

Virtual Currencies for Bankers: Thinking About New Ways to Pay

Payment Symposium
January 20, 2016

Jim Cunha, SVP
Federal Reserve Bank of Boston

jim.cunha@bos.frb.org

Agenda

- What is Bitcoin/bitcoin
- How it works
- Some bitcoin facts
- The Good, The Bad, and The Ugly
- Regulatory front
- What might the future hold
- Electronic legal tender
- What should banks do now

Currency Terminology

- Money – medium of exchange, store of value, unit of account
- Fiat Currency – Issued by a government, usually legal tender, not backed by anything specifically
- Commodity Currency – usually a precious metal used as money
- Representative Currency – something stands in to represent commodity money (e.g., gold certificate)
- Virtual Currency – none of the above three
- Crypto Currency – A virtual currency that relies on math and cryptography for its creation or validation

Bitcoin/bitcoin – The Facts

- Bitcoin = a payment system, bitcoin = a currency
- A math-based, private virtual currency
- No central authority, nothing backs bitcoins
- Open source = all rules, algorithms, security scheme are openly available
- Launched January 2009
- Currently about 15 million bitcoins issued, number of bitcoins is capped at 21 million, will reach capacity in 2140
- Currently, 25 bitcoins issued (“minted”) every 10 minutes (halved every 4 years)
- A bitcoin can be divided to 8 decimal places
- Market value of bitcoins ~\$6.4 billion
- CAN be very secure and CAN be anonymous

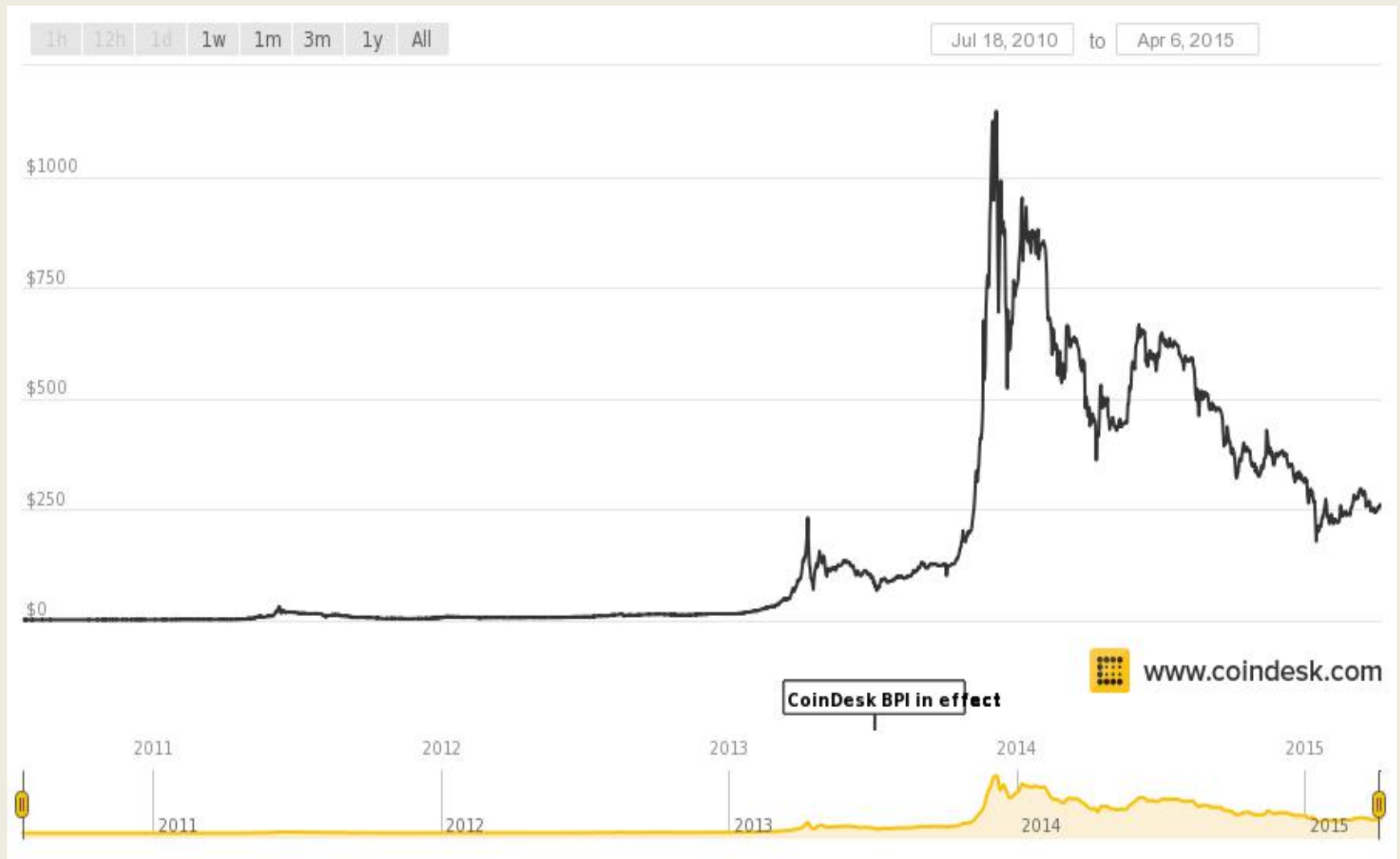
Bitcoin – Secret Sauce

- Block chain - A single distributed public ledger that records all transactions
- Public Key Encryption. Everyone has:
 - Public key – everyone can see this
 - Private key – you keep secret
 - I sign the transaction with my private key. Anyone can decrypt it with my public key and prove I signed it.
- Cryptographic Hashing
 - Publicly known series of calculations
 - Plus a variable
- Mining – The first to perform the complicated hash successfully, which is an expensive task, earns bitcoins
- When you request a bitcoin transaction, you can increase the incentive for a miner to process it quickly by adding a fee (aka tip)

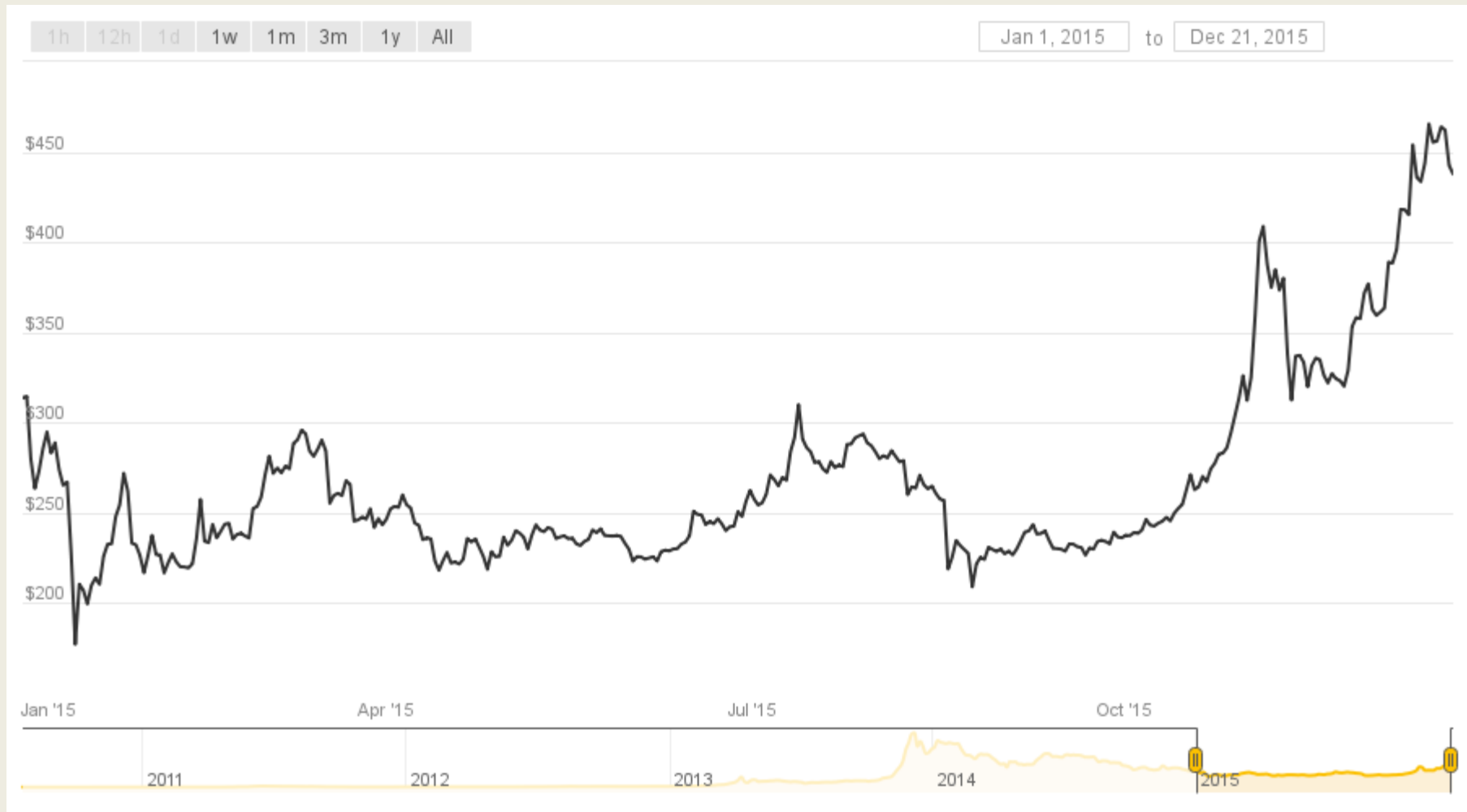
Bitcoin/bitcoin – Linda wants to pay Joe

1. Joe lets Linda know his public key (address for receiving bitcoins)
2. Linda signs the transaction with her private key and her Bitcoin wallet alerts Bitcoin miners everywhere about the transaction
3. Miners validate that Linda has the bitcoins, which involves a very complex calculation, and records the transaction in the block chain (about 10 minutes)
 - a) This calculation involves the actual transaction, a copy of the last valid transaction on the block chain, and a random number (“nonce”)
 - b) All the above are used to create a hash that proves the verification calculation was done
4. Other miners verify that the hash is accurate (which is a simple process) and update their block chains
5. The miner that solves the calculation gets 25 bitcoins and possibly a fee that Linda included
6. Linda and Joe can see that the transaction was complete and can finish the rest of their deal


Bitcoin Price Volatility 2011-Early 2015



Bitcoin Price Volatility 2015

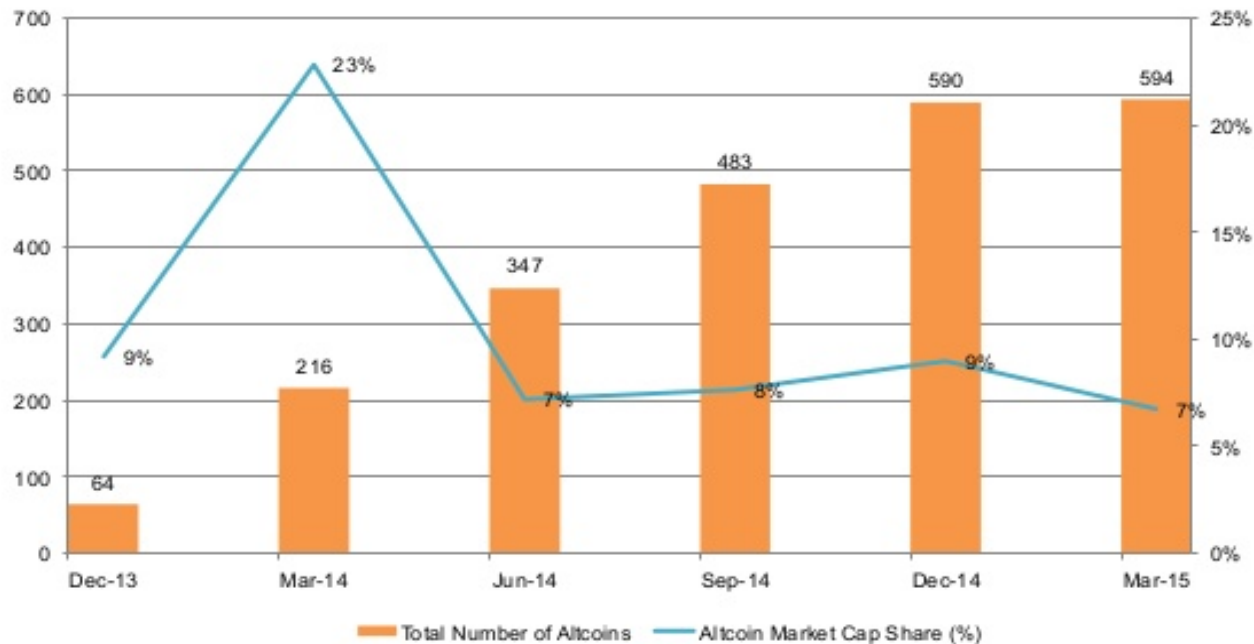


Market Capitalization

Symbol	Name	Market Cap	Price	Supply Issued/Sym	Volume 24 HR
1 	Bitcoin	\$ 6,479,287,913	\$ 430.48	15,051,275 BTC	\$ 32,881,700
2 	Ripple	\$ 201,449,005	\$ 0.006007	33,537,439,933 XRP	\$ 323,458
3 	Litecoin	\$ 151,916,526	\$ 3.46	43,933,048 LTC	\$ 1,961,320
4 	Ethereum	\$ 72,112,176	\$ 0.948230	76,049,245 ETH	\$ 296,049
5 	Dash	\$ 20,563,558	\$ 3.36	6,123,861 DASH	\$ 40,717
6 	Dogecoin	\$ 14,003,192	\$ 0.000137	102,544,664,665 DOGE	\$ 45,091
7 	Peercoin	\$ 9,202,641	\$ 0.401896	22,898,067 PPC	\$ 19,305
8 	Stellar	\$ 8,264,043	\$ 0.001708	4,837,356,606 LM	\$ 23,155
9 	BitShares	\$ 8,160,683	\$ 0.003216	2,537,344,209 BTS	\$ 40,439
10 	MaidSafeCoin	\$ 7,248,125	\$ 0.016016	452,552,412 MAID	\$ 9,491

Altcoin Numbers and Market Cap

Peak Altcoin? For the First Time, Quarter-over-Quarter Altcoin Growth Was Flat



*Note: Altcoin market cap share is calculated by dividing the sum of all non-bitcoin cryptocurrency market caps by all cryptocurrency market caps (including bitcoin). For example, a market value share of 7% for altcoins indicates that bitcoin by itself represents 93% of the market cap of all cryptocurrencies combined.

Data source: CoinMarketCap



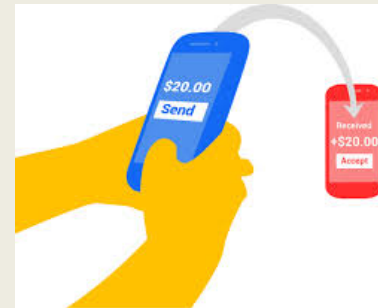
Inexpensive



Fast



Person to Person

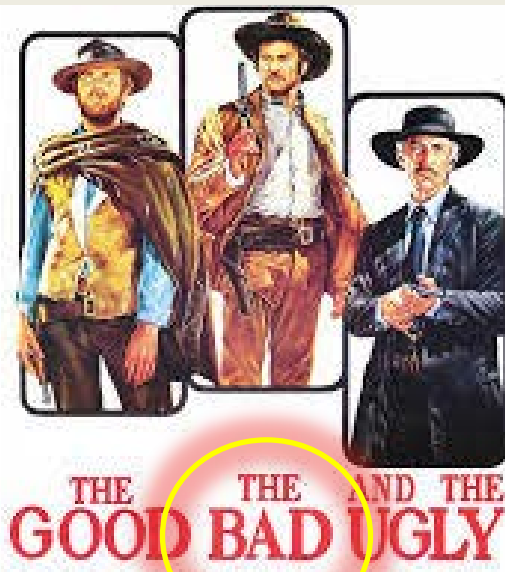


Trust



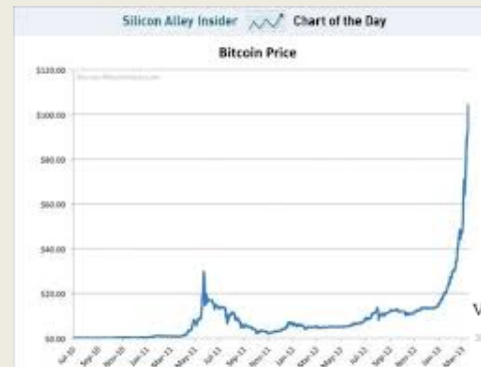
Anonymous



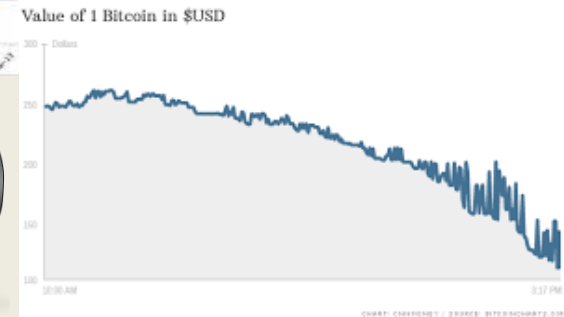


THE GOOD THE BAD AND THE UGLY

Who Do You Trust?



Volatile



Threatening to Banking Industry?



Criminal Activity



Mt. Gox - Before



Mt. Gox - After

Bitcoin – Regulatory Front

- **United States**
 - Federal Reserve – no authority to regulate
 - Treasury (FINCEN) – exchanges/processors are “Money Transmitters” and need to apply AML (Anti Money Laundering) safeguards
 - State of New York – issued new regulations to protect consumers and prevent illegal activity. One organization licensed.
 - California looked at licenses, but recently put the effort on hold
 - IRS – bitcoins are property, gains in value are taxable
 - Bank Regulators – don’t regulate bitcoins per se, but could impact AML/KYC, and banks safety and soundness
 - CFPB/SEC – issued advisory/investor alert
- FATF – Financial Watchdog Rethinks AML Guidance for Banks and Bitcoin
- China – bitcoin is not a currency and should not be used
- Iceland – may violate Icelandic Foreign Exchange Act
- Russia – using bitcoins is a misdemeanor and imposes fines
- Canada – like US, mainly focuses regulation on AML
- Norway, Portugal – property with gains taxed

Interesting Headlines – December 2015

- Chain Issues Investor Shares on Nasdaq Blockchain Platform (Linq)
- Visa Europe: The Blockchain is 'No Longer a Choice'
- 12 More Banks Join Blockchain Consortium R3
- IBM Creates Open-Source Blockchain With Linux and Big Banks
- DBS, Standard Chartered Develop Distributed Ledger for Trade Finance
- SEC Approves Overstock's Plan to Issue Blockchain Securities
- ING Exec: 'All Our Business Lines' Involved in Blockchain Exploration
- Deutsche Bank: Blockchain Tech Will Go Mainstream in Next Decade
- Goldman Sachs: Blockchain is Ready For Centre Stage
- Goldman Sachs Seeking Crypto Trade Settlement Patent

Who is Working in the “Blocktech” Space?

BLOCKTECH in FINANCIAL SERVICES VIRTUALscape

by William Mougayar

APPLICATIONS & SOLUTIONS



MIDDLEWARE & SERVICES



INFRASTRUCTURE & BASE PROTOCOLS



Bitcoin – The Future?

- I doubt that the bitcoin currency will be broadly adopted in the US or abroad, nor will any other virtual currency in the next 10 years, if ever
- However, the Bitcoin technology, specifically the block chain, could be leveraged for other purposes
 - Deeds, Titles
 - Contracts (self-enforcing “smart”)
 - Securities (when combined with above, a repurchase agreement (REPO) that cannot fail to settle)
- Might we see a Bitcoin-like network that carries electronic legal tender issued by the government (Cunha Cash)?



Bitcoin – Electronic Legal Tender?

- Similarities between Cash and Cunha Cash
 - Both could be anonymous
 - Both would be uniquely identifiable (dollar serial number)
 - Both require strong security features
 - Both could be “issued” by Fed/Treasury and distributed through banks
- Benefits of Cunha Cash
 - Cash is expensive to produce, process, transport, store. Electronic legal tender should be much cheaper
 - Could pay anyone anywhere instantaneously
 - Could help unbanked
 - World is shifting to instantaneous everything



Electronic Legal Tender- Open Questions?

- Lots of them
 - Legal tender must be accepted for debts public and private
 - Security concerns
 - If successful, counterfeiting could be a huge risk
 - Distributed Denial of Service (DDoS) attacks could impact commerce
 - Seigniorage
 - Privacy concerns versus KYC/AML
 - Centralized versus distributed authentication
 - Public ledger versus private accounts
 - Does electronic legal tender disrupt or complement existing players (debit/credit brands, banks)?



Bitcoin – So, what should banks do?

- **Don't panic!**
- Keep abreast of developments in virtual currencies and related regulations (Coindesk.com is a good source)
- If asked to be a party to a Bitcoin/virtual currency transaction, talk to your regulator
- Look at the technologies supporting virtual currencies
 - Are they applicable to other business transactions?
 - Ask your service provider what they are doing
- **Don't panic!**