SolidX

PARTNERS INC.

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

*Disruptive technologies tend to start off generating skepticism…*until they completely revolutionize how we live and work

"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…

Characteristics of centralized systems	***Separate Silos / fiefdoms***	***Artificial rules and controls***	***Errors***	***Fraud and hacking***	***Single point of failure***	***Legacy monopolistic profits***
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

Medical records today…

- Sit in several centralized records controlled by different physicians
- Not easily accessible during emergency
- Not controlled or easily accessible by patient

…vs. tomorrow

- Records across and among doctors, but easily shared and under patient control
- Access control and visibility determined by patient
- Easily available in case of emergency

Brokerage OTC trading today…

- Dominated by third parties
- Ties up capital for days
- Prone to errors

…vs. tomorrow

- Same day trade settlement
- Irrefutable audit trail
- Eliminate third parties / new revenue stream

Wills today…

- No formal retention method
- Frequently contested
- Subject to manipulation

…vs. tomorrow

- Certainty of execution timing
- Integrity of data

Event tickets today…

- Secondary market introduces extra costs
- Counterfeits
- Sluggish transfer

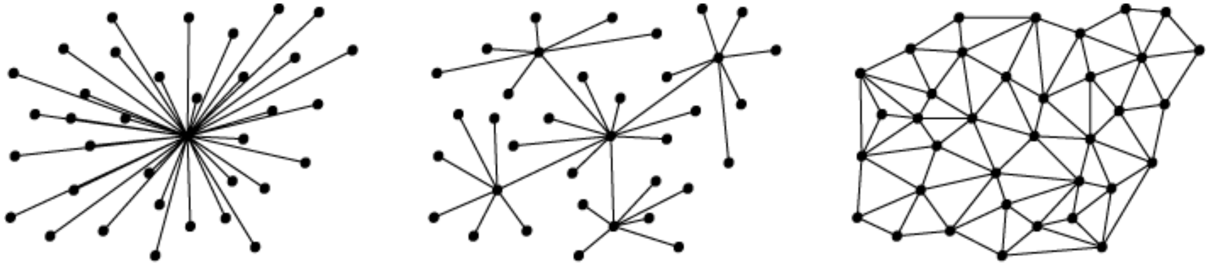
…vs. tomorrow

- Lower costs
- Eliminates counterfeits
- Allows for instant ownership transfer

The blockchain:
a decentralized database

HOW IS DATABASE DECENTRALIZATION RELATED TO THE BLOCKCHAIN?

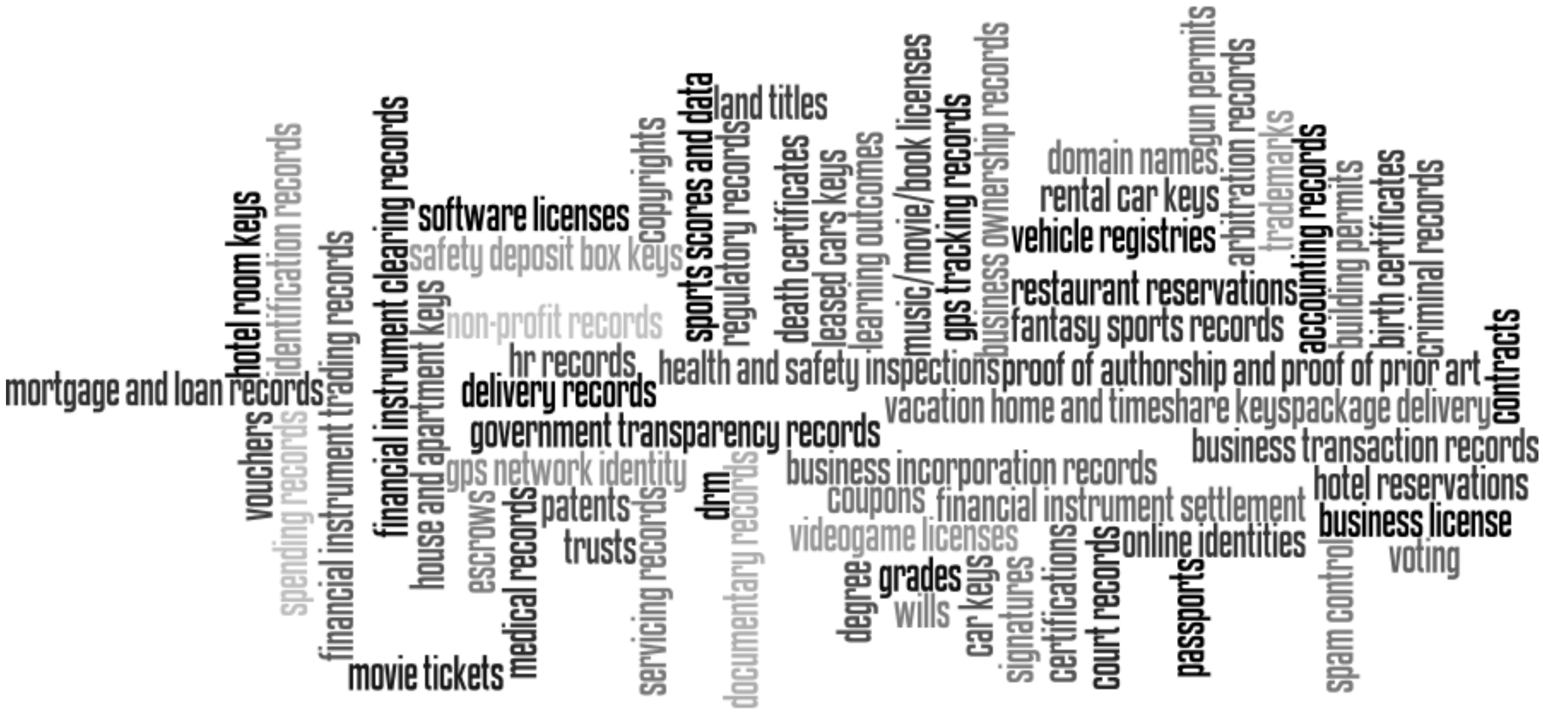
The blockchain is a decentralized database.



centralized *partially decentralized* *fully decentralized*

- 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:

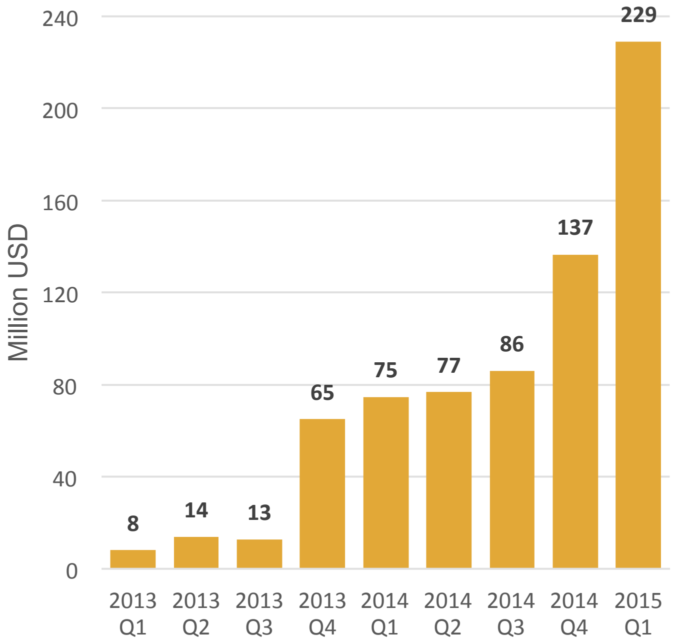
- Building on an existing peer-to-peer, open system that will change how we conduct business in the future

- 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

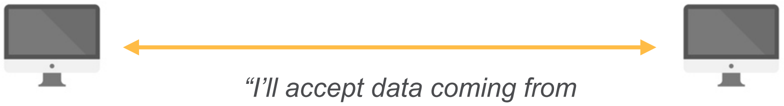


Blockchain deep dive:
how it works

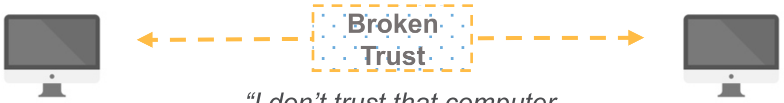
HOW DOES THE BLOCKCHAIN WORK?
HOW DOES IT ACHIEVE DATABASE DECENTRALIZATION?

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

Synchronization works well when computers ***trust*** each other…



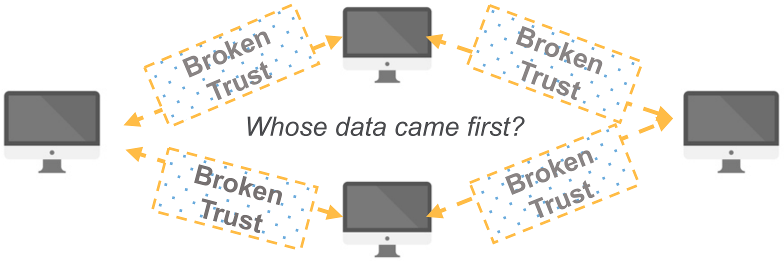
“I’ll accept data coming from the other computer.”



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

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

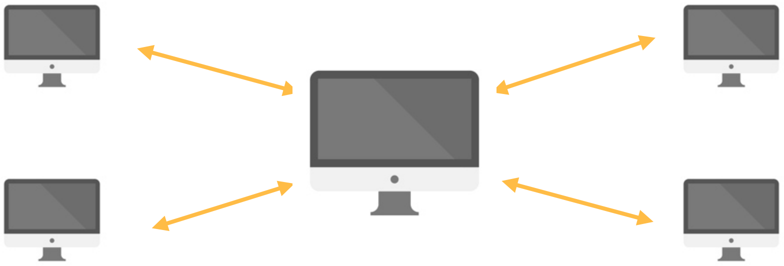
The trust problem ***grows exponentially*** with more computers…



Whose 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…

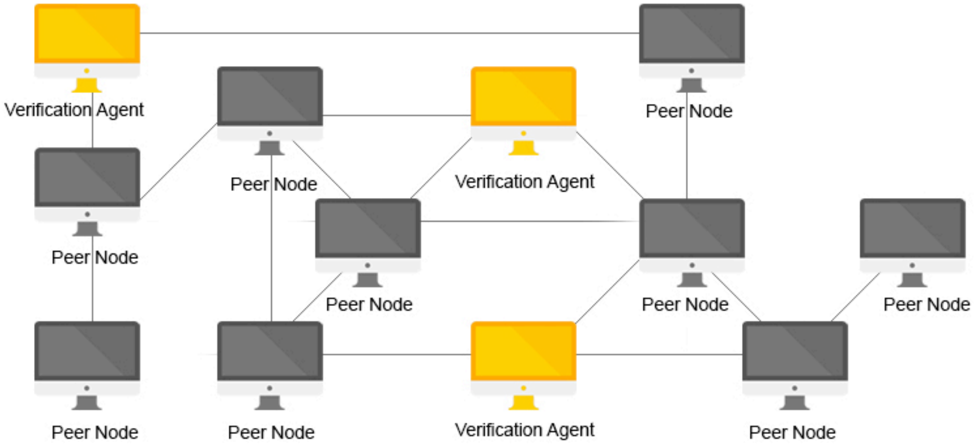


…but central parties are vulnerable to attack, error and fraud. They can introduce artificial rules and reap monopolistic profits. It’s great for shareholders, but it’s a situation ***ripe for disruption by new technology***.

THE BLOCKCHAIN SOLVES THE SYNCHRONIZATION PROBLEM USING A PEER-TO-PEER NETWORK…

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



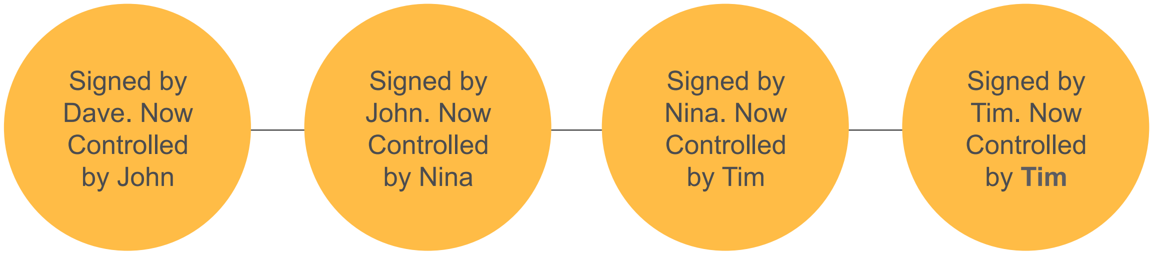
① Each computer on the P2P network running blockchain software has a copy of the database (the blockchain) and can receive ***updates*** at any time.

② Blockchain updates always ***refer to a prior database entry*** (hence the concept of updates and the suffix *"chain"* in block*chain*). 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

④ Each update in the blockchain is referred to as a ***transaction***. Transactions always refer to prior updates.



Signed by Dave. Now Controlled by John

Signed by John. Now Controlled by Nina

Signed by Nina. Now Controlled by Tim

Signed by Tim. Now Controlled by **Tim**

John has updated data to release. He proves control of the prior entry by providing a digital signature. He then gives Nina the authority to issue the next update.

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

⑤ 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.

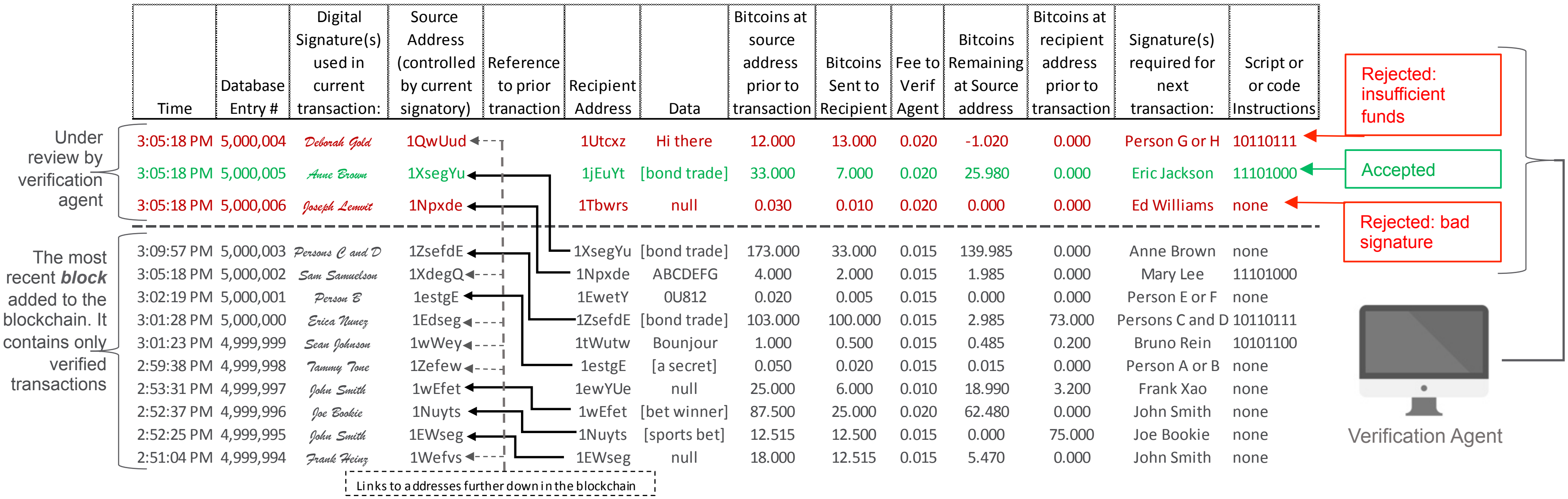
Time	Digital Signature(s) used in current transaction:	Source Address (controlled by current signatory)	Reference to prior tranaction	Recipient Address	Data	Bitcoins at source address prior to transaction	Bitcoins Sent to Recipient	Fee to Verif Agent	Signature(s) required for next transaction:
2:59:38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

Links to addresses further down in the blockchain

Not all entries are required at all times but some must always be included (examples: signatures, references to prior updates)

VERIFICATION AGENTS COMBINE VALID UPDATES INTO NEW BLOCKS, WHICH ARE ADDED TO THE BLOCKCHAIN…

Under the hood: a detailed look at transactions in the blockchain



Under review by verification agent

The most recent ***block*** added to the blockchain. It contains only verified transactions

Time	Database Entry #	Digital Signature(s) used in current transaction:	Source Address (controlled by current signatory)	Reference to prior tranaction	Recipient Address	Data	Bitcoins at source address prior to transaction	Bitcoins Sent to Recipient	Fee to Verif Agent	Bitcoins Remaining at Source address	Bitcoins at recipient address prior to transaction	Signature(s) required for next transaction:	Script or or code Instructions
3:05:18 PM	5,000,004	Deborah Gold	1QwUud		1Utcxz	Hi there	12.000	13.000	0.020	-1.020	0.000	Person G or H	10110111
3:05:18 PM	5,000,005	Anne Brown	1XsegYu		1jEuYt	[bond trade]	33.000	7.000	0.020	25.980	0.000	Eric Jackson	11101000
3:05:18 PM	5,000,006	Joseph Lemwit	1Npxde		1Tbwrs	null	0.030	0.010	0.020	0.000	0.000	Ed Williams	none
3:09:57 PM	5,000,003	Persons C and D	1ZsefdE		1XsegYu	[bond trade]	173.000	33.000	0.015	139.985	0.000	Anne Brown	none
3:05:18 PM	5,000,002	Sam Samuelson	1XdegQ		1Npxde	ABCDEFG	4.000	2.000	0.015	1.985	0.000	Mary Lee	11101000
3:02:19 PM	5,000,001	Person B	1estgE		1EwetY	0U812	0.020	0.005	0.015	0.000	0.000	Person E or F	none
3:01:28 PM	5,000,000	Erica Nunez	1Edseg		1ZsefdE	[bond trade]	103.000	100.000	0.015	2.985	73.000	Persons C and D	10110111
3:01:23 PM	4,999,999	Sean Johnson	1wWey		1tWutw	Bounjour	1.000	0.500	0.015	0.485	0.200	Bruno Rein	10101100
2:59:38 PM	4,999,998	Tammy Tone	1Zefew		1estgE	[a secret]	0.050	0.020	0.015	0.015	0.000	Person A or B	none
2:53:31 PM	4,999,997	John Smith	1wEfet		1ewYUe	null	25.000	6.000	0.010	18.990	3.200	Frank Xao	none
2:52:37 PM	4,999,996	Joe Bookie	1Nuyts		1wEfet	[bet winner]	87.500	25.000	0.020	62.480	0.000	John Smith	none
2:52:25 PM	4,999,995	John Smith	1EWseg		1Nuyts	[sports bet]	12.515	12.500	0.015	0.000	75.000	Joe Bookie	none
2:51:04 PM	4,999,994	Frank Heinz	1Wefvs		1EWseg	null	18.000	12.515	0.015	5.470	0.000	John Smith	none

Links to addresses further down in the blockchain

Rejected: insufficient funds

Accepted

Rejected: bad signature

Verification Agent

10110111 = Allow only certain recipients; 11101000 = Do not release until next Tuesday; 11101011 = Do not release until next Monday; 10101100 = Release only upon certain conditions

⑥ 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.)

⑦ 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.***

…BUT THE VERIFICATION AGENTS MUST BE PAID TO DO THEIR WORK

⑧ 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.

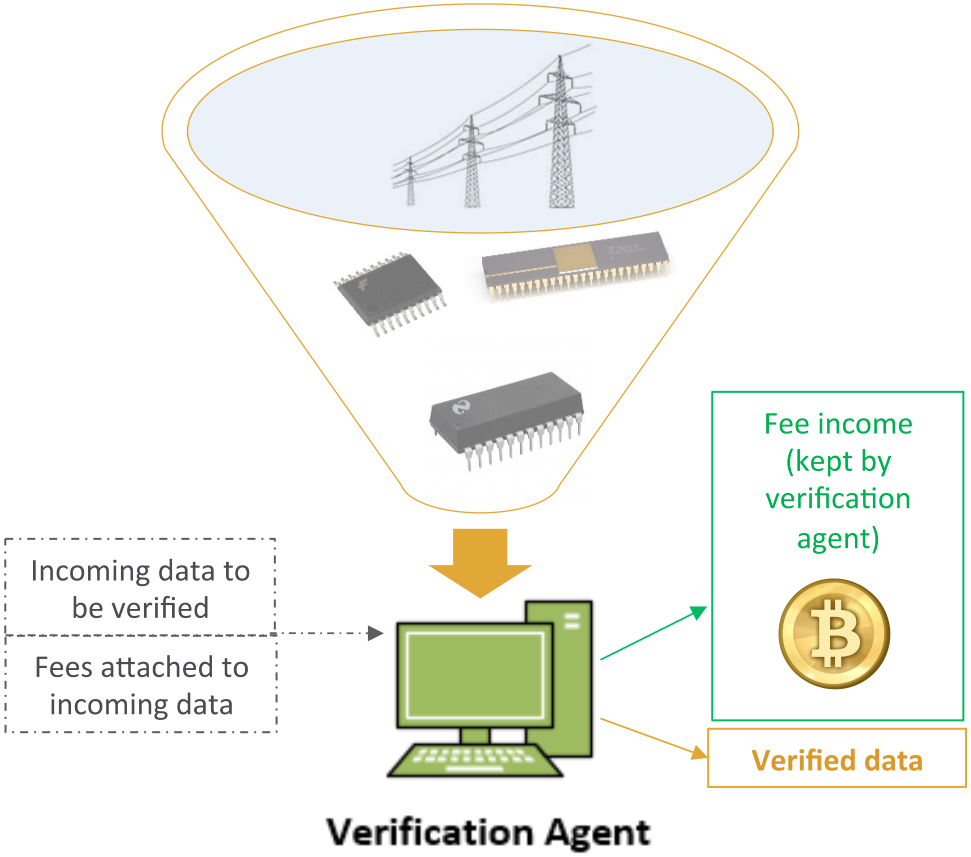
The blockchain requires as many verification agents as possible, all of whom compete to do the job.

⑨ 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.


Incoming data to be verified
Fees attached to incoming data
Fee income (kept by verification agent)
Verified data
Verification Agent

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.

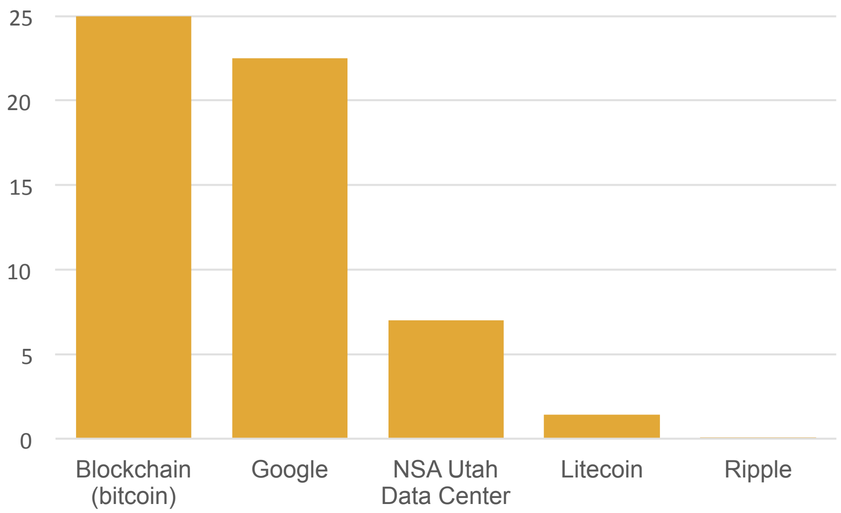
THE MORE VERIFICATION AGENTS AT WORK, THE SAFER THE BLOCKCHAIN

⑩ 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.

Verification agent electricity usage in million MWh / year



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

Time	Digital Signature(s) used in current transaction:	Source Address (controlled by current signatory)	Reference to prior tranaction	Recipient Address	Data	Signature(s) required for next transaction:
2:52:25 PM	C.H.E. clerk	1EWseg		1Nuyts	Elvis ticket 215	Concert producer
2:51:04 PM	Marilyn M	1Wefvs		1EWseg	Elvis ticket 216	Concert hall entrance clerk
2:32:04 PM	Ticket Issuer	1qEruY		1Wefvs	Elvis ticket 217	Marilyn M

- 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

	Blockchain storage	**Amazon cloud DB**
24x7x365 uptime	*Yes*	*No*
Cannot be modified by DBA	*Yes*	*No*
Indelible, irrefutable time stamps	*Yes*	*No*
Publicly available iterative history	*Yes*	*No*

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

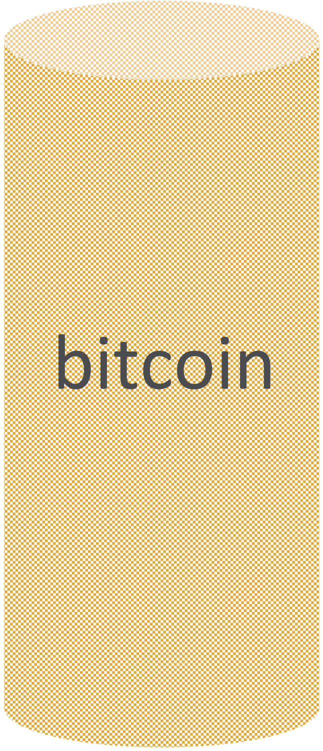
Approximately **200** startups

Elliptic
OneName
AlphaPoint
Ledger Melotic
Vaurum Korbit
Coinplug itBit
Block Cypher
TradeBlock Coinsetter
BlockScore
Colu KnC Miner
Blockstream 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

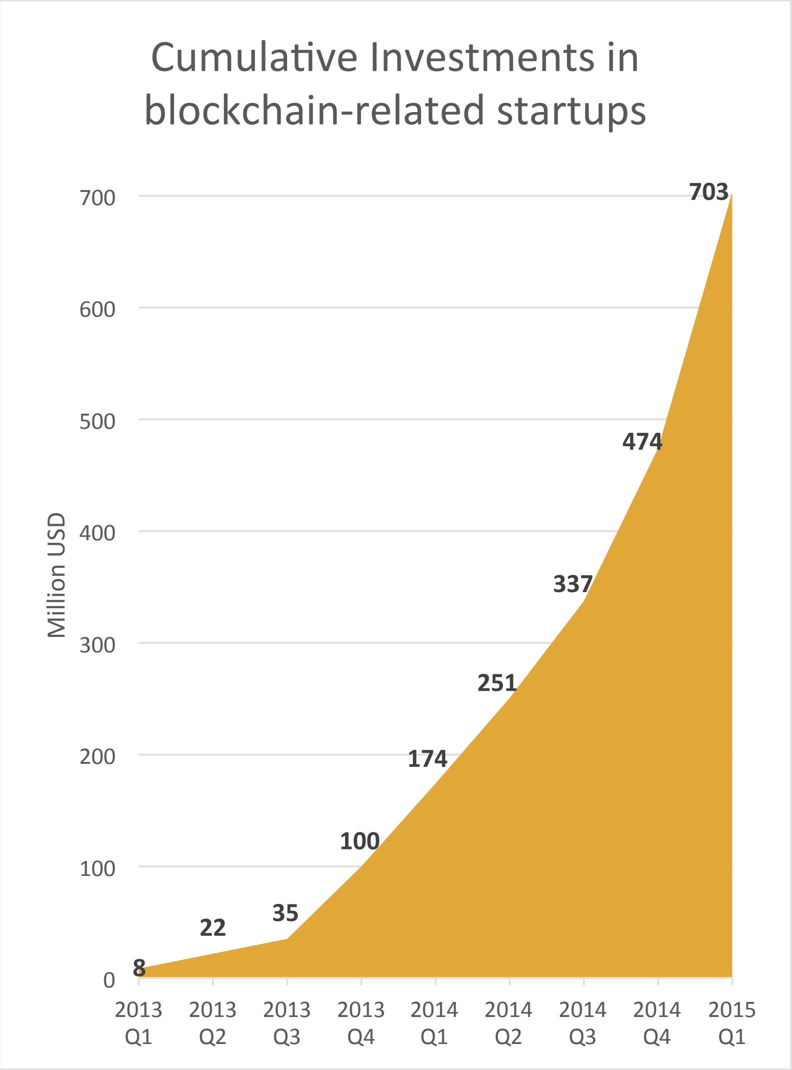
- Semiconductor companies: TSM, INTC (**both** are currently producing chips for blockchain-related applications)
- Fabless semi companies: QCOM, ARM.LN
- Internet-of-Things (IoT) architects: IBM
- Certain exchanges: NYX, NDAQ
- Government and military contractors for IT integration projects: CACI, SAIC, 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


Cumulative Investments in blockchain-related startups

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

(C) 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.

Supply and Demand for block chain-based CaaS

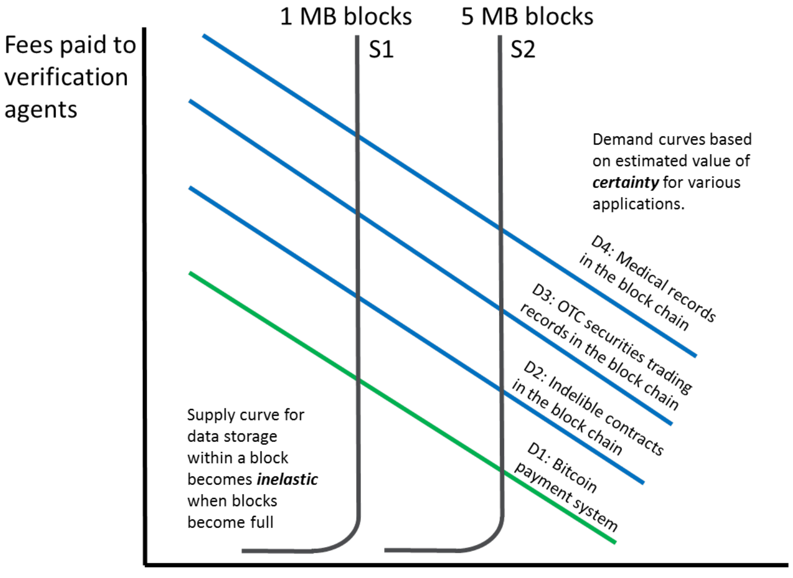
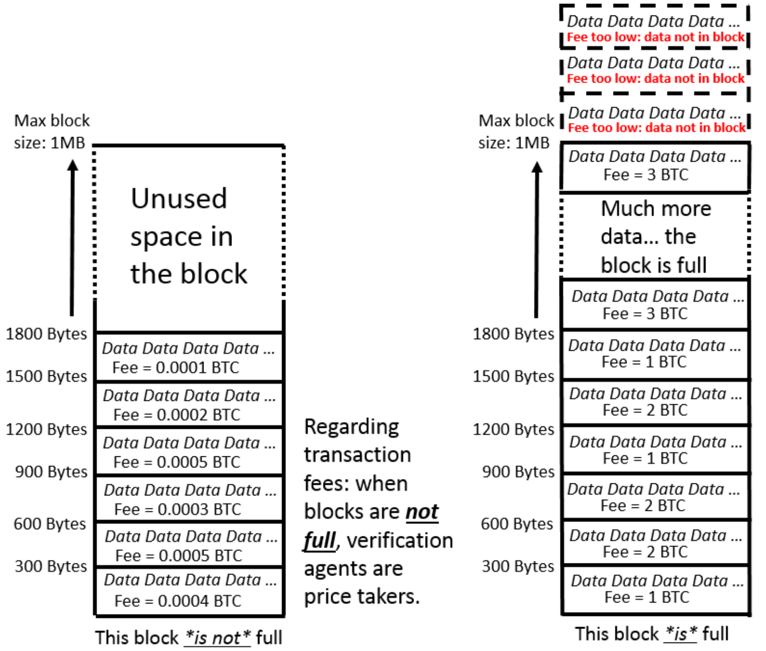


Figure 1

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


Max block size: 1MB
1800 Bytes
1500 Bytes
1200 Bytes
900 Bytes
600 Bytes
300 Bytes
Unused space in the block
Data Data Data Data ... Fee = 0.0001 BTC
Data Data Data Data ... Fee = 0.0002 BTC
Data Data Data Data ... Fee = 0.0005 BTC
Data Data Data Data ... Fee = 0.0003 BTC
Data Data Data Data ... Fee = 0.0005 BTC
Data Data Data Data ... Fee = 0.0004 BTC
This block *is not* full
Data Data Data Data ... Fee too low: data not in block
Data Data Data Data ... Fee too low: data not in block
Data Data Data Data ... Fee too low: data not in block
Max block size: 1MB
1800 Bytes
1500 Bytes
1200 Bytes
900 Bytes
600 Bytes
300 Bytes
Data Data Data Data ... Fee = 3 BTC
Much more data... the block is full
Data Data Data Data ... Fee = 3 BTC
Data Data Data Data ... Fee = 1 BTC
Data Data Data Data ... Fee = 2 BTC
Data Data Data Data ... Fee = 1 BTC
Data Data Data Data ... Fee = 2 BTC
Data Data Data Data ... Fee = 2 BTC
Data Data Data Data ... Fee = 1 BTC
This block *is* full

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.

Figure 2a, 2b

(C) DIRECT EXPOSURE TO BITCOIN: SUPPLY AND DEMAND

Demand for CaaS and supply of space in blocks determines the long-term equilibrium price for bitcoin

3. 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.)

Supply and Demand for bitcoin

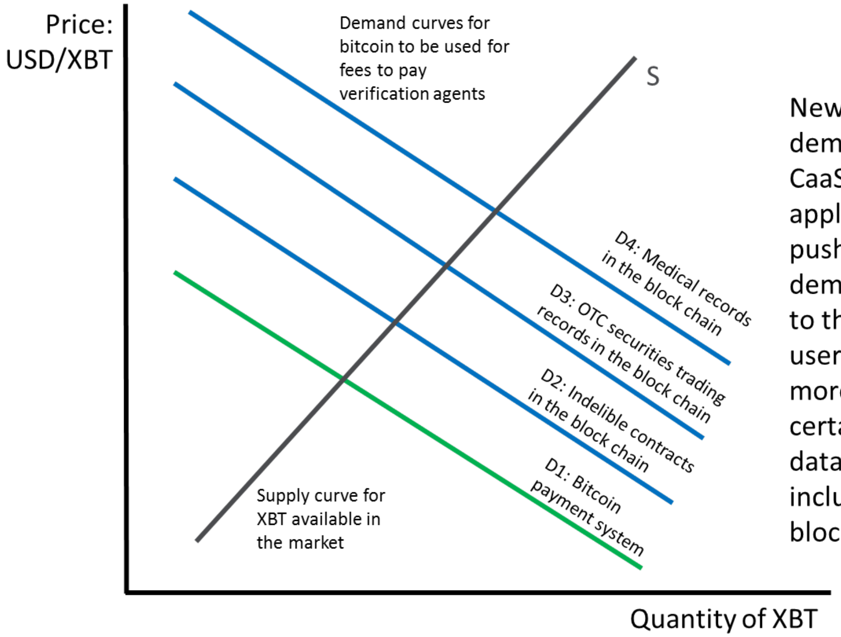


Figure 3

New drivers of demand for CaaS (new applications) push the demand curve to the right, as users need more fees to be certain their data will be included in a block

The intrinsic value of bitcoin is determined by supply and demand for CaaS

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.

(C) DIRECT EXPOSURE TO BITCOIN: CaaS AND DIGITAL FINGERPRINTS

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.

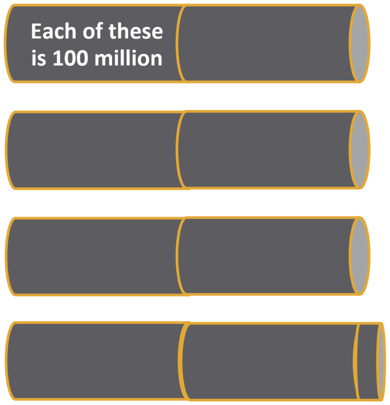
A digital fingerprint can be indelibly and securely written to the blockchain as a time stamped record of any document, event, etc. The person adding the entry to the blockchain can maintain exclusive control of it or allow others to control it.

(C) DIRECT EXPOSURE TO BITCOIN: EXAMINED QUANTITATIVELY THROUGH CaaS AND DIGITAL FINGERPRINTS

Digital fingerprints: supply / demand imbalance

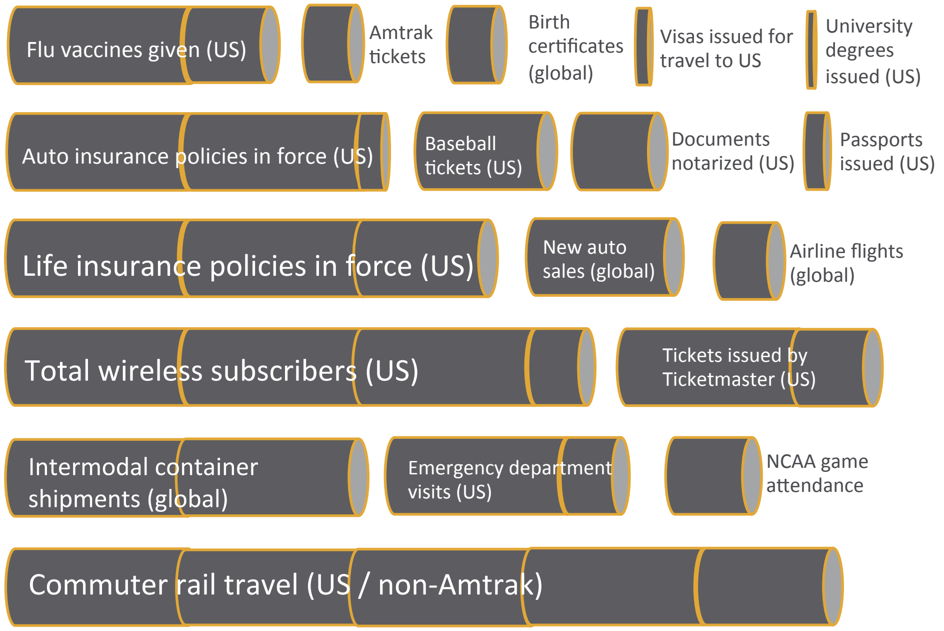
Supply is constrained

Block size (MB)	1
Est. transaction size with data payload (bytes)	768
Transactions per 1 MB block	1,365
Approx max digital fingerprints per transaction	12.0
Digital fingerprints per 1 MB block	16,384
Blocks per year	52,560
Digital fingerprints per year:	**861,143,040**



Demand categories are growing

A few sample items:



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

Source: http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list

*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*

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*

(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

BLOCKCHAIN AND THE INTERNET OF THINGS (IoT)

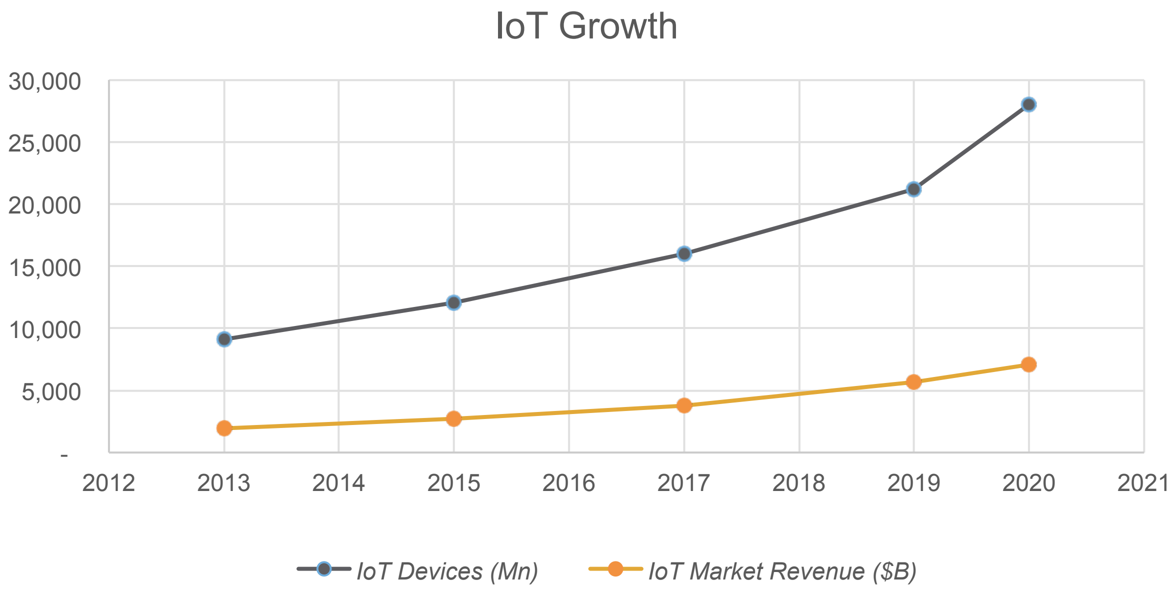
Examples

- 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

BLOCKCHAIN AND THE INTERNET OF THINGS (IoT)



Estimated $7.1Tn market and 28Bn devices by 2020

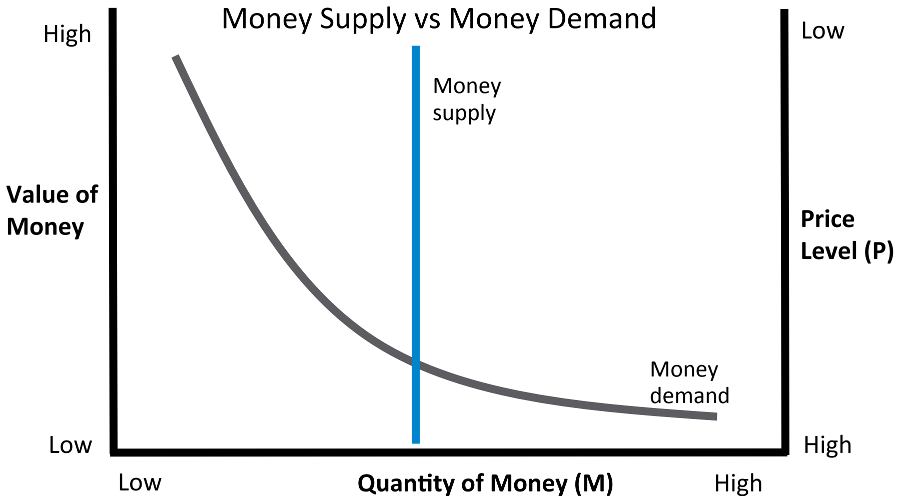
Machines are able to transfer data over a network without requiring human-to-human or human-to-computer interaction

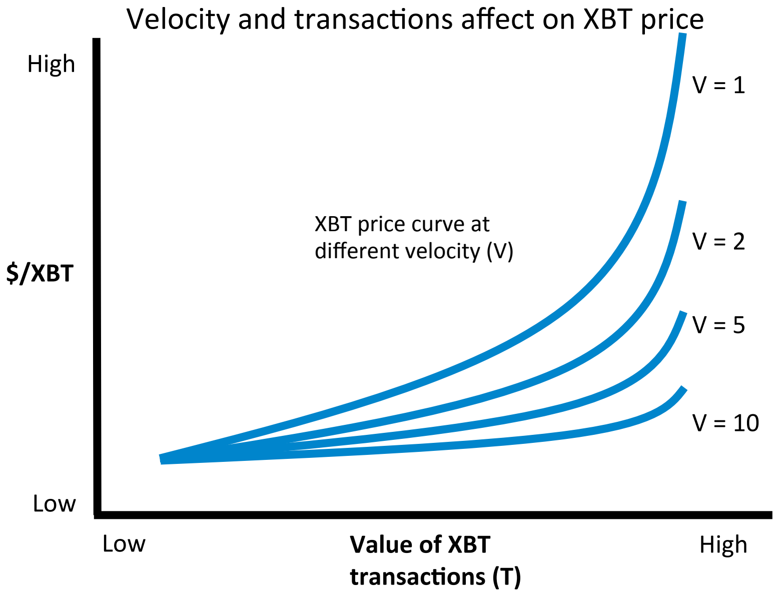
The blockchain database is where these devices will:

(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





$/XBT is related to the inverse of P (i.e., 1/P)

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 = 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. | info@sldx.com | (212) 273-9580 | 200 Park Avenue, 17th FL. New York, NY 10166

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.