Blockchain Technology and Its Applications

Andy Wang
October 15, 2016
Emerging Technologies

- Drone & Robotics
- Autonomous vehicles (driverless car, e.g.)
- Deep learning and machine intelligence
- Big data and cloud computing
- Cyber Physical Systems and IoT – “Internet of Things”
- Etc. etc.

What is the next “big thing”?
Agenda

- What is Blockchain?
- How does a Blockchain get built?
- Current applications of Blockchain technology
- Future applications of Blockchain technology
- Q & A
Cryptocurrency
What is Blockchain?

- Every viable transaction is stored in a public ledger.
- Transactions are placed in blocks, which are linked by SHA256 hashes.

A Blockchain is more than:
- Distributed
- Secure
- Logfile
A Chain of Transactions

Transaction

Owner 1's Public Key

Hash

Owner 0's Signature

Sign

Owner 1's Private Key

Transaction

Owner 2's Public Key

Hash

Owner 1's Signature

Verify

Owner 2's Private Key

Transaction

Owner 3's Public Key

Hash

Owner 2's Signature

Verify

Owner 3's Private Key
Why does it Matter?

### Bitcoin (BTC)

<table>
<thead>
<tr>
<th>Source</th>
<th>Pair</th>
<th>Volume (24h)</th>
<th>Price</th>
<th>Volume (%)</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitfinex</td>
<td>BTC/USD</td>
<td>$3,435,060</td>
<td>$642.90</td>
<td>Recently</td>
</tr>
<tr>
<td>2</td>
<td>BitMEX</td>
<td>BTC/USD</td>
<td>$3,394,470</td>
<td>$639.77</td>
<td>Recently</td>
</tr>
<tr>
<td>3</td>
<td>Kraken</td>
<td>BTC/EUR</td>
<td>$3,064,760</td>
<td>$642.37</td>
<td>Recently</td>
</tr>
<tr>
<td>4</td>
<td>GDAX</td>
<td>BTC/USD</td>
<td>$3,022,100</td>
<td>$638.25</td>
<td>Recently</td>
</tr>
<tr>
<td>5</td>
<td>Poloniex</td>
<td>ETH/BTC</td>
<td>$2,861,120</td>
<td>$640.90</td>
<td>Recently</td>
</tr>
</tbody>
</table>

### Market Analysis

- **Market Cap**: $10,205,960,273 (1 BTC), $57,756,000 (15,921,612 BTC)
- **Volume (24h)**: $57,756,000 (90,117 BTC)
- **Available Supply**: 15,921,612 BTC
- **Max Supply**: 21,000,000 BTC

---

**Website**

- [Explorer](#)
- [Message Board](#)
- [Message Board 2](#)

**Additional Links**

- Mineable
- Currency
Why does it Matter?

- A digital currency could transform the world in many different ways.
- While it carries regulatory and economic risk as a long-term store of value (as in the case of Bitcoin), it can be quite revolutionary as a transaction processing tool.
- It provides the framework facilitating transaction processing and coordination among interacting devices (IoT). Each manages its own roles and behavior, resulting in an "Internet of Decentralized, Autonomous Things."
- Democratizing of the digital world, and may be the real word!
Duomo in Florence, Italy
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest chain of events they receive as the true past. All nodes start with the same version of the past, and sync with each other using regular messages called 'headers'.
ICICI Bank is an Indian multinational banking and financial services company headquartered in Mumbai, Maharashtra, India, with its registered office in Vadodara.

ICICI Bank on Wednesday announced that it has successfully executed transactions in international trade finance and remittances using blockchain technology in partnership with a Dubai based bank Emirates NBD.
Government Adoption

- Honduras government has put all land records on a public ledger - the blockchain. The minute there is a change in ownership, it gets recorded publicly. Georgia and Sweden are moving toward this as well.

- The Australian Securities Exchange (ASX) announced this year that it would move Australia's equities clearing and settlement system on to blockchain.

- In October 2015, Nasdaq unveiled Linq, a solution enabling private companies to digitally represent share ownership using blockchain-based technology.
Other Applications

- Smart Contracts
  - Escrow-free exchange
  - Insurance
- Voting
- Distributed Autonomous Organizations
- Identity & Reputation Systems
- Student academic record
- CASA Advantages Credentials
- Degree audit system
- Faculty credential and evaluation system
- Competence-based education
- And so on so forth …
Things to Watch?

- Ethereum.org
  Turing complete contracts on a blockchain
- Contracts are the main building blocks of Ethereum.
- A contract is a computer program that lives inside the distributed Ethereum network and has its own ether balance, memory and code.
- Every time you send a transaction to a contract, it executes its code, which can store data, send transactions and interact with other contracts.
- Contracts are maintained by the network, without any central ownership or control.
- Contracts are written in languages instantly familiar to any programmer and powered by Ether, Ethereum's cryptofuel.
Questions?

Thank you!