Presenters

Peter Luce
Associate
Payment Systems

Jerry Wang
Associate
Intellectual Property and Technology
Agenda

1. How Crypto-Currencies Work: Bitcoin Example
2. Where Crypto-Currencies Fit In The Regulatory Framework
3. Crypto-Currency Ecosystem: Key Players and Business Models
4. Opportunities and Trends for Financial Institutions
5. Beyond Bitcoin: Decentralized Apps
6. Questions/Answers
1. How They Work: Background on Virtual Currencies

Not a New Concept:
- Private and local currencies go back centuries
- Digital currencies proposed in 80s and 90s
- **E-Gold:** 1999: backed 100% by gold bullion, other precious metals
- **Merchant-specific:** Facebook Credits, Amazon Coins
- **MintChip:** Canadian government-backed digital currency
- **Liberty Reserve:** tied to dollar and euro

So Why Now?
- 2008 Financial Crisis/Loss of faith in banking
- Fiat Currency Crises in Cyprus, Greece, Argentina, others
- Chinese currency exportation prohibitions
- Continued irritation with bank payment inefficiencies and costs
- **Technology breakthrough**
1. Why Bitcoin Was Created

Limitations of Incumbent Payment Systems:

- **Limited Access**:
  - Credit/debit not universally accepted
  - 50% of world population has no access to banking systems*
  - Credit and savings vehicles not available to unbanked/underbanked

- **High Costs**:
  - Fees: Interchange, Bank Fees, Payment Networks, Processors, ISOs
  - Infrastructure and compliance investment (POS, PCI/Security, KYC)
  - Chargebacks, reversals, refunds, fraud

- **Liquidity “Islands”**: moving small amounts of money around the world quickly and cheaply is very difficult

- **Privacy**: Internet transactions require sharing of personal data with third parties

- **Security**: inflation, devaluation, asset seizure, currency export controls

*Global Findex Database, 4/2012
1. What is Bitcoin? Reality vs. Myth

- **Above all, Bitcoin is a Platform:**
  - A Protocol: an open set of standards for communication
  - A Network: self-regulating, self-propagating
  - A Currency: universal and independent
  - A Payment System: medium for the exchange of value, and a public ledger
1. What is Bitcoin? Reality vs. Myth

**Bitcoin is the:**

- First (there are numerous others – Litecoin, XRP, Freicoin, etc.)
- Open-source (non-proprietary code = strength in transparency)
- Decentralized (no issuing authority)
- Peer-to-Peer (cash-like electronic transactions, no intermediary)
- Digital (built for the Internet)
- Alternative (not a replacement of fiat currencies)
- Cryptographic (based on principles of proven cryptography)
- Currency (medium of exchange, store of value, unit of value?)

**Bitcoin is not:**

- Anonymous (but it is pseudonymous)
- Risk-Free (it can be stolen/lost/hacked, just like cash)
- A Substitute for Government/Banks/Payment Networks (complementary - symbiotic)
- Free
1. The Fundamentals: Cryptocurrency: How Bitcoin Works

How a Bitcoin transaction works:

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

- **Wallets and Addresses**: Bob and Alice both have Bitcoin "wallets" on their computers.
- **Creating a New Address**: Bob creates a new Bitcoin address for Alice to send her payment to.
- **Wallets**: Wallets are files that provide access to multiple Bitcoin addresses.
- **Address**: An address is a string of letters and numbers, such as 1HULMwZEPkjEPCeh43BeKJ1ybLCWrFDpN.

Each address has its own balance of bitcoins.

Source: http://spectrum.ieee.org
1. How Bitcoin Works

Public Key Cryptography:

Elements of a Bitcoin Transaction:

- **Sender's Account Address:**
  Account ID = Public Key

- **Sender's Message:**
  “Transfer 1 BTC from Account A to Account B” (includes Account B’s Public Key Address)

- **Sender's Signature:**
  Transaction Message must be signed with Sender’s Private Key = “Password”

Source: http://spectrum.ieee.org
1. How Bitcoin Works

Transaction Verification: Mining

Consensus: verify key pairs
  +
Competition: incentive
  +
Proof of Work: complex math
  +
Reward: more Bitcoins*
  =
Successful Transaction

*And transaction fees...more on that later

Source: http://spectrum.ieee.org
1. How Bitcoin Works

But How Does It Really Work?

- **Miners** compete to solve **Blocks**
- **Blocks** = bundles of individual transactions (10 min. intervals)
- When Block is solved by a **Miner**, it is added to the **Blockchain**

**Blockchain:**
- Record of all Bitcoin transactions that have ever occurred
- Public Ledger of Accounts
- Extraordinarily difficult to hack
- Uses state of the art, industry standard cryptography
- (ECDSA + SHA 256)

Source: http://spectrum.ieee.org
1. How Bitcoin Works

- **Reward**: Winning Miner(s) rewarded with new Bitcoins
- **Built-In System Security**: Security increases with each cycle, or block (crypto-layers)
- **Velocity Controls**: Work required to earn Reward increases as network power grows
- **Other Key Points**:
  - Only 21 Million Bitcoins will ever exist (~11.96M today)
  - Bitcoins divisible to one hundred millionth of a Bitcoin (a “satoshi”) or $0.00000325
  - Last Bitcoin will be created in approximately 2140

Source: http://spectrum.ieee.org
### 1. Bitcoin Pros and Cons

<table>
<thead>
<tr>
<th><strong>PROS</strong></th>
<th><strong>CONS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ubiquity</strong>: send Bitcoin to anyone, anywhere…</td>
<td><strong>Small Community</strong>:…who has access to the Internet and a Bitcoin address; complicated</td>
</tr>
<tr>
<td><strong>Cash-like</strong>: easy to transfer, secure, and authenticate</td>
<td><strong>Cash-like</strong>: vulnerable to loss, theft</td>
</tr>
<tr>
<td><strong>Transactions Final, Irreversible</strong></td>
<td><strong>Transactions Final, Irreversible</strong></td>
</tr>
<tr>
<td><strong>Extremely Fast Settlement</strong>: much faster than ACH, SWIFT, Wire Transfer, and credit settlement time frames</td>
<td><strong>Slower Verification</strong>: card-based authorization in milli-seconds; full Bitcoin transaction verification at least 10 minutes, more for larger transactions</td>
</tr>
<tr>
<td><strong>Shiny and New</strong> - early adopter glow; high disruption potential; extremely sophisticated technology</td>
<td><strong>Slow Adoption</strong>: not well understood; lack of trust in currency not backed by govt.; regulatory concerns</td>
</tr>
</tbody>
</table>
## 1. Bitcoin Pros and Cons (Cont.)

<table>
<thead>
<tr>
<th>PROS</th>
<th>CONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inflation Resistant:</strong> limited supply of Bitcoins protects against inflation</td>
<td><strong>Bitcoins Scarce by Design:</strong> price fluctuation = settlement risk, hoarding</td>
</tr>
<tr>
<td><strong>Low Transaction Costs:</strong> enables true micropayments</td>
<td><strong>Transaction Fee Problem:</strong> sufficient reward for miners once last Bitcoin has been minted</td>
</tr>
<tr>
<td><strong>Extremely Secure:</strong> built on state of the art encryption standards: (same schemes used by banks, ISPs, etc.)</td>
<td><strong>But Not Invulnerable:</strong> susceptible to user/vendor error; loss and theft; no built in consumer protections</td>
</tr>
<tr>
<td><strong>Regulatory Approval:</strong> US Senate Hearings; IRS; many U.S. states already granting licenses to exchanges</td>
<td><strong>Regulatory Uncertainty:</strong> FinCEN and KYC; consumer protection concerns; State MTL compliance; Reg. E, FTC</td>
</tr>
<tr>
<td><strong>Decentralized, distributed network:</strong> Internet-like resilience</td>
<td><strong>Scalable?</strong> Visa = 4,000 tps Bitcoin = 7 tps (today)</td>
</tr>
</tbody>
</table>

Visa = 4,000 tps
Bitcoin = 7 tps (today)
1. Bitcoin Fluctuation Risks

**Present**
- Immature Market
- Disconnected exchanges
- Lack of Liquidity
- Uneven regulation, access

**Future**
- Professional, connected exchanges
- Derivatives market
- Regulatory clarity

---

This chart is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License.
2. How Crypto-Currencies Fit in Regulatory Environment

Regulatory Issues: FinCEN Guidance: 3/18/2013

- **Currency**: “the coin and paper money of the United States or of any other country that (i) is designated as legal tender and that (ii) circulates and (iii) is customarily used and accepted as a medium of exchange in the country of issuance.” (Bank Secrecy Act definition)

- **Virtual currency**: “medium of exchange that operates like a currency in some environments but does not have legal tender status in any jurisdiction.”

- **Convertible virtual currency**: virtual currency that has an equivalent value in real currency, or acts as a substitute for real currency.

- Outlines regulatory treatment of persons engaged in virtual currency transactions under the definitions of dealers in foreign exchange and money transmitters under the Bank Secrecy Act.
Three Roles in Virtual Currency Environments:

- **User**: a person that obtains virtual currency to purchase goods or services. User is not an MSB under the FinCEN regulations (in same way user of currency is not an MSB)

- **Exchanger**: person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency

- **Administrator**: 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
Three Categories of Convertible Virtual Currency: Characteristics

- **Centralized Virtual Currencies**: Administrator-controlled, central repository (E-Gold, Liberty Reserve, Linden Dollars on Second Life virtual world): administrators and exchangers of centralized virtual currencies are MSBs.

- **E-Currencies and E-Precious Metals**: Trading of digital certificates representing real positions in a real currency or real precious metal; brokers or dealers are MSBs if they transfer funds between a customer and a third party who is not part of the currency or commodity transaction.

- **Decentralized Virtual Currencies**: Virtual currency that has no single administrator and no central repository, persons may obtain the virtual currency through their own computing effort. You are an MSB if you:
  
  - create units of decentralized convertible virtual currency and sell those units to another person for real currency or its equivalent (But not an MSB if used to purchase real goods and services).
  
  - accept decentralized convertible virtual currency from one person and transmit it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency.
Prepaid Access Rule:

- “A person’s acceptance and/or transmission of convertible virtual currency cannot be characterized as providing or selling prepaid access because prepaid access is limited to real currencies.”

Prepaid Access: limited to access of funds or value of funds.

Footnote: “If FinCEN had intended prepaid access to cover funds denominated in a virtual currency or something else that substitutes for real currency, it would have used language in the definition of prepaid access like that in the definition of money transmission, which expressly includes the acceptance and transmission of “other value that substitutes for currency.”
Dealers in Foreign Exchange:

- Person must exchange the currency of two or more countries to be considered a dealer in foreign exchange.

- Because virtual currency is not legal tender, a person who accepts real currency in exchange for virtual currency is not a dealer in foreign exchange.
Refinements: January 2014 Letter Rulings

- Miners are not MSBs:
  - Clarifies initial guidance: if a miner receives a Block Reward and sells those Bitcoins for cash - not an MSB

- Bitcoin Investments not MSBs:
  - Companies that invest in Bitcoins of their own account are not MSBs, but if offering investment or brokerage services, then subject to BSA/AML requirements
  - Providing software to enable bitcoin sales not money transmission
2. Evolution of Regulatory Landscape

- **Early Law Enforcement Focus:**
  - **2012 FBI Report:** concerns over criminal activity (illicit drugs, weapons, child pornography)
  - **Seizure of Mt.Gox assets:** Summer 2013: >$5M in U.S. Accounts seized by DHS for operating an unlicensed MSB
  - **Silk Road Bust:** Fall 2013: DOJ now in possession of ~25K Bitcoins

- **To Regulatory Clarity:**
  - **Are Bitcoins “Money”?**
    - **FEC:** Bitcoins are not money (“in-kind contributions”)
    - **IRS:** Bitcoin is Property: taxation guidance
    - **Congress:** Senate hearings held Nov 2013
  - **State Licensing:** Very few Bitcoin companies have successfully obtained MTLs; applicability of state laws unclear
  - **WA:** Jan. 2014: Bitcoin is “money” for state MTL purposes
  - **NY DFS Hearings:** Jan. 2014: “Bitlicenses” likely
  - **TX:** April 2014: crypto-currency exchanges must be licensed
2. Evolution of Regulatory Landscape

**Future Issues:**

- **Consumer Protection:**
  - Applicability of state and federal laws
  - EFTA and Regulation E
  - Remittance Rule

- **State and federal Securities Laws**

- **Commodity Trading Rules**

- **Banking Law: Third Party Service Provider Rules**
3. Crypto-Currency Ecosystem: Players

- Miners
- Exchangers
- Wallet Providers
- Payment Processors
- Merchants
- Others
3. Crypto-Currency Ecosystem -> Miners

Miners: Some individuals, but increasingly, Groups or “Pools” using specialized hardware = rewards split (already commoditizing)
3. Crypto-Currency Ecosystem - Exchanges

**Bitcoin Exchanges:**
How to Get Bitcoins

- **B2C:**
  - Mt. Gox
  - BitStamp
  - CampBX
  - BTC China
  - Dozens of others

- **B2B:** institutional; large funds transfer
  - Kraken
  - CoinX

- **Exchange Software Platforms**
  - AlphaPoint
  - Buttercoin
3. Crypto-Currency Ecosystem -> Wallet Providers

Wallet Providers:

- Coinbase (hosted)
- Circle Internet Financial (Hosted)
- StrongCoin (hosted hybrid)
- BlockChain.info (hosted hybrid)
- Armory (desktop)
- Electrum (desktop)
- Bitcoin QT (desktop)

User-friendly: ☑️

Complex: ☐
3. Crypto-Currency Ecosystem -> Payment Processors

**Payment Processors:**
- Accept Bitcoins
  - BitPay
  - Coinbase
  - Circle
  - Square*
  - Stripe*

Create A Payment Button

- Payment Type: Buy now, Donation, Subscription (coming soon)
- Button Style: Pay with Bitcoin
- Item Name: Alpaca Socks
- Price: BTC 10.00
- Item Description: The ultimate in lightweight footwear
- Custom ID: ORDER1234 (optional, used to link an item back to your records)
3. Crypto-Currency Ecosystem -> Merchants

- shopify
- WordPress
- eGifter
- TigerDirect.com
- gyft
- zynga
- foodler
- okcupid
- overstock.com
- reddit
- CheapAir.com
- CHICAGO SUN-TIMES
3. Consumer Checkout Experience

Payment Information

- **Credit / Debit card**
  - Visa, Mastercard, American Express, Discover

  Card Number *
  
  Expiration Date *
  
  01 Jan ▼ 2014 ▼

Order Summary

- **Subtotal:** $399.99
- **Promo Savings:** $40.00
- **Shipping:** FREE

- **Total:** $359.99

Select Delivery & Gift Options

- **This order is being sent as a gift.**

- **Yes, I want FREE shipping and 5% back in Club O Dollars on this order.** Learn More

Items

<table>
<thead>
<tr>
<th>Options</th>
<th>Price</th>
<th>Shipping Options</th>
</tr>
</thead>
</table>

By clicking the box, you accept our terms and conditions.
3. Paying With Bitcoin

- Bitcoin uses QR Codes to encode payment information, but merchants can also integrate directly with wallet providers.
- Prices listed in dollars; payment processor converts to bitcoin.
3. Overstock.com: early results

- $1M in sales in first two months
- Averaging $30-$50,000 per day in Bitcoin sales
- $10-15M in Bitcoin sales projected in first year
- Bitcoin users spend 34% more on orders vs. credit card users
- Retaining 5-10% of Bitcoins received in reserve as hedging strategy
3. Crypto-Currency Ecosystem: Bitcoin Investment Vehicles

Hedge Funds and Bitcoin Investment Vehicles

EXANTE

Next Generation Prime Broker

Bitcoin Fund exclusively available on EXANTE’s platform

The fund that invests in the economy of the next generation. 1 Fund Unit = 1 Bitcoin.

secondmarket
3. Crypto-Currency Ecosystem: Self-Regulation and Advocacy

DATA
Digital Asset Transfer Authority

News

Following the summer 2013 announcement by the Committee on Digital Asset Transfer Authority, work has been underway to accomplish a number of objectives. The Committee met September 30, 2013 in San Francisco, with the purpose of laying the groundwork for the formation of a 501(c)6 Delaware based organisation with offices in New York and London.

DATA Membership

Membership to DATA is now open to digital asset companies and others beginning with Friends of DATA. Junior and Full Membership rights within DATA, while the Junior Member programme provides support for new and emerging digital asset companies. A Patron programme provides additional benefits for related companies that wish to support DATA efforts.

DATA dues are payable in traditional flat currency. Bitcoin or equivalent.

FRIENDS $1,000

Individuals, organisations and others who advise or support DATA

Bitcoin Foundation

- About
- Members
- Join Us
- Donate
- Blog
- Forum
- Contact
- Login

Developing a More Open Economy

Our mission is to help people exchange resources and ideas more freely.

We approach that mission with Bitcoin’s technology and community as our focus. There is tremendous potential in Bitcoin—from the opportunities it creates for entrepreneurs to the purchasing power it provides for citizens of countries large and small. Our goal is to help Bitcoin deliver on that potential.

Bitcoin Foundation has chosen three primary objectives for fulfilling its mission. We believe that these activities will be of the greatest benefit to the Bitcoin community.
4. Opportunities for Financial Institutions

- **Partner with Virtual Currency Companies:**
  - Exchanges, Payment Processors need bank accounts
  - Compliance Due Diligence: work with firms that understand compliance

- **Explore Issuance of New Financial Products:**
  - Debit Cards with Bitcoin Purse
  - Virtual currency-backed GPR Cards

- **Bitcoin Wallet = Checking Account?**

- **Leverage Existing Merchant Relationships**

- **B2B Funds Settlement:** direct challenge to ACH/wires
4. Future Role in Faster/Near-Real-Time Payments

- Fed: Apply to faster, near-real-time payments initiative?
- Leverage open source code to modernize incumbent systems
- Upgrade EMV to digital payment?

Payment System Improvement - Public Consultation Paper

The Federal Reserve Banks

September 10, 2013

The U.S. payment system is undergoing a remarkable period of change, driven by rapid adoption of technology and evolving end-user expectations. Going forward, opportunity exists to improve speed and efficiency of payments and to maintain payment system safety in the face of escalating threats. The Federal Reserve Banks believe that collaboration and engagement with the industry is the foundation of any enduring strategic improvements to the U.S. payment system and look forward to public input to this consultative paper.
5. Beyond Bitcoin: Emerging Possibilities

- Emergence of open payment networks
- Ripple
- Distributed Applications
5. Beyond Bitcoin: Open Payment Networks

From centralized and fragmented:

E-Mail Messaging:

Payments:
5. Beyond Bitcoin: Open Payment Networks

...to distributed and interoperable.
5. Beyond Bitcoin: Distributed Application Platforms

- Utilize cryptography and the Bitcoin concept of a distributed public ledger to enable:
  - Smart contracts
  - Custom currencies
  - Identity management
  - Physical and digital property ownership authentication
  - Decentralized currency and stock exchanges
  - Derivatives markets
  - Decentralized autonomous corporations
Peter T. Luce
Davis Wright Tremaine LLP
Washington, DC
202.973.4251
peterluce@dwt.com

www.paymentlawadvisor.com
http://www.paymentlawadvisor.com/virtual-currency-resources/
This presentation is a publication of Davis Wright Tremaine LLP. Our purpose in making this presentation is to inform our clients and friends of recent legal developments. It is not intended, nor should it be used, as a substitute for specific legal advice as legal counsel may only be given in response to inquiries regarding particular situations.

Attorney advertising. Prior results do not guarantee a similar outcome.

Davis Wright Tremaine, the D logo, and Defining Success Together are registered trademarks of Davis Wright Tremaine LLP.

© 2014 Davis Wright Tremaine LLP