Lecture 6 - Flaws

Rylan Schaeffer and Vincent Yang

May 8, 2016

Note: This lecture is based on Princeton University's BTC-Tech: Bitcoin and Cryptocurrency Technologies Spring 2015 course.

Blockchain Applications

- What it can do:

  Have a large number of nodes with up-to-date information.

  Account for dishonest nodes

  Determine with non-negligible certainty the existance of an operation

  High cost of rewriting history

  Solution for conflicting information

- Smart Contracts
- NameCoin - DNS Server
- Colored coin - just link something physical to each digital coin
- Decentralized P2P Energy Networks, P2P Communication, P2P Logistics, etc.
- Deloitte created MVP - warranty bot that lets users send an image of a specially designed receipt via FB Messenger.

  Then, Deloitte's product can 'unwrap' a QR code and store the information on a blockchain.

  Gives proof of ownership, can be transferred, and proof it existed.

- Trading Ownership in an Online Marketplace - creators as well

  Blockai uses blockchain to help artists protect intellectual property

- File Storage
- HyperLedger - Linux Foundation

  Business Networks - anything of value can be tracked and traded.

  Manage flow of goods (supply chain), and related payments/share production logs.

  Fluent - just supply chain

- Tierion - verifiable record of any data/business process in block chain

  Use case example: Insurance - collect claims data and issue a blockchain receipt. Gives verifiable record of the time and content of initial claim - reducing errors, fraud, and cost of auditing claims.

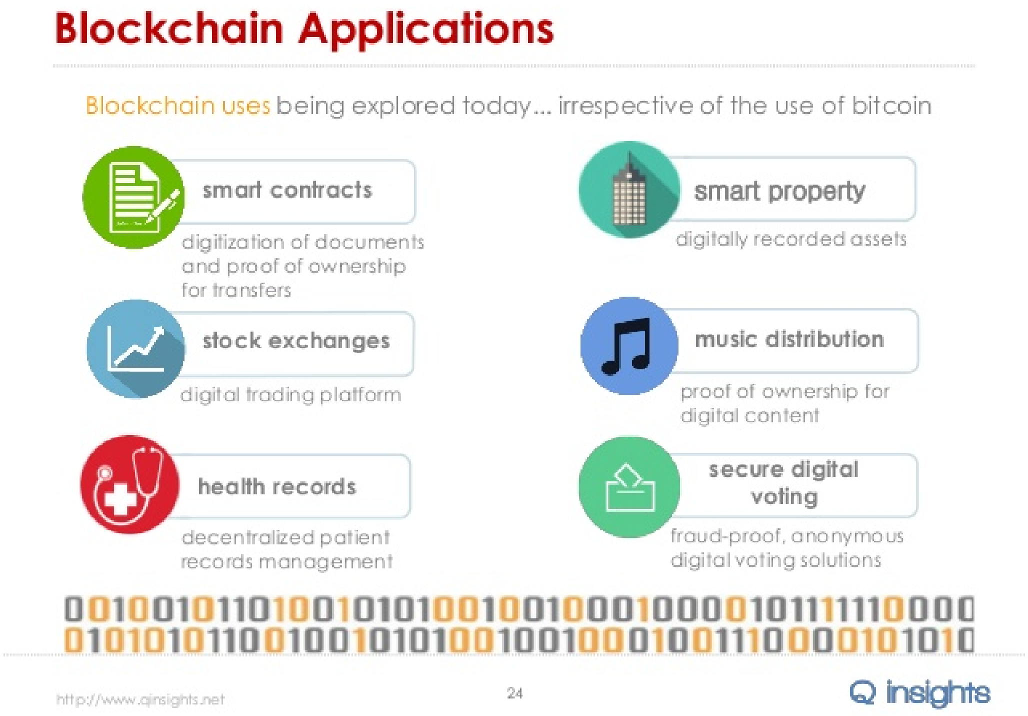
- Similar to Tierion - Everledger (With Barclays) working on creating reliable receipts for luxury goods.

  Diamonds - If you have a 5 carat diamond, then serial number + 4 C's (Carat Weight, Cut, Color, Clarity) + angels + pavilions... ultimately 40 metadata points.

- Edgelogic: Blockchain with Internet of Things

  Example: sensor reports when something starts to go wrong that is covered by insurance, and automatically makes transfer that can be logged and referred to (binding) from insurer to claimant's account, without even the person knowing.

- In summary:



Blockchain Applications

Blockchain uses being explored today... irrespective of the use of bitcoin

smart contracts
digitization of documents and proof of ownership for transfers

smart property
digitally recorded assets

stock exchanges
digital trading platform

music distribution
proof of ownership for digital content

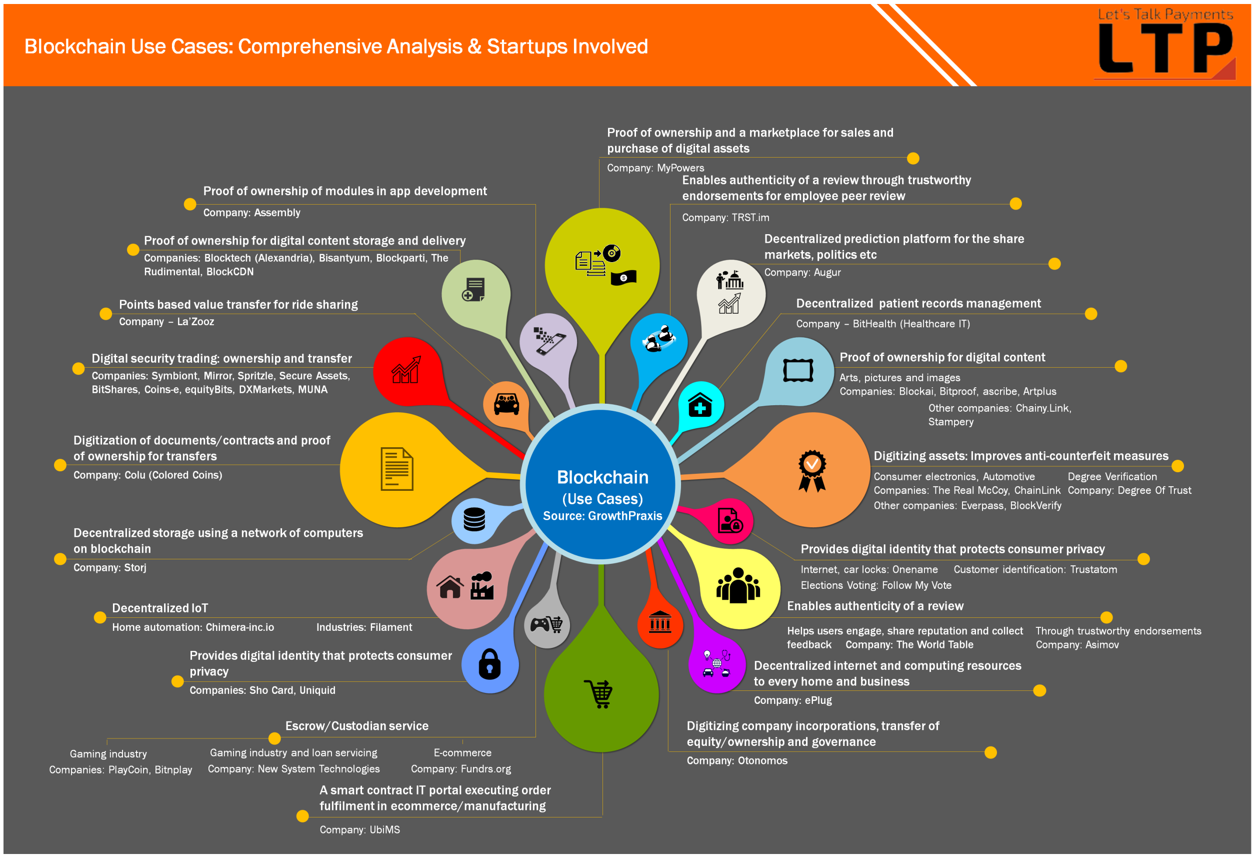
health records
decentralized patient records management

secure digital voting
fraud-proof, anonymous digital voting solutions

http://www.qinsights.net

24

Q insights



Blockchain Use Cases: Comprehensive Analysis & Startups Involved

Let's Talk Payments LTP

Blockchain (Use Cases) Source: GrowthPraxis

Proof of ownership of modules in app development
Company: Assembly

Proof of ownership for digital content storage and delivery
Companies: Blocktech (Alexandria), Bisantyum, Blockparti, The Rudimental, BlockCDN

Points based value transfer for ride sharing
Company – La'Zooz

Digital security trading: ownership and transfer
Companies: Symbiont, Mirror, Spritzle, Secure Assets, BitShares, Coins-e, equityBits, DXMarkets, MUNA

Digitization of documents/contracts and proof of ownership for transfers
Company: Colu (Colored Coins)

Decentralized storage using a network of computers on blockchain
Company: Storj

Decentralized IoT
Home automation: Chimera-inc.io
Industries: Filament

Provides digital identity that protects consumer privacy
Companies: Sho Card, Uniquid

Escrow/Custodian service
Gaming industry
Companies: PlayCoin, Bitnplay
Gaming industry and loan servicing
Company: New System Technologies
E-commerce
Company: Fundrs.org

A smart contract IT portal executing order fulfilment in ecommerce/manufacturing
Company: UbiMS

Proof of ownership and a marketplace for sales and purchase of digital assets
Company: MyPowers

Enables authenticity of a review through trustworthy endorsements for employee peer review
Company: TRST.im

Decentralized prediction platform for the share markets, politics etc
Company: Augur

Decentralized patient records management
Company – BitHealth (Healthcare IT)

Proof of ownership for digital content
Arts, pictures and images
Companies: Blockai, Bitproof, ascribe, Artplus
Other companies: Chainy.Link, Stampery

Digitizing assets: Improves anti-counterfeit measures
Consumer electronics, Automotive
Companies: The Real McCoy, ChainLink
Other companies: Everpass, BlockVerify
Degree Verification
Company: Degree Of Trust

Provides digital identity that protects consumer privacy
Internet, car locks: Onename
Customer identification: Trustatom
Elections Voting: Follow My Vote

Enables authenticity of a review
Helps users engage, share reputation and collect feedback
Company: The World Table
Through trustworthy endorsements
Company: Asimov

Decentralized internet and computing resources to every home and business
Company: ePlug

Digitizing company incorporations, transfer of equity/ownership and governance
Company: Otonomos

Project Planning

- Planning out your project is extremely important.
- Understand the overall goal of the program, as well as key functions for how each part comes together.
- Submit a plan by the end of the class. This plan should incorporate

  1. Each main component, as well as how you intend on completing it.
  2. This plan should also incorporate a brief description of each component, and a general idea of how it works.

     e.g. We want to create a mining based app, where people can only submit messages after completing proof of work. Two important components are the hash function and digital signatures. Cryptographic hash functions with signatures can be implemented with the Python rsa library.

     e.g. We want to create a rudimentary Cryptocurrency. MIT has a skeleton for this in java that we can pull from. Essential components are the BlockChain (universal ledger), Signatures, Hashing.
  3. Lastly, the plan should incorporate a two week projection of goals - where you expect to be in two weeks, with respect to the whitepaper and implementation, as well as who is working on what.

- Checkpoint 2 - this submitted paper.

Feel free to ask Rylan and I for help and feedback during this time.