The Federal Reserve Bank of Boston's

2016 Cybersecurity Conference

FEDERAL RESERVE
BANK OF BOSTON ™

Bitcoin/Blockchain and Potential Implications for Cybersecurity

Jim Cunha
SVP
Federal Reserve Bank of Boston

Objectives

Provide a basic understanding of how Bitcoin and other crypto currencies work, describe what the future might hold for the currencies and underlying technologies, and pose some potential implications for cybersecurity.

It’s 1990, you’re in a board meeting discussing your bank’s computer security strategy, Alvin Toffler (Author Future Shock) walks in ……

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 = rules, algorithms, security scheme
- 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 ~$6.5 billion

Bitcoin – Secret Sauce

- **Block chain** - A distributed public ledger that records every transaction
- **Public Key Encryption**. Everyone has:
  - Public key – everyone can see this
  - Private key – you keep 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 complex calculations
  - Plus a variable
- **Mining** – Performing a complicated hashing process to validate transactions. First miner to perform it successfully earns bitcoins

Market Capitalization

Symbol	Name	Market Cap	Price	Supply Issued/Acronym	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

Ripple Protocol/Currency

Not all crypto-currencies/networks are alike…..

- A network and a crypto-currency (XRP), but can be used to settle any two currencies.
- Instead of miners, Ripple has validator nodes
- Protocol requires a consensus of a supermajority of validators to authenticate a transaction as valid
- Currently, Ripple Labs runs the five validators that most servers rely on

Other Potential Uses of Distributed Ledger Technology

- Titles, deeds, licenses, other public documents describing ownership or status
- Smart contracts (self-executing)
- Remittances
- Stock exchanges, securities
- Security Repurchase Agreements (REPOs)
- Foreign Exchange

Government Issued Digital Currency

- In 2015, the Canadian mint cancelled a pilot of a small dollar digital currency to replace the 1 and 2 Canadian Dollar coins.
- Bank of England is looking at both distributed ledger for broad use in financial services and issuing its own digital currency (digital sterling)
- China and Russia have announced plans to issue digital currencies
- In 2015, Ecuador announced plans to issue a digital currency, but plans are moving forward slowly
- The Federal Reserve is monitoring above developments

It’s 2016, Alvin Toffler walks into your board room…

- Picture a future when: *
  - All deeds, mortgages, titles and marriage licenses are recorded on distributed ledgers managed by a consortium of states
  - NYSE, NASDAQ use distributed ledger technology/miners as their platform managed by the respective organizations
  - Government securities are recorded and traded on distributed ledgers where the Federal Reserve serves as validators of transactions
  - REPOs transactions are recorded via smart contracts and execute automatically on distributed ledger technology run by BNY Mellon and JPMChase
  - All FX transactions are cleared and settled though distributed ledger transactions managed by central banks, CLS, and SWIFT

* = Examples are totally ficticious and only for discussion purposes

Cyber Security Implications/ Questions

- I believe the technology will eventually see widespread use
- However, it's in its infancy so many implications are hard to predict

+ Distributed ledger technology, could dramatically improve resiliency

+ Miners/Validators could improve resiliency of the authentication process

+ Public Key Encryption coupled with encryption technology could improve identity management/authorization at an individual and process resiliency level

- The extent ledgers are open/public could create privacy issues and requires robust processes to restrict access on need-to-know

Cyber Security Implications/Questions

- Should corruption occur in any component, it could have extensive negative impact
- Security over private keys still critical to ensure identity is secure. Central storage facility obvious cyber threat target

± Alvin Toffler's world will require multiple distributed ledgers to communicate or be interconnected. This creates potential point of vulnerability or defense opportunity

± Also, banks will still need internal back-office systems, which must communicate/connect with the ledgers, which are also points of vulnerability or defense opportunity

± In Alvin Toffler's world, how do we think about the "weakest link" concept?

Jim Cunha
SVP Federal Reserve Bank of Boston
jim.cunha@bos.frb.org
617-973-3837