Intro to The Blockchain
What if I Told You ... the Blockchain Could Disrupt ... Everything

From Silicon Valley to Wall Street, technologists and investors alike are buzzing about the potential for the Blockchain to revolutionize ... well everything. The hype is high and the potential is real but roadblocks remain. The funding backdrop is healthy and the application eco-system is growing. Once considered the underlying pipes of Bitcoin, this technology is quickly taking center stage from its crypto-currency parent promising an ushering in of a new set of tools to cut costs and challenge the profit pool of the middle-man with a promise to make centralized institutions obsolete. This solution promises to not just address consumer opportunities but also those for the far more lucrative enterprise.

What if I told you that Bitcoin was just the opening act ... with the Blockchain ready to take center stage. In its purest form, the Blockchain is a digital platform that records and verifies transactions in a tamper- and revision-proof way that is public to all (Exhibit 1). Levering the same peer-to-peer technology first developed in a dorm room at Northeastern University with Napster (and subsequently built upon by folks like Skype and Spotify) the tool was first born out of a need to track and create Bitcoin. Specifically, Bitcoin and other cryptocurrencies required a way of building agreement between all parties involved in a transaction. From buying to selling to trading to storing, every transaction would be chained to each other so one could never duplicate or change the ownership of Bitcoin. This Blockchain allows information to be put in, but never deleted. This complete history ... a “shared public ledger” that a network (and the currency) relies on, if you will - made, in the user’s mind, the role of a Central Bank obsolete (Exhibit 2). The flat of the currency, as a result, was born of the citizens of the internet, not a central clearing institution or agency. Lastly, while the Blockchain associated with Bitcoin remains the most well known, there are growing sets of private and permission-driven shared ledgers gaining traction and worth focusing on.

Exhibit 1: The Blockchain is a distributed, public ledger, most commonly known as the core underlying technology for Bitcoin

Exhibit 2: The size of the Blockchain grows along with the no. of transactions

Source: Goldman Sachs Global Investment Research.
Why?
“In the mainframe’s early days, the 1950s, IBM sold the first era of mainframes to businesses that didn’t even know they needed them.”
Edgar F. Codd
1923-2003

Codd invented the relational database while working for IBM.

He revolutionised the way in which data was stored and retrieved.
and then...
Open Source Peer-to-Peer Money
## Bitcoin Network statistics (as of 2016-05-16 22:57:13)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Block</td>
<td>2009-01-03 18:15:05</td>
</tr>
<tr>
<td>Total number of full nodes on the network</td>
<td>5,635</td>
</tr>
<tr>
<td>Total monetary base</td>
<td>15,552,450 BTC</td>
</tr>
<tr>
<td>Total market capitalization</td>
<td>$ 7,061,994,286</td>
</tr>
<tr>
<td>24 hour trade volume</td>
<td>$ 60,323,200</td>
</tr>
<tr>
<td>Transactions per second</td>
<td>~ 7</td>
</tr>
<tr>
<td>Size of blockchain</td>
<td>68 GB</td>
</tr>
<tr>
<td>Hash rate of the network</td>
<td>1,616,378,377,000,000,000 hashes/second (exa)</td>
</tr>
</tbody>
</table>
A blockchain is a time-stamped, non-repudiable database that contains the entire logged history of transactions on the system.

Each transaction processor on the system maintains their own local copy of this database and the consensus formation algorithms enable every copy to stay in sync.
Blockchain networks are peer-to-peer networks. Open blockchain networks are permissionless - any client can sync to the network and begin to participate.
Consensus mechanisms determine the state of the blockchain database, as well as which state transitions are acceptable according to protocol rules. Transaction processors are often referred to as miners.
Cryptographic tokens (cryptocurrency) are cryptographically secured digital unit of account (numeraire), medium of exchange (currency), and a store of value. These tokens play an integral role in the incentivization mechanisms of public blockchain networks.

Token balances are stored via entries on the blockchain database. An account address is identified by the public key of a user.
A virtual machine enables programmable blockchain transactions. The virtual machine is the mechanism that allows for smart contract based decentralized applications.
ALMOST $1BN OF TOTAL INVESTMENT OVER THE PAST 36 MONTHS

<table>
<thead>
<tr>
<th></th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>#Investments</td>
<td>3</td>
<td>4</td>
<td>7</td>
<td>12</td>
<td>11</td>
<td>16</td>
<td>11</td>
<td>22</td>
<td>13</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>≥$10m</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Europe</td>
<td>#Investments</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>7</td>
<td>2</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>≥$10m</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>RoW</td>
<td>#Investments</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>11</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>≥$10m</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

2015 has marked a transition to investors backing leaders rather than experiments, with the top 10 companies raising more than 80% of the total funding this year.

Source: CoinDesk, Pitchbook, VentureSource, VentureScanner, Crunchbase
Note: Data as of December 1, 2015

© 2016 consensys.net
Blockchain (Use Cases)
Source: GrowthPraxis

- 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: Bloos, Bigproof, ascribe, Artius
    - Other companies: ChainyLink, Stampery

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

- 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

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

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

- Proof of ownership of modules in app development
  - Company: Assembly

- Proof of ownership for digital content storage and delivery
  - Companies: BlockIoT (Alexandria), BitHolder, Blockchain, The Rudimental, BlockICON

- Points based value transfer for ride sharing
  - Company: LaZooZ

- Digital security trading: ownership and transfer
  - Companies: Symbiant, Miner, Sortizte, Secure Assets, BitShares, Coins-e, equityStx, OXMarkets, Mutia

- 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: ChimeraInc.io
  - Industries: Filament

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

- Escrow/Custodian service
  - Gaming industry
    - Companies: PlayCoin, Bitplay
  - Gaming industry and loan servicing
    - Companies: New System Technologies
  - E-commerce
    - Company: Fundis.org
  - A smart contract IT portal executing order fulfillment in e-commerce/manufacturing
    - Company: UbEMS
The World Computer - Open Source Peer-to-Peer Applications
**Ethereum Network statistics (as of 2016-05-16 22:57:13)**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Block</td>
<td>2015-07-30 15:26:13</td>
</tr>
<tr>
<td>Total number of full nodes on the network</td>
<td>6,934</td>
</tr>
<tr>
<td>Total monetary base</td>
<td>80,098,146 ETH</td>
</tr>
<tr>
<td>Total market capitalization</td>
<td>$ ~ 1.1 B</td>
</tr>
<tr>
<td>24 hour trade volume</td>
<td>$ 32,997,600</td>
</tr>
<tr>
<td>Transactions per second</td>
<td>~ 20</td>
</tr>
<tr>
<td>Size of blockchain</td>
<td>18 GB</td>
</tr>
<tr>
<td>Hash rate of the network</td>
<td>2,100,000,000,000,000 hashes/second (tera)</td>
</tr>
<tr>
<td>Total funding raised by Ethereum projects</td>
<td>&gt; $125,000,000</td>
</tr>
</tbody>
</table>
An Ethereum smart contract to sell a website for "5000 by March"

First, store buyer's Ethereum address:
```
put BUYER 0x6af26739b9ffe8a2985252e5357fde
```

Then, store seller's Ethereum address:
```
put SELLER 0xfeab802c014588f08bfee2741086c375
```

April 1, 2014 is 1396310400 in "computer time"
```
put DEADLINE 1396310400
```

If the agreed amount is received on time:
```
when contract balance ≥ 5000 ether
and block timestamp ≤ data at slot DEADLINE
then ...
```
... then designate the buyer as the new website admin and pay the seller
```
in WEBSITE_ADMIN put data at slot BUYER
spend contract balance to data at slot SELLER
```
This New York Project Fuses Energy Microgrids With Blockchain Technology

A microgrid using TransActive Grid’s model could let you directly sell energy generated from your rooftop solar panels to your neighbor.

[Photo: [H]i[photo via Shutterstock]
ETH BaaS in the news

“The Ethereum project and ConsenSys, the company created by one of the project’s co-creators, have received a huge vote of approval from one of the world’s biggest enterprise software providers — Microsoft.”
- Tech Crunch

“It’s available as part of Microsoft Azure cloud and is primarily targeted at the financial services industry.”
- Wired

“Anything that can be digitized, cryptocurrencies, derivatives trading, securities trading and settlement, even property titles, is a potential service on Ethereum.”
- Wall Street Journal

“We’ve found Azure to be an efficient and powerful cloud to deploy our offerings and are looking forward to further collaboration with Microsoft. The initial offerings of BlockApps Strato and Ether.Camp will serve as foundational protocols and tools for developers to create blockchain applications immediately.”
- Coin Desk
Thank You!