Blockchain and Cryptocurrency

The good, some lessons learned, and scams

Jean Pawluk
ISSA presentation
June 16, 2017

Confusion Flourishes

* Separation of hype & noise vs. reality is difficult
* Threat or Opportunity or Both ?
  * Major disruptive technology meeting a mostly uninformed public

Revolution in Digital Trust

* Focus is now on blockchain not just Bitcoin or alternative cryptocurrencies
* It's really about TRUST *
    * Or lack thereof

History

Byzantine Generals problem (1982)

* Fault tolerance in systems issue required user consensus, when the users may or may not be trustworthy

Satoshi Nakamoto (2006) worked on the Byzantine Generals problem.

Solution (2009) realized in Bitcoin to show a proof of work.

* "You say to the whole network, 'I've got the hash'" and have the key, and the network can check that as the chain is built using chained blocks of signed transactions.
* The longest chain in the blockchain is the winner.

--As "the long chain wins," in the long run, there's no realistic chance of hacking and more agents who are involved, the stronger the chain becomes.

"You can see what x said to y. It's signed data. Everything that happens can be shown, and is known."

Definitions

* Bitcoin - digital currency using blockchain
* Block – set of transactions validated by network peers
* Blockchain – data structure for a chain of blocks linked to one another that contains the entire logged history of the blocks
* Altcoin - alternative digital currency
* Wallet – Used to store private key and digital currency
* ICO – Initial Coin Offering

Cryptocurrency

A digital currency that uses encryption techniques to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

* Decentralized
* Immutable
* Transparent
* Consensus driven
* Cryptographic token (coin)

Advantages of Bitcoin and Altcoins

* **Decentralized**

  Not controlled by one central authority. Every machine that mines bitcoin and processes transactions makes up a part of the network, and the machines work together.

* **Completely transparent**

  Every single transaction is stored in the network in a blockchain with a publicly used bitcoin address. (Anyone can see how many bitcoins are stored at an address but not who owns them)

* **Very low transaction fees**

* **Relatively fast**

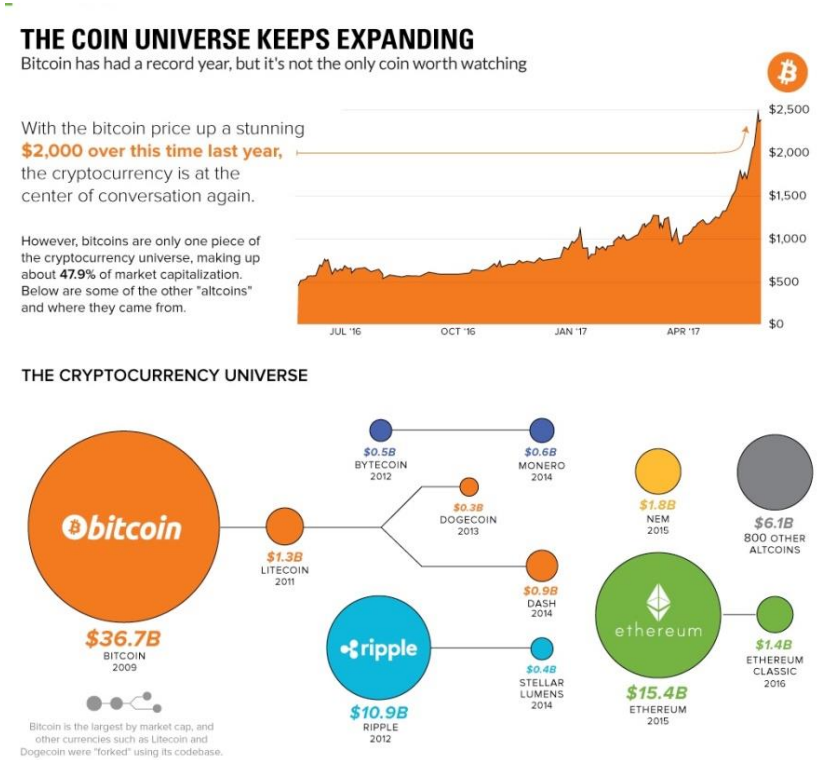
  As soon as the bitcoin or altcoin network processes the payment, it yours.

* **Irrevocable**

  No returns , No refunds

  Once sent, there's no getting coins back, unless the recipient returns them to you.

Explosion of Cryptocurrencies



* 800+ cryptocurrencies exist today
* Combined worth of coins shown as of April 2017 is over $76.5 Billion*

*Ford, HP, the Gap combined are worth $83.4 Billion

Cryptocurrency rollercoaster

Highly Volatile:

* Bitcoin's and Altcoin's value fluctuates 24*7

* Perceived value is affected by news and rumors
  - Security breach scares
  - Black Market activity damage to reputation

Big swings in value can make it difficult for everyday consumer to use

As of 05 June 2017 11:26:01 UTC+0:00
Bitcoin (BTC) **2624.74** USD ↑
Litecoin (LTC) **30.7** USD ↑
Ethereum (ETH) **242.73** USD ↓

Bitcoin Conversions

1 Bitcoin = 100 Million Satoshi

1m BTC = 0.001 BTC = 1 thousandth of a bitcoin

1 Bit = 0.000001 BTC = 1 Millionth of a bitcoin

1 Satoshi = 0.00000001 BTC = one 100 millionth of a bitcoin, the smallest unit.

Is Bitcoin Anonymous ?

* Yes but not untraceable
* Bitcoin is pseudo-anonymous

  - pseudonym (bitcoin address) is recorded, but identity is unknown.
* Tumblers / Mixers attempt to disguise source and destination of transactions that would connect to real id
* So how do you move your ill gotten gains in public view ?

- send and receive bitcoins to another bitcoin address on blockchain . Use several addresses and store coins elsewhere in wallets and / or in dark exchanges.

Bitcoin as legal currency

* *With recent interests from Japan and Russia to legitimize Bitcoin, these rules and regulations could help further cryptocurrency as a legitimate finance asset.*

Russia in 2018

* The state needs to know who at every moment of time stands on both sides of the financial chain," Moiseev said about the government's latest position.
* "If there's a transaction, the people who facilitate it should understand from whom they bought and to whom they were selling, just like with bank operations."

Blockchain

Why blockchains ?

* **Trust** – Through the use of Blockchain, all the parties involved in a transaction only have to trust the technology.
* **Transparency** – Because the ledger is distributed, all peers involved in the transaction network can view it (subject to security rights, of course).
* **Accountability** – Since all parties in the transaction can view the distributed ledger, everyone can agree on how the transaction is progressing while it is ongoing, and how it went once it is complete.

What the Blockchain IS NOT:

* Bitcoin or Altcoins
  - They use blockchain structures

* Blockchain is *not fast*
  - Looking at the longest chain in bitcoin can take a while

* Blockchain is *not simple*
  - complexity is greater as efforts increase around scalability issues such as sidechains, partial chains, light clients, pruning, cross-chains etc..

What is it good for ?

Vitalik Buterin, ethereum's founder perspective:

"The solution that is optimal for a particular industry depends very heavily on what your exact industry is. In some cases, public is clearly better; in others, some degree of private control is simply necessary. As is often the case in the real world, it depends"

Anticipated Blockchain Timeline

Hype vs. Reality

* Remember the "year of PKI" ?
  - Today it's "Blockchain Fever"

* Most R&D projects end in failure or pivot to new areas of research
  - R3 consortium dropped blockchain projects in 2017

* Need to identify where investments in blockchain R&D have the most impact based on:
  - current technology maturity
  - real savings in costs / processes
  - evolution of commercial ecosystems
  - public's willingness to embrace a blockchain economy

Peer to Peer distributed ledgers

* Blockchain technology is uses a peer-to-peer network of parties, who all participate in a given transaction.
* Uses a distributed ledger that is visible to all parties involved in the transaction.
* Through a consensus network, the ledger is guaranteed to be consistent.
* Ledger is distributed so everyone involved can see the "world state" at any point in time, and can monitor the progress of the transaction.
* Ledger is encrypted so that only parties allowed to view it may do so.

Smart Contracts

Contract

* A written or oral agreement, that is intended to be enforceable by law

Smart contract

* Code that facilitates, verifies, or enforces the negotiation or execution of a digital contract. Ideal for machine to machine business processes

Smart contract code on Blockchain

- Encapsulates Business logic as a computer program

- Represents the events which trigger that logic as message to program (allowed if pre-set conditions are met)

- Digital signatures used to prove who sent the message

Example

Car rental agencies could use smart contracts that automatically allow rentals when payment's received and insurance information is confirmed through a blockchain record.

Gartner predicts

Blockchain Will Grow UP

* By 2022, a blockchain-based business will be worth $10 billion.
* Blockchain technology is established as the next revolution in transaction or event recording. A blockchain ledger provides an immutable, shared view of all transactions between engaging parties in a distributed, decentralized network
* While the bitcoin blockchain ledger is itself well-understood, blockchain remains an immature technology.
* By 2020, new businesses and business models will emerge based on smart contracts and blockchain efficiencies. These smart contracts automate at a reliability, customization level and speed not achievable with traditional business systems.

Some Blockchain Use Cases

Cross-industry
- Identity management
- Capital asset management

Internet of Things
- Device management

Healthcare
- Electronic medical records
- Doctor-vendor RFP services & contracts
- Blockchain health research commons
- Blockchain health notaries

Government
- Government vendor processes
- Voting
- Taxes

Industrial
- Manufacturing processes

Other industries
- Gaming
- Music

Financial services
- Letters of credit
- Corporate debts and bonds
- Trading platforms
- Payment remittance
- Foreign exchange

Insurance
- Claims processing
- Insurance
- Ownership titles
- Sales & underwriting

Retail
- Loyalty points

Blockchain Consortiums

* Over 25 Blockchain Consortiums globally
* Usually organized by industry verticals
  * Research & Development questions
  * How blockchain will affect businesses, governments, consumers
  * Current Projects
  * What are my peers doing and who should we partner with
  * Cost and value drivers for blockchain

HASHED HEALTH

* Financial and Tech largest four consortiums

Types of Blockchains

Public Blockchain (Permissionless)

Everybody in the world can read, anyone can send transactions to and expect to see them included if they are valid, and anyone can participate in the consensus process

Private Blockchains (Permissioned)

* **Consortium Blockchain**

  Consensus process is controlled by a preselected set of nodes. Example is a consortium of several banks, each of which operates a node and of which some number of banks must sign every block in order for the block to be valid

* **Private Blockchain**

  Write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent.

DAO / DAC

* Decentralized Autonomous Corporations/Orgs
* A computer program, with its own code and state, that can programmatically manage flows using smart contracts to automate processes
  - Whole behavior of the program is pre-established

Public Blockchain Issues

* One of the drawbacks of a public blockchain is the substantial amount of compute power needed to maintain a distributed ledger at a large scale.
* To achieve consensus, each node in a network must solve a complex, resource-intensive cryptographic problem called a proof of work to ensure all blocks in chain are in sync.
* Openness of public blockchain

  little to no privacy for transactions

Lessons Learned

Gartner top 10 blockchain mistakes

1. Misunderstanding or ignoring the purpose of blockchain technology
2. Assuming that current technology is ready for production use
3. Confusing future blockchain technology with the present-day generation
4. Confusing a limited, foundation-level protocol with a complete business solution
5. Viewing blockchain technology purely as a database or storage mechanism
   Assuming interoperability among platforms that don't exist yet
6. Viewing blockchain technology purely as a database or storage mechanism
7. Assuming interoperability among platforms that don't exist yet (blockchain standards do not yet exist)

http://www.gartner.com/smarterwithgartner/top-10-mistakes-in-enterprise-blockchain-projects/

Gartner top 10 mistakes (cont.)

8. Assuming that smart contract technology is a solved problem
   -Smart contracts currently lack scalability, auditability, manageability and verifiability. there is no legal framework currently in existence — locally or globally — for their application.

9. Ignoring funding and governance issues for a peer-to-peer distributed network
   - Multiparty systems require new approaches to governance, security and economics that raise technical, as well as political, societal and organizational questions.

10. Failure to incorporate a learning process
    Enterprises must take a hands-on approach to blockchain projects.

http://www.gartner.com/smarterwithgartner/top-10-mistakes-in-enterprise-blockchain-projects/

Roadblocks
Fidelity Lessons Learned 1 & 2

Fidelity CEO Abigail Johnson reflects:

1 Technological shortcomings

* The first concerns blockchain technology itself, there were "still questions to be answered,"
* "We understand there are important trade-offs that need to get made as these systems grow," Johnson said. "We care about the trade-off between scalability, privacy, and achieving peer-to-peer settlement. "
* Of these three, privacy was the most important, calling it "a core customer need" that was an area of investment for Fidelity initiatives.

2 Regulation

* Johnson called regulation "the policy challenge," as innovation in the blockchain industry was happening so fast "that it is outpacing the regulator's ability to keep up."
* The Securities and Exchange Commission (SEC) ruled against a product that would have led to the first bitcoin-tracking exchange-traded fund* (ETF) citing a lack of regulation in the marketplace.
* "We need to continue to work with regulators to have an open dialogue about this technology,"

Roadblocks
Fidelity Lessons Learned 3 &4

3 Control

* "Networks like bitcoin, by design, have no formalized management structure," Johnson said.
  "They're open projects, which is great, but companies like Fidelity don't have the clarity on the future path they might take, or how to influence the developer communities."
* "The financial services industry will need to work to understand the risks associated with who controls the features of these new systems"

4 "Human Problems"

* "The human problem," is Johnson's reference to how bitcoin and blockchain are often seen as "solutions in search of a problem."
* Wider Consumer Acceptance issues
  - The cafeteria in the Fidelity headquarters began to accept payment in bitcoin--doubling the number of places in Boston that did" Johnson joked.
  "We don't just need these systems to be technically better; we need them to be more user friendly"

Perils ?

Initial Coin Offering (ICO)

Unregulated means by which funds are raised by crowd funding for a new cryptocurrency venture.

* Percentage of the cryptocurrency is sold to early backers of the project in exchange for cash or cryptocurrencies (usually Bitcoin)
* Bypasses the rigorous and regulated capital-raising process required by SEC, venture capitalists or banks
* Crypto tokens from venture are not stocks

Remember ?

Beanie Babies Bubble 1995 - 2001

Feeding Frenzy

* Speculators and scammers are rushing in

* People are "investing" in ICO's and cryptocurrencies
  - Maxing out credit & debit cards purchases
  - Draining bank accounts & retirement plans
  - Mortgaging homes

* Sound Familiar ?
  Some may win big, but many will lose most or all

* Are you and your customers financial savvy ?
  - Risks
    - No protection against loss
    - Not regulated or registered
    - Scarcity and volatility of tokens is not a guarantee of future profits
    - No guarantee that new ICO project will be there tomorrow

ROI

* *"In as much as Blockchain and the Distributed Ledger Technology (DLT) offers a huge platform for various kinds of innovations and investments, the promise of unrealistic returns on investment is a common characteristic that cuts across almost all cryptocurrency scams"*

Into the Darkness

* Dark Marketplaces are digital black markets for illicit goods on darknet
  - drugs , software and hacking services, weapons, counterfeit id's and currency, etc.
* Dark exchanges and dark escrow services for laundering money
* Online Gambling

AML and other dangers

Today little government oversight or backing

* Because cryptocurrencies are not associated with personal id
  * favorite medium for criminals seeking to launder money or purchase illegal goods and services.
* Security breaches have caused crypto products to crash & digital thieves have stolen tens of thousands of bitcoins in digital heists
* In United States
  * Only requires that administrators and exchangers of cryptocurrencies comply with the regulation, reporting, and recordkeeping regulations of the Financial Crimes Enforcement Network (FinCEN). The US Department of Defense is also exploring the potential implications of cryptocurrencies for terrorist activity.

Thieves & Scammers Heaven ?

ZEROFOX

ZeroFox Research shows

* Bitcoin's price rise this year, from $415.69 in March 2016 to now, fueling explosion in scams

* In March, 2017 ZeroFox identified 3,618 Bitcoin scam URLs, shared more than 126 million times on social media, including two that were shared over 40 million times each.

* Bitcoin is ideal for scamming purposes because
  - -- The lack of a central controlling authority to protect the currency from fiat devaluation or regulation, makes it impossible to police
  - , - Scammers are protected by anonymity .
  - - Unrecoverable because all transactions in the blockchain are irreversible (which is the whole point)

https://www.zerofox.com

Common Scams and Swindles

Fake Bitcoin wallets hiding malware downloads:

* Users click through bad URLs posted on social media . Promises Bitcoins to lure the user into following a URL which will download a malware-laden app
* Fake surveys are often used to distribute malware

Bitcoin phishing impersonators

* Impersonates Bitcoin & other cryptocurrencies brand databases to gain victim's trust and credibility.
* Users enter their private Bitcoin key to check it and the key then is used by the scammer to access the coin owner's wallet.

Bitcoin-flipping scams

* Instantly exchange Bitcoins for cash after paying an startup fee and /or promises to double your initial investment overnight scams

Bitcoin pyramid / Ponzi schemes

* **Uses high** yield investment programs and multi-level marketing.
* Promises a low initial investment will be augmented by signing up additional members using referral links to get others to join. Original scammer walks away and it all collapses then

Fake industry conferences

.

How to identify scams :

MANAGEMENT

* Who are the people behind the cryptocurrency? Are they trustworthy and competent? Are their names and resumes published for the public to review? Do they have a Google trail of promoting other scams? Do they have an experienced technology team behind the cryptocurrency? These are some of the questions that should be clarified by an investor towards any given prospective venture.

VALUE CREATION

* For entities that are out to promote a given cryptocurrency, questions should be asked about how they are creating value with their cryptocurrency? Are they providing retail products or services as a value to the marketplace to generate a profit? Why would anyone buy and use their cryptocurrency? What user benefit will be derived, outside of speculative trading?

RETURN ON INVESTMENT

* Every investor should be wary of claims of receiving an unusually high and fast return on investment. Some scams claim 1-2 percent of daily earnings or 100 percent monthly earnings. Obviously, too-good-to-be-true, but it hypnotizes the greedy into irrational thinking. The reality is that all or most of the returns on investment are being paid from new investors money (i.e. Ponzi scheme), that always collapse eventually.

SPECIAL TECHNIQUES

* Acclaimed methods for creating profits must be properly scrutinized. Profits from mining Bitcoins is a common claim that is deceptive due to the very competitive mining environment. Another claim is arbitrage, which is the ability to buy low on one public exchange and sell high on another. There is nowhere near the volume of opportunity to satisfy the promised profits. Finally, be wary of claims of widespread acceptance by merchants. When merchants accept a coin they typically have to sell the coin to pay their bills, which drops the coin price not increase it.

Ponder the following

* What will replace the current models of governance that control commerce and the internet? Will we need them in a totally transparent environment?
* Where might new sources of unexpected risk emerge in a "blockchain world" that is still in its infancy and so poorly understood by all but a small group of pioneers and enthusiasts?
* What are the implications for the way in which systems are developed and the approaches to educating and training tomorrow's software engineers?
* How might these technologies reshape our relationship to security?
* How is privacy defined within these applications and in an M2M environment?
* What are the incentives for participants ethical choices within an ecosystem?"

Shall we Make Better Mistakes Tomorrow ?

You can contact me at
jean.pawluk@issa.org
or via Linkedin

Mt Gox

* 2010 - Mt. Gox is the biggest bitcoin exchange
* June, 2011 - major security breach & fraudulent trading (Shut it down 7 days)
* 2014 - 744,408 bitcoins in a theft that went unnoticed for year

Questions ?