Blockchain: The Iceberg Beneath Bitcoin

John Callahan, PhD
JHU/APL

WARNING: many simplifications ahead
The promise of the blockchain

The trust machine

The technology behind bitcoin could transform how the economy works

Oct 31st 2015 | From the print edition

BITCOIN has a bad reputation. The decentralised digital cryptocurrency, powered by a vast computer network, is notorious for the wild fluctuations in its value, the zeal of its supporters and its degenerate uses, such as extortion, buying drugs and hiring hitmen in the online bazaars of the “dark net”.

Jon Berkeley
Barter
Money: fungibility
Banking
Banking 1.0

8
3
5
"ENTERTAINING AND INFORMATIVE." — THE ECONOMIST

JANE GLEESON-WHITE

DOUBLE ENTRY

HOW THE MERCHANTS OF VENICE CREATED MODERN FINANCE
Banking 1.0

8 3
3
5
Banking 1.0
Banking 2.0
Bitcoin: *a ledger of financial transfers?*

Assume all previous transfers leave a balance of 8 for each person.
Each transaction: IN = OUT

IN(s) | OUT(s)
---|---
8 | 4
4 | 4

- Hash pointer to previous transaction
- "returned" to sender
Bitcoin: a *public* ledger of financial *transactions*?
Bitcoin: a decentralized, public ledger of transactions

* on a peer-to-peer (p2p) virtual network
Step 1: “broadcast” new transaction to peers
Step 2: append new transaction to next “block”
Step 3: attempt to solve the block nonce puzzle

Note: no single entity should own >= 51% of computing cycles
Step 4: solve the block nonce puzzle*

* ... and collect a small transaction fee
Step 5: “broadcast” the valid nonce

Note: ... here be race conditions (and vulnerabilities)
Summary

1. YOU
   - “Broadcast” new transaction to peers

2. The Bitcoin Network
   - Append new transaction to the next block
   - Attempt to solve the block nonce puzzle
   - Solve the block nonce puzzle
   - “Broadcast” the valid nonce

3. PROFIT! :-)
Blockchain:
latest valid block appended to end of the “chain”

Note: this is a solution for achieving distributed consensus, but is still vulnerable to various attacks*

* Details of attacks and counter-measures NOT covered in this talk
Blockchain:
latest valid block appended to end of the *longest* “chain”
Blockchain: a generic protocol for transactions

private key: EB451
public key: 88AE7

private key: 1CE74
public key: 1CE74

private key: [redacted]
public key: [redacted]

private key: [redacted]
public key: [redacted]
Blockchain: a generic protocol for transactions dependent on public key encryption
Note: Here be simplifications...

previous transaction

signed
 EB451
 1CE74 88AE7

SCRIPTS!
Some standard transaction scripts

<table>
<thead>
<tr>
<th>Type</th>
<th>Script</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pay to Public Key Hash (P2PKH)</td>
<td>\texttt{OP_DUP \texttt{OP_HASH160} &lt;PubKeyHash&gt; \texttt{OP_EQUALVERIFY \texttt{OP_CHECKSIG}}}</td>
</tr>
<tr>
<td>Pay to Script Hash (P2SH)</td>
<td>\texttt{OP_HASH160 &lt;Hash160(redeemScript)&gt; \texttt{OP_EQUAL}}</td>
</tr>
<tr>
<td>Multisig</td>
<td>\texttt{&lt;m&gt; \texttt{&lt;A\ pub\ key\ &gt; [B\ pub\ key]\ [C\ pub\ key]\ &lt;n&gt; \texttt{OP_CHECKMULTISIG}}}</td>
</tr>
<tr>
<td>Null Data</td>
<td>\texttt{OP_RETURN &lt;0\ to\ 40\ bytes\ of\ data&gt;}</td>
</tr>
</tbody>
</table>

BY DESIGN, the scripting language is **stack-based** and **NOT Turing-complete**
Some standard transaction scripts

<table>
<thead>
<tr>
<th>Type</th>
<th>Script</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pay to Public Key Hash (P2PKH)</td>
<td><code>OP_DUP OP_HASH160 &lt;PubKeyHash&gt; OP_EQUALVERIFY OP_CHECKSIG</code></td>
</tr>
<tr>
<td>Pay to Script Hash (P2SH)</td>
<td><code>OP_HASH160 &lt;Hash160(redeemScript)&gt; OP_EQUAL</code></td>
</tr>
<tr>
<td>Multisig</td>
<td><code>&lt;m&gt; &lt;A pubkey&gt; [B pubkey] [C pubkey] &lt;n&gt; OP_CHECKMULTISIG</code></td>
</tr>
<tr>
<td>Null Data</td>
<td><code>OP_RETURN &lt;0 to 40 bytes of data&gt;</code></td>
</tr>
</tbody>
</table>

BY DESIGN, the scripting language is **stack-based** and **NOT Turing-complete**
OP_RETURN:
A decentralized, trusted means to “send” data

Recent Metadata in the Bitcoin Blockchain

Below is a list of metadata recently embedded in the bitcoin blockchain using OP_RETURN outputs. This method was made official in Bitcoin 0.9 due to user demand. Opinions differ strongly and the future is open.

Also from Coin Sciences: MultiChain for private blockchains with full compatibility with Bitcoin Core. More on OP_RETURN: CoinSpark protocol – Bitcoin 2.0 presentation – PHP and Python libraries.
Blockstore

Name registrations on the Bitcoin blockchain
Select a document and have it certified in the Bitcoin blockchain

Click here or drag and drop your document in the box. The file will NOT be uploaded. The cryptographic proof is calculated client-side.

<table>
<thead>
<tr>
<th>Document Digest</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>c8f1ccebe28241c3a0e746e47ced975a8d1c230cad2e8f4095b88d3cf8a8a61e</td>
<td>2015-11-16 17:21:32</td>
</tr>
<tr>
<td>ab80c7bbbaef379557c4684f6cbf9cd4e79f5bd49c3da56ca9fefe4732f43fe71</td>
<td>2015-11-16 17:20:35</td>
</tr>
<tr>
<td>ec9e5dc0a93e91ab5ed0679406064c8cbdf52c50b5d74763fe570e9bc160362</td>
<td>2015-11-16 14:08:33</td>
</tr>
<tr>
<td>c2d623cc7ea0094d7b07f1ef7da5ab95189e45ac92b0842aeea9a048d4e84a53</td>
<td>2015-11-16 13:39:44</td>
</tr>
<tr>
<td>315f5db78d078c43b8ac0064e4a0164612b1fce77c869345bfc94c75894edd3</td>
<td>2015-11-16 13:16:10</td>
</tr>
</tbody>
</table>
Bitcoin Entrepreneur Registers Birth of Child on the Blockchain

Santiago Siri, an entrepreneur and developer based in San Francisco welcomed the birth of his first child named Roma with a proof-of-birth registration on bitcoin’s blockchain. Siri used a blockchain verification...
Crypto-Currency to Crypto-Economics

- **Currency**
  - Transfers
  - Payments
  - Tips
  - Crowdfunding

- **Pegged Services**
  - Naming
  - Identity
  - Ownership
  - Membership
  - Voting

- **Smart Contracts**
  - Wagers
  - Bounties
  - Family Trusts
  - Performance Proofs
  - Escrow

- **Decentralized, Autonomous Organizations**
  - Transportation
  - Online Storage
  - Mesh Networks
  - Healthcare

Source: Mougayar 2014
What Are Smart Contracts? Cryptocurrency's Killer App

By giving computers control over contracts, we can make business more efficient and make the legal system more equitable.

By Jay Cassano

What if you could cut your mortgage rate, make it easier to update your will, and ensure that your buddy was never able to weasel out of paying up on a bet? That and much more is the promise of smart contracts, a technology that is getting closer and closer to reality thanks to cryptocurrency.

Smart contracts are computer programs that can automatically execute the terms of a contract. Someday, these programs may replace lawyers and banks for handling certain common financial transactions.

And the potential for smart contracts goes way beyond simple transfers of funds. The door of a car or a house could be unlocked by connecting smart contracts to the Internet of everything. But as always with this cutting edge of financial technology, major
**WHAT IS ETHEREUM?**

Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.

Ethereum is how the Internet was supposed to work.

Ethereum was crowdfunded during August 2014 by fans all around the world. It is developed by ETHDEV with contributions from great minds across the globe.

---

**WHAT IS THE FRONTIER RELEASE?**

Frontier is the first release of the Ethereum project, tailored specifically for developers. It’s a command line only interface with a Javascript environment that allows building, testing, deploying and using decentralized applications on the Ethereum blockchain.

Exploring the Frontier presents vast opportunities, but also many dangers, and is not for everyone.
Smart Property in Action

Smart property is to deeds as Bitcoin is to money. In the same way that Bitcoin revolutionized the concept of currency, smart property revolutionizes the concept of ownership, removing the need for a central authority to say who owns what. Our system of ownership is just one in a growing line of things to be decentralized, but will inevitably be among the most important. The question is, how can we enforce such a system without the firepower backing modern courts?

For those of you still trying to grasp this idea, it’s helpful to remember that bitcoins are not actually things: Bitcoin is a decentralized system for deciding who owns what.
## Pros and Cons

<table>
<thead>
<tr>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freedom of payment</td>
<td>Limited adoption</td>
</tr>
<tr>
<td>Extremely low fees</td>
<td>High value volatility</td>
</tr>
<tr>
<td>Micropayments are going without a hitch</td>
<td>Still a bit shaky and unfinished</td>
</tr>
<tr>
<td>Transparent and neutral</td>
<td>Facilitates illegal and dubious practices</td>
</tr>
<tr>
<td>Banking the unbanked</td>
<td>No recourse to authority</td>
</tr>
<tr>
<td>Protection and control</td>
<td>Coins can be stolen</td>
</tr>
<tr>
<td>Lower risk for sellers</td>
<td>A new and unfamiliar form of supervision</td>
</tr>
</tbody>
</table>
“Bitcoin...Stay away from it. It's a mirage, basically...” Warren Buffet

“It will be everywhere and the world will have to readjust”, John McAfee

“I'm a big fan of Bitcoin ... Regulation of money supply needs to be depoliticized.” Al Gore

“You need to be really rich, really idealistic, or really crazy to invest in Bitcoin”, Andrew Couts

“I want Bitcoin to die in a fire”, Charlie Stross

“Bitcoin is a technological tour de force.” Bill Gates

“Bitcoin is the beginning of something great: a currency without a government, something necessary and imperative.” Nassim Nicholas Taleb

“Bitcoin Is Evil”, Paul Krugman
Final notes: bumps in the road ahead

• Told to Richard Feynman by a Buddhist monk:
  “To every man is given the key to the gates of heaven; the same key opens the gates of hell”

• Existing and Undiscovered Vulnerabilities
  – 51% rule
  – Zero-day attacks?
  – Wallet security problems

• Slow Performance
  – Slow: minutes-to-hours per transaction
  – When to assume a transaction is “valid”?
    • Rule of thumb: after 6 blocks

• The future
  – Lots of Fear-Uncertainty & Doubt (FUD)
  – ... but one thing is for certain: Blockchain is here to stay
Nasdaq says to develop blockchain services in Estonia

NEW YORK | BY JOHN MCCRANK

A Bitcoin logo is displayed at the Bitcoin Center New York City in New York's financial district July 28, 2015. REUTERS/BRENDAN MCDERMID

Exchange and clearing house operator Nasdaq Inc plans to develop several applications for blockchain, the technology underpinning the digital currency bitcoin, using its Estonian settling and clearing business, a senior Nasdaq executive said on Friday.
Credits

• Noun Project icons
  – Iceberg by Florent from the Noun Project
  – Cow by Chris Pyper from the Noun Project
  – Chicken by Verena Gutentag from the Noun Project
  – Pig by Ealancheliyan from the Noun Project

• Bitcoin quotes image from “Block Chain 2.0: The Renaissance of Money”, Wired, January 2015


• NASDAQ to develop blockchain services in Estonia, Reuters (Brendan McDermid)