Blockchain
You want me to Trust a ‘Trustless Trust’ System?

Ed Featherston
Distinguished Technologist
Cloud Technology Partners, a Hewlett Packard Enterprise Company
First Things First

Blockchain ≠
Blockchain – Hype Cycle

Hype Cycle for Emerging Technologies, 2018

Blockchain Technology and the End of Corruption

Is blockchain the new tech bubble set to burst?

Blockchain technology can revolutionize the food supply chain, says IBM VP

Blockchain is a ‘pixie dust’ fad, and its benefits in finance are ‘little to nothing’
## Blockchain – The basic concepts

<table>
<thead>
<tr>
<th>Distributed Ledger</th>
<th>Irreversibility &amp; Immutability</th>
<th>Smart Contracts</th>
<th>Near Real-Time</th>
<th>No Intermediary</th>
</tr>
</thead>
<tbody>
<tr>
<td>The peer-to-peer distributed network records a history of transactions. The blockchain is distributed and highly available. A public blockchain does not typically preserve the identities of the parties or the transaction data, only the proof of the transaction existence.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The blockchain contains a certain and verifiable record of every single transaction ever made. This prevents past blocks from being altered and in turn stops double spending, fraud, abuse, and manipulation of transactions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stored procedures executed in a Blockchain to process pre-defined business steps and execute a commercially/legally enforceable transaction without involvement of an intermediary.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blockchain enables the near real-time settlement of recorded transactions, removing friction, and reducing risk.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blockchain technology is based on cryptographic proof instead of trust, allowing any two parties to transact directly with each other without the need for a trusted third party.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2018 Cloud Technology Partners, a Hewlett Packard Enterprise company / Confidential
Blockchain – It’s all about trust

- Trust is a fundamental aspect of interaction our society
  - Individual
  - Business
  - Technology
- Critical factor when considering new, disruptive technologies
- Imagine the reaction then, when told this new blockchain technology is a ‘trustless trust’ system
- To understand how we can trust a ‘trustless trust’ system, let’s take a brief detour through a literary classic

You want me to trust a ‘trustless trust’ system?
Scrooge was a money lender
He would call on people he extended loans to to seek payment
  - He and the individual would negotiate payment
  - Both he and the individual would sign an entry in a little black book he carried with him
At the end of the day, Scrooge would return to his office
  - His clerk, Bob Cratchit would transcribe the transactions from the little black book into Scrooge’s master ledger
Let’s say I want to create a transaction in the blockchain and send something to Mr. Scrooge. I’d do the following:

- Take the message I’m sending and create a unique signature using encryption technology and my private key.
- Combine the message and the unique signature, then add my public key as well as Scrooge’s (to whom I’m sending the message).
  - This message can represent any asset type, such as currency or other digital assets.
- This transaction is then sent out into the blockchain world for validation and entry into the actual ledger.
  - The combination of the message, the unique signature, and my public key is validated by encryption technology.
  - If there’s any attempt to modify the content of the message or the signature, the validation will fail—so I know I can trust the content.

At this point, I’ve signed Scrooge’s little black book. Now I need to get the transaction recorded in the ledger.
Scrooge in a blockchain world

In Scrooge's world he had Bob Cratchit:

- Bob trusts Scrooge as the source of the transaction (his little black book)
- Scrooge trusts Bob to transcribe the transaction sequentially into his central ledger

But, in the Blockchain World, not only does that relationship not exist, there is no one central ledger

- Blockchain is a distributed peer to peer ledger
- A copy of the ledger exists on all participants systems
- Participants must have a mechanism to reach consensus
- Once consensus achieved, the transaction is transcribed
  - The accepted transaction is encoded with hashtag of prior entry
  - Any attempt to modify or change is identified and rejected

Consensus is the Bob Cratchit of the Blockchain World!
Blockchain – Consensus is the key to ‘trustless trust’

- In the blockchain world there is no central authority, no single source

- Every node/participant has a complete copy of the ledger

- As new blocks are added, every node participating receives the transaction

- Distributed consensus and trust critical to ensure integrity of the system
Consensus – The Byzantine Generals Problem

- Group of generals encircle a city
- They want to coordinate an attack
- Can only communicate via messengers
- BUT
  - Some of the generals may be traitors
  - They may intercept or modify messages
- How do they know they are receiving the correct information?
- This conundrum is a frequent challenge in a distributed system
Consensus – Everything is a tradeoff

• There is no ‘one way’ to solve any challenge
• Always ask ‘what tradeoffs you are will to accept’
• Many techniques in use to solve the Byzantine General problem in blockchain
• Three of the most well known
  – Proof of Work
  – Proof of Stake
  – Byzantine Fault Tolerance
Blockchain – Proof of Work

• Most well known
• Requires significant effort/investment to add a block
• But minimal effort to validate
• ‘Miners’ look for next proposed block to add
  – They are challenged with a mathematical puzzle to solve
  – Resource/cost intensive to the miner
  – Whoever solves first, they validate the block can be added
  – They are rewarded for their efforts

The key tradeoff: Time to validation, solving puzzle takes time, reduces throughput
Blockchain – Proof of Stake

- Mining is done by participants that have stake in the ecosystem
  - Unlike PoW where mining can be anyone
- Complex algorithms based on
  - Cost associated with block
  - Total value(stake) participant has in ecosystem
  - Some pseudo-random selection to avoid risk of large stakeholders exerting control
- Benefit: less resource intensive than PoW, allowing higher throughput

The key tradeoff: Risk of ‘Nothing At Stake’ Scenario and/or large stakeholder dominance
Blockchain – Byzantine Fault Tolerance

- Takes a different perspective
- All participants in the ecosystem are known
  - Each participant has a public key
  - As block passes through their node, it is validated and signed with key
  - Once pre-defined number of participants sign, considered valid

- Benefits
  - Does not require the large amount of resources as Proof of Work
  - Less risk of largest stakeholder leverage as Proof of Stake

The key tradeoff: Requires some level of Central Authority to control/validate membership
Blockchain – Its Complicated

• Yes, blockchain is a distributed ledger…but
• It’s a lot more complicated than that
• Complex ecosystem
• This ecosystem is critical to creating a ‘trustless trust’ system that can be trusted
Blockchain – Technology is the Vehicle, Not the Destination

• Blockchain is a fascinating technology, that could potentially have transformative impact on a variety of industries.

• Ultimately, blockchain is still just the potential vehicle

• Your destination should always be business goals and values
Thank you for your time and interest.

Ed Featherston
Edward.Featherston@hpe.com
@efeatherston
https://www.linkedin.com/in/edfeatherston/