Bitcoin and Beyond

The Possibilities and Pitfalls of Virtual Currency

The views expressed are mine and do not necessarily reflect the official positions of the Federal Reserve Bank of St. Louis, the Federal Reserve System, or the Board of Governors.

Outline

- What is Bitcoin?
- How does it work?
- How is it different?
- What are its strengths/weaknesses?
- How will it affect money and payments?
- Beyond Bitcoin—broader applications?

What is Bitcoin?

- Bitcoin is a set of rules written in the form of a computer program designed to:
  - Manage a supply of digital objects (bitcoins).
  - Govern a global P2P payment system.

- Rules are not fixed—program is *open-source* and evolves over time.
  - Re: Linux operating system.
  - Bitcoin *is* what Bitcoin users *want it to be*.

How Does it Work?

- Users download free “wallet” software.

- Like owning a transparent P.O. box.
  - There is a public address (personal ID optional).
  - And a private key (password).
  - Where everyone can see account balances!

- Works just like online banking, except…
  - No banks (all exchange is P2P, like cash).
  - Pseudonymous, publicly observable accounts.

How Does it Work?

- P2P debit/credit requests are processed by account managers called “miners.”
  - Anyone can become a miner.
- Mining (processing payments) consumes resources.
- Miners paid in two ways:
  - New bitcoins as per Bitcoin protocol (“discovering” bitcoins).
  - Service fees provided by users.
- Total supply of bitcoins capped at 21M.

How Does it Work?

- Transactions are added to the blockchain—a *public* ledger.
  - A record of how every bitcoin has travelled from wallet to wallet.
- Less anonymous than cash.
  - Entire transaction history is publicly observable.
  - Good for transparency, bad for privacy.
  - Note: goods and services purchased are *not* observable (just like cash).
- The blockchain lives on every user's computer—a distributed network—not a central ledger.

How is it Different?

- Consider *Fedwire*--used to make payments across banks owning accounts at the Fed.
- Money supply (USD reserve balances) managed by FOMC, not computer algorithm.
- Ledger entries (reserve balances) are *private*, not public.
  - Only a trusted 3^{rd} party (the Fed) can see the ledger.
  - Member banks are identifiable (not pseudonymous).
- Debiting/crediting of accounts routed through and processed by trusted 3^{rd} party (not P2P + miners).

Strengths and Weaknesses?

- In terms of money supply, similar to gold.
  - Long-run purchasing power stability.
  - Short-run purchasing power instability.

- As a payment system, similar to P2P online banking (w/o the bank).
  - No barriers to opening an account, sending money easy as sending an email, low user fees.
  - Accounts are like cash (not insured).

Future of Money and Payments?

- Fiat money systems with good (politically insulated) protocols have little to fear.
  - Note: all currencies subject to fierce competition.
  - Mismanaged fiat systems will face added pressure.

- Total processing cost for Bitcoin is presently around 3%, similar to Visa, lower than Western Union.
  - Hope is that these costs will decline through better-designed incentive schemes for miners.

- Will likely find niche markets in advanced economies, broader acceptance in lesser-developed countries (the unbanked, the oppressed).
  - Big impact on market for international remittances.

Beyond Bitcoin

- Key innovation is the blockchain- a secure public ledger maintained by the community.

- Think of any activity that currently makes use of a middleman—these are all under threat.

    - Banking and money services businesses.
    - Brokerage, title transfer, escrow services.
    - Dispute resolution mechanisms, voting, etc.

Ethereum

- Ethereum: a blockchain with a built-in programming language used to write "Dapps".
- E.g., consider a financial contract to hedge EUR/USD exchange rate risk.
  - Two parties, A and B, accept (or write) a Dapp that has each committing $1000 to a pool.
  - In 10 days, if FX rate moves x%, then x% of deposit is transferred to A or B (depending if x is positive or negative).
  - Once dapp is accepted, all funds transfers are cleared by miners according to the contract (dapp).
  - No middleman, no recourse, no nonsense.

Thank you

David Andolfatto
VP Research, FRB St. Louis
November 16, 2014