Case Study:
Blockchain In Healthcare –
A Marriage Of Hype And Promise
Several in discussion across healthcare:

- **Supply chain**
  - Smart contracts, monitoring an activity throughout defined period.
  - Are tasks executed in the correct order, on time, according to specification?
  - How is data being shared among partners?

- **MPI**
  - Clean up the mess
  - Change the mindset about identity vs. data, drive towards true interoperability?
  - Build new rules for better monitoring

- **Longitudinal record**
  - Enabling precision medicine: compile wearable data, telehealth, telemedicine, primary care, inpatient, acute care.
  - How does a provider get a complete view of the patient? → Then use the data for research

- **Others**
HealthCare Security Solutions Challenges

….to name a few.
• CIA triad - Status quo isn’t working.
• We’re breaching data as we pass it around our own systems and with suppliers (Supply Chain, MPI)
• How to do analytics on data within the blockchain (smart people needed)
• Will it scale appropriately?
• Do we really want interoperability?
What is Dan working on?

• **Blockchain:**
  • Rogue Device Detection (not wireless).
  • Using blockchain and network data, can rules for identity of devices and peers be monitored and alerted?
  • Can we report on communications among devices and peers? Can we control access of devices and peers to protected data?

• **Innovation Role.**
  • Working with researchers, vendors, partners, Sentara IT and business to refine goals and target areas for improvement
Blockchain Overview

- Problem – How do distributed, distrusting stakeholders agree on current system state?

- Solution – If technology can help the stakeholders to reach consensus on history, agreement on current system state can be reached.
• Why not use centralized databases?
• Single point of compromise/failure
• Too much power vested in one entity
• Challenging to get every entity to agree on the one arbiter to trust
• Blockchain eliminates the need for a centralized trusted database
  • Share databases across diverse boundaries of trust
  • Transactions leverage self-contained proofs of validity and authorization
  • Multiple nodes provide validation through consensus
  • Robustness without need for expensive replication and disaster recovery
  • Automatically self-configure and synchronize in peer-to-peer fashion
• Decentralized Network
  • Peer-to-Peer architecture
  • Nodes can join/leave freely
  • No central arbitrator
  • Redundancy and robustness to link failures

• Distributed Consensus
  • Transaction record
  • Distributed public ledger
  • Validation by committee

• Cryptographically Secure
  • Immutable audit trail
  • Data tampering prevented
Blockchain Overview

- Chained sequence of hash records
  - No entity can change any past record.
- Several procedures for adding blocks to blockchain
- Validation of blocks
  - Enforced by consensus protocols

### Blockchain Overview

**Hash Chain**
- Building block of blockchains
- Curbs centralized arbitrator’s ability to modify history
- Cryptographic hash function (SHA256).
- Mathematically impossible to find two inputs with the same hash value.
- Translates to every record (N) has a commitment to N-1 which is committed to record N-2 and so on and so forth.

```
Index 1
<table>
<thead>
<tr>
<th>Data</th>
<th>d1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prev</td>
<td>0</td>
</tr>
<tr>
<td>Nonce</td>
<td>n1</td>
</tr>
<tr>
<td>Hash</td>
<td>h1</td>
</tr>
</tbody>
</table>

Index 2
<table>
<thead>
<tr>
<th>Data</th>
<th>d2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prev</td>
<td>h1</td>
</tr>
<tr>
<td>Nonce</td>
<td>n2</td>
</tr>
<tr>
<td>Hash</td>
<td>h2</td>
</tr>
</tbody>
</table>

Index 3
<table>
<thead>
<tr>
<th>Data</th>
<th>d3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prev</td>
<td>h2</td>
</tr>
<tr>
<td>Nonce</td>
<td>n3</td>
</tr>
<tr>
<td>Hash</td>
<td>h3</td>
</tr>
</tbody>
</table>

Index 4
<table>
<thead>
<tr>
<th>Data</th>
<th>d4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prev</td>
<td>h3</td>
</tr>
<tr>
<td>Nonce</td>
<td>n4</td>
</tr>
<tr>
<td>Hash</td>
<td>h4</td>
</tr>
</tbody>
</table>
```
Blockchain Overview

- **Attack on hashed chain**

<table>
<thead>
<tr>
<th>Index</th>
<th>1</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>d1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prev</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nonce</td>
<td>n1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash</td>
<td>h1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Index</th>
<th>2</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>d3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prev</td>
<td>h1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nonce</td>
<td>n2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash</td>
<td>h2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Index</th>
<th>3</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>d3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prev</td>
<td>h2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nonce</td>
<td>n3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash</td>
<td>h3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Index</th>
<th>4</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>d4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prev</td>
<td>h3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nonce</td>
<td>n4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash</td>
<td>h4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Blockchain Overview

- **Propagation of attack in hashed chain**
  - Changing record N results in changes to final hashes of records N+1, N+2, etc

<table>
<thead>
<tr>
<th>Index</th>
<th>Data</th>
<th>Prev</th>
<th>Nonce</th>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>d1</td>
<td>0</td>
<td>n1</td>
<td>h1</td>
</tr>
<tr>
<td>2</td>
<td>d3</td>
<td>h1</td>
<td>n2</td>
<td>h2</td>
</tr>
<tr>
<td>3</td>
<td>d3</td>
<td>h2</td>
<td>n3</td>
<td>h3</td>
</tr>
<tr>
<td>4</td>
<td>d4</td>
<td>h3</td>
<td>n4</td>
<td>h4</td>
</tr>
</tbody>
</table>
Blockchain Overview

- **Proof of Work**
  - Carry out large computation
    - Prove that computation was successfully
    - No additional work to check the proof
    - Limits the rate of new blocks
    - Expensive to add invalid blocks
    - Aids in deciding between competing chains by choosing the one with the most work.

- **Proof of Stake**
  - Achieve consensus by eliminating expense proof of work
  - Block creation tied to amount of stake

- **Byzantine Fault Tolerance**
  - Trusted entities work together to add records
  - Voting process for accepting a block on the chain
Blockchain Overview

- Permissionless Blockchain Infrastructures
  - Open access on the Internet
  - Anyone can use
  - Anonymous validators
  - Proof of Work consensus
  - Public network

- Permissioned Blockchain Infrastructures
  - Private network
  - Participation by members only
  - Trusted validators
  - Customized consensus protocol
  - Members set rules
  - Restricted access
Blockchain Overview

Incentives in permission-less infrastructure
• Miners ensure sustainability of system
• Incentive is the capital invested in Bitcoin
• Payoffs in Bitcoin involves moving money around

Incentives in permissioned infrastructure
• How to build payoff into consensus protocol to store medical records?
Blockchain Challenges

• Scalability and Validation Speed
  • Blockchain platforms take 10 minutes or longer to confirm transactions and 7 transactions/sec maximum throughput
  • Cannot yet match speed of mainstream payment processor
  • Bottlenecks in blockchain architecture limit high throughput and low latencies
  • Parameterization of block sizes and intervals will not be sufficient for high load blockchain deployments
  • Need for scalable consensus protocols, network topology and storage
Blockchain Challenges

• Privacy
  • Data breach attacks on permissioned blockchain platforms
  • Need for privacy guarantees in case of attack on validating nodes
  • Tradeoff between resilience and privacy
  • Need to include cryptographic techniques, such as, multi-party computation, homomorphic encryption, etc. within permissioned blockchain platforms
Blockchain Summary

- No need to trust each other or have a trusted third party
- Distributed system
- Agreement on history translates to agreeing on system state
- Nth record in the hash chain commits to all previous records.
- Any change in previous record invalidates hash chain
- A blockchain is a hash chain with procedures for validity and resolve disagreements
  - Permissionless vs. Permissioned infrastructure
  - Proof of Work vs. Proof of Stake vs. Proof of Storage, etc.
Blockchain Development Platforms

• Ethereum
  — Generalized blockchain platform
• Multichain
  — Permissioned blockchain network
• Hyperledger Fabric
  — Open standard for blockchain for business
• Tierion
  — Supports integration of applications within blockchain network
• Guardtime
  — Industrial scale blockchain service with keyless signature infrastructure and secure one way function
Hyperledger

- Permissioned, private blockchain option
- Access control, chaincode-based smart contracts
- Practical byzantine fault tolerance Consensus
- Includes anchors of trust to root certificate authorities
- Applicable to managing IoT devices in high-bandwidth situations

Source: http://hyperledger-fabric.readthedocs.io/en/v0.6/
Next Steps

• Develop blockchain-based platform for healthcare to enable a secure, trusted and efficient solution for data storage and sharing
  • Electronic health records,
  • Medical research data
  • Medical devices

• Collaboration with Sentara on development of prototype on Hyperledger