Digital Currency and Blockchain Overview

Ryan Pierce, Co-Chair Digital Currency/Blockchain Working Group, FIX Trading Community, Director and Technology Architect, Engineering & Execution, CME Group
What is a Digital Currency?

- Digital currency is nothing new. Most currency is digital. Examples:
  - Fedwire, ACH
  - Visa, MasterCard, PayPal
- These are relatively “easy” solutions for digital currency, because they have two constraints:
  - They use fiat currency, e.g. issued by a government.
  - They place absolute trust in a central party to maintain a ledger.
- Eliminating either of these two constraints becomes “hard”.
- Bitcoin is, arguably, the first successful digital currency to overcome both of these constraints.
- Bitcoin’s Blockchain technology opens up amazing possibilities.
- This is the beginning of a new revolution in finance and technology.
Properties of a Successful Digital Currency

- Guaranteed scarcity:
  - A currency cannot have value if it isn’t scarce.

- Fair creation and distribution:
  - It must be generated and distributed via a fair mechanism that its users support.

- Prevention of double spending:
  - A person spending money cannot spend it again.
  - A person receiving money needs a verification mechanism that money was successfully sent.

- Elimination of trust in a central party:
  - The digital currency needs to exist independently of its inventor.
  - One can attack the currency by attacking the central party.
  - Risk of liability for a central party operating a digital currency.
  - Example: e-gold digital currency collapsed in 2008 due to US criminal charges even though there was no intent to engage in illegal conduct.
The Byzantine Generals Problem – Demonstration

- Do the majority of generals vote to attack New York City? Or retreat?
- All generals need to come to consensus on one answer!

Photo credit: https://en.wikipedia.org/wiki/Byzantine_Empire
The Byzantine General Problem

- Preventing double spending is a form of the Byzantine Generals Problem:
  - Ledger 1 believes consensus is that Alice paid Bob.
  - Ledger 2 believes consensus is that Alice paid the same coin to Carol.
  - Bob and Carol might both sell Alice goods yet just one gets paid!

- Achieving consensus when:
  - Most participants are motivated by self-interest, not altruism
  - Some participants are motivated by malevolent interests
  - No widely trusted party exists

  is a REALLY HARD problem to solve efficiently!

- Bitcoin, arguably, is the first digital currency to solve this problem and be implemented on a wide scale.
What is Bitcoin?

- Launched in 2009 by “Satoshi Nakamoto” – an unknown person or collaboration
- A digital currency
  - Not issued by any government
  - Not backed by any assets
  - Like cash, a bearer instrument with no recourse
  - Pseudonymous
- A decentralized peer-to-peer payment network
- Implemented by the Blockchain
  - A decentralized ledger with no central trusted party

Photo credit: https://www.casascius.com/photos.aspx
What is Bitcoin

- Guaranteed scarcity:
  - Limit of 21 MM Bitcoins
  - Initially, 50 Bitcoins “mined” every 10 minutes, halves every 4 years

- Fair creation and distribution:
  - The “miners” that invest computing power securing the Bitcoin network are rewarded with newly issued Bitcoins and (small) transaction fees

- Prevention of double spending:
  - Via the Blockchain

- Elimination of trust in a central party:
  - Via the Blockchain
Historic Bitcoin Price

What is the Blockchain?

- Decentralized ledger consisting of a list of blocks that contain transactions and a header that includes:
  - A hash of the prior block
  - A hash of all transactions in the current block
  - A timestamp
  - A “nonce” that is exceedingly difficult to compute, making a “signature”

- Modifying any transaction in the blockchain invalidates all subsequent blocks.

- The longest, valid blockchain is considered the truth.

- “Miners” spend massive computational resources competitively generating blocks. Security is guaranteed by “Proof of Work”.

- To “rewrite history” one would need to amass more computing power than all other miners in the world combined, e.g. “51% attack”

- The “difficulty factor” changes every two weeks to preserve a 10 minute average to mine a block.
Using Bitcoin

- Bitcoin is “stored” in the Blockchain itself.
- A “wallet” is collection of public and private keys that one can use to spend Bitcoin.
- Wallets can be implemented in:
  - Software
  - Hardware
  - Offline / Cold Storage (e.g. paper keys kept in a safe deposit box to reduce the risk of theft)
- Bitcoins can be mined, purchased on an exchange, or received as payment from other users.
- Bitcoins are divisible to 8 decimal places: 0.00000001 BTC.
- Bitcoin transactions are:
  - Authorized by signature using the wallet’s private key.
  - Sent via the peer-to-peer Bitcoin network.
  - If valid (signature, hasn’t been spent before, etc.) they are included in a block by “miners”.
  - Permanently become part of the public ledger.
  - The recipients confirm receiving the funds by watching the Blockchain.
- Linking wallet addresses to people destroys anonymity.
  - This makes Bitcoin a poor choice for criminals; the Blockchain is also an “evidence locker”.
  - Users can create many wallet addresses and use them for unique transactions.
Much Alternative Digital Currencies. Wow.

- Bitcoin is by far the largest, at $6.9 Billion
- Hundreds of others exist….
- Ripple
  - Uses a consensus algorithm without mining or Proof of Work.
  - Allows creation of arbitrary assets, e.g. bank deposits in USD.
- Ethereum
  - Focuses on “smart contracts”
- Dogecoin
  - Mascot is a really cute dog that talks in Comic Sans…

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Market Cap</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$6,960,917,759</td>
<td>$470.29</td>
</tr>
<tr>
<td>2</td>
<td>Litecoin</td>
<td>$216,599,007</td>
<td>$5.03</td>
</tr>
<tr>
<td>3</td>
<td>Ripple</td>
<td>$178,380,750</td>
<td>$0.005380</td>
</tr>
<tr>
<td>4</td>
<td>Ethereum</td>
<td>$72,276,321</td>
<td>$0.970664</td>
</tr>
<tr>
<td>5</td>
<td>Dogecoin</td>
<td>$16,470,030</td>
<td>$0.000162</td>
</tr>
</tbody>
</table>

Photo credit: http://indogewetrust.com
Alternate Blockchain Uses

- Blockchain technology need not be limited to digital currency!
- It is disruptive technology that fundamentally alters the nature of trust, eliminating the need for trusted third parties in transactions.
- Can record ownership of traditional assets:
  - Fiat currencies
  - Bonds, stocks, gold deposits
  - Recording title to real estate (pilot project in Honduras)
- Can act as a notary:
  - Trade repositories
  - Regulatory / audit records
  - Protecting log files against tampering
- Can be used for “smart contracts” that do not require trusted third parties to enforce:
  - Binary options that pay the appropriate party
  - Bonds that pay interest to their owners
  - Ownership of stock shares that directly prove voting rights
Advances in Blockchain Technology

- Multi-signature Transactions
  - E.g. digital signature by 2 of 3 keys needed to spend funds.

- Hierarchical Deterministic Wallets
  - Greatly simplifies key management and storage.

- Confidential Transactions
  - Transactions are still recorded in the public ledger, but…
  - Details like quantity can only be decrypted by the Buyer, Seller, and designated parties like Regulators.

- Private / Permissioned Blockchains
  - Participation limited to firms in one’s ecosystem.
  - Rules can be customized for specific applications, e.g. faster block creation times, no reward for mining transactions.

- Interoperability between Blockchains
  - Sidechains – Assets can be locked on their primary chain, transferred to a second chain, exchanged, and transferred back to the primary chain.
  - Interledger Protocol – One can exchange different assets on different chains without having to trust your trading partner or trusting a third party for escrow.
FIX Protocol Use Cases

- Adding Bitcoin and other digital currencies into the existing FIX Protocol.
  - Enables FX trading, market data, etc.
  - Digital currencies can benefit from FIX’s existing workflows.
- Adding Blockchain Settlement to FIX.
  - FIX already supports traditional settlement instructions.
  - Extend FIX to indicate that trades are settling on a blockchain.
- Embedding FIX in a Blockchain.
  - FIX has extensive data modelling for financial transactions.
  - Eliminates the need for blockchain protocols to re-invent the wheel.
  - Allows for greater integration of blockchain technology into existing business use cases where participants already use FIX.