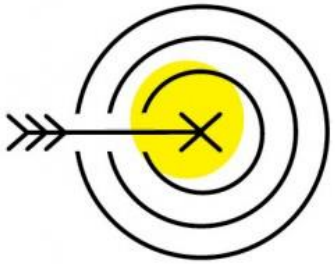
Healthcare Blockchain

Byoung-Kee Yi, PhD
Samsung Medical Center
Dept. of Digital Health, SAIHST, SKKU
HL7 Korea
ISO/TC215 Health informatics
ISO/TC307 Blockchain and distributed ledger technologies
IEC/SyC Active Assisted Living

Top 10 Strategic Technology Trends for 2018



Intelligent

AI Foundations

Intelligent Apps and Analytics

Intelligent Things

Digital

Digital Twins

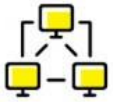
Cloud to the Edge

Conversational Platform

Immersive Experience

Mesh

Blockchain



Event-Driven

Continuous Adaptive Risk and Trust

gartner.com/SmarterWithGartner

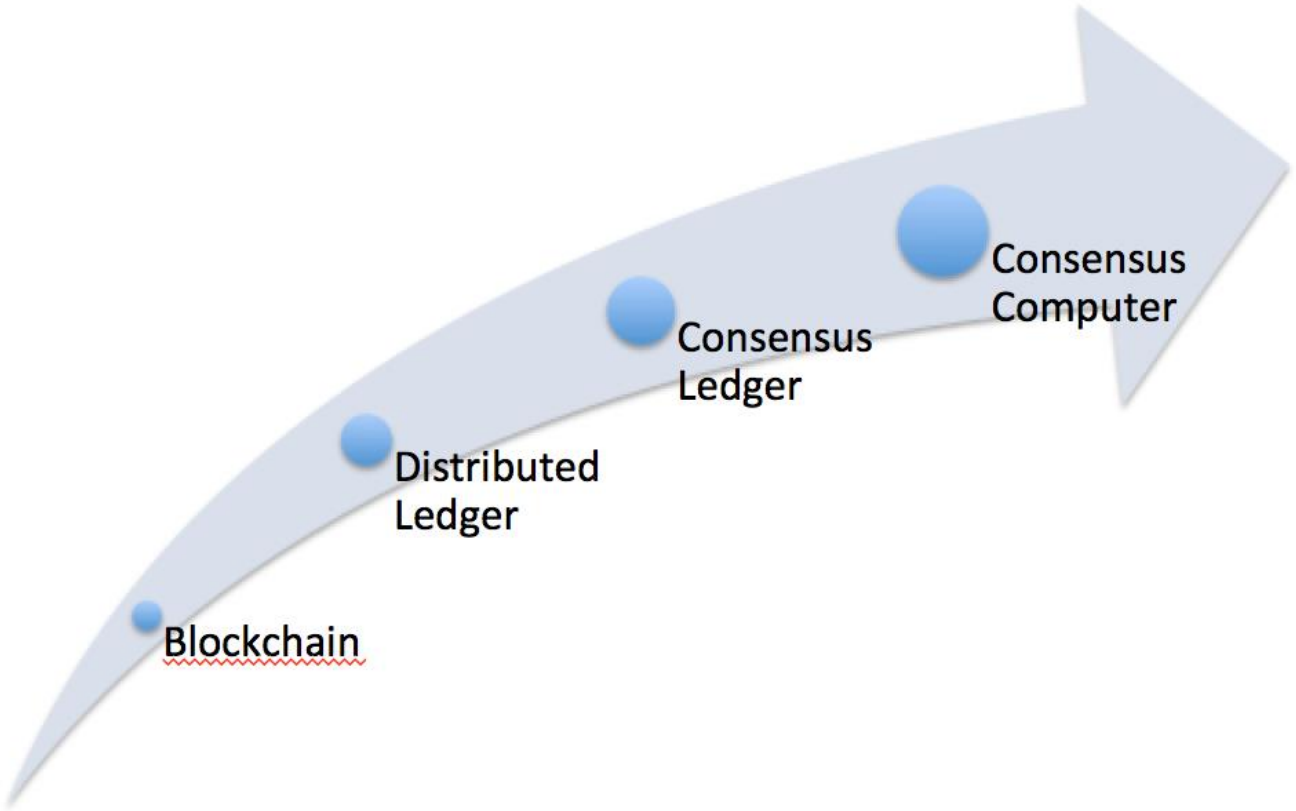
Source: Gartner

Gartner

Blockchain

- Distributed ledger technology originally developed for digital money or cryptocurrency
  - E.g. Bitcoin, Ethereum, etc.
- "Ledger" definition by *Oxford Learner's Dictionaries*
  - a book in which a bank, a business, etc. records the money it has paid and received
- Confusion of terms
  - Blockchain, distributed ledger, ...

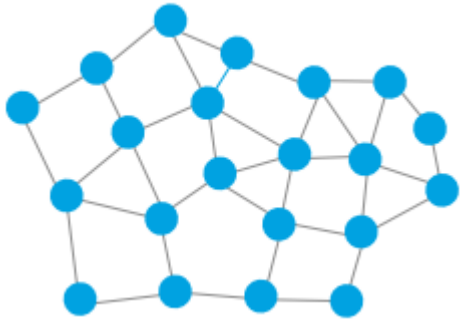
Taxonomy of terms*



*From http://finiculture.com/taxonomy-is-important-consensus-computer-is-the-end-game/

Centralized v. distributed ledger

- Centralized ledger
  - A single copy of ledger kept at one place
  - Eg) Conventional bank ledger
- Distributed ledger
  - A single copy or multiple copies of ledger kept at multiple places
  - Eg) P2P network
- We only focus on distributed ledgers
  - A "ledger" implicitly means a "distributed ledger" hereafter



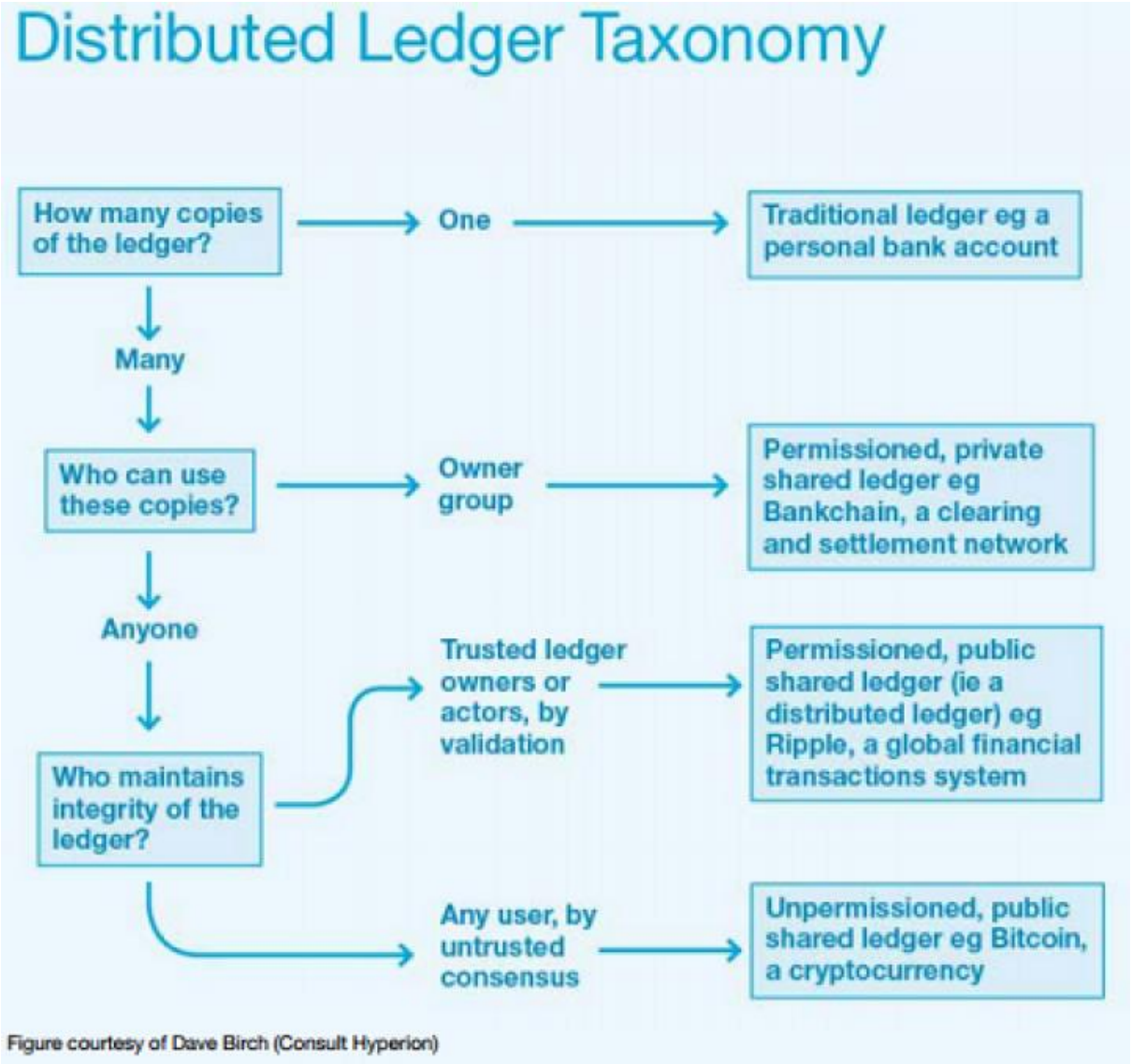
Private v. public ledger

- Depends on who can use the leger
- Private ledger
  - Only a small group of owners
- Public ledger
  - Anyone

Permissioned v. permissionless

- Depends on who maintains the integrity of the ledger
  - Or who can update the ledger
- Permissioned ledger
  - Only trusted ledger owner(s)
- Permissionless ledger
  - Anyone

In summary…


Distributed Ledger Taxonomy
How many copies of the ledger?
One
Traditional ledger eg a personal bank account
Many
Who can use these copies?
Owner group
Permissioned, private shared ledger eg Bankchain, a clearing and settlement network
Anyone
Who maintains integrity of the ledger?
Trusted ledger owners or actors, by validation
Permissioned, public shared ledger (ie a distributed ledger) eg Ripple, a global financial transactions system
Any user, by untrusted consensus
Unpermissioned, public shared ledger eg Bitcoin, a cryptocurrency
Figure courtesy of Dave Birch (Consult Hyperion)

How to maintain integrity of a ledger?

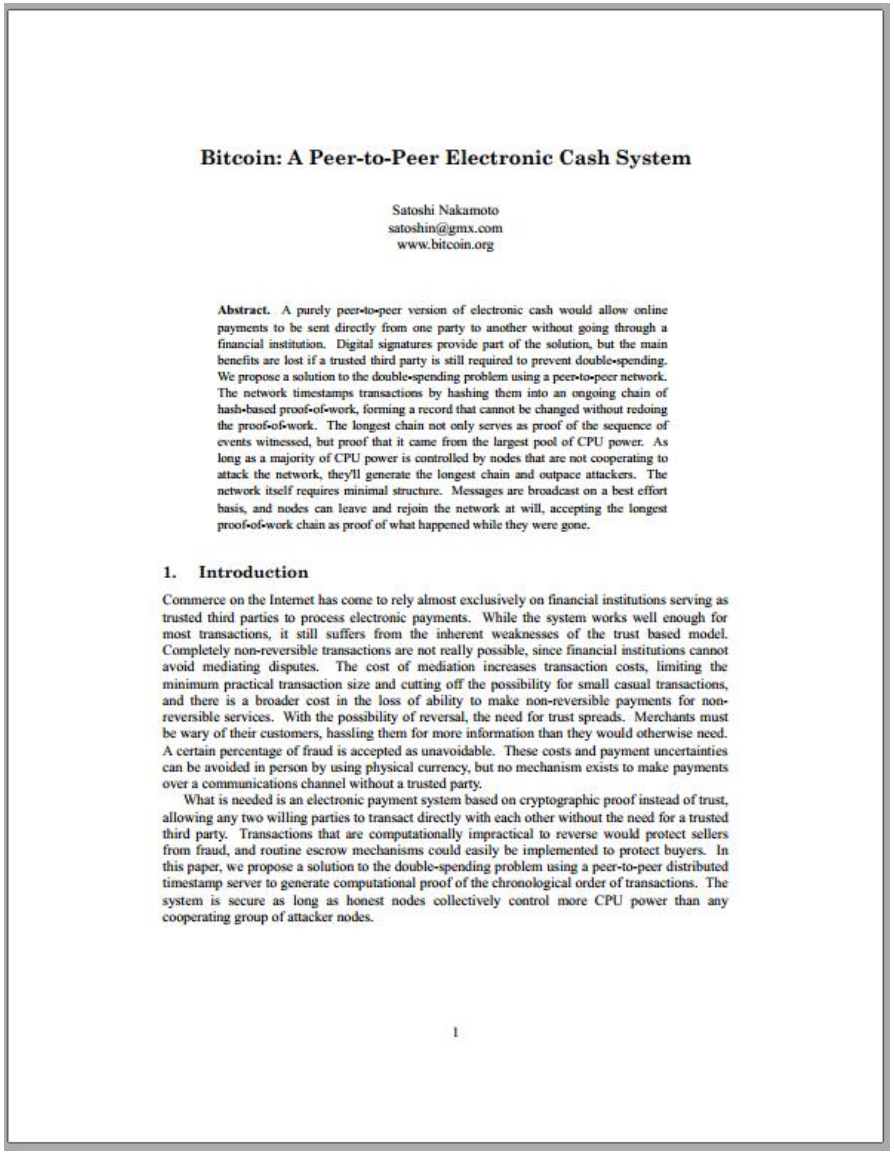
- Alternatively, how to provide "trust"?
- Conventionally, by a trusted entity (intermediary)
  - Governments (or central bank) for currency
  - Banks for transactions
  - Usually regulated by laws
- But what about distributed ledgers?
  - Easier for private ledgers
  - Rather easy for permissioned public ledgers
  - Not so easy for permissionless public ledgers where you cannot trust anyone

Byzantine Generals Problem

- Each division of Byzantine army are directed its own general
- Generals, some of which are traitors, communicate each other by messengers
- Requirements:
  - All loyal generals decide upon the same plan of action
  - A small number of traitors cannot cause the loyal generals to adopt a bad plan

Genesis: Bitcoin & Blockchain

- In October 2008, Satoshi Nakamoto proposed a combined digital asset and P2P payments system in his paper, "Bitcoin: A Peer-to-Peer Electronic Cash System"
- The first Bitcoin was minted on January 4th 2009
- The first payment occurred on January 11th
- And the software was released as open source on the 15th
- For a long time, there was little interest in Bitcoin.
- Then, roughly a third of the way through 2012, the transaction volume started to grow exponentially.
- In early 2013, Bitcoin's market capitalization started to follow the same path.



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

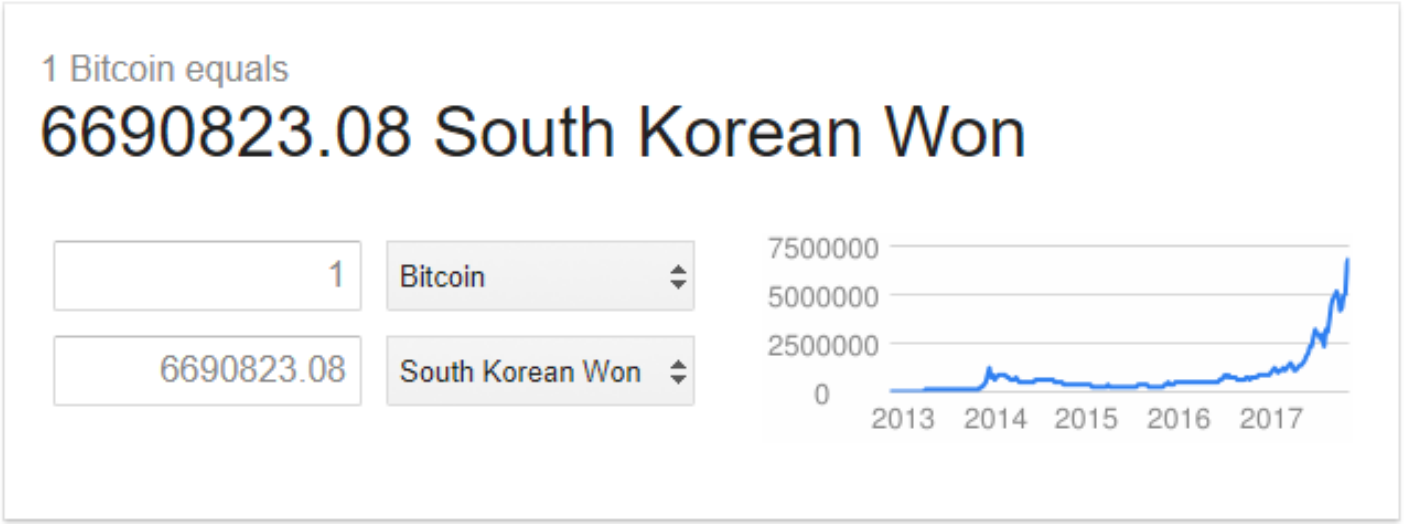
Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

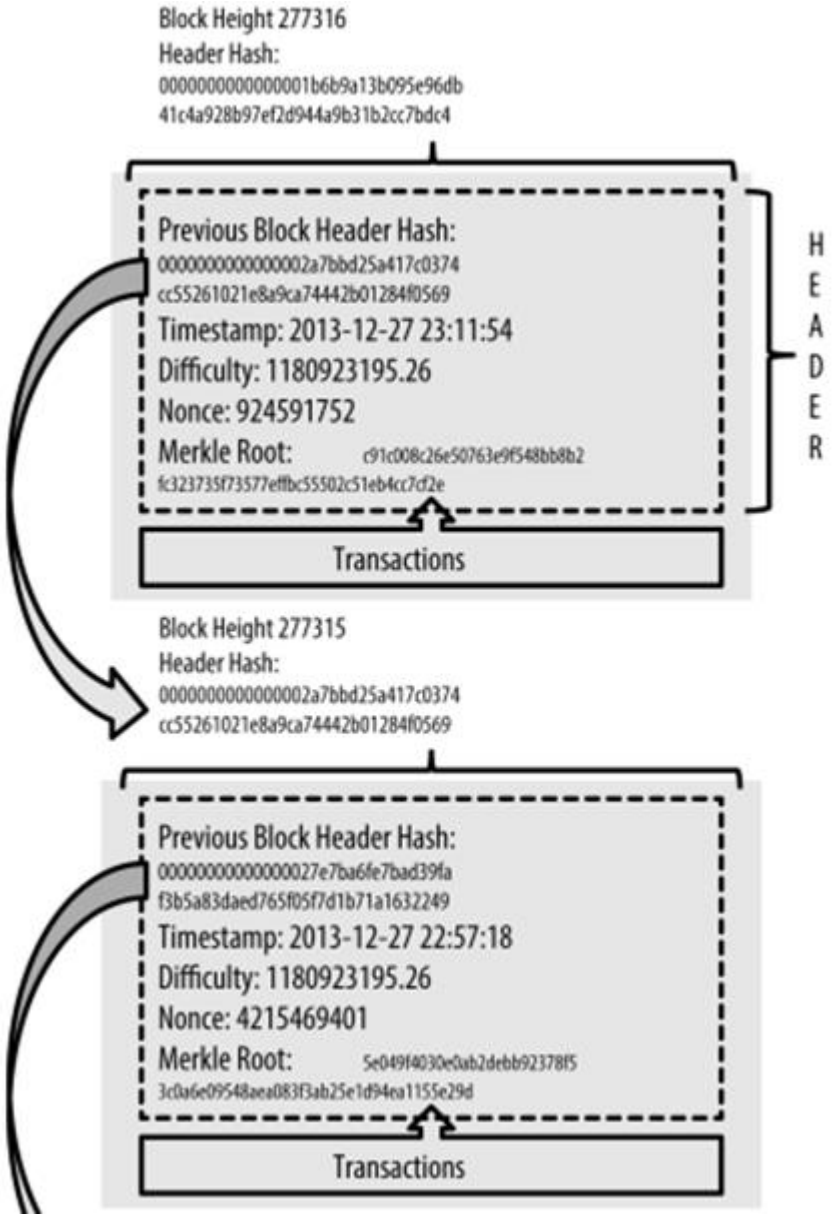
1

And Today...

- As of 1:05am, October 27, 2017 KST

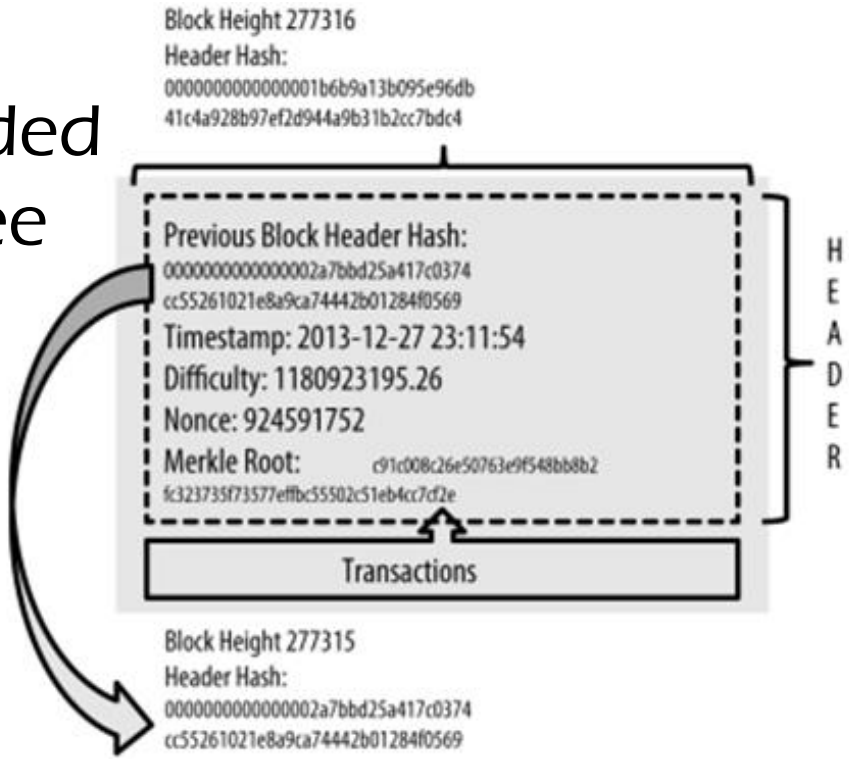


Blockchain = Chain of (Hashed) Blocks



Mining as Proof of Work (PoW)

- PoW is a type of consensus algorithm
- Mining is a process to solve a cryptographic quiz
  - Hash(prevblock+nounce) = 00...0(other_bits)
  - The number of leading zeros determine difficulty
- A winning miner is rewarded with coins + transaction fee
- Easy to test its validity
- The longer the chain, the harder to alter it (exponentially)



Other consensus algorithms

- PoW requires a lot of computations (really!)
  - ASICs for mining

- Instead, some algorithms are based on randomized block selection
- Proof of Stake (PoS)
  - Hash(prev+addr+timestmp) <= 2^256*balance/diff

Other consensus algorithms (cont.)

- Proof of Elapsed Time (PoET)
  - Each validator requests a waiting time
  - The validator with the shortest waiting time for a block wins
- Proof of Authority (PoA)
  - Consensus is achieved by referring to a list of validators
  - No actual mining is performed
  - Adopted by Hyperledger and Ripple

Ethereum

- Ethereum is another public DLT with scripting functionality called "Smart Contracts"
  - "Smart Contracts" were originally proposed by Nick Szabo in 1996
- Adopts an ASIC-resistant PoW consensus algorithm called Ethash

Smart Contracts

- Computing via Ethereum Virtual Machine (EVM)
  - Cf. JVM
  - Turing complete
- Useful for automating contracts
  - Hence "Smart contracts"
  - Eg) House or car rentals
- Issues
  - Performance
  - Vulnerability

Hyperledger

- Open source project for blockchains and tools
  - Initiated by Linux foundation
- Participants include big names
  - IBM, Intel, Cisco, and so on...
- Platforms
  - Hyperledger Burrows
  - Hyperledger Fabric
  - Hyperledger Iroha
  - Hyperledger Sawtooth (← PoET)

Desirable characteristics

- Distributed Database
  - Each party has access to the entire database and its complete history.
  - No single party controls the data or the information.
- Peer-to-Peer Transmission
  - Communication occurs directly between peers instead of through a central node.
  - Each node stores and forwards information to all other nodes.
- Transparency with Pseudonymity
  - Every transaction and its associated value are visible to anyone with access.
  - Each node, or user, on a blockchain has a unique 30-plus-character alphanumeric address that identifies it.
  - Users can choose to remain anonymous or provide proof of their identity to others.
  - Transactions occur between blockchain addresses.

Desirable characteristics (cont.)

- Irreversibility of Records
  - Once a transaction is entered in the database and the accounts are updated, the records cannot be altered
  - Various computational algorithms and approaches are deployed to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network.
- Computational Logic (a.k.a. Smart contracts)
  - The digital nature of the ledger means that blockchain transactions can be tied to computational logic and in essence programmed.
  - So users can set up algorithms and rules that automatically trigger transactions between nodes.
  - Today humans manually attempt to reconcile medical data among clinics, hospitals, labs, pharmacies, and insurance companies.

Why Blockchain in Healthcare?

- Blockchain addresses many issues in healthcare informatics
  - Interoperability*, accessibility, and data integrity
  - Privacy and security
  - Healthcare delivery models and cost
  - Fraud and abuse
  - Process and complexity
  - Consumer engagement
  - Procurement and contracting
  - Governance and compliance

* DISCLAIMER: Personally, the presenter does not agree on this.

Healthcare Challeges & Blockchain Opportunities

	HIE pain points	Blockchain opportunities
	**Establishing a trust network** depends on the HIE as an intermediary to establish point-to-point sharing and "book-keeping" of what data was exchanged.	**Disintermediation of trust** likely would not require an HIE operator because all participants would have access to the distributed ledger to maintain a secure exchange without complex brokered trust.
	**Cost per transaction**, given low transaction volumes, reduces the business case for central systems or new edge networks for participating groups.	**Reduced transaction costs** due to disintermediation, as well as near-real time processing, would make the system more efficient.
	**Master Patient Index** (MPI) challenges arise from the need to synchronize multiple patient identifiers between systems while securing patient privacy.	**Distributed framework for patient digital identities**, which uses private and public identifiers secured through cryptography, creates a singular, more secure method of protecting patient identity.
	**Varying data standards** reduce interoperability because records are not compatible between systems.	**Shared data** enables near real-time updates across the network to all parties.
	**Limited access to population health data**, as HIE is one of the few sources of integrated records.	**Distributed, secure access** to patient longitudinal health data across the distributed ledger.
	**Inconsistent rules and permissions** inhibit the right health organization from accessing the right patient data at the right time.	**Smart contracts** create a consistent, rule-based method for accessing patient data that can be permissioned to selected health organizations.

*Deloitte Whitepaper, "Blockchain: Opportunities for Health Care"

6 BIG THEMES FOR BLOCKCHAIN TECHNOLOGY IN HEALTHCARE

Health Data Interoperability

Provide ubiquitous security infrastructure for seamless health data exchange without reconciliation or trusted 3rd party.

Value-based Care

Trusted workflows with 'single source of truth' provide radical new possibilities for outcome-based care delivery and reimbursement models.

Healthcare Business Models

Transform the digital health economy to create new business and monetization models for health data/asset exchange.

Healthcare Consumerism

Ensure co-creation of trust and self-sovereignty for patient-centric blockchain health ecosystem.

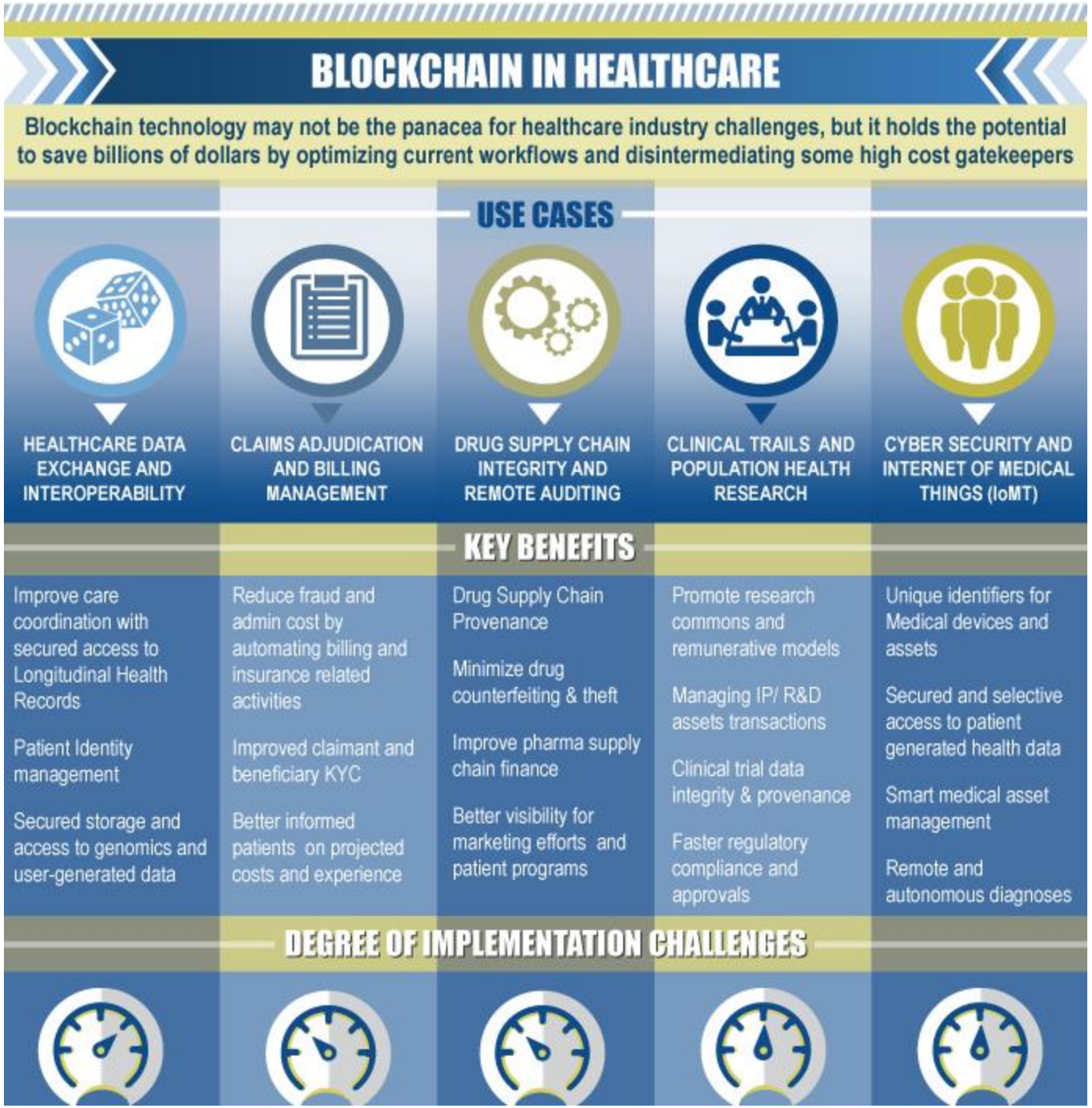
Cybersecurity

Distributed network consensus with cryptography techniques provides additional layer of trust to minimize cybersecurity threats for healthcare IT systems.

Precision Medicine Practice

Allow patients to permit access to their anonymized personal health information for research commons and remunerative models .

Source: Frost & Sullivan



Source: Frost & Sullivan

Healthcare use cases

- Notarization / Identity Verification
  - Registration of EMR, insurance, and other healthcare records
- Collaborative Crowdsourcing
  - Open bazaar for services, transparency in pricing, and health property exchange
- Medical Banking
  - Disintermediating counterparties
- Counterfeit Drug Prevention and Detection
  - Introduce blockchain-enabled solutions to protect and enhance the pharmaceutical supply chain
- Genomics Research
  - Accessibility to genetic data secured on blockchain

*IBM, "Blockchain: The Chain of Trust and its Potential to Transform Healthcare – Our Point of View"

Healthcare use cases (cont.)

- Population Health Management
  - A blockchain-based personal health record (PHR) system measuring consumer outcomes and influencing medical actions (for example, cases of influenza and preventative vaccines)
- Internet of Things and Blockchain
  - Consumer-generated health data meets IoT wearables through data accessibility and interconnection with health records
- Validation and Payment of Claims
  - Reduce process time and friction, including compliance with contract terms
- Outcome-Based Payments
  - Assigns each consumer a unique digital identity with data from blockchain (payers measure metrics for positive outcomes)

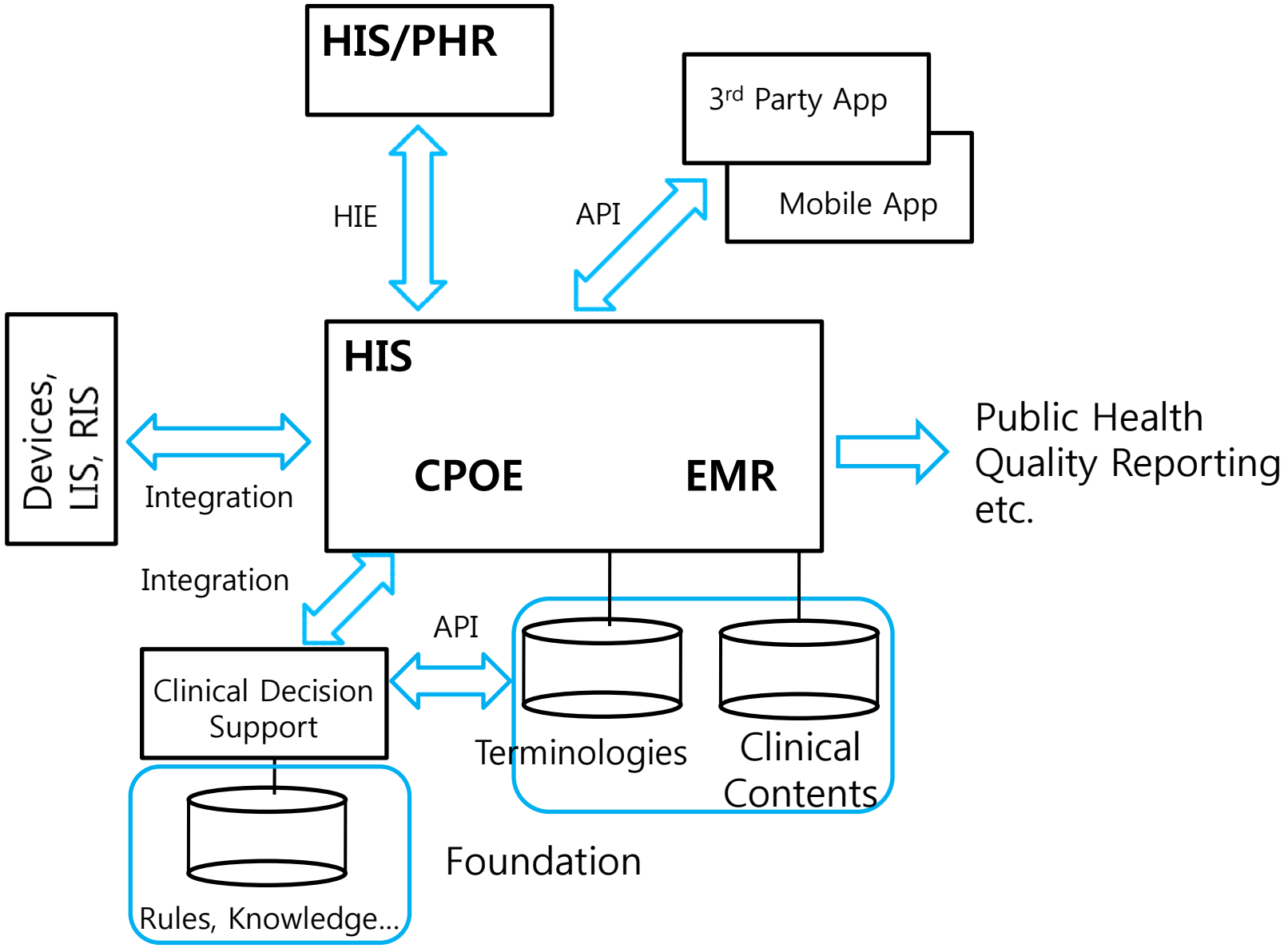
*IBM, "Blockchain: The Chain of Trust and its Potential to Transform Healthcare – Our Point of View"

Healthcare use cases (cont.)

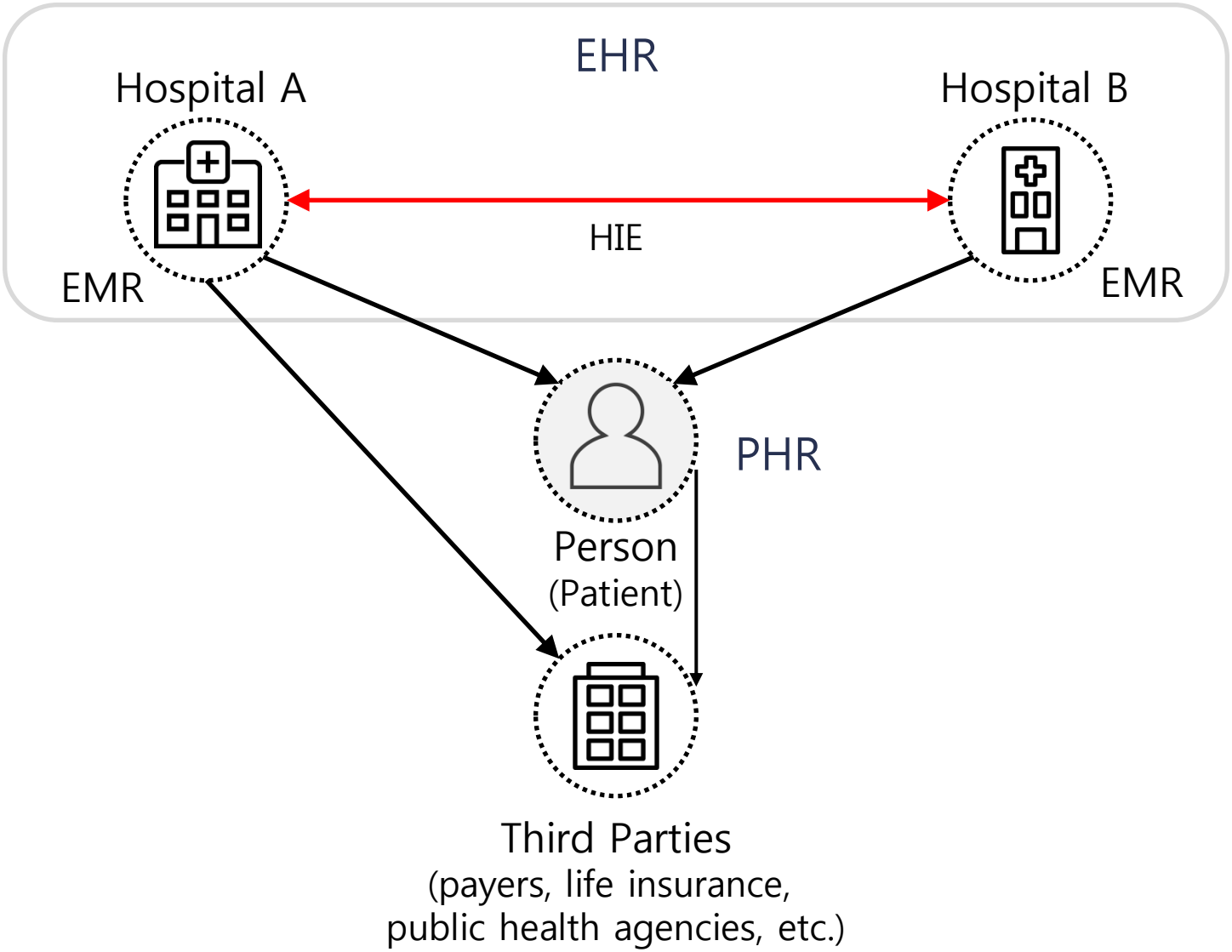
- Clinical Trial Results
  - Improve accountability and transparency in the clinical trial reporting process
- EMR
  - Personal health record storage and access administered using blockchain, with user-key permission for doctors and other authorized parties
- Health Research Commons
  - Aggregated personal medical records, quantified self data commons (DNA bits), genome and connectome files[27]
- Health Document Notary Services
  - Proof-of-insurance, test results, prescriptions, status, condition, treatment, physician referrals
- Doctor-Vendor RFP Services
  - Similar to Uber car services, doctors and health practices bid to supply medical services, possibly using automated bidding over tradenets

*IBM, "Blockchain: The Chain of Trust and its Potential to Transform Healthcare – Our Point of View"

Health IT Interoperability Contexts



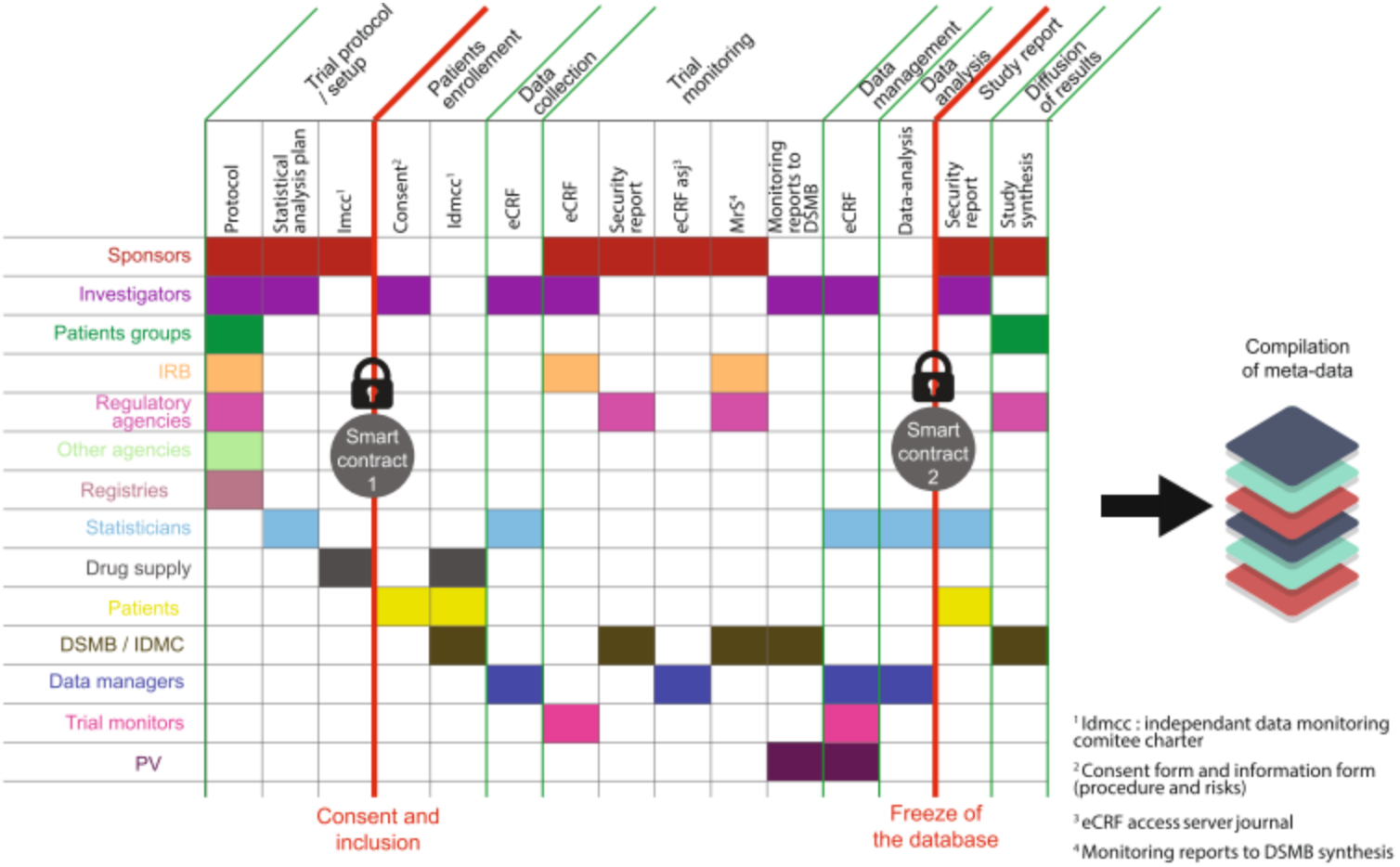
EMR, EHR, PHR & HIE



My pick of promising use cases

- Clinical research
- Health document authentication
- Drug supply chain
- Health insurance claim

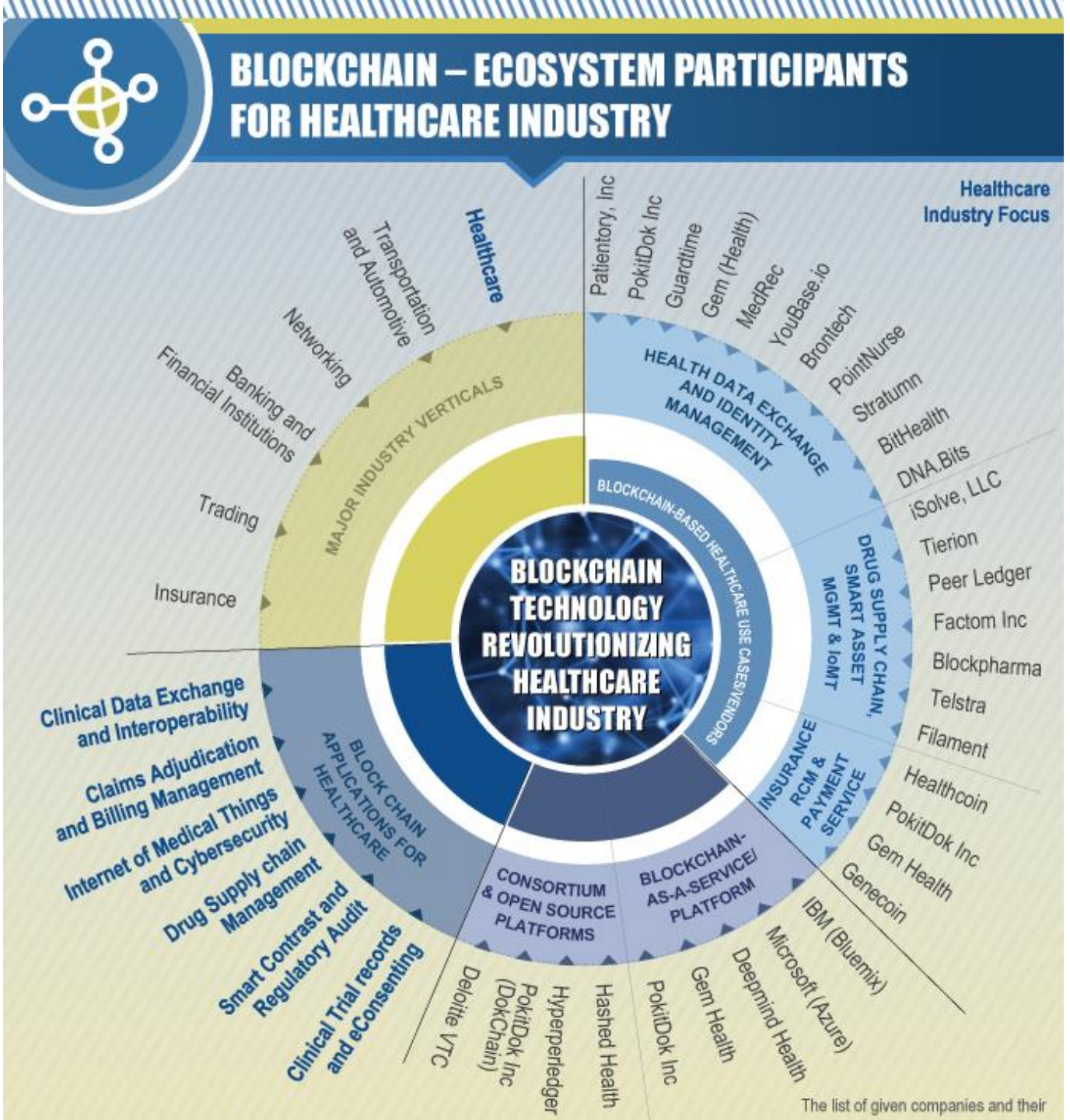
Clinical Research



Source: Benchoufi and Ravaud, Trials (2017) 18:335

Health Document Authentication

- AS IS: 공인전자문서센터
  - 과거에 공인전자문서등록소
  - “전자문서 및 전자거래 기본법”에 근거
- TO BE: Blockchain 기반 전자문서 인증



Source: Frost & Sullivan

Potential Issues

- Transaction volumes v. computing power
- Data standardization and scope
- Adoption and incentives for participation
- Operation costs
- Regulatory considerations

What's next?

- In Healthcare Blockchain Summit, Washington DC, March 21, 2017,

KEYNOTE ADDRESS: BLOCKCHAIN IN HEALTHCARE: WHY SO MUCH HYPE AND SO LITTLE IMPLEMENTATION?

Blockchain represents a solution set with several key integrated capabilities. Numerous effective applications exist in the financial sector. Many startups are building healthcare solutions with blockchain components, but none have reached widespread adoption. Because of the integrated set of services provided by a blockchain platform, many

Q & A

-

감사합니다.