



# ***A Virtual Currency Primer: What You Need to Know***

**EPCOR Payments Conference  
October 24, 2016**

Pam Cerny, AAP, CTP  
Federal Reserve Bank of Dallas



## The Requisite Disclaimer...

The views expressed are those of the presenter only, and do not necessarily represent the views of the Federal Reserve Bank of Dallas or the Federal Reserve System



# Virtual Currency (VC)

- “A type of stored-value product or digital money...issued and usually controlled by its developers, and used and accepted among the members of a virtual community.”  
(FRB Board)
  - a.k.a. digital currencies, alternative currencies, cryptocurrencies, altcoins; decentralized Internet protocols
- Not issued by a federal government (“fiat currency”) or backed by a central bank
- Generally used in electronic, Web-based transactions



# Virtual Currencies

- “Open source”
  - All rules, algorithms, security scheme, etc., openly available
- May involve legal, credit, liquidity, fraud, operational, information security, privacy, law enforcement, and other payment system risks



# Potential Benefits of VCs

- Reduction in transaction costs
  - Especially for cross-border transactions
  - Possibly for merchant processing
- Useful in countries where:
  - Social or political climate may lead to distrust of local currencies and
  - There is a high degree of Internet connectivity



# Potential Benefits of VCs

- Opportunities in areas like “smart contracts,” notary services and tracking asset ownership
  - See “blockchain” below...



# Bitcoin



- Launched 2009 (“Satoshi Nakamoto”)
- Permits transfer of currency online, directly, anonymously and outside government control
- Origins: Fundamentally political; attracted followers among libertarian and anarchist groups
  - A means of removing the money supply from the hands of government
- Subsequently attracted attention from computer developers, venture capitalists, and merchants (alternative to traditional payments)



# Bitcoin

- All transactions are recorded in the “blockchain”
- Searchable public ledger where all transactions are confirmed, in a matter of minutes, by a network of computers working to perform complex algorithms
- New bitcoins are created through “mining”
  - The first to perform the complicated hash correctly earns bitcoins
  - When you request a bitcoin transaction, you can increase the incentive for a miner to process it quickly by adding a fee (a.k.a. tip)
  - The average person can’t really be a bitcoin miner, because of the computing power now required





# Blockchain

- Each part of the network maintains a copy of the ledger
- About 6 times an hour, a new group of accepted transactions—a block—is created, added to the chain and broadcast to the other parts of the network
- Thus, all transactions are recorded and linked and can be traced
- It is nearly impossible to modify past blocks in the chain
- By downloading Bitcoin software, anyone can gain access to the Blockchain, search it and submit transactions to the network

SOURCE: "Data Security Is Becoming the Sparkle in Bitcoin," by Sydney Ember, *The New York Times*, Mar. 1, 2015



# Blockchain

- “When many of the players in payments talk about the power of bitcoin these days, they aren’t talking about bitcoin at all.” —pymnts.com, Mar. 6, 2015
- VCs could change the traditional financial system, but also the way we transfer and record financial assets like stocks, contracts, property titles, patents and marriage licenses...
  - ...anything for which we have traditionally used a trusted “middleman” for verification



# Blockchain

- May reduce potential for single point of failure in the case of operational issues or cyber-attack:
  - Reduces interconnectedness among various parties
  - If one point in the network of nodes fails, the other points in the network are still available with the same information.

SOURCE: "A Conversation with Blythe Masters," in *Morgan Stanley Global Insight: Blockchain in Banking: Disruptive Threat or Tool?*, April 20, 2016



# Blockchain

- “Imagine getting in your car...
- Through your mobile device, the car locates your identity code and proof of purchase in the Blockchain...
- This allows the car to start...
- But say you have missed 3 payments on your car loan...
- Additional terms in the Blockchain make sure the car will only start for the person or institution that lent you the money.”

SOURCE: “Do Cryptocurrencies Such as Bitcoin Have a Future,” *WSJ*, Mar. 2, 2014



# Bitcoin

- Can be traded on a number of exchanges, or privately
- Can be divided to 8 decimal places
- Finite supply of 21m bitcoins can be created; determined by an algorithm
  - 14m currently in existence
  - 25 bitcoins created every 10 minutes (halved every 4 years)



# Bitcoin - Security

## ■ Public Key Encryption

### – Everyone has:

- Public Key: Everyone can see this
- Private Key: Secret
- I sign a 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



# Bitcoin

- Highly-volatile exchange rate:
  - Jan. 2013: **\$14** (Mt. Gox)
  - Nov. 28, 2013: **\$1,172** (WSJ, 11/29/2013)
  - October 10, 2016: **\$615.85** (Coinbase)
- “80% of all activity on the Coinbase app is people buying, selling, and storing bitcoin as an investment, and only 20% of the time is it used as a wallet for day-to-day spending.”\*

SOURCE: “What a Tech Startup’s Pivots Say About Bitcoin’s Future,” by Penny Crosman, AmericanBanker.com, April 12, 2016



# Issues - Volatility

- Can a currency with this level of volatility be an effective medium of exchange?
- Mitigants:
  - Services like Coinbase and BitPay can shield merchants from volatility risk by using instant exchanges
    - When orders come in, Coinbase instantly converts Bitcoin to USD so merchants don't bear exchange risk
  - Bitcoin exchanges can charge trading fees to discourage speculative trading





# Bitcoin & Merchants

- Some merchants accept VCs/bitcoin as payment for goods and services
  - Overstock.com (Jan. 2014)
    - Bitcoin payments save Overstock credit-card acceptance fees; Overstock offered incentive to customers paying with bitcoin: 1% back on purchases (in-store credit)
  - Others: Sacramento Kings (NBA); TigerDirect, Newegg, DISH, Expedia, Dell, Wikipedia, United Way, Google
  - Most merchants (e.g. Overstock) contract with a service (e.g., Coinbase), which converts consumers' bitcoins into dollars and transfers dollars to the merchant



# Bitcoin & Merchants

- Bitcoin transaction costs are generally cheaper than those associated with credit/debit cards.
  - Fees for credit card acceptance average 2-3%
  - Fee for a service like Coinbase is around 1%



# Bitcoin & Merchants

- Bitcoin does not allow chargebacks
  - At least theoretically, less protection for consumers
  - On the flip side, more protection for merchants



# Issues – AML/BSA/USA Patriot Act

- Compatibility with AML/BSA/USA Patriot Act
- Blockchain provides an audit trail, making it easy to track potential illicit activity
  - But individual users remain anonymous; difficult or impossible to determine who is conducting transactions or moving funds
- Federal regulators may need to clarify: How far is an FI expected to go in monitoring its customers' customers after they convert dollars to VC or vice versa?
  - Should the FI treat a bitcoin transaction like an ATM withdrawal?



## Issues – AML/BSA/USA Patriot Act

- To comply with BSA, and avoid running afoul of federal laws banning unlicensed money transmitters...
- ...Money transmitters (e.g. Western Union; PayPal) are required to enact AML controls, file SARs, register with FinCEN and obtain state licenses in 47 states that require them (and D.C.)
  - State licensing process can be arduous; expensive



# Issues – Theft

- Theft
  - No consumer protection
  - Mitigation: Storing bitcoins in “cold storage” (i.e., on machines that are not connected to the Internet.)





## Issues – Infrastructure

- Infrastructure: Can the existing infrastructure support an increasing number of payments?
- Verification of a Bitcoin transaction might take 10 minutes



# Issues: Bitcoin & The Banking System

- Risk/Issue: Bridging VCs/Bitcoin with the traditional banking system
  - Bitcoin exchanges, payment processors and other startups need banks/CUs to connect them to the existing payments system and provide basic services like checking accounts
  - To do that, the companies must convince bank regulators that bitcoins aren't being used to conceal illicit activity





# The Fed & Bitcoin

- “Bitcoin is a payment innovation that’s taking place outside the banking industry. To the best of my knowledge, there's no intersection at all in any way between Bitcoin and banks the [Fed] has the ability to supervise or regulate. The [Fed] simply doesn’t have the authority to supervise or regulate Bitcoin in any way.”
- “Certainly, it would be appropriate for Congress to ask questions about what the right legal structure would be for digital currencies.”
- However, it’s “not so easy to regulate because there’s no central issuer or network operation.” —Janet Yellen, Feb. 2014



# The Fed & Bitcoin

- “At the Fed... we approach these issues from the perspective of policymakers safeguarding the public interest in safe and sound core banking institutions, financial stability, particularly as it pertains to the wholesale financial markets, and the security and efficiency of the payment system...
- As we engage with industry and stakeholders to assess the potential applications of digital ledger and related technologies in the payment, clearing, and settlement arena, we will be guided by the principles of efficiency, safety and integrity, and financial stability.” —Federal Reserve Gov. Lael Brainard

[“The Use of Distributed Ledger Technologies in Payment, Clearing, and Settlement.”](#) Governor Lael Brainard, at the Institute of International Finance Blockchain Roundtable, Washington, D.C., April 14, 2016



# FinCEN

- March 2013: U.S. Treasury's FinCEN issued guidance regarding treatment of users, exchangers and administrators of decentralized VCs
  - Exchangers and administrators who transmit, buy or sell VC are considered money transmitters under FinCEN regs
  - Companies operating VC exchanges are now likely subject to BSA requirements and must register with FinCEN as money services businesses (MSBs)



## States – Kansas

- June 6, 2014: Office of the State Bank Commissioner issued Guidance Document MT 2014-01
  - Cryptocurrencies are not considered “money” or “monetary value” by the OSBC and are not covered by the KMTA
  - Exchange of cryptocurrency for sovereign currency between two parties is not money transmission under the KMTA
  - Exchange of one cryptocurrency for another cryptocurrency is not money transmission



## States – Kansas

- Guidance Document MT 2014-01 (cont'd):
  - Exchange of cryptocurrency for sovereign currency through a third party exchanger is generally considered money transmission and thus would need to be licensed
  - Exchange of cryptocurrency for sovereign currency through an automated machine may or may not be money transmission
    - Machines that act as intermediaries between buyers and sellers of the currencies would fall under the definition of money transmitters, while machines that do not involve third parties would not



## States – CSBS

- 12/2014: Conference of State Bank Supervisors (CSBS) Emerging Payments Task Force released its model for regulating VCs at the state level
  - Commissioner Cooper is a member of the Task Force
- Model allows states to decide if they want to create new structures (e.g. NY DFS BitLicense) or regulate new currencies under existing rules (e.g. Kansas)
- In many ways, similar to the NY DFS BitLicense proposal



## States – CSBS

- Model regulatory framework targets businesses that exchange, transmit, hold and/or control VC
  - Recommends these businesses be subject to state licensure and supervision
  - Requirements cover wallets, vaults, merchant acquirers, payment processors and kiosks, such as Bitcoin ATMs



## States – Others

- New York Division of Financial Services (NYDFS)
  - VC firms must obtain “BitLicense” and hold higher levels of capital
- “California State Legislators Halt Bill to Create BitLicense,” AmericanBanker.com, Aug. 15, 2016
  - “Shelved”





# Uniform Law Commission

- Uniform Law Commission: model Virtual Currency Businesses Act
- Slated to be finalized summer 2017

See "How Treasury Is Trying to Shape State Digital Currency Regs," by Lalita Clozel, AmericanBanker.com, March 30, 2016



## Despite the various issues...

- “Protocols like Ripple and Stellar are ‘getting rid of bilateral legacy processes that banks have been using for years to keep money in their pockets.’” —Cheryl Gurz, managing director, emerging technology segment, BNY Mellon Treasury Services
  - See, for example, Ripple...

SOURCE: “Cryptocurrency Technology Set to Shake Up Correspondent Banking,” by Sarah Todd, AmericanBanker.com, Mar. 3, 2015



# Ripple

- [www.ripplelabs.com](http://www.ripplelabs.com)
- “Ripple network provides a direct connection between banks in the network, enabling the secure, real-time movement of money 24/7.”
- “Ripple electronic ledger relies on a distributed network of trusted institutions—a few dozen known “validators”—to settle transactions in any currency pair every 5 seconds as new transactions are encrypted into it.”
- “Ripple doesn’t require consensus nodes to carry the whole ledger of all transactions that ever happened. Instead, nodes only need to use the ‘last closed ledger’ to come to agreement on the changes to the present ledger.”

SOURCE: “Bitcoin Tech: Catching On with Treasurers?” by John Hintze, [afponline.org](http://afponline.org), Aug. 7, 2015; “A Very Public Conflict Over Private Blockchains,” by Bailey Reutzel, *PaymentsSource*, July 13, 2015



# Ripple

- Has several bank clients
- May 2015: Fined \$700,000 by FinCEN over BSA violations

See "Ripple Labs Fined for AML Violations, Agrees to Change Protocol," by Sarah Todd, AmericanBanker.com, May 5, 2015



# Overcoming Limitations?

- Most new blockchain proposals are looking at:
  - Limited participant nodes (“permissioned” ledger; only permitted, known participants can validate transactions);
  - Centralizing all or part of the blockchain ledger;
  - Paring the blockchain ledger under certain circumstances;
  - Making blockchain sizes and their analysis more variable;
  - Incorporating data analytics and probabilities into the verification process

SOURCE: *Morgan Stanley Global Insight: Blockchain in Banking: Disruptive Threat or Tool?*, April 20, 2016



## Bank Efforts

- Royal Bank of Canada “is interested in the potential of a permissioned blockchain to bring real-time exchange for merchant partners and consumer clients. That would open the door to turning points into currency at POS.”
- “Banks including JPMC and Citi have successfully tested [blockchain] on credit-default swaps, a move that could help the technology gain a foothold in mainstream finance.”

SOURCE: “RBC Applies Blockchain as a Loyalty Boost,” By Tanaya Macheel, AmericanBanker.com, April 13, 2016; “Bitcoin’s Blockchain Proves Itself in a Wall Street Test,” by Telis Demos, *The Wall Street Journal*, April 8, 2016



## R3 Blockchain Consortium

- “R3 is a financial innovation firm that leads a consortium partnership with over 40 of the world’s leading banks, to design and deliver advanced distributed ledger technologies to global financial markets. ...collaborate with partner banks on research, experimentation, design and engineering to bring the ultimate users of this technology into the design and production process from the outset.”
  - U.S. participants include: BofA, BNY Mellon, Citi, JPMorgan, Goldman Sachs, Morgan Stanley, Northern Trust, State Street, U.S. Bancorp, Wells Fargo
  - R3 is also in partnership with Microsoft



# The Hyperledger Project

- “A collaborative effort created to advance blockchain technology by identifying and addressing important features for a cross-industry open standard for distribute ledgers that can transform the way business transactions are conducted globally. The Project is a Linux Foundation Collaborative Project and implements many open-source best practices...”
  - U.S. participants include: JPMorgan, BNY Mellon, State Street, Wells Fargo
  - DTCC, CLS
  - Accenture, Digital Asset Holdings, R3, IBM





# Questions?

Follow us on:



@DallasFed



DallasFed