IMPACT OF THE BLOCKCHAIN

A Summary for Investment Professionals

June 2015
EXECUTIVE SUMMARY

A disruptive technology is creating a unique opportunity
- The status quo: dependence on centralized databases with a single point of failure
- The blockchain: enables secure access, secure time stamps, 24x7x365 uptime and indelible data

Security and decentralization are core to blockchain functionality
- A peer-to-peer network with digital signatures and specialized verification agents
- Economic value and security on the blockchain are inherently intertwined
- Unique incentive structure

Facilitates new categories and services
- Certainty-as-a-Service
- An innovative and important interaction model within the Internet-of-Things

A dynamic and compelling investment landscape
- Effects on publicly traded companies will not be immediate
- Certain types of blockchain venture opportunities have already become crowded while others remain largely unexplored and present interesting possibilities for investment
- Direct exposure to the blockchain is a unique and compelling opportunity
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The status quo: centralized recordkeeping</td>
<td>5</td>
</tr>
<tr>
<td>The blockchain: a decentralized database</td>
<td>8</td>
</tr>
<tr>
<td>Blockchain deep dive: how it works</td>
<td>13</td>
</tr>
<tr>
<td>The synchronization problem</td>
<td>14</td>
</tr>
<tr>
<td>Peer-to-peer networks</td>
<td>15</td>
</tr>
<tr>
<td>A detailed look</td>
<td>17</td>
</tr>
<tr>
<td>The economics of verifying data</td>
<td>18</td>
</tr>
<tr>
<td>Certainty-as-a-Service (CaaS)</td>
<td>20</td>
</tr>
<tr>
<td>Blockchain technology: ways to invest</td>
<td>24</td>
</tr>
<tr>
<td>Public companies</td>
<td>26</td>
</tr>
<tr>
<td>Private companies</td>
<td>27</td>
</tr>
<tr>
<td>Direct exposure</td>
<td>28</td>
</tr>
<tr>
<td>The blockchain beyond CaaS</td>
<td>33</td>
</tr>
<tr>
<td>Catalysts</td>
<td>36</td>
</tr>
<tr>
<td>Key takeaways</td>
<td>37</td>
</tr>
</tbody>
</table>
Disruptive technologies tend to start off generating skepticism... until they completely revolutionize how we live and work.

“We’re not convinced the economics of blockchain work out for anything but a few high-intensity use cases.”

Financial Times

“Television won’t be able to hold on to any market it captures after the first six months. People will soon get tired of staring at a plywood box every night.”

Darryl Zanuck, 20th Century Fox

“Half the adults in America do not have Internet access and 57% of those non-users are not interested in getting online. This suggests that the booming growth of the American Internet population in the past few years will slow.”

Pew Research Center

“We’re not convinced the economics of blockchain work out for anything but a few high-intensity use cases.”

Financial Times
The status quo:
centralized recordkeeping
WE ARE ACCUSTOMED TO A WORLD IN WHICH CENTRALIZED RECORDKEEPING IS THE STATUS QUO

Centralization is the norm but it has drawbacks. Consider the benefits of a world *without* database centralization…

**Abundant examples: systems reliant on a central server**
- iMessage?
- Whatsapp?
- WeChat? All are terrific. Too bad they’re not interoperable.
- Your medical records reside on some company’s servers in the cloud—but are inaccessible to you!
- “Sorry, we don’t have your reservation in our system”
- “ Hackers found a way into our network and got your SSN from our server. Sorry.”
- Would you prefer trade settlement at DTCC, DTCC or perhaps DTCC? Remember Hurricane Sandy?
- Title insurance: it’s 2015 – why does it still exist?!

**A version without a central server**
- Messaging becomes more like email: *anyone can reach anyone.*
- Your personal medical data is *under your control* – you choose who to provide it to.
- Your reservation cannot magically disappear
- Sensitive data isn’t kept on servers that you don’t control. There is nothing for the hackers to steal.
- A decentralized database runs on thousands of computers around the world. *Uptime is 24x7x365.* No disaster can shut it down.
- Disintermediation means there is no ambiguity about ownership. No more paying for useless paperwork.
### DATABASE DECENTRALIZATION AND RECORDKEEPING

**Disintermediation Have Powerful Consequences**

<table>
<thead>
<tr>
<th>Medical records today…</th>
<th>…vs. tomorrow</th>
</tr>
</thead>
<tbody>
<tr>
<td>‣ Sit in several centralized records controlled by different physicians</td>
<td>‣ Records across and among doctors, but easily shared and under patient control</td>
</tr>
<tr>
<td>‣ Not easily accessible during emergency</td>
<td>‣ Access control and visibility determined by patient</td>
</tr>
<tr>
<td>‣ Not controlled or easily accessible by patient</td>
<td>‣ Easily available in case of emergency</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Brokerage OTC trading today…</th>
<th>…vs. tomorrow</th>
</tr>
</thead>
<tbody>
<tr>
<td>‣ Dominated by third parties</td>
<td>‣ Same day trade settlement</td>
</tr>
<tr>
<td>‣ Ties up capital for days</td>
<td>‣ Irrefutable audit trail</td>
</tr>
<tr>
<td>‣ Prone to errors</td>
<td>‣ Eliminate third parties / new revenue stream</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wills today…</th>
<th>…vs. tomorrow</th>
</tr>
</thead>
<tbody>
<tr>
<td>‣ No formal retention method</td>
<td>‣ Certainty of execution timing</td>
</tr>
<tr>
<td>‣ Frequently contested</td>
<td>‣ Integrity of data</td>
</tr>
<tr>
<td>‣ Subject to manipulation</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event tickets today…</th>
<th>…vs. tomorrow</th>
</tr>
</thead>
<tbody>
<tr>
<td>‣ Secondary market introduces extra costs</td>
<td>‣ Lower costs</td>
</tr>
<tr>
<td>‣ Counterfeits</td>
<td>‣ Eliminates counterfeits</td>
</tr>
<tr>
<td>‣ Sluggish transfer</td>
<td>‣ Allows for instant ownership transfer</td>
</tr>
</tbody>
</table>
The blockchain:

a decentralized database
HOW IS DATABASE DECENTRALIZATION RELATED TO THE BLOCKCHAIN?

The blockchain is a decentralized database.

- Runs on a peer-to-peer network of computers around the globe
- Each computer in the network contains a copy of a continuously updated database
- That continuously updated database is the blockchain
- Records data indelibly, securely and with an irrefutable time stamp
- Ensures only designated parties have control of data
- Creates certainty of script/code execution
Use of the blockchain improves an abundance of applications across many verticals.
THE BLOCKCHAIN DELIVERS A NEXT-GENERATION TECHNOLOGY SOLUTION

Every item of verified data in the blockchain is:

- Permanent, unable to be altered
- Controlled by a specific party (or group) via digital signature(s)
- Time-stamped, available 24x7x365
- Without any single point of failure
- Not at risk of hacking or a central administrator’s accident
- Not subject to artificial rules or rule changes
THE PROMISE OF THE BLOCKCHAIN IS INCREDIBLY COMPELLING AND CAPTURING INTEREST

Venture capital is pouring in, developers are excited and industry players are taking note.

They see a vision of:

- Building on an existing peer-to-peer, open system that will change how we conduct business in the future
- A world where agents interact with each other securely and directly, from afar, for everything—that mechanism is the blockchain
- Mutual contracts, deposits, escrow, dispute mediation, insurance, trading and micro-transactions, property registration and transfer…all being enabled by the blockchain, at a negligible cost
- An efficient interaction process for the Internet-of-Things

![Investments in blockchain-related startups](chart.png)
Blockchain deep dive:
how it works
HOW DOES THE BLOCKCHAIN WORK?
HOW DOES IT ACHIEVE DATABASE DECENTRALIZATION?

The blockchain solves a long-standing synchronization problem that had prevented decentralized databases in the past.

Synchronization works well when computers trust each other…

"I'll accept data coming from the other computer."

...but if there is a lack of trust, synchronization becomes impossible.

"I don’t trust that computer. I won’t accept its data."

The trust problem grows exponentially with more computers…

Who’s data came first?

...as does the complexity of verifying data.

The easiest way to solve the synchronization problem is simply to use a central party to coordinate. Network participants can be relatively certain of the sanctity of the data…

...but central parties are vulnerable to attack, error and fraud. They can introduce artificial rules and reap monopolistic profits. It’s great for shareholders, but it’s a situation ripe for disruption by new technology.
Instead of the *relative confidence* provided by central servers, the blockchain provides *certainty* by solving the synchronization problem. The solution starts with a peer-to-peer (P2P) network...

**P2P Network**

1. Each computer on the P2P network running blockchain software has a copy of the database (the blockchain) and can receive *updates* at any time.

2. Blockchain updates always *refer to a prior database entry* (hence the concept of updates and the suffix “chain” in *blockchain*). Anyone sending an update must include a unique *digital signature* proving control of the prior entry.

3. Certain peer computers function as *verification agents* that (a) check the digital signature, (b) confirm that the sender hasn’t previously sent a conflicting update (i.e., conceptually similar to verifying that the sender hasn’t signed two conflicting contracts referencing the same piece of property), and (c) verify that nothing else in the update is invalid.
...With time stamps, digital signatures, references to prior updates and verification agents

Each update in the blockchain is referred to as a *transaction*. Transactions always refer to prior updates.

Users can provide control to themselves for subsequent updates, as Tim has done here.

The structure of the blockchain contains entries for: time stamps, digital signatures, data, references to prior updates, amounts of bitcoins, verification agent fees, subsequent signature requirements, scripts to be run and other items.

<table>
<thead>
<tr>
<th>Time</th>
<th>Digital Signature(s) used in current transaction:</th>
<th>Source Address (controlled by current signatory)</th>
<th>Reference to prior transaction</th>
<th>Recipient Address</th>
<th>Data</th>
<th>Bitcoins at source address prior to transaction</th>
<th>Bitcoins Sent to Recipient</th>
<th>Fee to Verif Agent</th>
<th>Signature(s) required for next transaction:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:59:38 PM</td>
<td>Tammy Tone</td>
<td>12efew [limited]</td>
<td>1estgE [a secret]</td>
<td>0.050</td>
<td>0.020</td>
<td>0.015</td>
<td>Person A or B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:53:31 PM</td>
<td>John Smith</td>
<td>1wEfet [null]</td>
<td>1ewYUe [null]</td>
<td>25.000</td>
<td>6.000</td>
<td>0.010</td>
<td>Frank Xiao</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:52:37 PM</td>
<td>Joe Bookie</td>
<td>1Nuyts [null]</td>
<td>1wEfet [bet winner]</td>
<td>87.500</td>
<td>25.000</td>
<td>0.020</td>
<td>John Smith</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:52:25 PM</td>
<td>John Smith</td>
<td>1EWseg [null]</td>
<td>1Nuyts [sports bet]</td>
<td>12.515</td>
<td>12.500</td>
<td>0.015</td>
<td>Joe Bookie</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:51:04 PM</td>
<td>Frank Heinz</td>
<td>1Wefw [null]</td>
<td>1EWseg [null]</td>
<td>18.000</td>
<td>12.515</td>
<td>0.015</td>
<td>John Smith</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Not all entries are required at all times but some must always be included (examples: signatures, references to prior updates)
The verification agents are on the lookout for new updates (transactions) sent by users. Upon receipt of a new transaction, a VA will examine it for validity. Once confirmed by a VA, the valid transactions will be grouped into a block and the entire block will be added to the blockchain (hence the prefix block in blockchain.)

The process of adding a new block occurs approximately once every ten minutes. There is no way of knowing in advance which VA will be in charge of collecting the most recent valid transactions and combining them into a block. Different VAs will be in charge at different times. The constant changing of VAs ensures a lack of centralization.
The system works well but hinges on the active participation of verification agents, without whom the system would be completely unsecure.

The system can’t rely on just one verification agent – that would be similar to relying on a central server.

The blockchain requires as many verification agents as possible, all of whom compete to do the job.

But the verification process is costly: it requires electricity, computer hardware and various other expenses.

Why would anyone engage in this activity? That answer lies within the transaction fees.

Every transaction includes a small fee to be collected by the verification agent. The fee is denominated in bitcoin. Using bitcoin in this manner is a requirement: in order for the system to remain independent and decentralized, it must have its own indigenous unit of economic value.

Bitcoin isn’t a currency, per se. It is the blockchain-native unit of economic value used for compensating the verification agents.

The work of the verification agent enables the blockchain to provide strong certainty regarding verified data.

Put differently, the blockchain provides Certainty-as-a-Service (CaaS). Users pay to have a much higher level of certainty than would be provided by a central server.
THE MORE VERIFICATION AGENTS AT WORK, THE SAFER THE BLOCKCHAIN

To maintain the security of the database, the blockchain looks for as much participation as possible in the verification process. The algorithm underpinning the blockchain automatically runs verification contests approximately every ten minutes (the approximate time since the most recent block was added.)

The winner of the contest is responsible for verifying all of the new data since the prior contest was won. In exchange for verifying the data, the winning verification agent is granted all of the transaction fees within the data being verified.

The probability of winning the verification contest is proportional to the amount of computing power dedicated to the task. As more people – and now businesses – are recognizing the demand for certainty-as-a-service (strong certainty) offered by the blockchain, more have entered the verification race.

Electricity usage is a good proxy for the amount of computing power dedicated to the verification process. Usage has grown continuously since 2011 and now stands at approx. 25 million MWh / year.

Note: in this presentation we refer to verification agents. In the blockchain lexicon, the verification agents are referred to as miners. Miners receive not only transaction fees but also extra bitcoins referred to as the block reward (the creation of newly minted bitcoins). Right now, the block reward is more valuable than the transaction fees, but over time that will change.
The blockchain enables
Certainty as a Service (CaaS)
THE BLOCKCHAIN CREATES CERTAINTY-AS-A-SERVICE (CaaS)

Every item of verified data in the blockchain is:

- Indelible
- Time-stamped
- Controlled by a specific party (or group) via digital signature(s)
- Not at risk of hacking or a central administrator’s accident
- Without any single point of failure
- Not subject to artificial rules or rule changes
- Available 24x7x365

-but-

- Certain resources within the blockchain are inherently scarce
- Security requires economic incentives (bitcoins)

The blockchain enables Certainty-as-a-Service. Never before available, CaaS is often superior to the relative confidence provided by centralized databases.
CaaS PROVIDES INNOVATIVE IMPROVEMENTS TO LEGACY BUSINESS PROCESSES

Example: event tickets on the blockchain

- Counterfeits are not possible
- Tickets cannot be stolen
- Control: ticket issuers can provide partial or full control to purchasers regarding secondary market sales (i.e. enable issuer participation in secondary market revenue)
- Allow participation of intermediaries at the discretion of the issuer
- Enable the sales of supplemental items after the ticket has already been purchased
- Enables proof-of-attendance (e.g. for non-entertainment events)
- No concerns about server failure: the blockchain provides 24x7x365 uptime
- Tickets accessible on your smartphone... or, if you lose your smartphone, you can access the tickets from any smartphone
FOR NUMEROUS APPLICATIONS THE BLOCKCHAIN IS SUPERIOR TO TRADITIONAL DATABASES

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Blockchain storage</th>
<th>Amazon cloud DB</th>
</tr>
</thead>
<tbody>
<tr>
<td>24x7x365 uptime</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Cannot be modified by DBA</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Indelible, irrefutable time stamps</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Publicly available iterative history</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Characteristics of applications that benefit most from the blockchain:**

- Public broadcast
- Permanently recorded
- Pay-as-you-go
- Tiny payload
- High value
- Security derived from confirmation time
Blockchain technologies: ways to invest
THE BLOCKCHAIN AND CaaS ARE INTERESTING INNOVATIONS: HOW CAN INVESTORS GET INVOLVED?

Three pathways for investors: public companies, private ventures and direct investment. **Most attractive right now: private ventures and direct investment**

(A) Public
Many companies impacted

- TSM, INTC, QCOM, ARM.LN, IBM, NYX, NDAQ, CACI, SAIC, BAH, ACN, UPS, FDX, BPTY.LN, AYA.T, ZNGA, LM, UBS, AMZN, Rakuten (3755.T), EXPE, DISH, MSFT

Not yet attractive insofar as timing is somewhat nebulous

(B) Private
Approximately 200 startups

- EllipBc
- OneName
- AlphaPoint
- Ledger
- MeloBc
- Vaurum
- BitPay
- Coinplug
- BlockCypher
- TradeBlock
- Coinsetter
- BlockScore
- Colu
- KnC Miner
- Bitstream
- Bitreserve
- Chain
- Bitnet
- PeerNova
- Bitstamp
- Kraken
- Bitpay
- BitGo
- Gem
- BitFury
- Circle
- 21e6
- Coinbase

Attractive, but access to deal flow and strong understanding are required

(C) Direct
Exposure to bitcoin

- bitcoin

Attractive, but with unique requirements for participation
(A) PUBLIC COMPANIES:
MANY WILL BE AFFECTED, BUT TIMING IS UNCERTAIN

The blockchain will impact many established players. The hard part is determining the magnitude and timing of the impact.

**POTENTIAL WINNERS**
- Semiconductor companies: TSM, INTC (both are currently producing chips for blockchain-related applications)
- Fabless semi companies: QCOM, ARM.LN
- Internet-of-Things (IoT) architects: IBM
- Certain exchanges: NYX, NDAQ
- Government and military contractors for IT integration projects: CACI, SAIC, BAH, ACN
- Logistics: UPS, FDX
- Online gambling / gaming: BPTY.LN, AYA.T, ZNGA
- Forward thinking financial institutions: LM, UBS
- E-commerce: AMZN, Rakuten 3755.T, EXPE, DISH, MSFT

**POTENTIAL LOSERS**
- Title Insurers: FNF, FAF
- Event ticketing: LYV, CVT, Eventbrite (private for now)
- Electronic Health Records Companies: ATHN, MDRX, MCK
- Automotive records: TRAK
- Online education companies: APOL, STRA
- Domain names: GDDY, WWWW
- File storage: BOX, Dropbox (private for now)
- Clearinghouses: CME, ICE
- Custody banks, records keepers: NTRS, STT, BNY
- Remittances: WU, MGI
- Currency printing: DLAR.LN
(B) PRIVATE INVESTMENT:
A GROWING POOL OF STARTUPS TO CHOOSE FROM

Private ventures: a good way to gain exposure but selectivity is required

Many opportunities but certain varieties of startups are inherently better positioned than others

- Exchange space is cramped
  - Bitstamp, Bitfinex, Coinbase, OKCoin, Noble Markets, many others

- Mining: difficult economics
  - BitFury, KnC, Ghash.io, AntMiner, Spondoolies

- Wallets and storage: possibly interesting
  - BitGo, Xapo, Elliptic

- “2.0” investments seem most compelling
  - Factom, Edgelogic, World Passport, ChromaWay, Blockstream, Swarm

Cumulative Investments in blockchain-related startups

Million USD

<table>
<thead>
<tr>
<th>Year</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>
<th>Q4</th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>8</td>
<td>22</td>
<td>35</td>
<td>100</td>
<td>251</td>
<td>337</td>
<td>474</td>
<td>703</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2014</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2015</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
**DIRECT EXPOSURE TO BITCOIN: A UNIQUE OPPORTUNITY**

Bitcoin provides investors with direct economic exposure to usage of the blockchain. But what valuation framework can investors use? The answer: look at supply and demand for CaaS.

1. Given that bitcoin is a non-earning asset, a supply/demand approach is required. One method is to examine the supply and demand for CaaS. In any given period of time, the supply of CaaS is provided by space for data in new blocks added to the blockchain. As of now, the maximum block size is 1 MB.

2. When blocks are not full, verification agents are price takers. When blocks are full, the supply of space for data is completely inelastic, and verification agents can choose the data items with the highest fees. As CaaS applications demand more space within each block, CaaS users must increase the bitcoin fees paid to verification agents.

---

**Limited supply in the blockchain: full blocks vs. unfilled blocks**

Regarding transaction fees: when blocks are not full, verification agents are price takers. Regarding transaction fees: when blocks are full, the verification agent that won the contest has a monopoly on the block. It chooses only data / transactions that have the highest fees, fills the block and excludes data with insufficient fees.
Demand for CaaS and supply of space in blocks determines the long-term equilibrium price for bitcoin

With verification agents holding momentary monopolies on the addition of data to a block, CaaS applications will require higher fees to ensure their data ends up in a block.

The equilibrium point for fees will be determined on an application-by-application basis, with user willingness to pay related to the value of CaaS vs. alternatives.

Different demand curves exist based on the relative value of CaaS for each application (figure 2.)

Example: demand for CaaS will likely be higher for medical records than for concert tickets.

As demand curves for fees move to the right, so too will demand curves for bitcoin in the marketplace (figure 3.)

Note: the 1 MB limit was originally set as an arbitrary parameter. Technically, a size increase is not impossible, but it would require the participation / approval of many parties, which would be difficult to achieve. Beyond the difficulty of achieving consensus regarding a block size increase, there are limitations: large blocks will be impracticable both for network propagation and for processing by verification agents. 10 MB blocks would be quite difficult to implement. At any given block size, supply is inelastic once blocks are full.
A straightforward way of examining supply of CaaS is to look at *digital fingerprints*. Each digital fingerprint is a compressed piece of data that can be stored in the blockchain (secure, time stamped, etc.)

Like human fingerprints, digital fingerprints are unique: a concert ticket for a particular person on a specific date with a specific seat will have a unique digital fingerprint, requiring only a tiny amount of data.

A digital fingerprint can be indelibly and securely written to the blockchain as a time stamped record of any document, event, etc. The person adding the entry to the blockchain can maintain exclusive control of it or allow others to control it.
(C) DIRECT EXPOSURE TO BITCOIN: EXAMINED QUANTITATIVELY THROUGH CaaS AND DIGITAL FINGERPRINTS

Digital fingerprints: supply / demand imbalance

Supply is constrained

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Block size (MB)</td>
<td>1</td>
</tr>
<tr>
<td>Est. transaction size with data payload (bytes)</td>
<td>768</td>
</tr>
<tr>
<td>Transactions per 1 MB block</td>
<td>1,365</td>
</tr>
<tr>
<td>Approx max digital fingerprints per transaction</td>
<td>12.0</td>
</tr>
<tr>
<td>Digital fingerprints per 1 MB block</td>
<td>16,384</td>
</tr>
<tr>
<td>Blocks per year</td>
<td>52,560</td>
</tr>
<tr>
<td>Digital fingerprints per year:</td>
<td>861,143,040</td>
</tr>
</tbody>
</table>

Each of these is 100 million

Demand categories are growing

A few sample items:

- Flu vaccines given (US)
- Amtrak tickets
- Birth certificates (global)
- Visas issued for travel to US
- University degrees issued (US)
- Auto insurance policies in force (US)
- Baseball tickets (US)
- Documents notarized (US)
- Airline flights (global)
- Life insurance policies in force (US)
- New auto sales (global)
- Tickets issued by Ticketmaster (US)
- Total wireless subscribers (US)
- Intermodal container shipments (global)
- Emergency department visits (US)
- NCAA game attendance
- Commuter rail travel (US / non-Amtrak)

Blocks have a fixed amount of space creating a limitation on supply...

... versus growing demand...

Leading to the conclusion that demand will likely exceed supply by a wide margin
(C) DIRECT EXPOSURE TO BITCOIN: CaaS AND DIGITAL FINGERPRINTS USE CASES

There are an abundance of use cases for CaaS using digital fingerprints, many of which involve data insertions that would exceed the available supply in the blockchain. Example: movie tickets sold in the US: 1.27 billion per year, 47% greater than the capacity in the blockchain.

Given the abundance of use cases, we expect higher value use cases to crowd out lower value use cases. Example: healthcare applications will likely crowd out entertainment applications.

In this context, crowd out implies that a particular application will warrant greater verification agent fees than another application competing for space. Consequently, fees will increase as will demand for bitcoin.

### I. Financial Records
1. Spending records
2. Trading records*
3. Mortgage / loan records
4. Servicing records
5. Accounting records
6. Securities custody*
7. Clearing and settlement*
8. Voting rights for financial instruments

### II. Public Records
9. Land titles*
10. Vehicle registries
11. Business incorporation*
12. Regulatory records
13. Criminal records
14. Passports
15. Birth certificates
16. Death certificates
17. Voter IDs
18. Health / Safety Inspections
19. Building permits
20. Gun permits
21. Forensic evidence
22. Court records

### III. Private Records
23. Contracts*
24. Signatures*
25. Wills
26. Trusts
27. Escrows

### IV. Other Semi-Public Records
28. Degree
29. Certifications
30. Learning Outcomes
31. Grades
32. HR records
33. Medical records*
34. GPS trails
35. Delivery records
36. Arbitration

### V. Physical Asset Keys
37. Home / apartment keys
38. Hotel room keys
39. Car keys
40. Rental car keys
41. Locker keys
42. Safety deposit box keys
43. Package delivery
44. Betting records*
45. Fantasy sports records*

### VI. Intangibles
46. Coupons
47. Vouchers
48. Reservations
49. Movie tickets
50. Patents
51. Copyrights
52. Trademarks
53. Software licenses
54. Videogame licenses
55. Music/movie/book licenses (DRM)
56. Domain names*
57. Online identities*
58. Proof of authorship*


*Startups or established players are already at work on a blockchain-based mechanism for this category

Note: for clarity, in this presentation, we use the term digital fingerprint. The technical term (from the computer science field) is a hash function
(C) MECHANISMS TO GAIN EXPOSURE TO BITCOIN

Direct bitcoin purchase:
- Good for retail investors and some tech-savvy HNW investors, but difficult for institutions
- “Self storage” is a reasonable choice for individuals but troublesome for institutions
- The greater the amount, the greater the risk
- No licensing procedures exist for third-party custodians
- Lack of established customs for clearing and settlement
- Regulatory hurdles -- no ability for SEC reporting; custody, compliance, risk and security concerns
- Exchange sourcing: a shifting landscape -- unregulated, unlicensed and mostly overseas
- AML and counterparty risk

Total Return Swaps – direct USD economic exposure to bitcoin:
- Traded directly via prime broker
- Easily customized: size, duration and other parameters
- Conventional execution and reporting
- Commonly used to access frontier markets

Other derivatives or alternative exposure methods:
- Non-deliverable forwards: available via SEF
- Online swaps: mostly for retail investors, significant counterparty risk

Exchange traded fund:
- Not yet approved
- GBTC bitcoin investment trust: not an ETF, 12-month lockup for fund investors, lacks custodian and involves counterparty risk
- Bitcoin Tracker One XBT: Note traded on Swedish Nasdaq exchange. Not an ETF, but rather a claim on the assets of a small private company. Significant counterparty risk
The blockchain beyond CaaS
Examples

- Printer detects component failure
- References blockchain for warranty info
- Places work order for technician service visit

- Vehicle detects maintenance is needed
- Sends security token to owner's calendar
- Schedules maintenance visit at optimal time
- Pays for maintenance cost

- Vending machine senses low inventory
- Sends bids to multiple suppliers
- Enters into contract and purchases goods
Machines are able to transfer data over a network without requiring human-to-human or human-to-computer interaction.

The blockchain database is where these devices will:
(a) store records
(b) exchange value

By using the blockchain for recordkeeping, IoT will have an *indirect* affect on the value of bitcoin by adding to demand for space within blocks.
GROWTH IN IoT HAS CONSEQUENCES FOR THE BLOCKCHAIN AND THE DIRECT VALUE OF BITCOIN

Bitcoin is a likely candidate for a medium of exchange – a money – in IoT, and its usage will have a direct effect on its value.

Example: A city street is embedded with smart parking meters. Specific parking spot inventory is recorded on the blockchain. As a car leaves a parking spot, its departure is recorded on the blockchain. A second car takes the newly empty parking spot and automatically pays using bitcoin.

The quantity theory of money underscores the relationship among bitcoin price, transactions and velocity: \( P = \frac{MV}{T} \). Price Levels (P) are affected by Velocity of Money (V), Transactional Demand (T), and Quantity of Money (M).

At any given point in time, M (i.e., XBT supply) is fixed, leaving V and T as the determining factors for P. Growth in IoT is likely to have two effects: an increase in V and an increase in T.

Growth in the quantity of IoT economic participants is likely to lead to an increase in T that is greater than the increase in V (assuming, that is, a refrigerator and a toaster don’t continuously pay each other for no good reason).

Consequently, as T increases, P decreases and the real value of XBT increases. Growth in IoT is a significant positive driver for XBT.
# CATALYSTS IN THE BLOCKCHAIN ECOSYSTEM

## NEXT 6 MONTHS

### Incremental projects coming online
- Blocktrace – blockchain tracking of diamonds for the insurance industry (+P&C insurers)
- World Passport – blockchain-based secure storage of identity documents
- Swarm – blockchain-based corporate governance
- Factom – flexible record keeping software

### Beginning of institutional participation
- Total return swaps available for bitcoin

### Increased liquidity
- Two bitcoin investment vehicles are in the process of getting listed
- BitLicense is decreasing regulatory uncertainty
- US Marshals’ seized bitcoin auctions: overhang finishing

## NEXT 12 MONTHS

### Major projects coming online
- 21 Inc's mining ubiquity (+INTC, +XBT)
- BitFury build out (+TSM)
- Abra (+XBT, –WU, –MGI)

### VC involvement / emerging tech
- VC-backed projects from 2013 and 2014 coming online
- Blockchain involvement in Internet-of-Things (IoT) (+ARM.LN, +XBT)

### Large cap companies focusing on blockchain-based financial services applications
- Back office opportunities (+IBM, +XBT)
- Involvement of established exchanges (+NYX)

### Morphing into an institutional asset class
- Emergence of ETF (+XBT)
- Capital flows into a constrained environment (+XBT)
CATALYSTS IN THE BLOCKCHAIN ECOSYSTEM

**NEXT 18 MONTHS**

- VC investment in blockchain and bitcoin-related projects
  - Approximately $700m in VC investment
  - Over $220m YTD 2015

- Large impending bitcoin supply cut
  - “Block-halving” expected Aug 2016 (+XBT)

**18 MONTHS +**

- Additional regulatory clarity
  - UK, others come out in full support of blockchain usage

- Widespread institutional integration
  - Blockchain for settlement and recordkeeping purposes.

- Future supply cuts
  - Additional block-halving in 2020 (+XBT)

- Usage of XBT as a longer-term store of value
  - This will take time and will require price stability
  - (+XBT, −GLD)
KEY TAKEAWAYS

The blockchain avoids the pitfalls of database centralization and creates opportunity

- Such a mechanism has never before existed.
- The blockchain has numerous applications across various industries.
- Large, established businesses are beginning to embrace the blockchain for a variety of applications.

Economic value

- The blockchain enables CaaS.
- Verification agents (miners) require compensation in the form of bitcoin which is the indigenous token of value on the blockchain.
- The blockchain has a finite capacity for CaaS, and the value of bitcoin is affected by supply and demand for CaaS.

The blockchain landscape is active and growing

- Many catalysts are emerging.
- Venture investment is a reasonable way to gain exposure, but the competitive landscape and potential upside varies widely.
- Direct exposure to bitcoin is another way to take advantage of the emergence of the blockchain.
ABOUT SOLIDX PARTNERS

SolidX Partners Inc. provides strategic consulting services as well as management and execution for blockchain project implementations.

The company also enables the availability of bitcoin total return swaps via prime brokers and swap dealers.

Disclaimers

This document is provided to you solely for informational purposes by SolidX Partners Inc. This document is designed to serve as a general summary of the services and products that SolidX may offer from time-to-time.

This document does not constitute an offer or agreement, or a solicitation of an offer or agreement, to enter into any particular contractual relationship with SolidX. Any use of the services and products offered by SolidX must be preceded by your acceptance of binding legal terms and conditions.

This document is confidential, for your private use only, and may not be shared with others. Any reproduction or distribution of the document by you must be authorized in advance by SolidX in writing.