropriate minimum standards to minimize risk to consumers.
 - It is CSBS policy that entities performing activities involving third party control of virtual currency should be subject to state licensure and supervision like an entity performing such activities with fiat currencies.

What does licensing look like?

- Background check
- Capital requirements
- Permissible investment requirements
- Record keeping and regular examinations
- Bonding requirement
- New product approval
- No threshold
- State-based
 - \$250k - \$500k to apply for BitLicense per Adam

Existing state MT law applies to Bitcoin

- Just because a state has not acted does not mean Bitcoin is unregulated
- Example: Florida: Money Transmitter means “receiv[ing] currency, monetary value, or payment instruments for the purpose of transmitting the same by any means, including transmission by wire, facsimile, electronic transfer, courier, the Internet, or through bill payment services or other businesses that facilitate such transfer within this country, or to or from this country.”
- Florida Local Bitcoins exchanger Pascal reid charged with violating state MTL - Dec. 2014
 - State judge ruled MTL applied
 - Exchanger pled guilty to unauthorized MT
 - 90 days in prison, 5 year probation, forfeit bitcoins
- Bitcoin businesses have been regulated since January 2009
- It’s up to the regulator and courts to interpret how existing law applies

Challenges of applying existing law

- Existing money transmission licensing statutes and regulations do not anticipate Bitcoin
- Result can be irrational and unintended consequences
- Example: Permissible Investments

Wyoming Money Transmitter Act

"Permissible investments" means:

- A. Cash;
- B. Certificates of deposit or other debt obligations of a financial institution, either domestic or foreign;
- C. Bills of exchange or time drafts drawn on and accepted by a commercial bank, ...;
- D. Any investment securities bearing a rating of one (1) of the four (4) highest grades ...
- E. Investment securities that are obligations of the United States, its agencies or instrumentalities, ...;
- F. Shares in a money market mutual fund, interest bearing bills, notes or bonds, ...;
- G. Any demand borrowing agreement made to a corporation or a subsidiary of a corporation whose capital stock is listed on a national exchange;
- H. Receivables which are due to a licensee from its authorized delegates ...; or
- I. Any other investments or security device approved by the commissioner.

Coinbase suspends operations in Wyoming - April 2016

Who is a money transmitter?

- CSBS says it should only be parties who hold custody
- Reality is that definitions of money transmission rarely turn on custody
 - Example: Colorado: "Money transmission" means ... engaging in the business of ... transmitting money ... by any means[.]
- Reason is that custody has been integral to transmission, but Bitcoin upends this
 - Does Blockchain.com qualify?
 - Is a miner?
 - Is a multisig provider?
- No threshold

Who is a money transmitter?

- Right now it's very much at the discretion of the regulator.
- Example: California regulator has determined it could apply existing MTL, but it is choosing to forbear
- Result is uncertainty
 - Bad for business, bad for innovation
 - PATRIOT Act - 18 U.S.C. § 1960
 - Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both.

Who is a money transmitter?

- Missed opportunities
 - Multisig for consumer protection (holding 1 of 3 keys poses less risk)
 - Proof of reserves better than annual audit
- How do we fix all this? New law
 - Either amend existing law and licenses OR create new type of license
 - Example: NY BitLicense

New York's BitLicense

(q) Virtual Currency Business Activity means the conduct of any one of the following types of activities involving New York or a New York Resident:

- (1) receiving Virtual Currency for Transmission or Transmitting Virtual Currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of Virtual Currency;
- (2) storing, holding, or maintaining custody or control of Virtual Currency on behalf of others;
- (3) buying and selling Virtual Currency as a customer business;
- (4) performing Exchange Services as a customer business; or
- (5) controlling, administering, or issuing a Virtual Currency.

The development and dissemination of software in and of itself does not constitute Virtual Currency Business Activity.

New York's BitLicense

- Gives us more clarity, but not enough
- Good
 - Software development is excluded
- Bad
 - Does this cover multisig?
 - Does this exclude mining?
 - Does this cover colored coins? Does The DAO need a BitLicense?
- Still at the discretion go the regulator

California's AB 1326

- (c) “Virtual currency business” means maintaining full custody or control of virtual currency in this state on behalf of others.
- 26004. The following are exempt from the licensing requirement[]:
 - (f) A merchant or consumer that utilizes virtual currency solely for the purchase or sale of goods or services.
 - (h) A person or entity developing, distributing, or servicing a virtual currency network software.
 - (i) A person or entity contributing software, connectivity, or computing power to a virtual currency network.
 - (j) A person or entity providing data storage or cyber security services for a licensed virtual currency business.

ULC Model Digital Currency Act

- Usual exclusions
- (3) “Control” means possession of sufficient virtual currency credentials or authority on a virtual currency network to execute unilaterally or prevent indefinitely virtual currency transactions, but does not include possessing, for a reasonably time-limited period, virtual currency credentials sufficient to prevent virtual currency transactions to provide a service such as escrow or transaction management.
- PLUS rolling 30-day exclusion

Problems remain for all of these: Still state-by-state, so expensive and inconsistent, need a federal solution

Comparison to EU

- EU states generally have unitary governments
 - Means one regulator/license
 - National innovation policy possible
- Principles-based vs. rules-based
 - Sandboxing
- Passporting

Financial Surveillance

Rationale for financial surveillance

- Create a paper trail to aid law enforcement detect and prosecute crimes
- Bitcoin is not anonymous, it is pseudonymous
- Ross Ulbricht
 - Law enforcement found and seized Silk Road server w/ wallet
 - Seized laptop contained thousands of dollars in Bitcoin
 - Ulbricht claimed bitcoins were profits from day trading
 - Prosecution showed direct link between Silk Road wallet and Ulbricht coins
 - In this case they had a suspect and were trying to prove a link
- Bitcoin investigations are reverse of traditional LE investigations
 - Traditional: Police has a suspect, they ask FI for his records
 - Bitcoin: Police have a transaction, they ask FI for identity
- This presumes that FIs are identifying users and maintaining records of transactions

Bank Secrecy Act (1970)

Obligates Money Service Businesses (MSBs) to do certain things:

- Registration with FinCEN
- Know Your Customer (KYC)
- Recordkeeping
- Anti-Money-Laundering (AML) Program
- Reporting
 - SAR - \$2,000+ and suspicious
 - CTR - \$10,000+ in cash

So, is a Bitcoin user or company an MSB?

FinCEN VC Guidance (March 2013)

- Certain Bitcoin actors have always been MSBs and BSA has always applied (guidance, not rule)
- Creates three categories of actors: "user," "exchanger," and "administrator."
 - A user is a person that obtains virtual currency to purchase goods or services.
 - An exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency.
 - An administrator is 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 VC Guidance (March 2013)

- Administrators - don't apply to decentralized cryptocurrencies.
- Users exempted (or are they?)
 - "A user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services is not an MSB under FinCEN's regulations."
 - What about a political contribution or other gift?
- Exchangers
 - "An [] 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, unless a limitation to or exemption from the definition applies to the person."

FinCEN VC Guidance (March 2013)

- Limited to exchanges - on and off ramps
- Implicitly, non-exchange wallet services are excluded
- Miners later found to be exempted because considered 'users'
- Merchant processors later found to NOT be exempted because not between regulated FIs

Example: Silk Road Corruption Case

- Carl Mark Force IV was DEA agent investigating Silk Road
- Stole seized funds, including for fake hit
- Sold intelligence to Ulbricht
- Tried to cash out through BitStamp
- BitStamp had KYC'd Force
- BitStamp reported suspicious activity and Force was caught
- Part of indictment was blockchain trail

Challenges of applying existing law

- Ambiguities like political donations, miners, merchants
- Poor fits of new technology with old law
 - Example: the 'travel rule'

The 'Travel Rule'

- For transmittals of funds between two financial institutions where the amount transmitted equals or exceeds \$3,000), the transmitting FI must retain:
 - (A) The name and address of the transmitter;
 - (B) The amount of the transmittal order;
 - (C) The execution date of the transmittal order;
 - (D) Any payment instructions received from the transmitter with the transmittal order;
 - (E) The identity of the recipient's financial institution;
 - (F) As many of the following items as are received with the transmittal order:
 - (1) The name and address of the recipient;
 - (2) The account number of the recipient; and
 - (3) Any other specific identifier of the recipient; and
 - (G) Any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order
- The originating FI must then pass this information on to the recipient's FI. It is this traveling data that has earned 31 C.F.R 1010.410 the name of Travel Rule.

The 'Travel Rule'

- Solutions
 - Don't allow transactions over \$3,000
 - Change law (go to two FIs instead of one)
 - Change the technology

Comparison to EU

- Generally, same principles as US apply under individual member-state laws
- After Paris attacks, EC has considered applying the 4th Anti Money Laundering Directive (4AMLD) to exchanges
 - Reason: Perception that "different approaches between Member States towards high-risk countries create weak spots"
- Also considering regulating wallet providers through 4AMLD or the Payment Services Directive 2 (PSD2)
- Also considering submitting VC exchange platforms to a fully fledged prudential licensing and supervision regime under PSD2

Sanctions Enforcement

Sanctions Enforcement

- Increasingly important tool in foreign policy
 - Iran, Russia, North Korea, ISIS,
- Office of Foreign Asset Control (OFAC)
- Specially Designated Nationals (SDN) List
- Strict Liability (there is no compliance)
- Stiff penalties
 - Last year PayPal fined \$7 million for 486 violations over four years
- Challenge: Again, Uneasy Fit
 - Given random address, how can you tell?
 - Miners in sanctioned countries?
- Status: Wait and see

Securities Regulation

Rationale for securities regulation

- Investor protection: To ensure that buyers of securities receive complete and accurate information before they invest in securities
- Requirements: Registration of securities offerings and disclosure

What qualifies as a security?

Howey Test

- a contract, transaction or scheme whereby a person
 - invests his money
 - in a common enterprise and
 - is led to expect profits solely from the efforts of the promoter or a third party,
- it being immaterial whether the shares in the enterprise are evidenced by formal certificates or by nominal interests in the physical assets employed in the enterprise.

Bitcoin Savings & Trust (2011-12)

- Trendon Shavers claimed to have been selling bitcoins to local tight-lipped buyers, and started BST to provide more volume to these buyers.
- "By selling invested bitcoins at a high rate and rebuying them at the market price, [Shavers] was supposedly able to offer a very high-yield interest rate of 7% per week."
- This attracted many investors (up to \$4.5 million).
- Apparently there was no real business, and Shavers was just paying old investors with new investor money. (Ponzi scheme.)
- Arrested and prosecuted for offer and sale of securities not registered with SEC
- Plead guilty and now in prison

Is a cryptocurrency a security?

- **Investment of money**
 - How is the cryptocurrency distributed? Democratic vs presale
 - A line of cases, generally dealing with memberships in country clubs or private parks, suggests that sales of common assets that are, as of yet, unrealized or undeveloped are more indicative of an investment than sales of common assets already developed.
- **Common enterprise**
 - Horizontal commonality — pooling of investor funds such that the fates of all investors rise or fall together
 - Vertical commonality — investor's fate is tied to the fate of the promoter
 - Is it like gold or like a company?
- **Expectation of Profits thru Third-Party Effort**
 - whether the actions of a particular third party are the cause of increased profits and, more precisely, whether buyers rely on those efforts
 - the more open and decentralized a network is, the less reliance on third parties

Case studies

- Bitcoin
- Paycoin
- The DAO

The Securities and Exchange Commission has not yet acted.

Taxation

U.S. Federal Tax - IRS Guidance (2014)

- U.S. has no national consumption or sales tax
- IRS determined Bitcoin is “property,” not “currency”
- If currency, ordinary income, but de minimis exemption
- If property, capital gains tax, but no de minimis exemption
- Congress may revisit
 - Ideally: Capital gains tax with de minimis exemption
 - Not likely to happen anytime soon

Sales or Consumption Tax

- Would make typical use of Bitcoin pointless
- Not subject to sales tax :o)
 - NY - Dec. 2014
 - Wisconsin, Missouri
 - ECJ Ruling - Oct. 2015
 - Singapore,
- Subject to sales tax :o(
 - Australia
 - Classification as property means 10% GST - Aug. 2014
 - Process is underway to redefine as money
 - Japan - 8% consumption tax
 - Diet finance committee debated repeal Feb. 2016

Takeaways

Takeaways

- Bitcoin applications have always been subject to regulation
- There is much more clarity today about how regulations apply, but not total
- Uncertainty and compliance is expensive, so clarity and consistency needed
- There is global policy competition, but broadly similar laws
- Regulation has been focused on custodians and exchangers
 - Promotes innovation in new risk models
 - This may change
- Challenges on the horizon:
 - More anonymity and decentralization (Zcash, decentralized anonymous markets, decentralized applications)
 - Protocol level regulation

Thank you.