Biomedical and Healthcare Applications for Blockchain

Tiffany J. Callahan
Computational Bioscience Program
Hunter/Kahn Labs

Network Analysis Working Group – 01.25.2018
Outline

• Introduction to bitcoin + blockchain
  — Obtaining + storing bitcoin
  — Creating transactions
  — Mining via hashcash

• Applications to healthcare
Bitcoin + Blockchain
Bitcoin

- Alternative, digital currency, “cryptocurrency”
  - Created in 2008 by Satoshi Nakamoto

- Decentralized financial infrastructure

- Purchased through exchange platform
  - 1 BTC = $11,151.03 (highest market value ~$19 billion)

- Storing bitcoins
  - Encrypted software wallets

- Transactions - verified by proof-of-work
How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.
How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.
Wallets are files that provide access to Bitcoin addresses, which are stored as strings of letters and numbers.

Each address carries an independent balance.
Bob and Alice both have Bitcoin “wallets” on their computers.

Wallets are files that provide access to Bitcoin addresses, which are stored as strings of letters and numbers.

Each address carries an independent balance.
Bob creates a new Bitcoin address so Alice can send him a payment.
Alice tells her Bitcoin client that she’d like to transfer the purchase amount to Bob’s address.

There is no third-party (e.g. PayPal, ApplePay, banks) in a decentralized system to verify the legitimacy of a transaction.

- All transactions, must be verified via proof-of-work (i.e. mining)
- Solutions, must be verified by members of the distributed network
- Enables trustless transaction

Alice tells her Bitcoin client that she’d like to transfer the purchase amount to Bob’s address. When Bob generates a new address he is actually creating a cryptographic key pair: private and public keys. The private key is known only to Bob, while the public key remains in Bob’s wallet so it can be used publicly for transaction verification.
Alice tells her Bitcoin client that she’d like to transfer the purchase amount to Bob’s address. When Bob generates a new address, he is actually creating a cryptographic key pair: a private and public key. The private key is known only to Bob, while the public key remains in Bob’s wallet so it can be used publicly for transaction verification. Alice’s Bitcoin client signs her transaction request with the private key of the address she’s transferring from.

Gary, Garth, and Glenn are Bitcoin miners. Their computers bundle the last 10 minutes of transactions into a new transaction block.

**Mining** serves 2 primary purposes:

1. Verification of all transactions in a *transaction block*
   - Avoids double-spending
2. Creation of new Bitcoin
   - Via rewarding successful miners

Hard to solve the problem, but easy to verify the solution.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magic Number (4)</td>
<td>Blockchain identifier with constant value, includes:</td>
</tr>
<tr>
<td></td>
<td>1. The start of the block</td>
</tr>
<tr>
<td></td>
<td>2. That data comes from a production network</td>
</tr>
<tr>
<td>Version (4)</td>
<td>Bitcoin protocol version</td>
</tr>
<tr>
<td>Previous Block Hash (32)</td>
<td>Previous block Hash: hash of the last added block</td>
</tr>
<tr>
<td>Merkle Root (32)</td>
<td>Merkle Root: a single hash resulting from repeated pairing and hashing of block transactions</td>
</tr>
<tr>
<td>Difficulty Target (4)</td>
<td>Difficulty target: a numeric representation of problem difficulty (# of zeros)</td>
</tr>
<tr>
<td>Nonce (4)</td>
<td>Nonce: increment counter; until problem solved</td>
</tr>
<tr>
<td>Transaction Counter (Variable: 1-9)</td>
<td>Transaction counter: count of transactions in that block</td>
</tr>
<tr>
<td>Transaction List (Variable: Upto 1 MB)</td>
<td>Transaction list: stores digital fingerprint of all transactions in that block</td>
</tr>
<tr>
<td>Block Size (4)</td>
<td>Block size: tells you how large a block is. Each block is fixed to 1 MB</td>
</tr>
<tr>
<td>Timestamp (4)</td>
<td>Timestamp: stores time of transactions and is included to increase the difficulty of hashing the block</td>
</tr>
</tbody>
</table>
Gary, Garth, and Glenn are Bitcoin miners. Their computers bundle the last 10 minutes of transactions into a new transaction block.

Miner’s computers calculate cryptographic hash functions.

A **Cryptographic hash function** transforms data into an alphanumerical string of a fixed length.

- Small changes (i.e. *nonces*) to original string result in large changes to the hash making it almost impossible to predict the initial data set responsible for each hash.

Different hash values of the same data are created using *nonces* - random number added to the data prior to hashing.
Mining computers calculate new hash values using the previous hash value, the new transaction block, and a nonce.

Bitcoin requires all new hashes follow a specific format - start with a certain number of zeros.

Mining computers calculate new hash values using the previous hash value, the new transaction block, and a nonce. Miners have no way to predict which nonce will produce a hash value with the required number of zeros.

**Mining** is a process of inverse hashing:
- Determine the nonce so that the *cryptographic function* of block data results in less than a given threshold (i.e. **difficulty target**)
  - The more computing power added to the network, the higher the difficulty target

Mining computers calculate new hash values using the previous hash value, the new transaction block, and a nonce.

Miners have no way to predict which nonce will produce a hash value with the required number of zeros.

A transaction *coinbase* keeps track of the miner’s work and award’s the miner that successfully solves the problem.

As time passes, Alice’s transaction to Bob gets buried under more recent transactions. To modify the ledger, would require re-doing Gary’s hard work - finding another winning nonce - a very difficult task.

A solution to a **transaction block** must reach consensus from other members in the network:

- Once verified, **transaction block** gets added to the **blockchain**, the distributed public ledger of all transactions in the network
  - Assumption that 51% of miners are honest
APPLICATIONS TO HEALTHCARE
Healthcare Chain

Blockchain technology in health care: A primer for surgeons

by ALEXANDER W. PETERS, MD, BRIAN M. TILL, JOHN G. MEARA, MD, DMD, MBA, FACS, and SALIM AFSHAR, MD, DMD, FACS
PUBLISHED DECEMBER 6, 2017 • PRINT-FRIENDLY

Blockchain technology—the platform underpinning Bitcoin, a global digital payment system—has attracted more than $1.2 billion of investment from some of the world's leading corporations for its security and immutability. More than 130 million secure Bitcoin transactions have occurred since the digital currency launched in 2009. Today, Bitcoin can be used to make purchases from Microsoft, buy food in neighborhood cafes, book flights and hotel rooms, and even pay for medical care.

For the health care industry, blockchain technology stands to revolutionize the interoperability, security, and accountability of electronic health records (EHR) and health information technology (HIT), medical supply chains, payment methodologies, research capabilities, and data ownership. In fact, in the 2015 report "Connecting Health and Care for the Nation, a Shared Nationwide Interoperability Roadmap," the Office of the National Coordinator for Health Information Technology set a goal of establishing full EHR interoperability by 2024.
Blockchain technology— the platform underpinning Bitcoin, a global digital payment system—has attracted more than $1.2 billion of investment from some of the world’s leading corporations for its security and immutability. More than 130 million secure Bitcoin transactions have occurred since the digital currency launched in 2009. Today, Bitcoin can be used to make purchases from Microsoft, buy food in neighborhood cafes, book flights and hotel rooms, and even pay for medical care.

For the health care industry, blockchain technology stands to revolutionize the interoperability, security, and accountability of electronic health records (EHR) and health information technology (HIT), medical supply chains, payment methodologies, research capabilities, and data ownership. In fact, in the 2015 report “Connecting Health and Care for the Nation, a Shared Nationwide Interoperability Roadmap,” the Office of the National Coordinator for Health Information Technology set a goal of establishing full EHR interoperability by 2024.
How does blockchain actually work for healthcare?

To say the technology is advanced is an understatement, but hospitals should understand the reasons that it’s getting so much attention.

By Mike Miliard | April 13, 2017 | 12:25 PM
How does blockchain actually work for healthcare?

To say the technology is advanced is an understatement, but hospitals should understand the reasons that it’s getting so much attention.

“It’s the answer to interoperability.”

“the technology can solve healthcare’s looming security problems.”
Exploring the Use of Blockchain for EHRs, Healthcare Big Data

Blockchain has the potential to revolutionize EHR interoperability and the exchange of healthcare big data.
Exploring the Use of Blockchain for EHRs, Healthcare Big Data

Blockchain has the potential to revolutionize EHR interoperability and the exchange of healthcare big data.

“Providers can add a new record associated with a particular patient, and patients can authorize sharing of records between providers”
Review

Blockchain distributed ledger technologies for biomedical and health care applications

Tsung-Ting Kuo,¹ Hyeon-Eui Kim,¹ and Lucila Ohno-Machado¹,²

¹UCSD Health Department of Biomedical Informatics, University of California San Diego, La Jolla, CA, USA and ²Division of Health Services Research and Development, Veterans Administration San Diego Healthcare System, La Jolla, CA, USA

Corresponding Author: Lucila Ohno-Machado, 9500 Gilman Dr, San Diego, CA 92130, USA. E-mail: lohnomachado@ucsd.edu; Phone: +1 (858) 822-4931.
Key Benefits

• Decentralized management
• Immutable audit trail
• Data Provenance
• Robustness/Availability
• Security/Privacy
Key Benefits

• Decentralized management
  – Patient-managed health care records\textsuperscript{85}
  – Real-time claim processing\textsuperscript{94}
  – Improved data sharing\textsuperscript{13}

• Decentralized health data backbone would allows the incorporation of patient-generated and EHR data accessible to providers and patients\textsuperscript{101}
Key Benefits

• Immutable audit trail
  – Unalterable patient records\textsuperscript{77}
  – Improved claim auditing and fraud detection\textsuperscript{92}
  – Trackable, timestamped patient-generated data\textsuperscript{76,102}

• Unchangeable log of clinical research protocols - would ensure any changes to research protocol are transparent to all members of network\textsuperscript{76,105}
Key Benefits

• Data Provenance
  – Source-verifiable medical records\textsuperscript{78}
  – Verifiable records for claim quantification\textsuperscript{95}
  – Evidenced provenance for medical research data\textsuperscript{96,97}

• Tamper proof transfer of data is transparent, facilitates the tracking and identification of poor quality or forged data\textsuperscript{76,105}
Key Benefits

• Robustness/Availability
  – Protected patient recordkeeping\textsuperscript{85}
  – Enhanced data accessibility\textsuperscript{92}
  – Improved healthcare data availability\textsuperscript{86}

• Blockchain-enabled anti-tampering prevents drug counterfeiting when supplying and dispensing medication\textsuperscript{92}
Key Benefits

• Security/Privacy
  – Medical record encryption\textsuperscript{85}
  – Increased insurance security\textsuperscript{92}
  – Secured data sharing\textsuperscript{86}

• Improved patient confidence in recording and storing of consent documentation\textsuperscript{89}
Connectivity

Who Will Build the Health-Care Blockchain?

Decentralized databases promise to revolutionize medical records, but not until the health-care industry buys in to the idea and gets to work.

by Mike Orcutt September 15, 2017

A Case Study for Blockchain in Healthcare:
“MedRec” prototype for electronic health records and medical research data

White Paper

Ariel Ekblaw*, Asaph Azaria*, John D. Halamka, MD†, Andrew Lippman*

*MIT Media Lab, †Beth Israel Deaconess Medical Center

August 2016
Conclusions

- Benefits of blockchain for healthcare
  - Decentralized management
  - Immutable audit trail
  - Data provenance
  - Robustness
  - Security/Privacy

- While very promising, more work is needed to motivate uptake by hospitals and clinics
Thank you!

Questions?
Blockchain Resources

- http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency
- https://www.dash.org/
- https://books.google.com/books?id=jk5zAgAAQBAJ
- https://en.bitcoin.it/wiki/Proof_of_burn
- https://www.bigchaindb.com/whitepaper/