parc
A Xerox Company

Emerging Technology
Blockchain
ALC Supply Chain Technology Summit 2018

The Business of Breakthroughs®

Aki Ohashi
Director of Business Development

PARC LEGACY: A History of Inventing the Future

1971
Laser Printer

1973
Personal Workstations

1973
Ethernet

1975
Graphical User Interface

1979
Corporate Ethnography

1980
Programming Languages

1988
Ubiquitous Computing

1975, 1984, 1992, 2003, 2009
Turing Award

parc

Ralph Merkle, the inventor of the Merkle Tree, a foundational blockchain technology, was a PARC researcher

Conceptually: Put many transactions inside a block

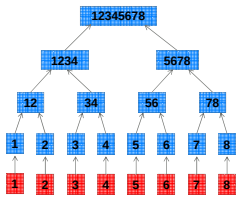
Payment Instruction
Source Address = 9876asf098gsa87d
Amount Transferred = 1.5
Destination Address = a5g8s92nhvfc2k44
Time Stamp = August 31, 2016, 2:45:23

Digital signature of instruction using Private key = i986542hdg268gvhnb

Transaction
Alice pays Bob 1.5 BTC

Block
1
2
3

In practice: Put a Merkle hash tree of transactions inside a block



parc

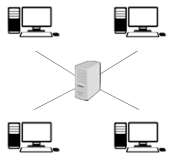
If you remember one thing from the panel today, remember that:

Bitcoin ≠ Blockchain

Bitcoin is the most widely adopted and most publicly talked about instantiation of blockchain. However, there are many other applications for blockchain technology

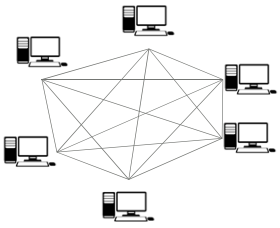
parc

Conventional Ledger, e.g., Paypal, Banks, etc.



Single point of "failure"

Blockchains are a Distributed Ledger of Transactions



Nodes "gossip" until everyone has received novel transactions or blocks.

parc

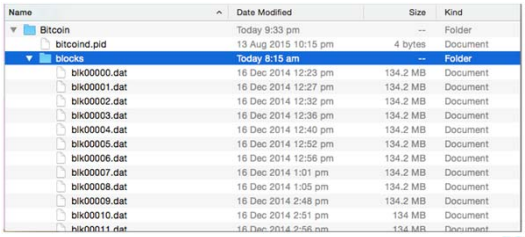
Blockchain is a data structure that can...

- Store transactions.
- Serve as a distributed ledger of transactions.
- Allow "anyone" to verify past transactions.
- Establish consensus about which transactions are genuine.
- Be a linked list of hash pointers.
- Serve as "a machine for creating trust." [Economist, 2015]

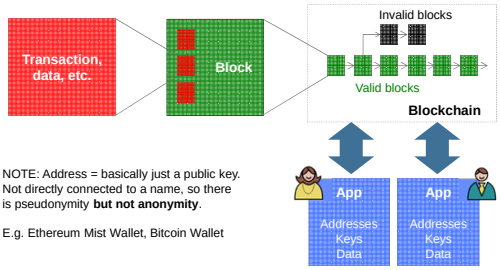
parc

Blockchains are distributed

Blockchains are just a collection of files stored on various computers around the world. [https://bitsonblocks.net]



Elements of a Blockchain



NOTE: Address = basically just a public key. Not directly connected to a name, so there is pseudonymity **but not anonymity**.

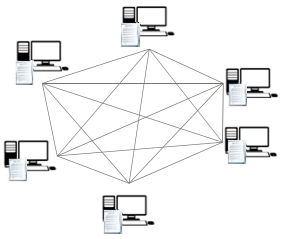
E.g. Ethereum Mist Wallet, Bitcoin Wallet

Ethereum

- Public Blockchain-based computing platform
- Developed by crowdfunding in 2014. Launched 2015.
- Currency: **Ether**
- **Smart Contract Functionality**: Every node runs a smart contract before it runs a cryptocurrency transaction.
- Currently on Proof-of-Work, but will move to Proof-of-Stake in 2018.

A Smart Contract

- *is a piece of software that stores rules for negotiating terms of a contract, automatically verifies the contract, and then executes the agreed terms.*
- *is stored on the blockchain, and is accessible to everyone. If anyone changes the contract, they will be caught.*
- *allows untrusted parties to transact without a middleman.*



When should you consider blockchain?

Ask the following questions:

- Is the database distributed?
- Is it modified by several parties?
- Is there scope for mutual distrust?
- Is there anything wrong with a centralized intermediary?
- Is the database itself an asset? OR Is it costly to augment the database?

If the answer to any of the questions is "No," blockchain might not be the right solution.