

Blockchain

A technical primer with a case discussion of **MedRec**

Dennis Porto MD, MPH, FAAD

For use in the MBA curriculum at Harvard Business School: Frontier Technologies with Prof Rajiv Lal



H A R V A R D | B U S I N E S S | S C H O O L

Problem: healthcare data silos

United States: patient health data is owned by hospitals and clinics that don't communicate with each other

Results in patient morbidity and waste when important health data is not available to a patient's physician during a clinical decision

- Examples:
 - A patient is administered a medication they are allergic to, which was documented in an outside, siloed medical record
 - A patient with a positive pregnancy test at a siloed lab is prescribed a medication not safe in pregnancy
 - An obtunded patient in the ICU deteriorates as the patient's physician tries to pull together their outside records





Is blockchain
a solution?

Blockchain: a primer

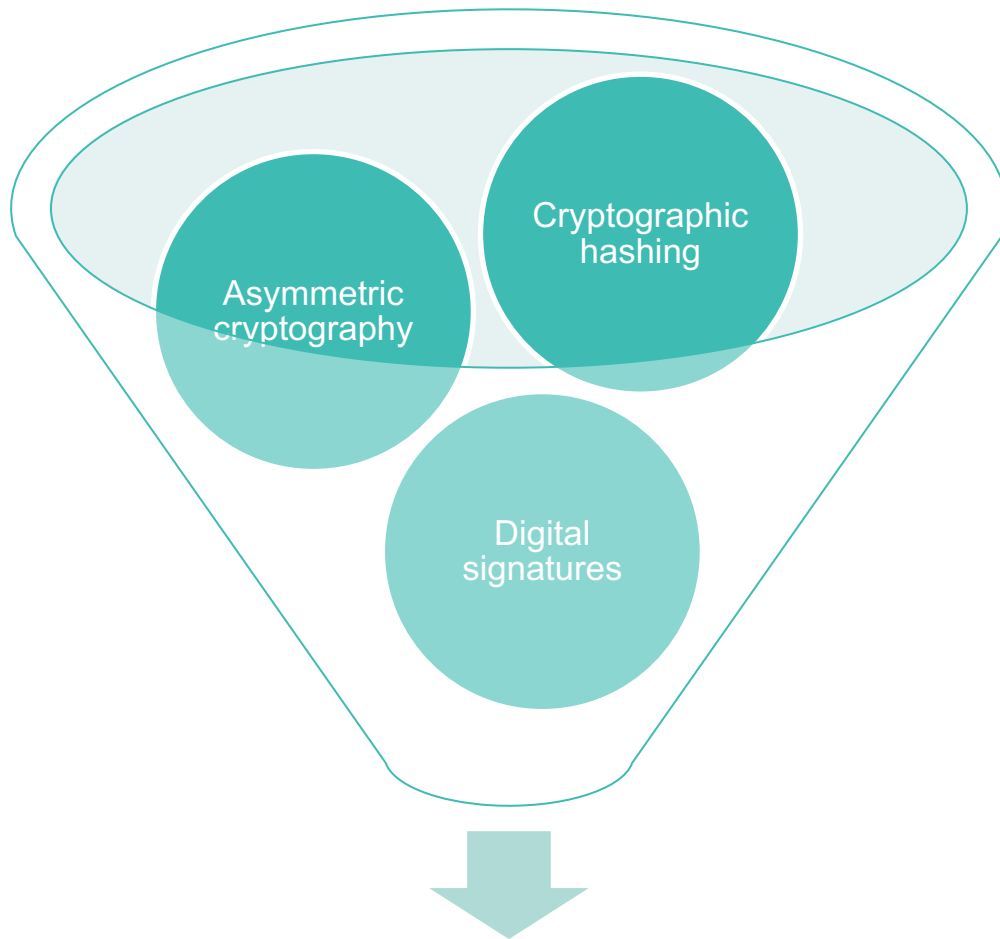
Broadly: a decentralized append-only ledger of “transactions” which can represent any kind of data. What is included in the ledger is determined by one of various consensus mechanisms.

Key features:

- Trust minimized: blockchains distribute trust among multiple nodes, negating the need for a trusted third party (approaching “trustlessness”)
- Tamper resistant: past transactions cannot be lost, modified, or corrupted (approaching “immutability”). Sometimes called “censorship resistance”
- Consensus-guided: blockchains have different mechanisms to arrive at consensus whereby they create a shared ledger



Bitcoin: a convergence of enabling technology



Bitcoin

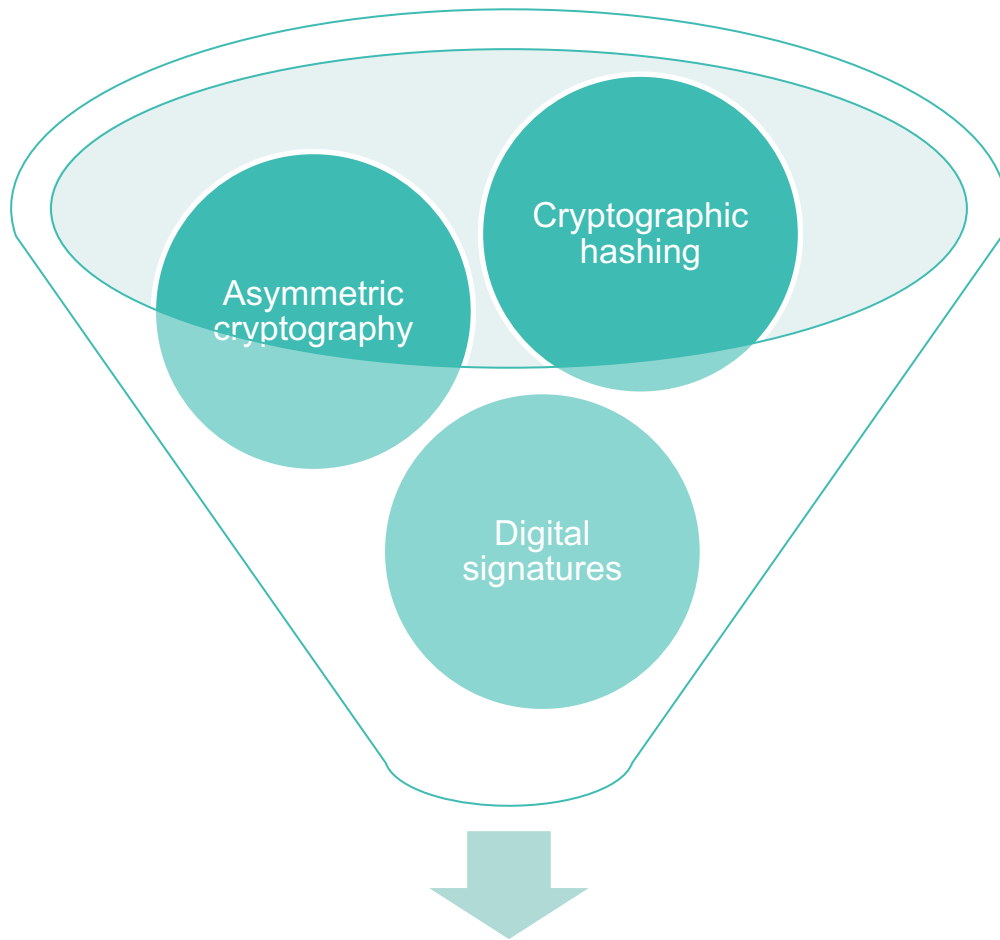
- Cryptographic Hashing
 - Take any data of any size or type as an input
 - Apply a cryptographic hash function
 - Achieve a consistent and unique output at fixed size
 - Even small changes in the input results in a completely different output
 - Hashing is unidirectional: cannot recreate inputs from the output
 - Collision resistance: ideally no two inputs result in the same output (ie, outputs are “unique”)
 - Hashing used frequently in bitcoin: public/private key pairs, linking blocks together, the proof of work puzzle

Table 1: Examples of Input Text and Corresponding SHA-256 Digest Values

Input Text	SHA-256 Digest Value
1	0x6b86b273ff34fcea19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	0xd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
Hello, World!	0xdfdf6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

Yaga D et al (2018) “Blockchain Technology Overview.” National Institute of Standards and Technology. US Dept of Commerce





Bitcoin: a convergence of enabling technology



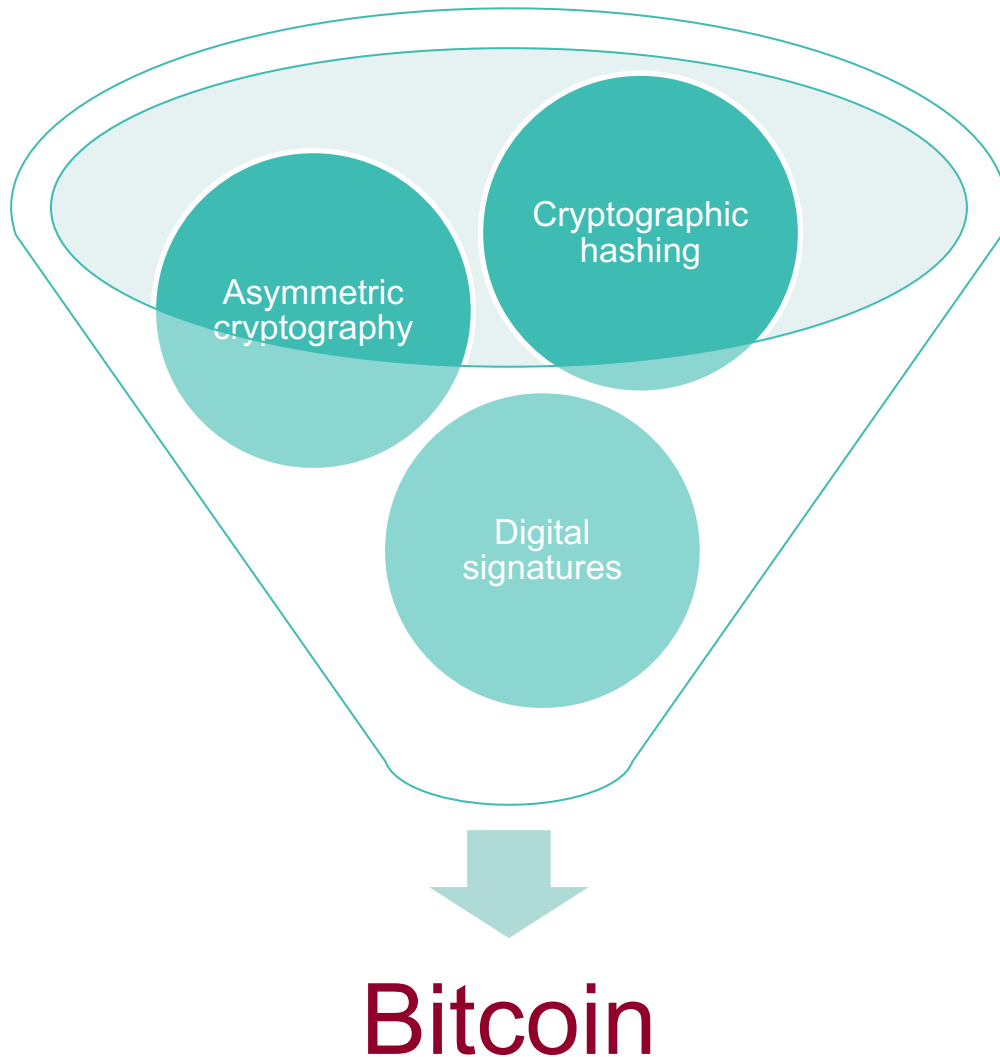
Bitcoin

Yaga D et al (2018) "Blockchain Technology Overview." National Institute of Standards and Technology. US Dept of Commerce

- Asymmetric cryptography & Digital signatures
 - Users have a **public address** and **private key**
 - The key and address are mathematically related and unidirectional
 - The user keeps the private key secret. Knowledge of the private key is what proves ownership of the public address
 - The public address is used to receive bitcoin
 - The private key is used to “sign” transactions to send bitcoin, proving ownership of the bitcoin sent
 - Essentially infinite public/private key pairs can be freely created, allowing anyone to participate in bitcoin and enables “pseudonymity”

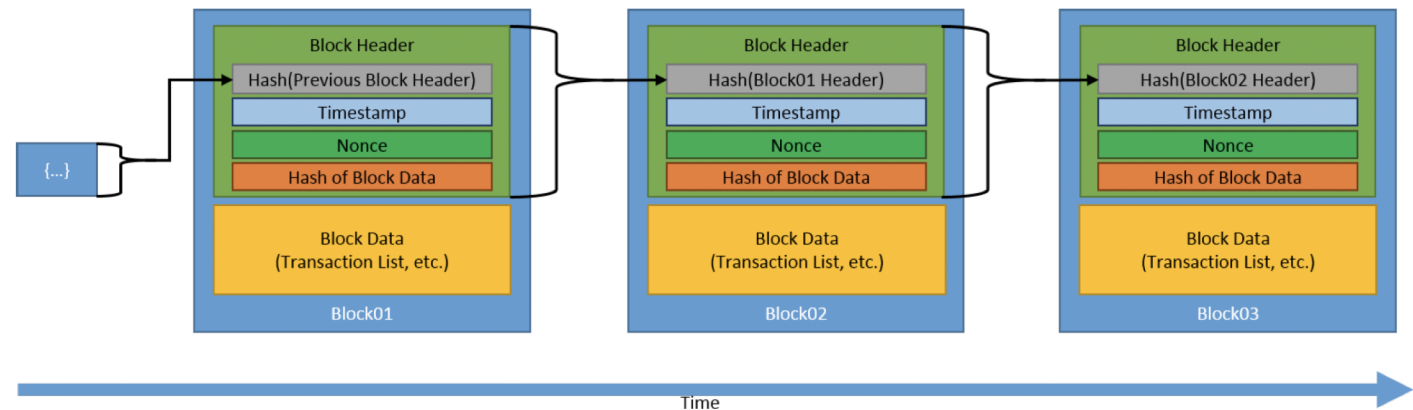
Bitcoin Address	Private Key (Wallet Import Format)
	
<p>Public Key</p> 	<p>Private key</p> 
1M3RLrXve5wcT2ZcJu8WxoXjdh4WXcWQA9	5K8BwE76VsAtQiRa5wJpGng7758FAz4vLkMxAry8Qny2TdQJxPn

Bitcoin: a convergence of enabling technology



The blocks

- Users use software called a “wallet” to submit transactions to the network
- Transactions organized into blocks by miners for a reward
- Each block is cryptographically linked to the previous block with a hash
- Each new block added makes it harder to tamper with prior blocks
- Block contents:
 - Header: contains metadata
 - Hash: links blocks together
 - Timestamp
 - Nonce: used in proof of work
 - Block data: the ledger of transactions, etc



Yaga D et al (2018) “Blockchain Technology Overview.” National Institute of Standards and Technology. US Dept of Commerce

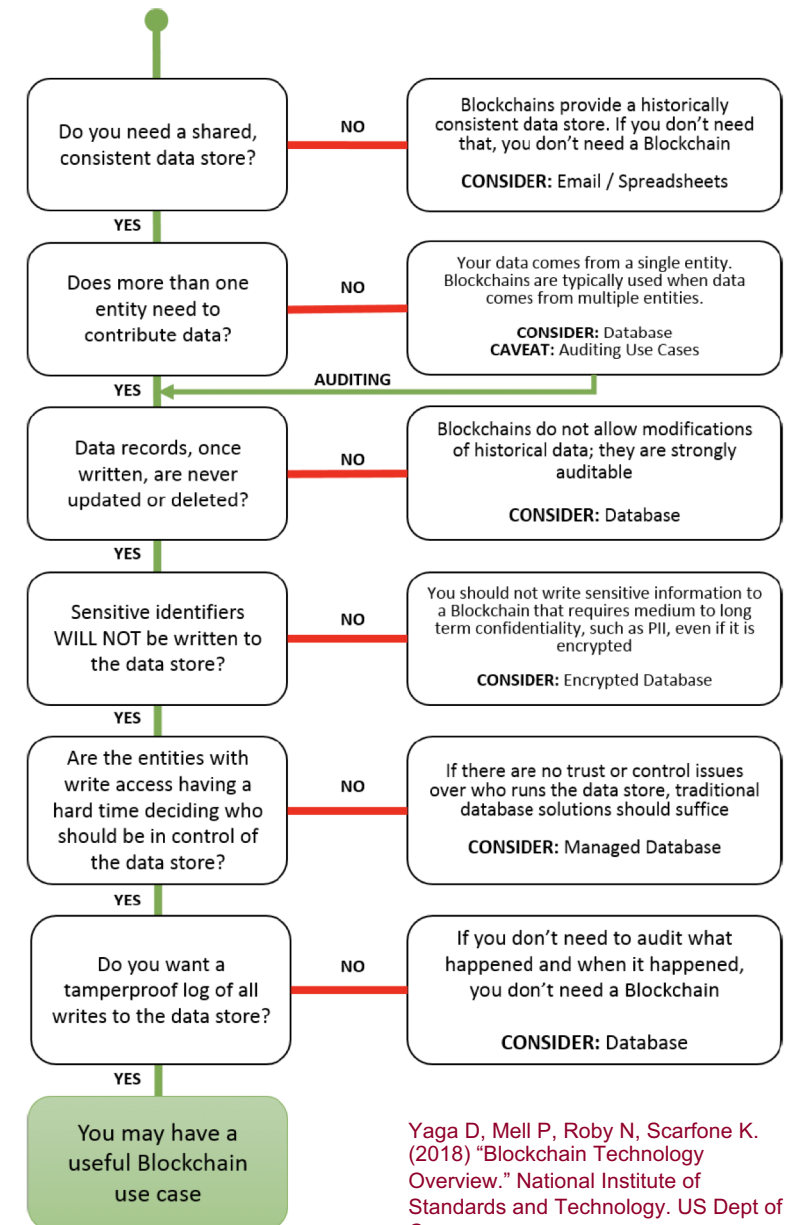
Blockchain: what is it good for?

Blockchain may be useful when the following criteria are met:

- ✓ There are multiple stakeholders who wish to interact with a shared ledger
- ✓ These stakeholders may not trust each other
- ✓ The traditional intermediary is inefficient

Example: Bitcoin mediates financial transactions between parties who do not know each other, without the cost and inefficiency of traditional banks and without any requirement of trust.

Example: Maersk created the TradeLens enterprise blockchain with IBM so that all stakeholders (even competitors and customs officials) in a shipping supply chain can transparently coordinate.



Yaga D, Mell P, Roby N, Scarfone K. (2018) "Blockchain Technology Overview." National Institute of Standards and Technology. US Dept of Commerce

Healthcare example: supply chains



Al Jazeera America

Healthcare example: global health



Huffington Post

Healthcare example: provider credentialing



Healthcare example: genomics

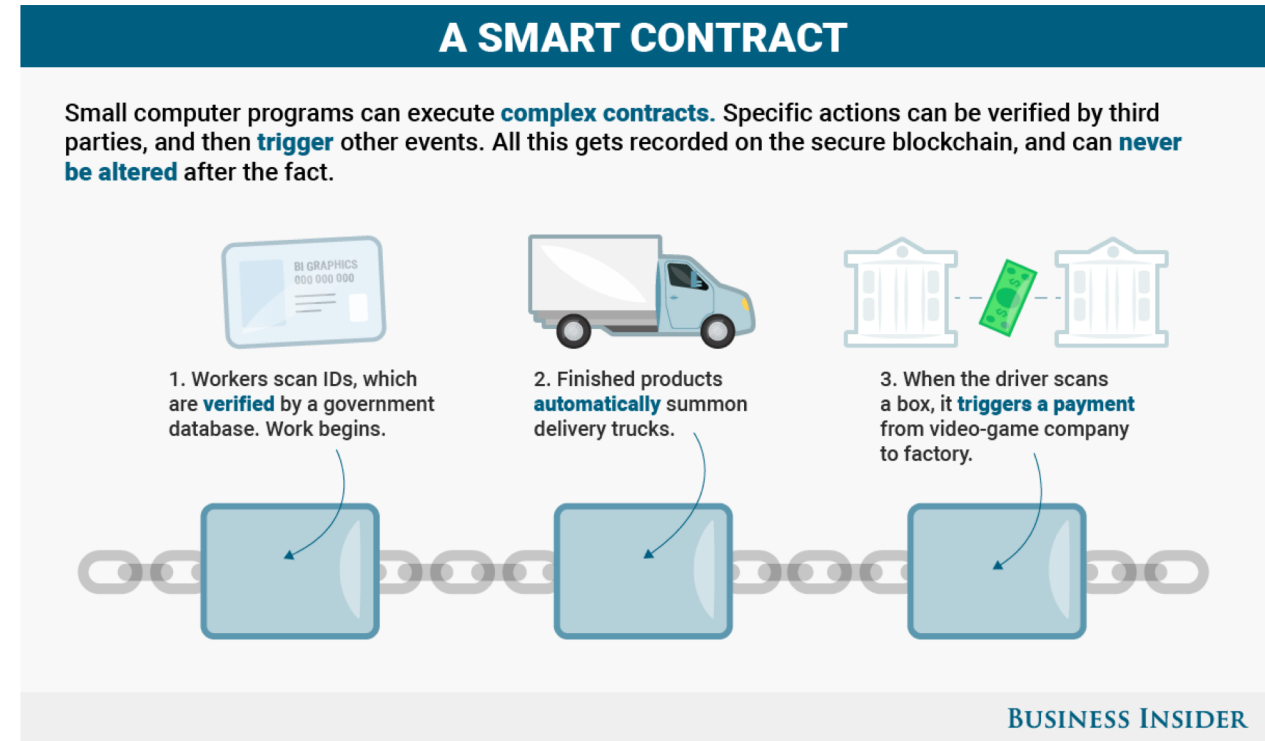


Choosing a blockchain: key considerations

- Smart contract capability
- Public vs private
- Consensus mechanism

Smart Contracts

- Bitcoin enabled the digitization of value and transactions using a blockchain
 - Example: Bob sends 1 bitcoin to Alice
- Ethereum enabled more complex transactions
 - Software deployed on and executed by computers running Ethereum nodes
 - Examples:
 - Prediction markets like Augur
 - Games like “Cryptokitties”
 - ICOs as an IPO-like security offering
- There are now many smart contracts platforms, and Bitcoin is also developing smart contracts



Public vs Private blockchains

- **Public or “Permissionless” blockchains**
 - Anyone can participate in any role (miner, user, node, etc)
 - Potential privacy challenges as the blockchain is visible
 - Resource-intensive consensus mechanisms (eg, Proof of Work or Stake) must be used to thwart malicious users leading to relatively poorer performance
 - Gold standard trust minimization and censorship resistance
 - Apps tend to be B2C
 - Examples: Bitcoin, Ethereum, Litecoin, Monero, EOS
- **Private or “Permissioned” blockchains**
 - Only selected individuals can run a node, publish blocks, send transactions, and/or read the blockchain
 - Similar to a consortium with algorithmatized consensus
 - As participants are “pre-approved,” can forgo resource intensive consensus mechanisms, leading to better performance
 - Require some degree of trust of the blockchain participants
 - Potential for enhanced privacy
 - Apps tend to be B2B
 - Examples: Hyperledger Fabric (IBM), JPMorgan Quorum, Microsoft Azure, Parity Ethereum



Blockchain: consensus mechanisms

Public blockchains:

- **Proof of Work:** miners must complete an intensive computational process in order to append a block to a ledger and receive an award. Miners compete to be the first to “solve” this computational puzzle. In the event of a dispute between two or more chains, the chain with the most accumulated “work” prevails
 - Strengths: most time tested and robust, anyone can participate
 - Weaknesses: energy intensive, susceptible to centralization in data centers
 - Example cryptocurrency: Bitcoin, Ethereum
- **Proof of Stake:** validators (rather than miners) are selected at random based on the number of tokens they hold to append the next block and receive a transaction fee. Those with more tokens are more likely to be selected.
 - Strengths: resource-friendly as mining is not required, anyone can participate
 - Weaknesses: **still in development**, wealth concentration, susceptible to collusion
 - Example cryptocurrency: EOS, Cardano, Ethereum Casper (in development)

Private blockchains:

- **Proof of Authority:** a centralized consensus algorithm whereby individuals reveal their identity and in exchange are allowed to append a block to the blockchain.
 - Strengths: resource friendly, improved performance
 - Weaknesses: requires manual validation of identity, identity is validated by a centralized “authority node”
 - Example blockchains: Microsoft Azure, Parity Ethereum
- **Voting-based consensus:** trusted nodes vote to confirm proposed transactions and blocks.
 - Strengths: resource friendly, improved performance
 - Weaknesses: requires trusted nodes
 - Example blockchain: Hyperledger Fabric, JPMorgan Quorum

Putting it all together

	Proof of Work	Proof of Stake	Proof of Authority	Other consensus mechanisms
Public	Bitcoin <ul style="list-style-type: none"> - Scalability: limited, in development - Smart contracts: limited, in development - Gold standard trust minimization - Examples: “Digital Gold”, Blockcerts/MIT Diplomas 	EOS* <ul style="list-style-type: none"> - Scalability: yes - Smart contracts: yes - Requires trust of elected stakeholders - Example: Everipedia – Wikipedia with incentives 	N/A	Various: Stellar, Ripple, Iota, Dash, Decred, Nano
	Ethereum <ul style="list-style-type: none"> - Scalability: limited, in development - Smart contracts: yes, B2C - Trust minimized - Examples: augur, CryptoKitties, ICOs 	In development: Cardano*, Ethereum Casper <small>*EOS and Cardano use a variant called Delegated Proof of Stake</small>		
Private	Private Ethereum blockchain <ul style="list-style-type: none"> - Scalability: limited - Smart contracts: yes - Requires trusted nodes - Uncommonly used due to performance 	N/A	Private Ethereum blockchain (eg, Microsoft Azure) <ul style="list-style-type: none"> - Scalability: yes - Smart contracts: yes, B2B - Requires trusted nodes - Example: UN providing Syrian refugees w\ food vouchers 	Hyperledger fabric (eg, IBM blockchain) <ul style="list-style-type: none"> - Scalability: yes - Smart contracts: yes, B2B - Requires trusted nodes - Example: Tradelens

MedRec: overview

MedRec is an open source blockchain solution for health data that mediates which MDs have access to which patients' health data.

Aims to address four issues in US Healthcare:

1. **Fragmentation:** all of a patient's providers can access records (as allowed by the patient)
2. **Interoperability:** any medical record platform can draw data from MedRec
3. **Patient agency:** patients rather than providers/hospitals own records
4. **Data for clinical research:** anonymized health data available for research

Ekblaw A, Azaria A, Halamka JD, Lippman A. (2016) "A Case Study for Blockchain in Healthcare: MedRec prototype for electronic health records and medical research data"

Timeline

- December 2015: the MedRec idea was borne by Ariel Ekblaw and Asaph Azaria in a class with the MIT Digital Currency Initiative
- July 2016: MedRec 1.0 was piloted at Beth Israel with Chief Information Officer Dr. John Halamka
- August 2016: Whitepaper wins HHS competition
- February 2017: Ekblaw's master's thesis describing MedRec 1.0
- September 2017: MedRec 2.0 begins with a "Proof of Authority" consensus mechanism
- Today: MedRec subsumed by Dr. Halamka at BI Health Technology Exploration Center (HTEC)

MedRec 1.0

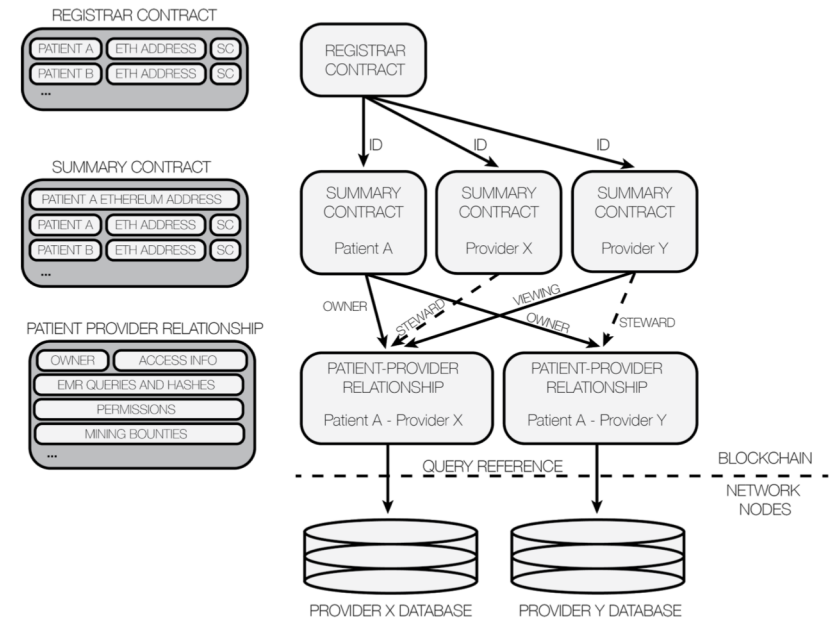
Private Ethereum blockchain with a Proof of Work consensus mechanism

Academic medical centers act as miners and are rewarded with anonymized patient data for clinical research. Each block “rewards” the miner with a “bounty” of some aggregate health data (eg, aggregate blood iron levels).

The actual medical records remain on hospital servers and MedRec just mediates access to these

MedRec 1.0 smart contracts enable three specific functions:

1. **Registrar contract:** Patients and physicians are assigned an ID (ETH address) on the blockchain
2. **Relationship contract:** Patients identify which physicians they have a clinical relationship with. This smart contract mediates which physicians can access which records.
3. **Summary contract:** contains a summary of each patient’s list of MDs and each MD’s list of patients.



MedRec 1.0 vs MedRec 2.0

Consensus mechanism changed to Proof of Authority

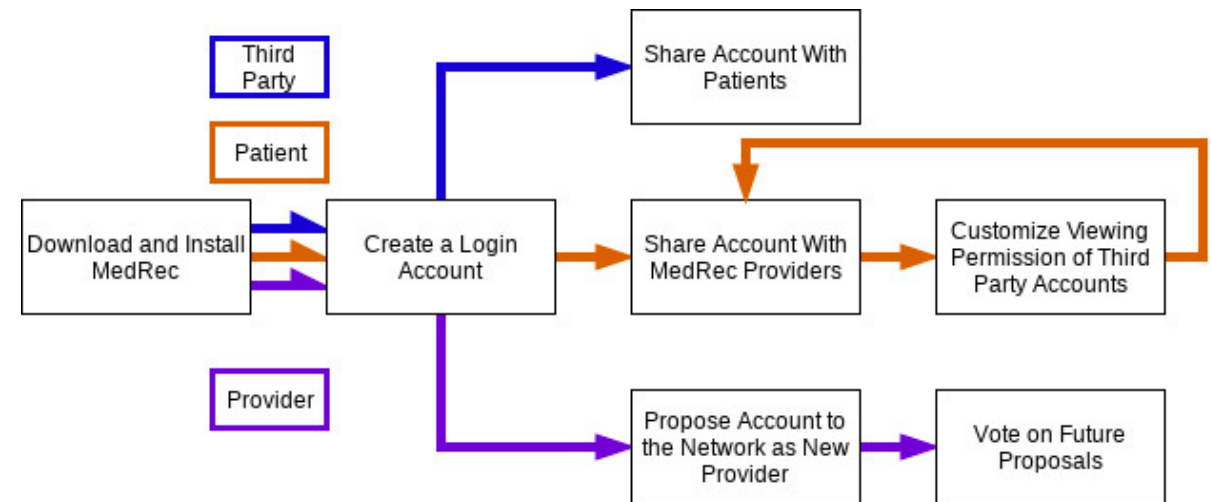
- We already trust health care providers (HCPs)
- Allows improved performance and scalability
- HCPs act as “authorized signers” and can append blocks and broadcast transactions
- Authorized signers can vote in and out other authorized signers

Providers and patients interact with MedRec via PC or phone applications.

Other performance optimizations

- MedRec 1.0 was notifying users via the blockchain every time a change was made to their medical record. This ended in 2.0

Technical changes: programming language changed to Solidity/Geth.



Will it work? Future considerations

Strengths

- Development at premier academic institutions
- Can be adopted incrementally
- Could provide valuable research insights
- Open source
- Funding by Robert Wood Johnson

Weaknesses

- Challenges with data self-ownership by children, the elderly, psychiatric patients
- Challenges with privacy around MD-patient relationships maintained on the blockchain

Opportunities

- Future development with Dr. Halamka at Beth Israel HTEC
- Blockchain as a promising emerging technology
- Paradigm shift to patient self-ownership of health data
- Not health specific. Architecture can be used for identity and permission management generally

Threats

- Complex regulatory landscape
- Well established industry incumbents
- US healthcare characteristically slow to adopt disruptive technology

Blockchain: key points

- Narrow use case:
 - Multiple parties
 - Shared ledger
 - Lack of trust between parties
 - Inefficient intermediaries
- Not a panacea: real tradeoffs vs a traditional database
- Disruption in healthcare still years away
- Always happy to talk more: dennisporto@alumni.harvard.edu

References

- Back A. (2002). “Hashcash – a denial of service counter measure.”
- Nakamoto S. (2008) “Bitcoin: a peer-to-peer electronic cash system.”
- Ekblaw A, Azaria A, Halamka JD, Lippman A. (2016) “A Case Study for Blockchain in Healthcare: MedRec prototype for electronic health records and medical research data
- Ekblaw A. (2017) “MedRec: Blockchain for Medical Data Access, Permission Management and Trend Analysis.”
- Yaga D, Mell P, Roby N, Scarfone K. (2018) “Blockchain Technology Overview.” National Institute of Standards and Technology. US Dept of Commerce
- Lal R, Johnson S. (2018). “Maersk: Betting on Blockchain.” Harvard Business School.
- Lippman A, Nchinda N, Retzepi K, Cameron A. (2018). “MedRec: Patient Control of Medical Record Distribution.”
- Thanks to: Prof Lal, Prof Lippman, Prof Halamka, Ariel Ekblaw, Agnes Cameron