CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Blockchain: everyone wants to sell me that - but is that really right for my application?

Dr. Marco Ermini, CISA, CISM, CISSP, ITILv3, GCIH, RCSS, PhD
Senior Security and Compliance Officer, Orange Business Services

Why? “Blockchain revolution”

Financial	Public Sector	Retail	Insurance	Manufacturing
Trade Finance	Asset Registration	Supply chain	Claims processing	Supply chain
Cross currency payments	Citizen Identity	Loyalty programs	Risk provenance	Product parts
Mortgages	Medical records	Information sharing (supplier – retailer)	Asset usage history	Maintenance tracking
	Medicine supply chain		Claims file	

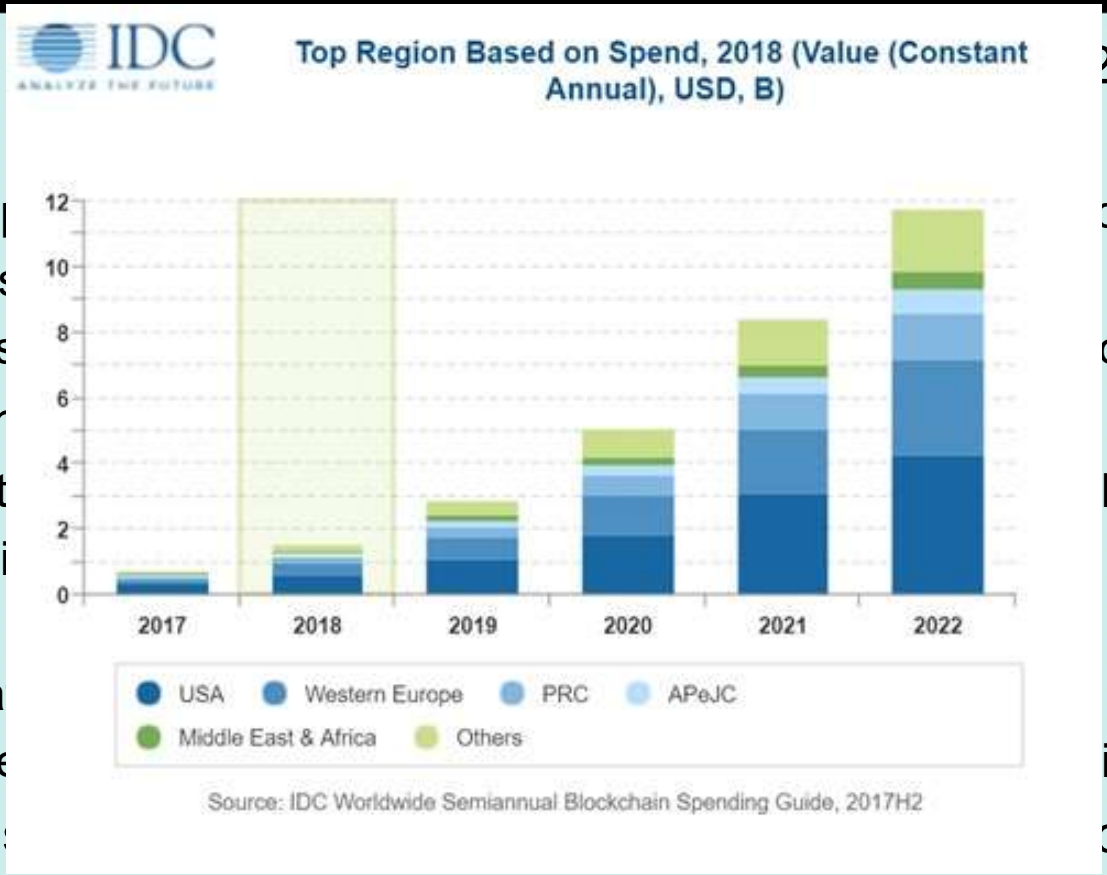
Is blockchain overhyped?

Another day, another article praising blockchain's untapped potential: it will start a new era, revolution the financial system, disrupt every industry and will change the world.

…or will it not? and is that really what I need for my next project?

The size of the “hype”

- Blockchai 2016
- However
  - A group d technology
  - In trans do with it
  - Long Is ocks go up 200%
- Investmer
  - market D
  - 2.1 billi
  - 42.8%
  - 3x rela
  - 13% se ies in PoC
- Financial cts



https://cointelegraph.com/news/vermont-considering-blockchain-tech-for-state-records-smart-contracts

https://coinjournal.net/singapores-ida-teams-banks-deve

https://www.technologyreview.com/s/608088/chinas-central-bank-has-begun-cautiously-testing-a-digital-currency

https://venturebeat.com/2015/11/13/visa-is-e

https://www.ccn.com/singap

https://techcrunch.com/2018/08/03/starbucks-drops-major-hint-at-plans-to-accept-bit

https://www.porsche.com/usa/aboutporsche/pressreleases/pag/?lang=none&pool=international-de&id=479342

COINTELEGRAPH

BTC

News

Fea

By Brian

CCN

BTC/

MIT Technology Review

Log in

Topics+

The Download

Porscheusa.com

My Porsche

PORSCHE

Models | Inventory Events & Racing Service & Accessories Company & Brand Diesel Engine Settlement

Current Press releases

Porsche introduces blockchain to cars

Fast and secure transactions thanks to decentralised protocol

Stuttgart. In collaboration with the Berlin-based start-up XAIN, Porsche is currently testing blockchain applications directly in vehicles. This makes the Zuffenhausen-based company the first automobile manufacturer to implement and successfully test blockchain in a car. Transactions based on this technology are both secure and can be processed far more quickly than anything that has come before. The applications tested include locking and unlocking the vehicle via an app, ten[illegible] access authorisations and new business models based on encrypted data logging. This could be developed further, for [illegible], to improve autonomous driving functions.

TC

Startups
Apps
Gadgets
Events
Videos
—
Crunchbase
More

Search

Apple Hardware Event
2018
Nintendo
Blockchain
Amazon

Login / Sign up

Starbucks drops maj
plans to accept Bitco

Brian Heater @bheater / Aug 3, 2018

Holberton School and Bitproof are simplifying this [illegible]

al Bank
utiously
al

ped a digital currency
of transactions made

UPCOMING EVENTS

BLUEPRINT: Oct. 9 - 11

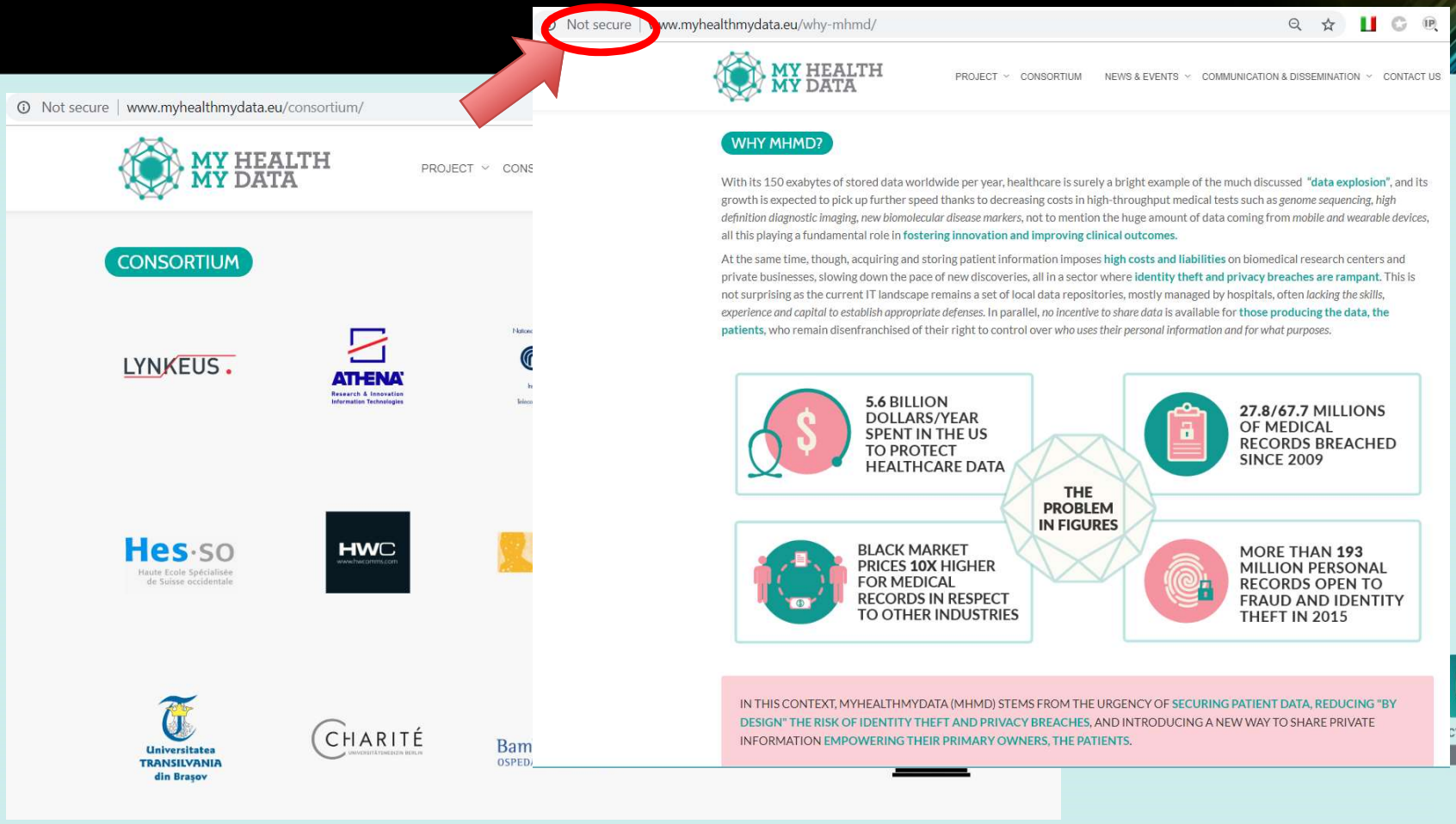
VB Summit 2018: The best in AI. A

CSX 2018 EUROPE

ERSECURITY NEXUS

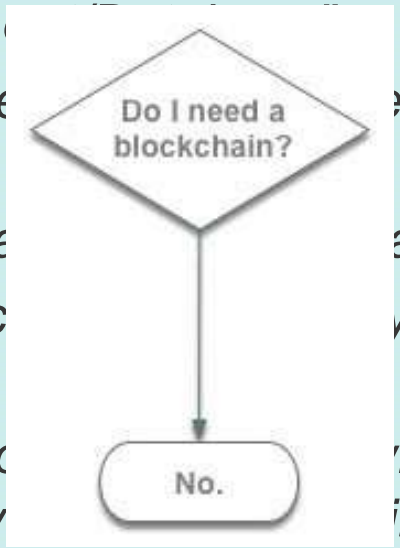
N ISACA CYBER EVENT

Consortiums are starting



Fierce critics exist

- *"Blockchain Is The Most Over-Hyped Technology Ever, No Better than a Spreadsh*
- *"Shitcoin" is a pejorative* *escribe an altcoin that has become worthless.*
- *Ten years in, nobody ha* *a use for blockchain*
- *Blockchain is not only c* *y but a bad vision for the future*
- *There is no single perso* *who had a problem they wanted to solve, discov* *ilable blockchain solution was the best way to solve it, and therefore became a blockchain enthusiast.*



Key challenges

- Technology overall is at an early stage; security risks and best practices vary dramatically
- Technologies making up the ecosystem carry significant risks
- Cryptocurrency has made many public missteps
- There is no legal/compliance framework or deployment best practices
- Smart contracts are code, with all that this carries on

Key questions

1. What is blockchain and why is it important?

2. What does the technology landscape look like, and how does blockchain change the way industry and commerce operate?

3. What is the next phase of blockchain evolution?

4. What steps should a CIO or business leader take to prepare for a blockchain future?

What is the aim of this talk

- understand the basic
  - there will be some hand waving
- being able to answer the excessive counter-critiques
- identify potentially successful blockchain project
- how to find a good candidate within your organization

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Opportunities and Risks

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Valid Criticisms – Debunking Myths

- Blockchain in itself…
  - …does not provide security
  - …can be slow
  - …no governance
  - …still requires IT infrastructure
  - …is not secure

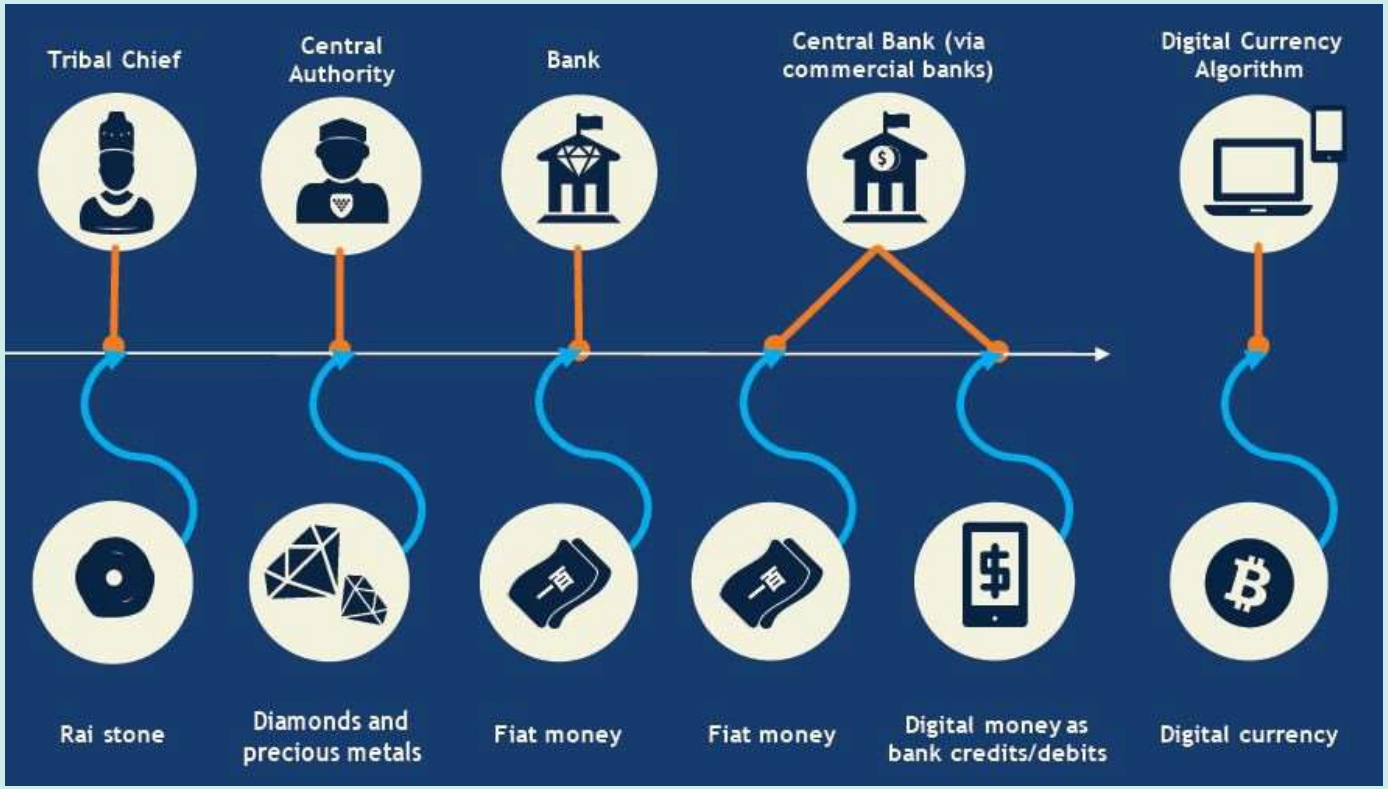
Benefits and uses for blockchain do exist

- Mitigating Trust and Transparency Issues
- Providing community control and Data Integrity
- Use cases abound
  - mostly, where a centralized trust arbiter does not appeal anymore
- Ability for independent nodes to converge on a consensus
- Certainty of determination that a transaction does or does not exist
- Ensuring the Integrity of Digital Assets – fraud mitigation
- Increasing Fault Tolerance and Resilience – e.g. DoS protection
- Can enabling entire new business opportunities

Risks also exist

- Marketing Hype, Inconsistent Definitions
- Scalability
- Response Time
- Blockchain Is Not Immune to Cyberattacks or Fraud
- The Difficulty in Assessing Risk and Exposure Across the Range of Blockchain Offerings

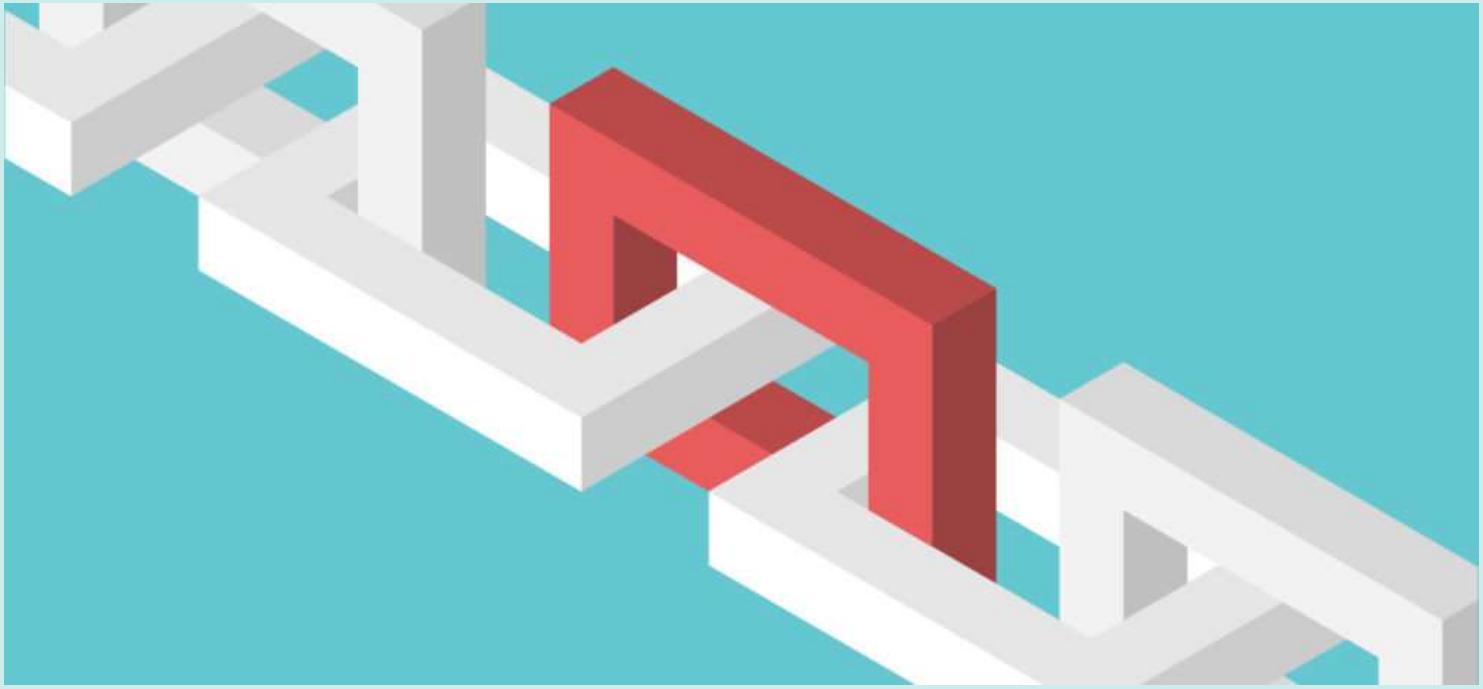
The promise of the blockchain



Next step

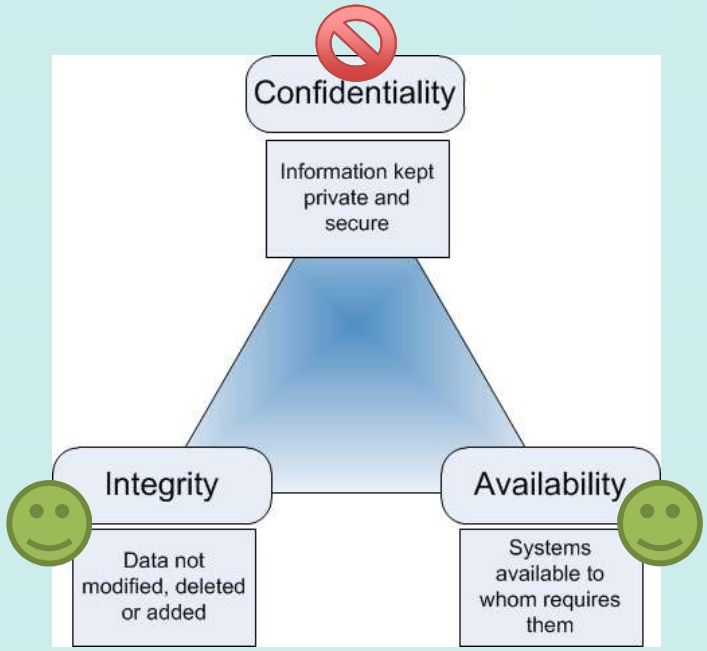
- understand blockchain's technology
- extract business value blockchain technologies
- integrate blockchain with enterprise systems
- planning for changes that blockchain may require

Basics of the blockchain



What is the blockchain about?

- Decentralised, asynchronous processing
- A logic to include/exclude participants
- An algorithm to reach consensus
- Immutability
- Resilience
- Transparency



What are the design goals of the blockchain?

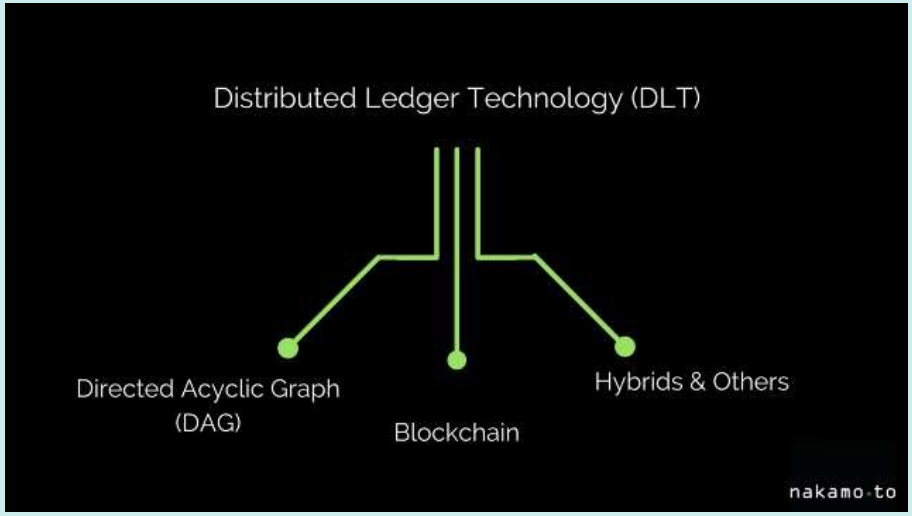
- *"Designed to Disintermediate and Disrupt"*
- Digital representation of value, privately issued
- Varying levels of production/issuance and convertibility
- Payment flows directly peer to peer, around established institutions
- Design goal is to make central authorities irrelevant
  - DAO raised $200M in 3 weeks with crowdfunding, without banks, law firms, marketing or advertising

Blockchain Core Concepts

- Mechanism for adding trust in an untrusted environment
- Create and exchange multiple, various assets and forms of value
- An irrevocable record of significant data and events, such as monetary transactions, property records or other valued assets
  - just a passive data record, or
  - optionally can add dynamically programmed behaviour to events
- Transactions are sequentially grouped into blocks, validated (via consensus) and propagated across a network
- Each block of transactions is chained to the previous and immutably recorded using cryptographic trust and assurance mechanisms
- Depending on the type of distributed ledger, transactions can include programmability to enabled autonomous actions

What is a DLT?

- Distributed Ledger Technology (DLT) is the generic definition of an expanding list of cryptographically signed, irrevocable transactional records shared by all participants in a network

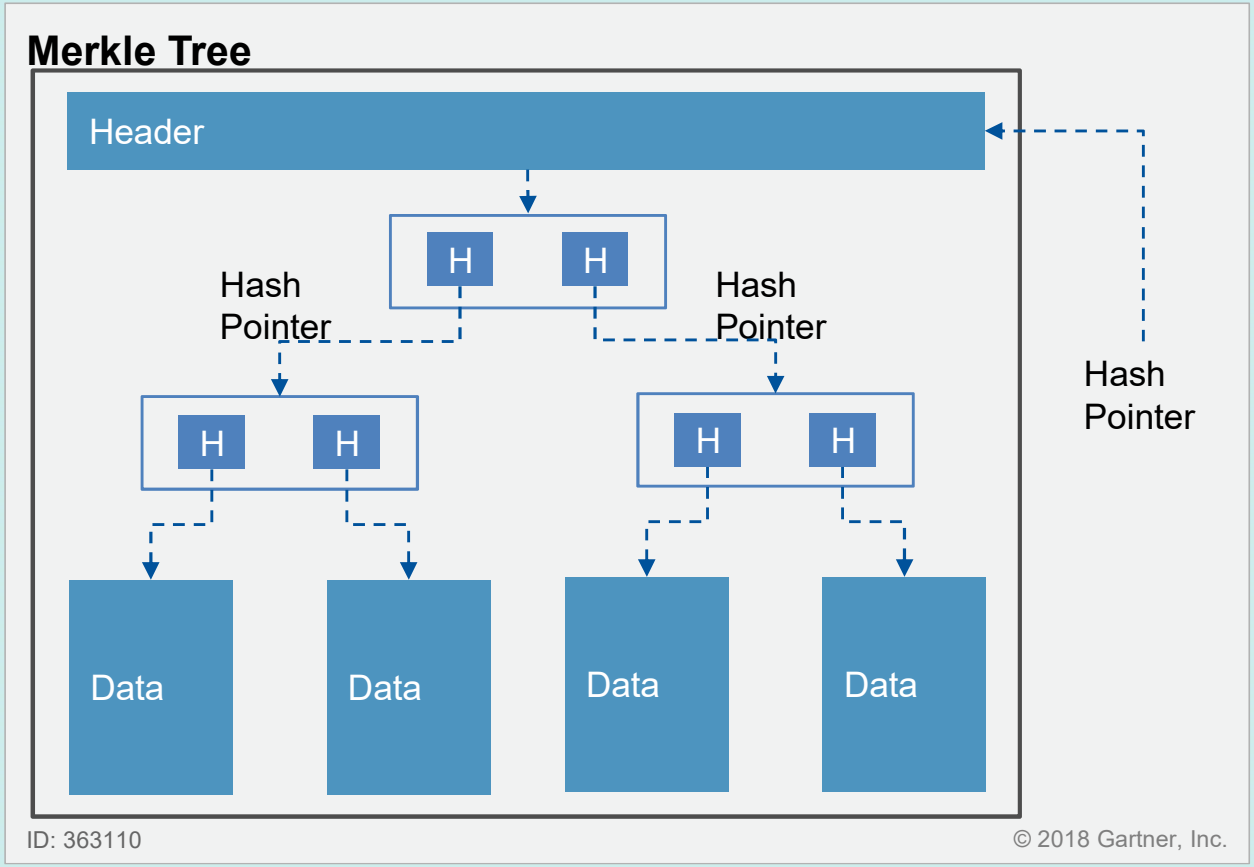


- Synonym with blockchain – but not the same

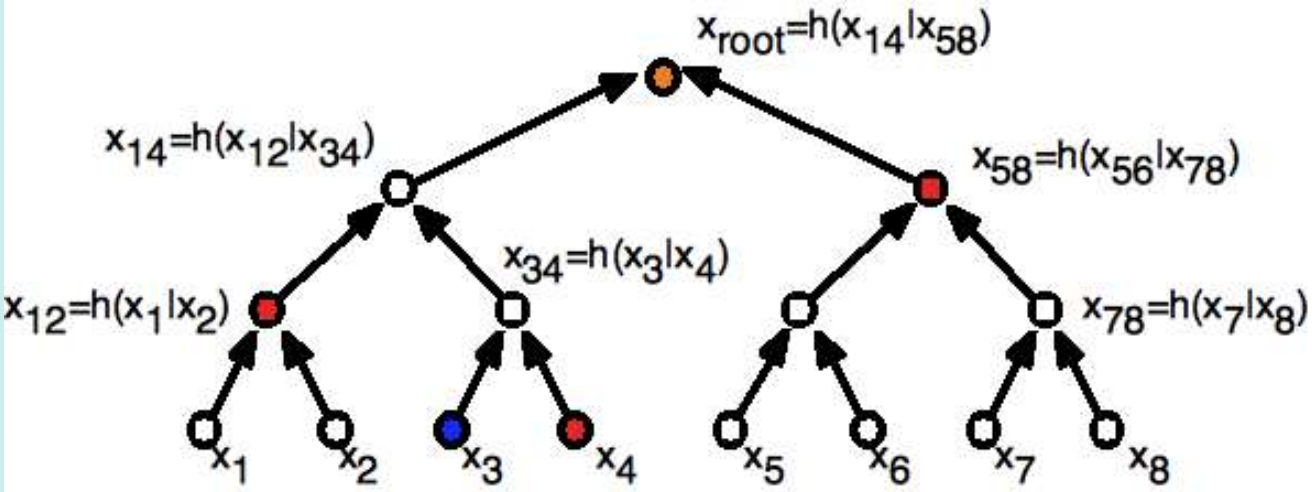
What exactly is a blockchain?

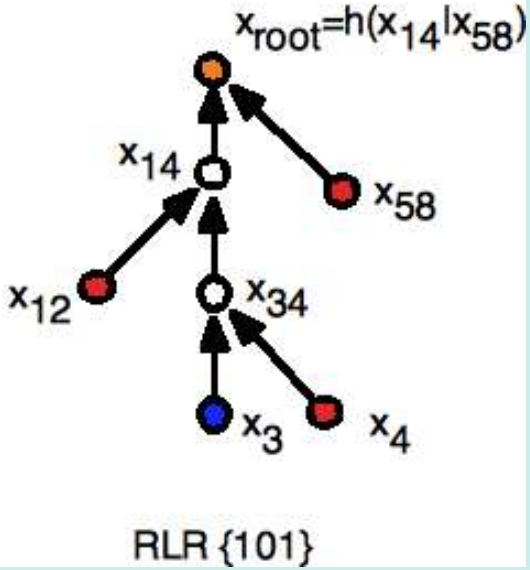
- A linear Merkle tree (hash chain) implementing a distributed, “trustless” architecture incentivised by a value token
- Value token
  - Money is an entry in a record (wallet)
  - Any system can issue tokens of value
- Can be used for many other purposes, not just token issuing
- Original Bitcoin whitepaper from Satoshi Nakamoto in 2008
  - Blockchain
  - Proof of Work
  - Consensus algorithm

Merkle Tree



Hash tree vs linear Merkle tree





$$h(h(h(h(x)))) = h^4(x)$$

Password authentication with hash chains

$h^{999}(password)$

$h^{998}(password)$

$h^{998}(password)$

$h^{1000}(password)$

$h^{1000}(password) = h(h^{999}(password))$

$h^{999}(password)$

$h^{999}(password) = h(h^{998}(password))$

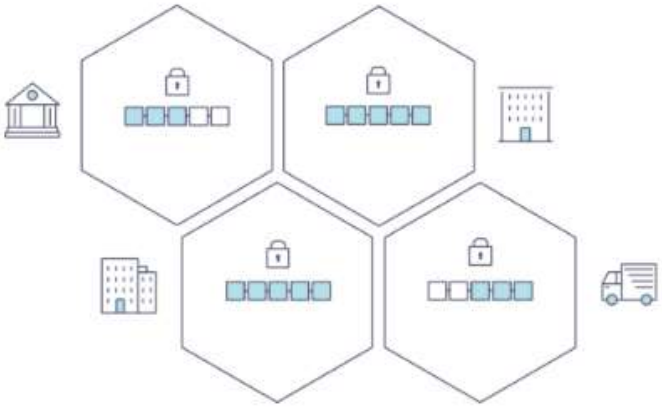
$h^{998}(password)$

$h^{998}(password) = h(h^{998}(password))$

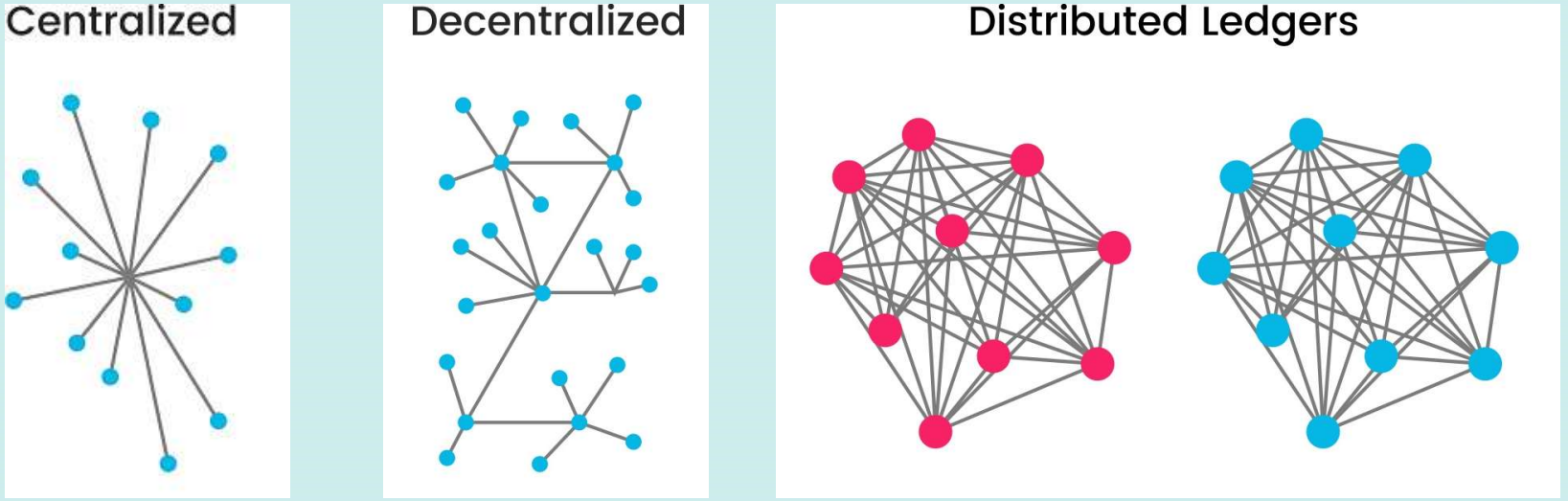
$F^{1000}(x), ..., F(F(F(x))), F(F(x)), F(x)$

How does a blockchain ledger usually looks like

- Distributed Ledger Technology (DLT)
  - Append only and peer-to-peer
- Decentralised
  - Disintermediation
- Collaborative
  - Consensus logic as a function
- Data Repository / Database
- “Eligible participant”: access policy
  - Example, Bitcoin: public
  - Private: requires cybersecurity
- Headers are always available to all participants (transparency)
  - Requires awareness of the data stored – use CIA



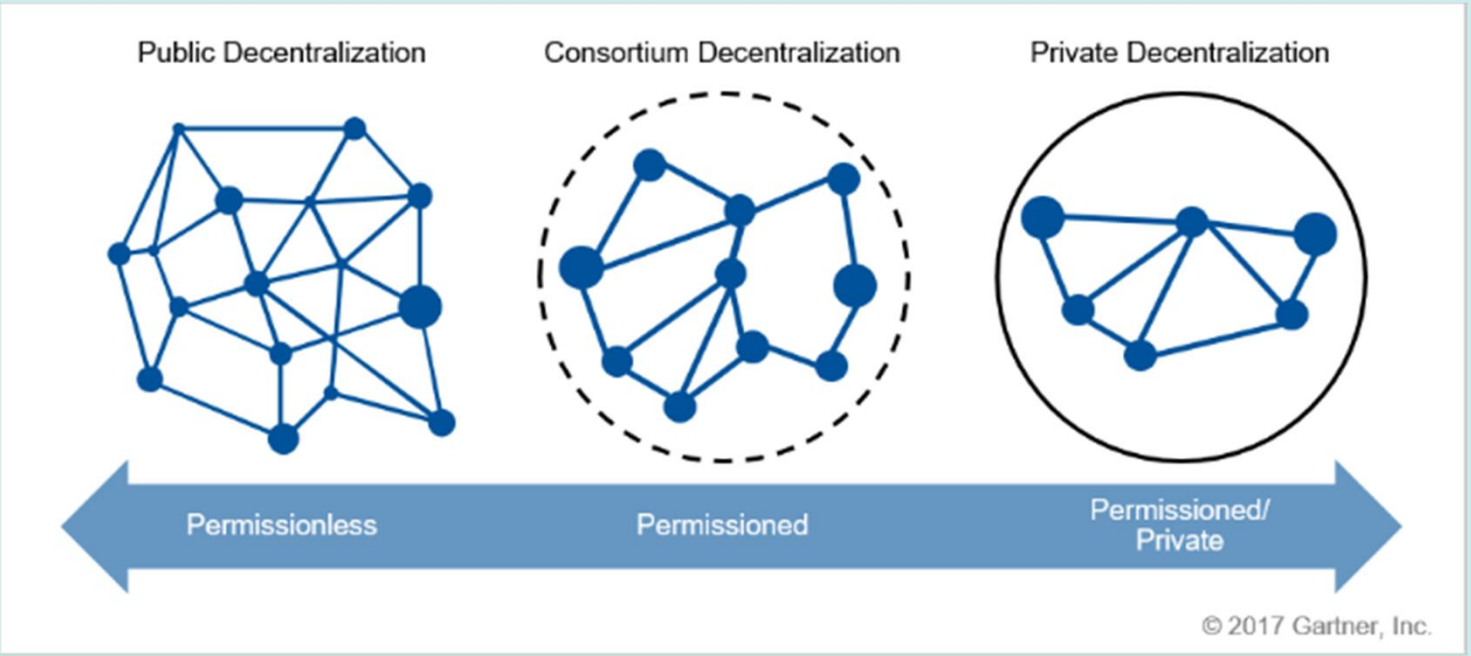
Consensus Distribution Models



- On Distributed Ledger, there is no central authority
- Peer-to-peer
- Authority and trust are transferred to a decentralised virtual network called blockchain

Public vs Private vs Consortium-based

- Define the notion of “eligible participant”



Surviving your company's Blockchain initiative

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

FAKE! …but still…

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Make sense of the blockchain

- Blockchain can be viewed as a protocol
- It must support real, needed business process, like HTTP supports e-commerce

1. Verify that blockchain makes sense for the initiative
2. Ensure that implementing blockchain produces new digital business that cannot be realized in other ways
3. Perform the Ground Work from the next slides
4. Perform the Risk Assessment as explained later

Ground work

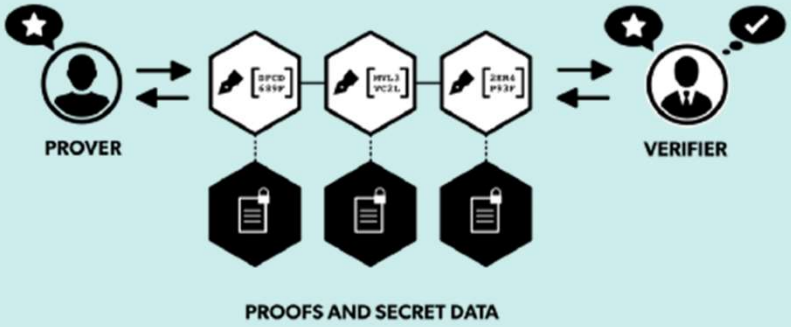
- Blockchain technology are immature from a technology perspective
- There are too many platforms to actively track and understand
- Because of difficulty in grasping the differences, organisations tend to focus on consortium-based approaches
- Blockchain is still subject to cyber threats – requires crypto-agility
- What you should do:
  - engage with the blockchain initiatives, inform and advise of the risks
  - don’t trust vendors – and prophets
  - be aware of the data created, stored and used
  - leverage the old fashioned CIA model
  - eventually apply data-centric security (encryption)

Other things necessary

- Readiness assessment: are processes ready for decentralization?
  - If processes are designed for a centralized model, traditional components will be more suitable
  - decentralizing processes is the real way
- Select an architecture strategy
- Compare candidate platform
- Strategy should be kept flexible
  - immature
  - lack standards
  - lack deployment best-practices
- May need readjustment in little time

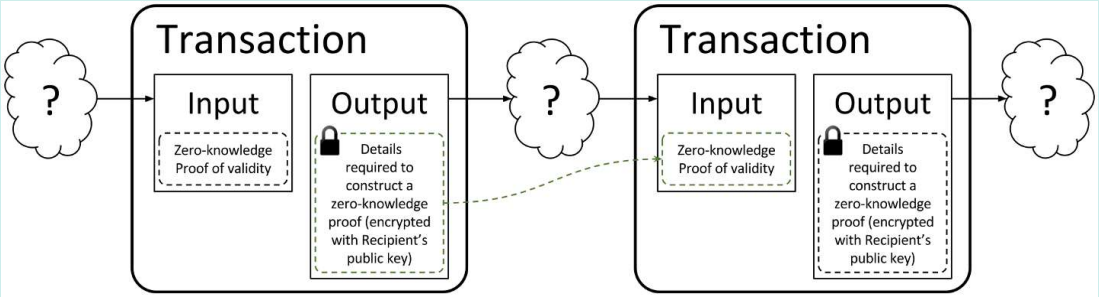
Adoption Challenges

- Very few projects are production-ready in an enterprise setting
- Regulatory challenges waiting at the horizon
- In payment use cases, price volatility
- Many PoCs are about permissioned blockchains
  - it is not feasible for a company to join multiple private blockchains from all their partners
  - the unique option is **zero-knowledge proof**



Privacy-preserving blockchains

- **zk-Snarks** – Zero-knowledge protocols enable the transfer of assets across a blockchain network with complete privacy
- Other participants only know that a valid transaction has taken place

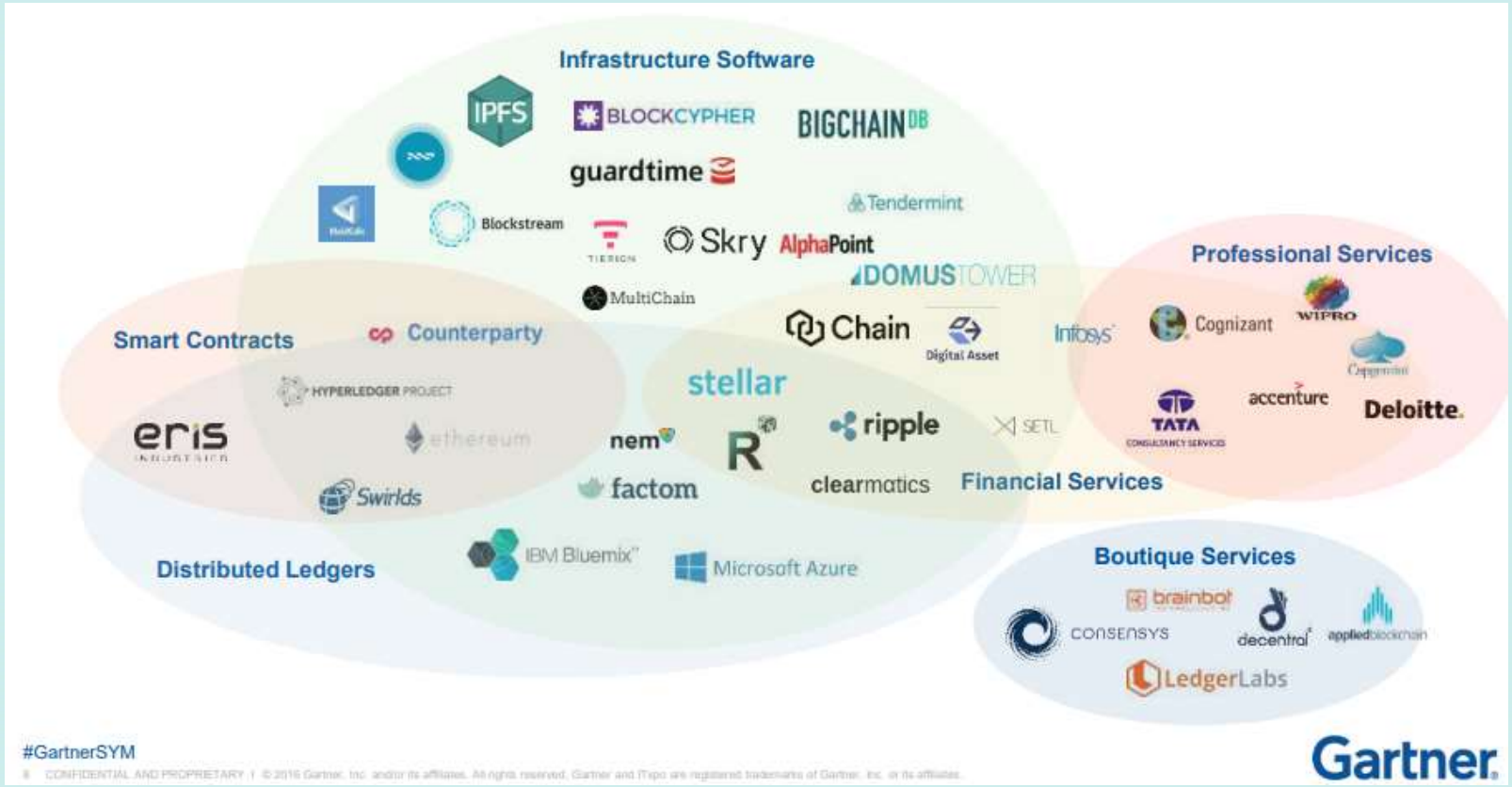


- First notable implementer was ZCash, then Ethereum
- Problem: it is still too computationally expensive

Possible timeline

- **First week**
  - Clarify how your organization understands blockchain technology… and educate management
  - Conduct internal IT meeting to assess opportunities for development using a blockchain technologies – e.g., in security, open platforms, etc.
- **Next 90 Days**
  - Conduct an assessment of your internal capabilities
  - Assess vendors talking about blockchain and analyse their capabilities
  - Select a limited and simple narrow-scope use case for real deployment
- **Next 12 Months**
  - Assess whether users are enabled to everyday use, fit for business and consumer context.

Vendors' Panorama



CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

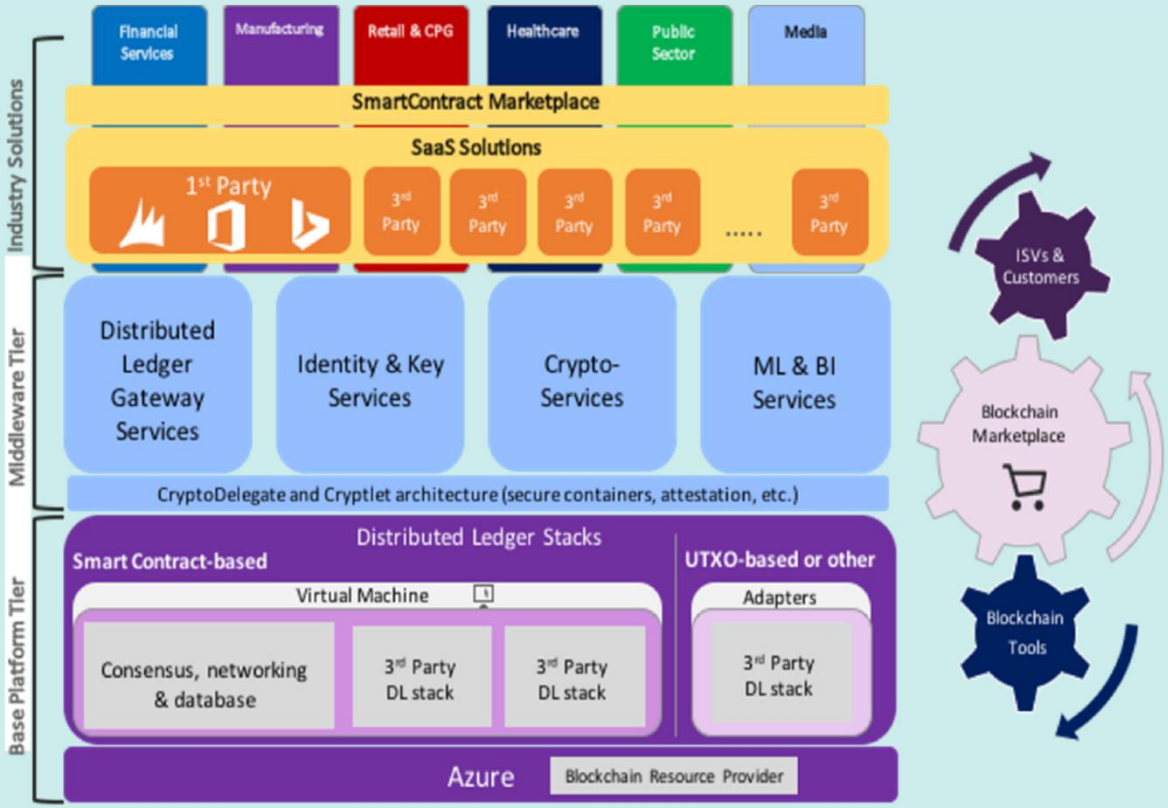
Snapshot of current known PoCs

	Foundational Technology	Transform Operations	Transform the Business	New Opportunities
Banking	✓	✓		
Insurance		✓	✓	
Telecom	✓	✓		
Tech	✓	✓	✓	✓
Media		✓	✓	
Healthcare		✓		
Pharmaceuticals		✓		
Automotive		✓	✓	✓
Travel & Transportation		✓	✓	
Retail		✓		
Energy		✓	✓	
Chemicals		✓		

Blockchain as a Service

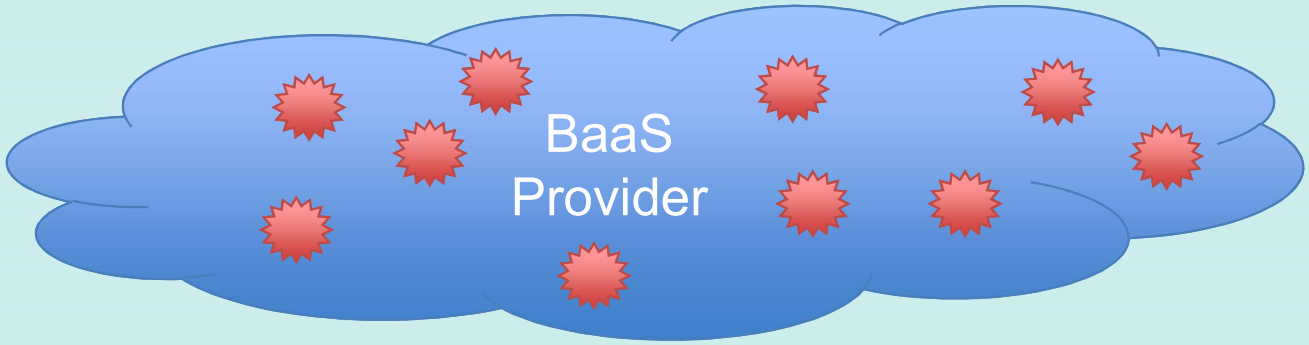
- BaaS as an emerging possibility for the supporting infrastructure
- Similar to a “cloud” offering
  - Economies of scale
  - Elasticity
  - Expertise
  - Security + standards
- Main providers
  - IBM (Hyperledger Sawtooth Lake – Bitcoin)
  - Microsoft (Coco Framework – Ethereum)
  - AWS (Ethereum Network)
- Private and Permissioned
  - Current BaaS focus: “safe” experimentation

Microsoft's Project Bletchley



CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Architectures



Organization A

Organization B

Organization C

Key Considerations

- The provider is the tenant of the Smart Contract
  - The tenant owner pays for running them
  - Trusted execution environment (enclaves)
- Function as ledger mediator for multiple parties
- Who controls what still depends on the organizational structure and the system architecture
  - Consortium or Federation?
- More secure?
  - Depends on the risk profile and how much can participants see
- Risk and Security themes overlap with “trusted cloud”

Legal and Regulatory Challenges

- **Jurisdiction** – challenged by the concept of decentralization
- **Service levels and performance** – vendors are unable to offer warranties
- **Liability** – especially in trading platform like cryptocurrencies
- **Intellectual Property** – vendors will likely try to capitalize on this
- **Data Privacy** – not alterability of data and transparency
- **DAOs** – legal status unclear
- **Smart Contracts enforceability**
- **Compliance with financial services regulation** (where applicable)
- **Exit assistance**
- Common Law's **concept of "property"**
- **Due diligence** is yet to be clearly defined

Phase 1: Business Processes

- What specific features unique to blockchain do we need for this project?
- What is the lifetime of this project and its resulting business applications, and will we be able to support the business and technical requirements?
- What impact will the blockchain aspects of this project and its associated application have on how end users interact with the system?
- What would be the impact to the project if parts of the blockchain were locked due to human or technology error, such as loss of control of private keys?
- What additional skills will be required to support a blockchain-based project and resulting application?

Phase 2: the Trust Model

- What are the relevant advantages or disadvantages of public versus private or consortia blockchain for this project? What risks do each model pose, and who would own those risks?
- What are the organizations that will be involved, and what is the trust model for them?
- What is the governance model (trust framework) for participating organizations and their members?
- How are responsibilities for the blockchain distributed?

The choice of trust model can affect the initiative outcome.

Phase 3: Business Logic and Execution/Resiliency

- What is the business life cycle for blockchain participants?
- What is the expected frequency of change to the business logic (application) and supporting infrastructure?
- What is the business logic for joiners, movers and leavers?
- Who issues credentials, and how are they managed?
- What plain-text data will be captured in each block?

Phase 4: Risk Management and Compliance

- What are the relevant regulatory issues for the project?
- What are the options for meeting them within the blockchain protocol?
- What data will be carried in plain text by the blockchain?
- Who in the organization or consortia will regulators look to for answers?

Phase 5: Identity and Key Management

- What is the full life cycle of the keys that blockchain participants will use for the project?
- How are the details of identity managed?
- Are block payloads encrypted?
- For identities, are privacy-preserving methods needed for anonymity?
- How are keys managed and revoked?
- What mechanism will be used to protect private keys?
- What will be the approach to problems such as crypto-agility and identity theft?

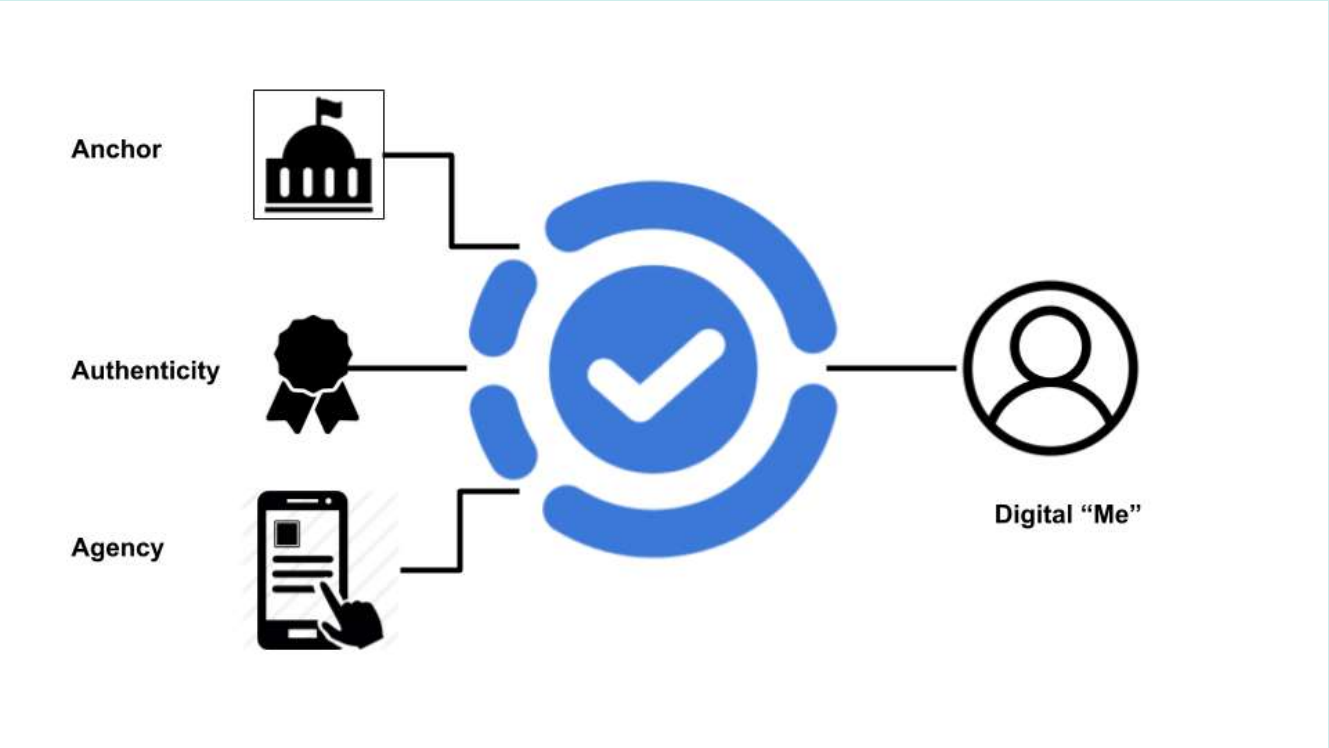
Phase 6: Threat/Network/Node Management

- What is the logic for resolving blockchain block collisions?
- How do you keep track of distribution nodes in the system, and what would a critical fault event look like?
- What is the disaster recovery plan for your blockchain participants?
- How to deal with out-of-context problems, like net neutrality, or with older networks that may introduce lags?
- Are there any race conditions in the distribution of nodes that would allow a person or small group to control the blockchain?

Phase 7: Physical Layer Management

- What is the minimal security posture for blockchain clients or wallets for participation in the projects?
- How do physical processes get conducted through smart contracts or blockchain instructions?

Self-sovereign decentralized identity



Blockchain-enabled Identity Services

- Privacy-preserving decentralized identity services are becoming feasible
- Service Providers use these records to verify authenticity of an identity
- PoCs are around B2C
- Decentralized identity and related evolving standards will be disruptive
- Self-sovereign decentralized identity models put users in control
- Identity trust fabric (ITF) immutably stores proof of identities cryptographically
- Optimized Blockchain platforms can provide a suitable environment
  - Blockchain platforms are not mature yet!
  - Do not inherently meet all requirements for production ready ITF
- Evolves in Self-sovereign Identity networks and verification services
- Connecting identity owners, consumers, and services

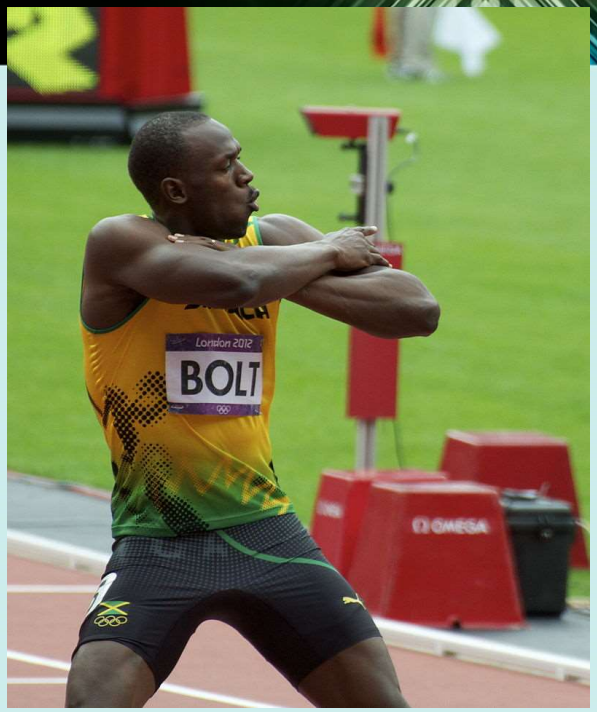
- Identify relevant decentralized identity use cases for employees, business partners and consumers
  - especially to replace old register-store-verify methods of collection
- Explore decentralized identity architectures
- Establish a decentralized identity team for a small-scale PoC
- Evaluate requirements against open issues such as compliance, initial identity collection, user experience, scalability, data revocation and update
- Select solution partners, evaluate participation in consortium
- Consider implication of direct user control of identities into life cycle processes

Opportunities and Challenges

- Successful blockchain enterprise production examples are still rare
- Business leaders may not have clear where the value can be achieved
- Most current experiments are just renovation attempts
- There are still several business and technology challenges to adoption
- What You Need to Know
  - Exploiting blockchain demands enterprises be willing to embrace decentralization in their business models and processes
  - Blockchain projects are not another arrow in the quiver
  - Reimagine by design thinking
- Today's technology are immature; will need pivoting in two years
- Experiment, focus on the business problem, avoid vendor lock-in

Characteristics of the Winners

- Sustainable — or not yet "on the scene"
- Functional governance
- Open source
- Configurable agreed formats
- Open architecture/APIs
- Tested in a public environment but able to run in private and public
- Smart contract capabilities at multiple levels
- Secure



Practice sound security and risk principles

- Blockchain is early in its development, and long-term investments can be risky.
  - Complexity, cryptography and implementation errors may cool enthusiasm for blockchain and pose risks for users
  - Clarify risks at the business, technical and cryptographic levels
  - Evaluate the risks for any blockchain-based project, including technology, governance and compliance, human misunderstanding, and value at risk
  - Evaluate preparedness and incident response plans that will address critical security events during the blockchain life cycle, as these are to be expected
- Temper the hype with effective risk-mitigation techniques

Minimum Self-Defence

- Be prepared to answer questions
  - how to securely implement blockchain-enabled business processes and applications
- Understand the differences regarding trust models
  - private, public and consortium
- Evaluate the technical security aspects of blockchain platforms under consideration
- Carefully evaluate applications for their suitability for integration with the specific blockchain systems and subsystems
- Implement a vulnerability and incident management program
- Continue to monitor key vendors

Embrace Digital Risk Management

- The challenges:
  - Digital transformation has become business transformation and optimization, and blockchain is a potential critical capability enabling that convergence
  - Digital risk thinking and action is required to address blockchain risks
  - Blockchain risks can have requirements similar to DevOps
- Evolve an effective risk management strategy:
  - Incorporate the new risk considerations – value transfer, contractual, resilience, privacy – when assessing blockchain initiatives
  - Develop a simple framework mapping strategic business risks with operational and IT risks

Bonus Slides

GDPR and Blockchain – CNIL opinion (2018)

- Participants are **Data Controller** if:
  - individual person, data treatment is professional or commercial
  - legal entity, writing personal information
- If more than one person decides to **process personal data**:
  - Make arrangements regarding responsibility for processing
  - Creation of a legal entity that acts as data controller
  - Nominate a participant to act as a data controller
  - If not, everyone is a controller
- **Data Processors** can also be "smart contract" developers and miners
- On Public Blockchains, encouraged contractual solutions between participants

Blockchain and e-voting – 1/2

- It can’t be used unless violating basic democratic principles
  - A voter must be a citizen (authenticity)
  - Their voting choices must not be known, especially not on a public ledger (confidentiality)
  - The vote they cast isn't tampered with (integrity)
  - A voter shouldn't be able to prove who they voted for (avoiding bribery and vote trading)
  - A public final count so multiple people can validate the system as a whole
- I have a key pair; the public key is signed by the State authority
- Cast my vote by signing it with my private key and add it to the public ledger

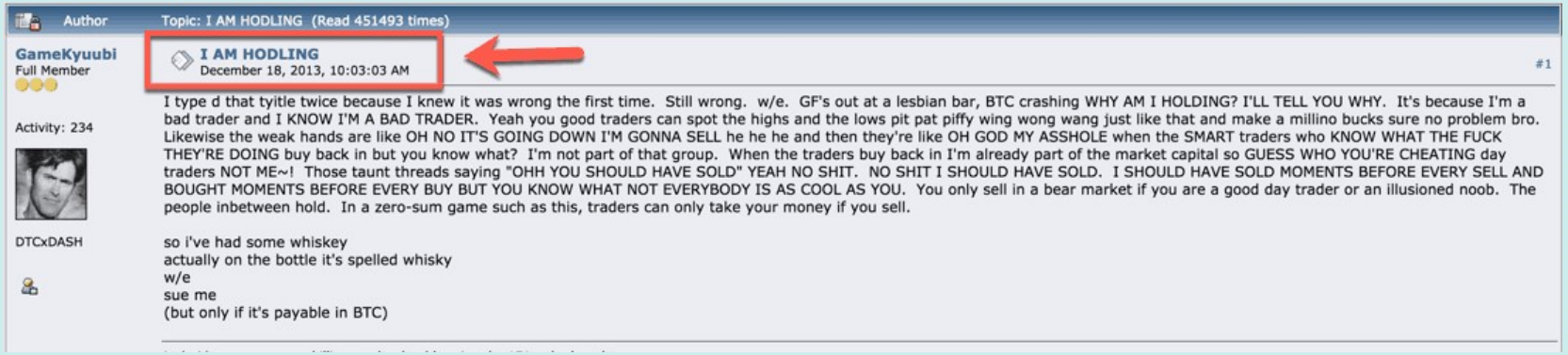
Blockchain and e-voting – 2/2

- However…
  - The State authority can use the signature to identify me and my vote
  - The State authority can create as many "citizens" as they want
  - Verifying a signature gives a cryptographic guarantee of exactly who I voted for
- You can have a secret final count, but it still relies on “classical” security (e.g. server protection, network security)
- Conclusions:
  - You have to choose between a secret ballot or a public ledger
  - If you choose secret ballot, the blockchain is useless
  - The State authority can direct the result by creating fake votes
  - Incompatible with “software independence”
- Many of these applies to e-voting in general

Decentralized Autonomous Organizations (DAOs)

- Online, digital entities that operate through the implementation of pre-coded rules
- The thought is that if bitcoin can do away with financial middlemen, then maybe companies and other organizations can one day operate without hierarchical management
- They need minimal to zero input into their operation
- They work by executing smart contracts, recording activity on the blockchain
- Described by What Hearn in 2009 as a company operating a driverless car fleet
- Legal status: futuristic

HODL



Author | Topic: I AM HODLING (Read 451493 times)

GameKyuubi
Full Member

Activity: 234

DTCxDASH

I AM HODLING
December 18, 2013, 10:03:03 AM

#1

I type d that tyitle twice because I knew it was wrong the first time. Still wrong. w/e. GF's out at a lesbian bar, BTC crashing WHY AM I HOLDING? I'LL TELL YOU WHY. It's because I'm a bad trader and I KNOW I'M A BAD TRADER. Yeah you good traders can spot the highs and the lows pit pat piffy wing wong wang just like that and make a millino bucks sure no problem bro. Likewise the weak hands are like OH NO IT'S GOING DOWN I'M GONNA SELL he he he and then they're like OH GOD MY ASSHOLE when the SMART traders who KNOW WHAT THE FUCK THEY'RE DOING buy back in but you know what? I'm not part of that group. When the traders buy back in I'm already part of the market capital so GUESS WHO YOU'RE CHEATING day traders NOT ME~! Those taunt threads saying "OHH YOU SHOULD HAVE SOLD" YEAH NO SHIT. NO SHIT I SHOULD HAVE SOLD. I SHOULD HAVE SOLD MOMENTS BEFORE EVERY SELL AND BOUGHT MOMENTS BEFORE EVERY BUY BUT YOU KNOW WHAT NOT EVERYBODY IS AS COOL AS YOU. You only sell in a bear market if you are a good day trader or an illusioned noob. The people inbetween hold. In a zero-sum game such as this, traders can only take your money if you sell.

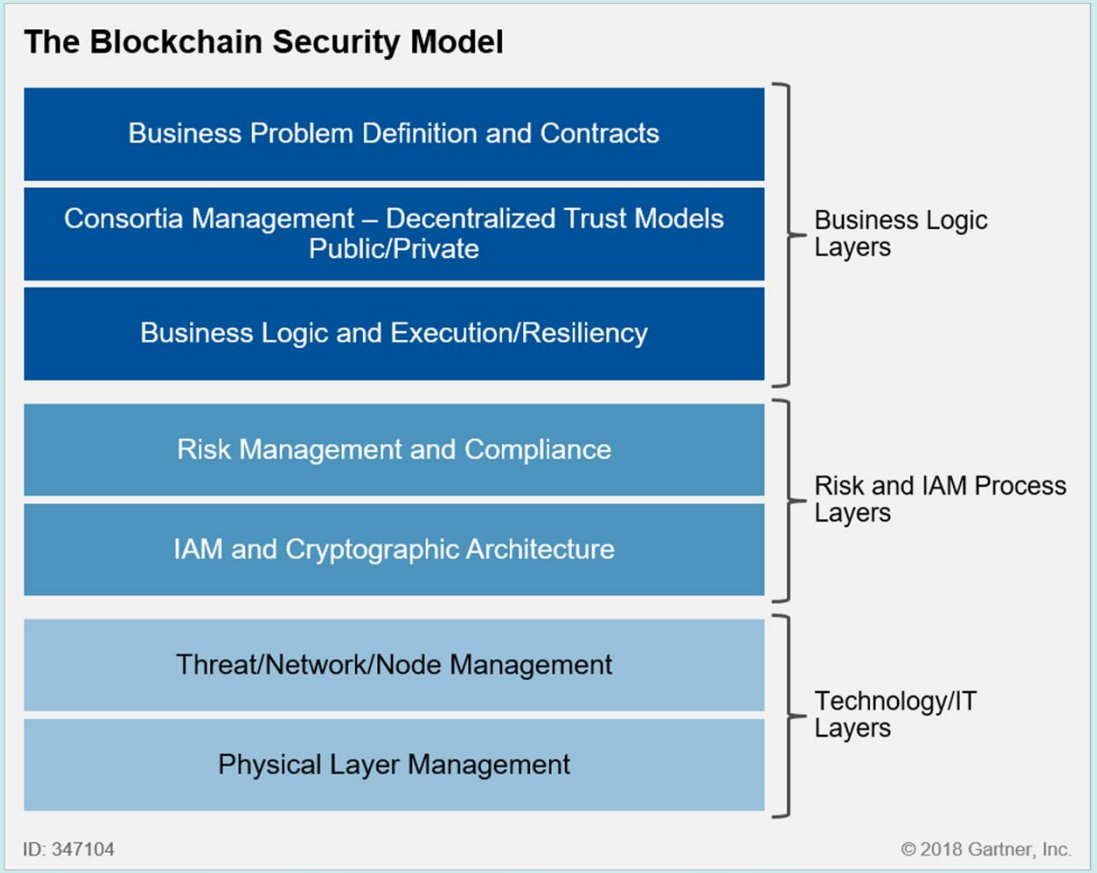
so i've had some whiskey
actually on the bottle it's spelled whisky
w/e
sue me
(but only if it's payable in BTC)

- Slang term used originally in a bitcoin talk forum in 2013
- The user was blatantly drunk and misspelled “holding”
- He wanted to convey that we was holding despite the serious fall
- The term become then very popular and has originated the backronym “Hold On for Dear Life”

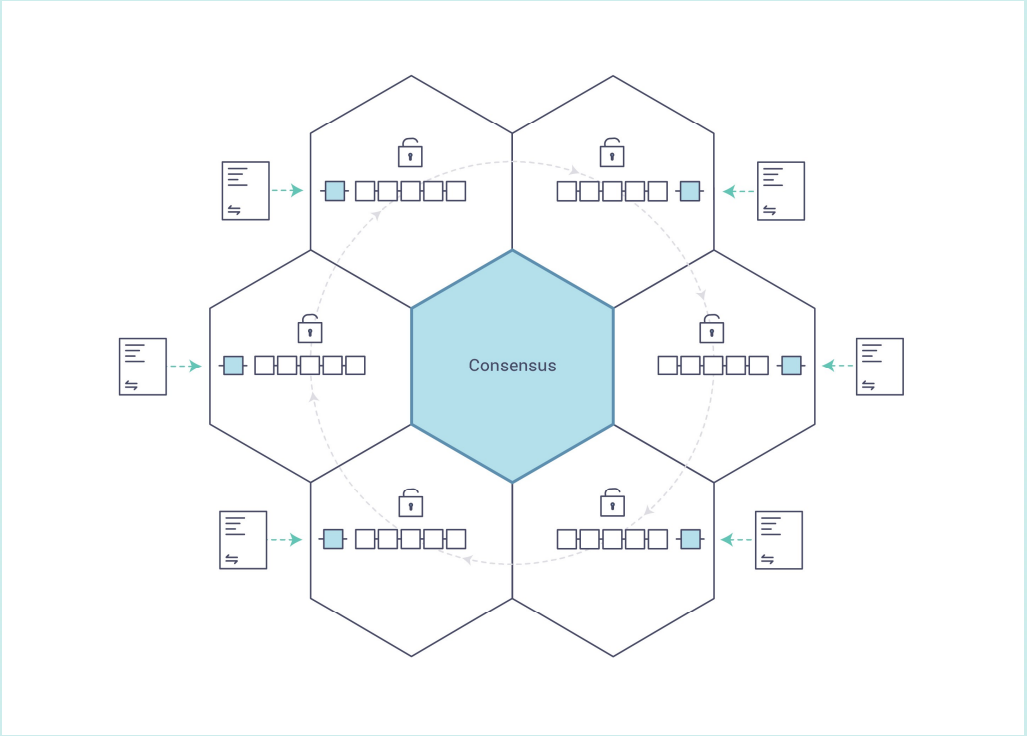
Other Cryptocurrency Slang

- **Airdrop**: the process of distributing tokens to wallets
- **Altcoin/Alt**: any coin that isn't Bitcoin.
- **Moon/Mooning** is when a coin goes on a "bull run", that is, when the price goes up quick
- **FOMO**: Fear Of Missing Out, an emotional response that makes people impulse buy tokens at their all-time high
- **Gas**: The Ethereum network requires one to pay "gas" to send a transaction or otherwise execute a smart contract
- **ICO**: An initial coin offering
- **Lambo**: Lambo is short for Lamborghini – sort of a status symbol, goal post, and/or meme.

Gartner's blockchain Security Model

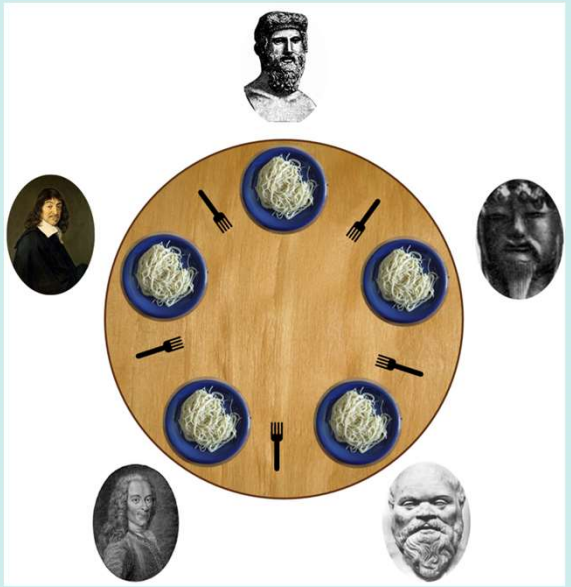


Consensus Mechanisms



The story of consensus: the dining philosophers

- Five philosophers sitting at a table
- A fork between each of them
- Must alternatively think and eat
- Can only eat if they have two forks
- Forks are single use
- Can take a fork as it becomes available
- But cannot start eating before they have two
- Infinite supply and demand



- Test: develop a concurrent algorithm which avoids deadlocks

Computational Consensus: Paxos protocols

- Protocols for solving consensus in an unreliable environment, assuming participants and/or communication failures
- Distributed computing spun off from here
- Trade-offs on
  - number of processors
  - number of message delays before learning the agreed value
  - activity level of individual participants
  - number of messages sent
  - types of failures
- Standard Paxos is slow and does not solve Byzantine Generals problem

The Byzantine Generals Problem

- A group of generals, each commanding a portion of the Byzantine army, encircle a city
- These generals wish to formulate a plan for *coordinated* and *agreed* attack or retreat
- Treacherous generals can cast suboptimal votes selectively
- Generals are physically separated, messengers may lose or forge the vote
- BFT can be reached if the loyal, non-faulty generals reach a majority
- The metaphor is: computers are generals, networks are messengers

Byzantine Generals' Problems really happens

- Not an academic discussion – it happened!
  - Mostly in aeronautics and space missions
- A practical solution requires:
  - 3f + 1 replicas to tolerate for ≤ f faulty nodes (to allow 2f + 1 quorum)
  - quorums(f + 1) out of 2f + 1 nodes in every operation
  - dealing with malicious primary
  - use a 3-phase protocol to agree on sequence number
  - dealing with loss of agreement
  - using strong cryptography so the adversary is unable to subvert it
- Practical solutions based on fault tolerance are very complex, and can only tolerate 1/3 corruption of the nodes
  - Unpractical on large networks

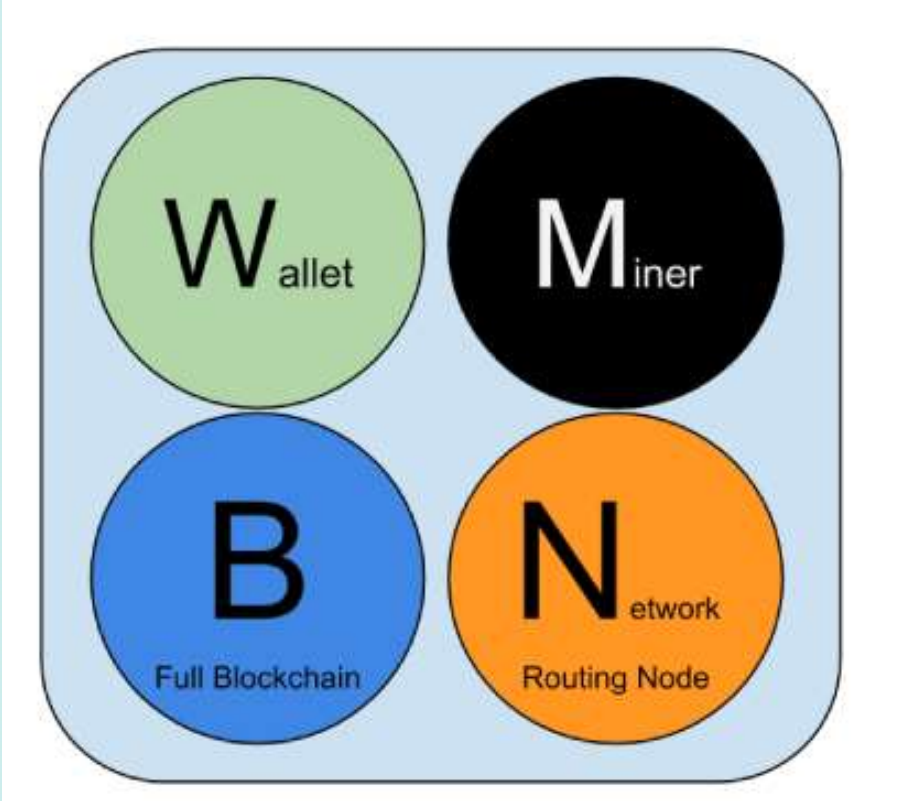
Bitcoin

CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

Bitcoin is born

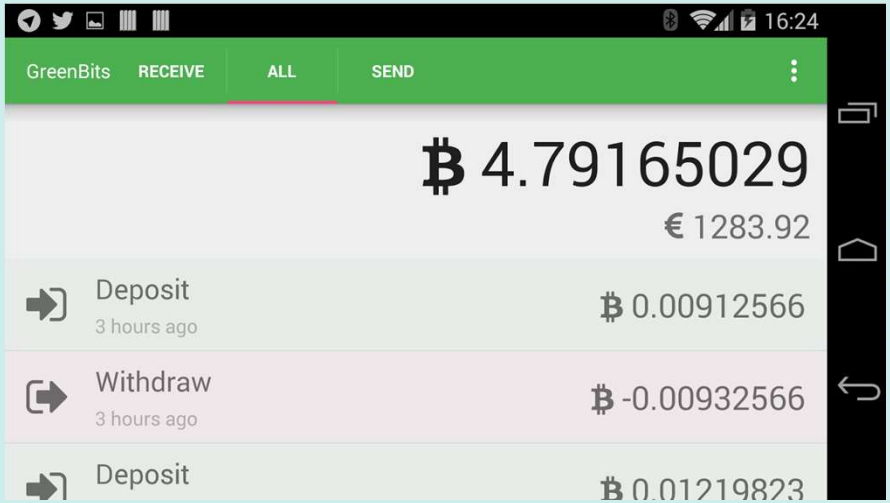
- The first and most widely used **cryptocurrency**
  - built upon a history of failed ones
  - inspired by Cypherpunk Movement of the 1980s
  - As Hashcash, relies on Proof-of-Work, a peer validation protocol
  - As Digicash, every node maintains a full copy of the ledger
  - As B-money, each node has its own identity
- Bitcoin vs bitcoins vs satoshis
- Aims to be pseudonymous, trustless, decentralized, immutable, democratic
  - Each computer is a node in the network
  - minting and distribution of bitcoins happens through mining
- Deflationary currency

Four key functionalities of Bitcoin



Wallets

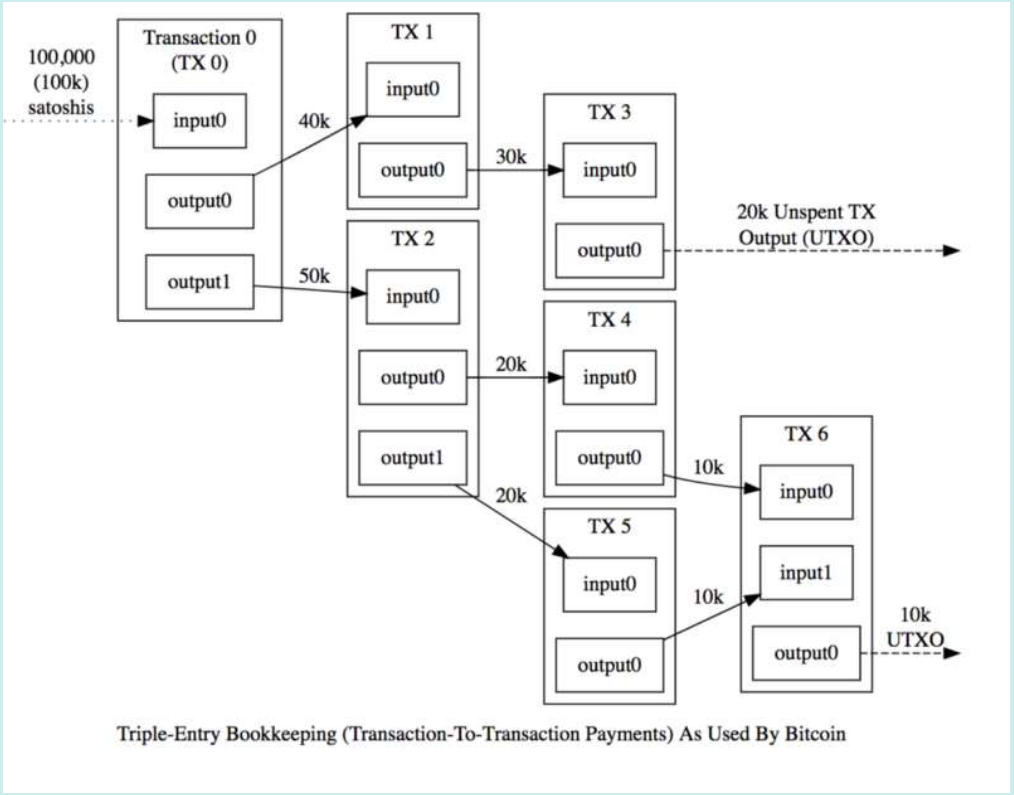
- Keep tracks of identities
- Generate keys, track transactions
- Do not store bitcoins! **Control over private keys is essentially control over identity and bitcoins**



Bitcoin exchanges

- Easy to use interface, low entrance curve
- Wallets are stored online
- Single points of failures
- Decentralized exchanges uses “proxy tokens”
- Loses the “JOBK” approach from wallets
  - hard to scale
- Use Hierarchically Deterministic Wallets
  - Controller of parent is the controller of children
- 80/90% of transactions

Unspent Transaction Output (UTXO)



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

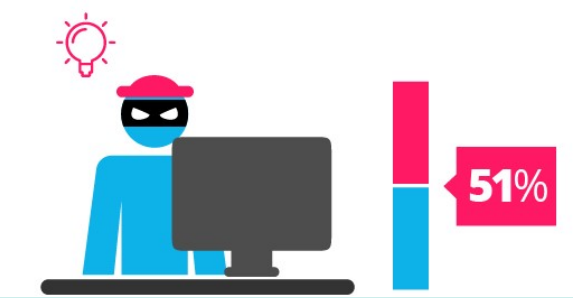
What makes a transaction valid?

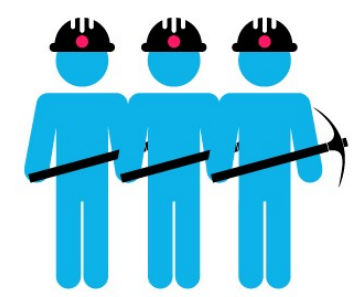
- Proof of ownership
- Funds must be available
- No other transactions using the same funds
  - storing transactions in “blocks”
  - transaction is sent to the network
  - transaction is “unconfirmed” until the next block is created (mined)
  - transaction is verified and included in the block
  - the transaction has now one confirmation
  - transaction fee given to the miner
- Blockchain can only reach “eventual consistency”

Bitcoin consensus is a complicated concept

- There is no absolute notion of “permanently included”
- Agree on which update is added to the blockchain
  - prevention of Double Spend Attacks
- Everyone can cast votes, but to do so requires computational power
  - Proof of Work – mining – prevention of Sybil Attacks
- Need to be part of the winning fork
- Reorganizations can happen, leaving “orphans”
- Single blocks are orphaned daily, but rarely more than one
- 6 blocks is the standard confirmation period, but it can vary
- 1 block every 10 minutes, 6 blocks = 1 hour

Proof of Work (PoW) in Bitcoin





- The concept is to use **resources** instead of **identities**
- Through blockchain and PoW, Bitcoin successfully overcome the difficulties of:
  - ensuring every node holds a consistent version of the transaction history
  - identifying malicious actors
  - blocking both **Sybil** and **Double-Spend** attacks
- Innovative combination of PoW, signatures, Merkle chains, P2P

Bitcoin is robust

- Bitcoin is robust because it serves the same functions as a bank:
  - Account management
  - Legitimacy
  - Record-keeping
- Unlike a bank, is decentralized and ensures a high degree of privacy and trust
  - authentication based on public/private key pairs
  - public keys are used to send and receive funds
  - private keys to prove ownership and redeem sent funds
  - each individual is responsible for their own keys
  - private keys are randomly generated
  - much cheaper than a bank (for big transactions)

First bitcoin physical purchase

Bitcoin critics

Bitcoin had its share of vulnerabilities

https://www.cvedetails.com/vulnerability-list.php?vendor_id=12094&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec...

CVE Details
The ultimate security vulnerability datasource

Search | View CVE (e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Vulnerability Feeds & Widgets New www.itsecdb.com

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :

Bitcoin : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

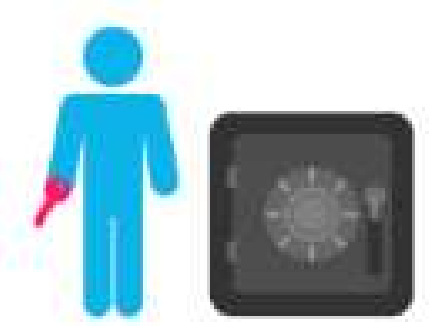
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-9230	338			2017-05-24	2018-06-13	5.0	None	Remote	Low	Not required	Partial	None	None
** DISPUTED ** The Bitcoin Proof-of-Work algorithm does not consider a certain attack methodology related to 80-byte block headers with a variety of initial 64-byte chunks followed by the same 16-byte chunk, multiple candidate root values ending with the same 4 bytes, and calculations involving sqrt numbers. This violates the security assumptions of (1) the choice of input, outside of the dedicated nonce area, fed into the Proof-of-Work function should not change its difficulty to evaluate and (2) every Proof-of-Work function execution should be independent. NOTE: a number of persons feel that this methodology is a benign mining optimization, not a vulnerability.													
2	CVE-2016-10725	310			2018-07-05	2018-08-27	5.0	None	Remote	Low	Not required	None	None	Partial
In Bitcoin Core before v0.13.0, a non-final alert is able to block the special "final alert" (which is supposed to override all other alerts) because operations occur in the wrong order. This behavior occurs in the remote network alert system (deprecated since Q1 2016). This affects other uses of the codebase, such as Bitcoin Knots before v0.13.0.knots20160814 and many altcoins.														
3	CVE-2016-10724	400		DoS	2018-07-05	2018-08-27	7.8	None	Remote	Low	Not required	None	None	Complete
Bitcoin Core before v0.13.0 allows denial of service (memory exhaustion) triggered by the remote network alert system (deprecated since Q1 2016) if an attacker can sign a message with a certain private key that had been known by unintended actors, because of an infinitely sized map. This affects other uses of the codebase, such as Bitcoin Knots before v0.13.0.knots20160814 and many altcoins.														
4	CVE-2013-5700	189		DoS	2013-09-10	2013-09-13	5.0	None	Remote	Low	Not required	None	None	Partial
The Bloom Filter implementation in bitcoind and Bitcoin-Qt 0.8.x before 0.8.4rc1 allows remote attackers to cause a denial of service (divide-by-zero error and daemon crash) via a crafted sequence of messages.														
5	CVE-2013-4627			DoS	2013-08-02	2013-10-11	5.0	None	Remote	Low	Not required	None	None	Partial
Unspecified vulnerability in bitcoind and Bitcoin-Qt 0.8.x allows remote attackers to cause a denial of service (memory consumption) via a large amount of tx message data.														
6	CVE-2013-4165	200		+Info	2013-08-02	2013-10-11	4.3	None	Remote	Medium	Not required	Partial	None	None
The HTTPAuthorized function in bitcoinrpc.cpp in bitcoind 0.8.1 provides information about authentication failure upon detecting the first incorrect byte of a password, which makes it easier for remote attackers to determine passwords via a timing side-channel attack.														
7	CVE-2013-3220	399		DoS	2013-08-02	2013-10-11	6.4	None	Remote	Low	Not required	None	Partial	Partial
bitcoind and Bitcoin-Qt before 0.4.9rc2, 0.5.x before 0.5.8rc2, 0.6.x before 0.6.5rc2, and 0.7.x before 0.7.3rc2, and wxBitcoin, do not properly consider whether a block's size could require an excessive number of database locks, which allows remote attackers to cause a denial of service (split) and enable certain double-spending capabilities via a large block that triggers incorrect Berkeley DB locking.														
8	CVE-2013-3219	264		Bypass	2013-08-02	2013-10-11	5.0	None	Remote	Low	Not required	None	Partial	None
bitcoind and Bitcoin-Qt 0.8.x before 0.8.1 do not enforce a certain block protocol rule, which allows remote attackers to bypass intended access restrictions and conduct double-spending attacks via a large block that triggers incorrect Berkeley DB locking in older product versions.														
9	CVE-2013-2293	399		DoS	2013-03-12	2013-03-18	5.0	None	Remote	Low	Not required	None	None	Partial

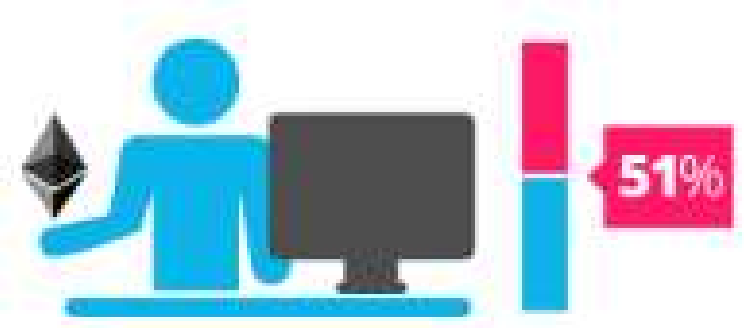
CSX 2018 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

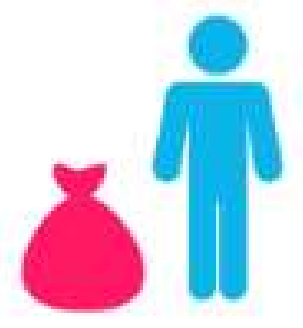
Ethereum and the Account/Balance model

- Ethereum designed to run “smart contracts”
  - users pay for running their code
  - uses a simplified system for transactions
- Less privacy than Bitcoin
- Exposed to Double Spending Attacks
- However, simpler and more efficient
- Hyperledger adopts UTXO
- Ethereum suffered a hack and fork in 2016

Ethereum and the Proof-of-Stake model







- The creator of the new block is chosen deterministically, depending on its “wealth” – also defined as Stake
- All digital currencies are already minted. In the PoS model there is no block reward, so the miner takes the transaction fee
- Currencies based on PoS are expected to be thousands of times more cost effective

Smart Contracts and Smart Assets

- Piece of business logic codified into programming language – “Dapp”
- Coupled with a blockchain transaction
- Participates to the verification of the transaction
  - Digitally facilitates, verify, or enforce negotiation or performance of a contract
  - The contract must be executed for the transaction to complete
  - Allows for parties to include provisions on how funds are released
  - Has usually a UX that emulate the logic of contractual clauses
- The idea is that many kinds of contractual clauses may be made partially or fully self-executing and/or self-enforcing
- Aim to be more secure than traditional contracts and reduce costs
- Smart Assets are digital properties

Other Consensus Mechanism

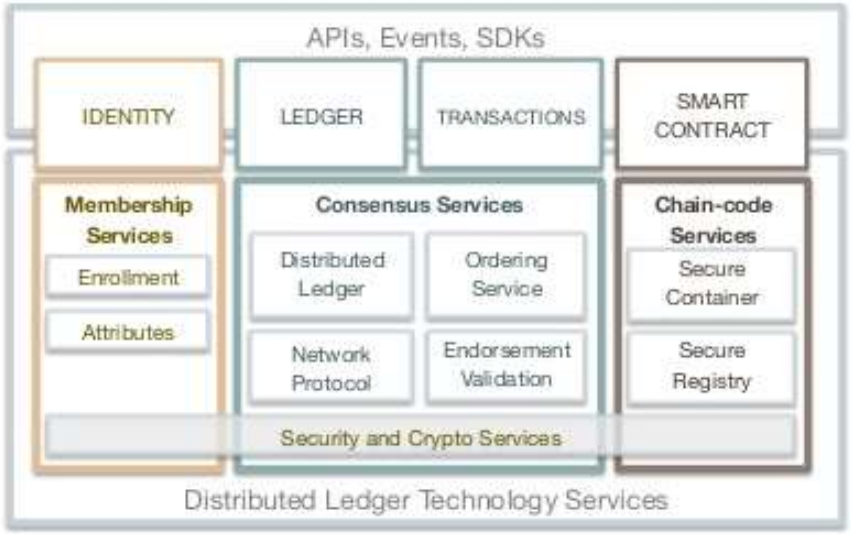
- Different uses of blockchains and different use cases require different consensus mechanisms
- Some want to address ASIC resistance, other resistance to centralization, other wants the proof to be delegated off-blockchain, others to address scalability and performance, etc.
  - Proof of Elapsed Time (PoET) = by Intel, used by Hyperledger Sawtooth
  - Delegated Proof of Stake (DPoS) = faster version of PoS using delegates
  - Proof of Burn (PoB) = burn some tokens to get the chance to vote
  - Proof of Authority (PoA) = validators stake their reputation in the network
  - Practical Byzantine fault-tolerant (PBFT) = low latency version of BFT
  - Byzantine Altruistic Rational (BAR) = assumes rational adversaries
  - several others….

Security Concerns of Smart Contracts/Assets

- They are software (often DevOps), and therefore contain flaws
  - bitcoin addresses it by reducing the capability of the language
  - Ethereum has several issues in the language – insecure constructs, ambiguity, compiler bugs, VM bugs, attacks on the network
  - Also, Ethereum has no clear vulnerability documentation
- Flaws in a blockchain have serious repercussions
  - fraudulent transaction are difficult to detect, and cannot be easily rolled back
  - “immutability of the blockchain” implies “immutability of the bugs”
- Expand current security assurance regime to include smart contracts and assets
- Accept the risk of asymptotic failure within organizational tolerance

Hyperledger

Reference Architecture



IDENTITY
Pluggable, Membership, Privacy and Auditability of transactions.

LEDGER | TRANSACTIONS
Distributed transactional ledger whose state is updated by consensus of stakeholders

SMART-CONTRACT
"Programmable Ledger", provide ability to run business logic against the blockchain (aka smart contract)

APIs, Events, SDKs
Multi-language native SDKs allow developers to write DLT apps

What is Hyperledger?

- An umbrella project of open source blockchains and related tools
- Built by the Linux Foundation on IBM/Intel blockchain projects
  - More than 100 members
- Deliberate choice of not having a coin/value token
- Composed of several platforms
  - Fabric: IBM's blockchain design and architecture
  - Sawtooth: Intel blockchain, implements Proof of Elapsed Time (PoeT)
  - Iroha: Soramitsu Iroha's blockchain, used by two Japanes companies
  - Burrow: smart contract machine along the specification of Ethereum
- Tooling is available
- Implemented in several PoCs where use cases are not monetary