Making Blockchain Real for Business

Explained
Blockchain is a technology for a new generation of transactional applications that establishes trust, accountability and transparency while streamlining business processes. Think of it as an operating system for interactions. It has the potential to vastly reduce the cost and complexity of getting things done.

Blockchain is a design pattern made famous by its use in Bitcoin. But it’s uses go far beyond.

Blockchain can reimagine the world’s most fundamental business interactions and open the door to invent new styles of digital interactions.

IBM is adopting Blockchain to a very broad range of business applications.
Blockchain in an emerging platform for transaction services

Blockchain technology has the potential to radically transform multi-party business networks, enabling significantly faster, less expensive, lower risk transactions and innovative new business models.

Inefficient, expensive, vulnerable

- Difficult to maintain a single source of truth
- Difficulty to maintain transparency
- Not timely in delivery or access
- Business logic implementation linking transactions can be different between parties
- Can be overly complex due to the evolution and use of older technology.

Attributes

- Shared replicated immutable ledger
- Digitally signed/encrypted transactions
- Business logic linking transactions into business processes
- Automation

Types of Use Cases

- Trusted registry of ownership of assets
- Asset transfer
- Smart contracts

Digitally signed/encrypted transactions and ledger

All parties have same replica of the ledger
1. It all starts with one node

2. Each node has the shared ledger

3. Nodes form a peer network

4. Users submit transactions

5. Consensus and leader election

6. Execution & Recovery

Each block has a digital fingerprint of the previous block.
- Distributed ledger is implemented as a chain of blocks
- Transactions are recorded in each block
Blockchain underpins Bitcoin ...

... Digital currencies different from cryptocurrency
How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin “wallets” on their computers.

Bob creates a new Bitcoin address for Alice to send her payment to.

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

VERIFICATION OF THE TRANSACTION

Gary, Garth, and Garry are Bitcoin miners.

The miners’ computers are set up to calculate cryptographic hash functions.

Each block includes a “coinbase” transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

PUBLIC KEY CRYPTOGRAPHY 101

When Bob creates a new address, what he's really doing is generating a “cryptographic key pair,” composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

Bob and Alice have Bitcoin "wallets" on their computers.

WALLETS are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HGZ77z7PbX1nKgFkJ5m5BkQ7aS9xH3qv.

Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string of a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it’s essentially impossible to predict what initial data set will create a specific hash value.

The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that’s added to data prior to hashing. Changing the nonce results in a wildly different hash value.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they’re forced to generate many hashes with different nonces until they happen upon one that works.

The root of all evil??

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The root of evil is 0000000000000000000000000000000000000000000000000000000000000000

The root of evil is 0000000000000000000000000000000000000000000000000000000000000000

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she’s transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

The mixer computers bundle the transactions of the past 10 minutes into a new "transaction block."

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.
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
Proof of Work

- Proof of Work asks for nodes to demonstrate they have burned CPU in order to win the right to create the next block.
- Mining is usually the process by which this proof occurs.
- Nodes attempt to solve mathematics problems.
- Called ‘miners’ because they receive payment for being the first to solve a problem.
- Hash functions make it easy for other nodes to validate solutions:
  - Difficult to find (Brute Force)
  - Easy to Check
Mining & Miners

- Transactions are broadcast to Miners for “Consensus”

- Example:
  - Miner1 & Miner2 “process” the broadcast transactions
  - Miner1 & Miner2 collect transactions into a block
  - Miner1 & Miner2 work to solve a difficult maths problem based on the block
  - Consider “Miner1” reaches the “solution” first
  - Miner1 broadcasts the “solution” to Miner2
  - Miner2 verifies the “solution”
  - Miner2 also broadcasts consensus
  - Block is added to the chain – by Miner1
Mining & Miners

Very CPU intensive process!
Industrial Blockchain Characteristics

- Shared single source of truth (ledger)
- Secure tamper proof
- Private un-linkable identity
- Scalable architecture
- Confidential permission control
- Auditable prove identity & ownership
Blockchain for business ...

Append-only distributed system of record shared across business network

Shared ledger

Smart contract

Business terms embedded in transaction database & executed with transactions

Ensuring appropriate visibility; transactions are secure, authenticated & verifiable

Privacy

Consensus

All parties agree to network verified transaction

... Broader participation, lower cost, increased efficiency
Records all transactions across business network

Shared between participants
Participants have own copy through replication
Permissioned, so participants see only appropriate transactions
THE shared system of record
Smart contract

Business rules implied by the contract … embedded in the Blockchain and executed with the transaction

Verifiable, signed

Encoded in programming language

Example:

Defines contractual conditions under which corporate Bond transfer occurs
Ledger is shared, but participants require privacy

Participants need:
  Transactions to be private
  Identity not linked to a transaction

Transactions need to be authenticated

Cryptography central to these processes
**Consensus**

... the process by which transactions are verified

**When participants are anonymous**
- Commitment is expensive
  - *Bitcoin cryptographic mining* provides verification for anonymous participants but at significant compute cost (proof of work)

**When participants are known & trusted**
- Commitment possible at low cost

**Multiple alternatives**
- proof of stake where fraudulent transactions cost validators (e.g. transaction bond)
- multi-signature (e.g. 3 out of 5 participants agree)
- PBFT (cross checked secure message exchange)

**Industrial Blockchain needs “pluggable” consensus**
## Comparison of consensus approaches

<table>
<thead>
<tr>
<th>Management Entity</th>
<th>None</th>
<th>Multiple Organizations</th>
<th>Single Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Type</td>
<td>Public</td>
<td>Consortium</td>
<td>Private</td>
</tr>
<tr>
<td>Participants</td>
<td>Free</td>
<td>Permissioned</td>
<td>Identified and trusted</td>
</tr>
<tr>
<td></td>
<td>Anonymous, could be malicious</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consensus Mechanisms</td>
<td>Mining (Proof-of-Work)</td>
<td>Voting / multi-party consensus algorithm</td>
<td>Lighter, faster, Low energy consumption, Enable finality</td>
</tr>
<tr>
<td></td>
<td>• Large energy consumption</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No finality</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 51% attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction Approval Frequency</td>
<td>Long (e.g., 10 min)</td>
<td>Short (100x msec)</td>
<td></td>
</tr>
<tr>
<td>Use Cases</td>
<td>Crypto Currency</td>
<td>Transactions in business networks, e.g., cross-border payment, securities transactions, etc.</td>
<td></td>
</tr>
</tbody>
</table>

In business use, it is important that the platform supports different consensus mechanisms depending on the use case.
Contents

What is Blockchain?

Why is it relevant for our business?
Blockchain benefits

Saves time
Transaction time from days to near instantaneous

Removes cost
Overheads and cost intermediaries

Reduces risk
Tampering, fraud & cyber crime

Increases trust
Through shared processes and recordkeeping
3 Trends Appear in the Gartner Hype Cycle for Emerging Technologies, 2016

Are blockchain, smart machines, IoT and other emerging technologies on their way up or down the Hype Cycle?

August 19, 2016
Contributor: Kasey Panetta

You won’t be surprised to learn that blockchain, still five to ten years from mainstream adoption, nears the peak of the Gartner Hype Cycle for Emerging Technologies, 2016. With its ability to store multiple bank transactions in one centralized ledger, accessible by all parties and regulated by a decentralized network, blockchain will have a transformational impact on business. While bitcoin steals the show as the only proven blockchain, the term blockchain has grown to encapsulate nearly two dozen distributed-ledger products with more than two dozen offerings in the market, thus the hype.

Right now, blockchain is gaining traction because it holds the promise to transform industry operating models. It is also one example of an enabling technology of the platform revolution trend,
Goldman Sachs: Blockchain Tech Could Save Capital Markets $6 Billion a Year

Pete Rizzo (@pete_rizzo_) | Published on May 25, 2016 at 23:44 BST

A new report from Goldman Sachs Investment Research projects that the implementation of blockchain technology could streamline the clearing and settlement of cash securities, saving capital markets $2bn in the US and $6bn globally on an annual basis.

The figures are supported by breakdowns of the specific market areas where Goldman Sachs sees the technology as valuable, as it projects up to $900m could be saved in reduced personnel and $700m could be saved from IT systems improvements.
Our analysis suggests blockchains can drive down inefficiencies across networks

Blockchains have a leveling effect by making business networks more homogeneous in how they can operate.

This illustrative example of shrinking inefficiencies suggests that enterprises, ecosystems and economies can function at substantial higher levels of efficiency and trust.

Source: IBM Institute for Business Value analysis
We expect blockchains to fundamentally change how we do business in three radical ways:

1. **A new science of organizations**
   - Highly efficient distributed business networks will challenge our notions of traditional enterprise management.

2. **The tightening of trust**
   - Codifications of contracts, compliance and certifications will redefine how trust is embodied in business transactions.

3. **A new nexus for value exchange**
   - Efficient and accessible market-places built on blockchains will accelerate the exchange of value and flow of wealth.

Source: IBM Institute for Business Value analysis
Summary

Blockchain ...
- is a shared, replicated, permissioned ledger technology
- can open up business networks by taking out cost, improving efficiencies and increase accessibility
- addresses an exciting and topical set of business challenges, which cross every industry

IBM ...
- supports the Linux Foundation Hyperledger open standard, open source, open governance Blockchain
- has an easy to access, proven and incremental engagement model giving customers the confidence to get started NOW
Thank you!