Blockchain is Not Secure by Itself

Mitch Parker 07/09/2018

Indiana University Health

Purpose of presentation

- Explore DLT/blockchain's potential benefits
- Demonstrate how we addressed our emerging needs in that space
- Provide a framework to address the larger problem of distributed computing as our industry moves toward converged resources

Special thanks to

- Jamie Kurtz, CTO, Diagnotes
- Alex Yuriev, Former CTO, Livestream.com (acquired by Vimeo)
- Dan Bowden, CISO, Sentara Health
- Terence Rice, CISO, Merck
- Wafaa Mamilli, VP/CISO, Eli Lilly
- Susan Ramonat, CEO, Spiritus Partners (UK)
- Chuck White, CTO, Fornetix
- Ammon Fillmore, Attorney, Hall Render

How might distributed ledger technology (DLT)/blockchain help us?

Blockchain is a technology that allows for the distributed verification and validation of data using strong cryptography

- Allows communities to cross-verify transactions with each other
- Could significantly reduce the time it takes to look up and verify transactions
- Avoid “swivel chairing” and errors going between legacy systems
- Could solve a vexing accounting problem using a distributed ledger

Who's doing what in healthcare?

- Multiple healthcare vendors who have either stated their intention to use it or have already started pilot projects
- National provider directory undertaken by consortium
- Supply chain use cases (pharmaceuticals, medical devices)
- Several large IT providers now offering this as a service:
  - IBM Hyperledger
  - Amazon
  - Microsoft
  - Oracle

No, really. How might blockchain help?

- Potential to change how we approach security
- Opportunity to define and establish shared standards for data sharing and security to protect systems
- Opportunity to create real incentives to secure our systems and evolve from legacy technology
- Foundation for building communities of mutually assured security with real penalties

Are you serious?

Yes, I am

- Current approach is *unsustainable*
  - Grafting modern technologies onto legacy systems
  - Ignoring core business processes that drive our systems
  - Using faxes and pagers more than anyone else?
- True innovation and modernization are *overdue* for patients, clinicians and the organizations who serve them
- Most important, stop introducing new technologies as solutions looking for problems and think about *real impacts*

What's happening in our sector?

- Highly touted implementations often just pilots or research projects
- Limited due diligence and focus on governance
- Unwarranted optimism that blockchain-enabled ecosystems will work "naturally" without conscious management, monitoring and governance
- Lack of enforceable contractual protections, even by some large health systems

Challenges presented by blockchain's immaturity

Evaluate and perform due diligence at the outset:

- Blockchain assumed to be inherently secure and reliable
- Some health systems have implemented without proper controls and are storing patient data on blockchain systems

Understand and address risks:

- Limited or no governance across system and entities
- Vulnerabilities and potential attack surfaces should be explored and mitigated
- Gaps between technology hype and commercial implementation

What have we done?

- Spoken with industry experts:
  - Blockchain, esp. healthcare/pharma
  - Large-Scale Distributed Inter-networking Security
  - Financial risk
  - Cryptography
  - Cybersecurity law
- Developed in-house expertise:
  - HIPAA Security Rule and PCI-DSS
  - 3rd party due diligence

What else?

- Conducted our own gap analysis of blockchain implementations
- Developed root cause analyses of Bitcoin hacks:
  - Failure to patch outdated system components
  - Really, really bad code (esp. Mt. Gox) giving free reign to attackers
- Analyzed Border Gateway Protocol (BGP) hijacking – Methods and potential to cause serious Internet disruptions
  - Putin has been proven to use this in Ukraine
  - This led us to DNS Hijacking as well!
- Translated 20 “Areas of Concern” into contractual protections

Areas of concern

- Storage of regulated data (HIPAA, PCI-DSS, FERPA, Privacy Act) on blockchains – Reading is not auditable
- No minimum cryptographic standard specified for hashing (SHA 256)
- Potential for compromise should someone control more than 50% of the total computing power of the distributed system

Areas of concern (cont.)

- No SLAs for vulnerability management - All the system components
- No requirement for a security management program
- No requirement for segmentation of access to these services
  - Treat like credit card processing devices or financial instruments
  - Configure any device that processes blockchain transactions to PCI-DSS standards
- No requirement for minimum necessary communication – Base requirement of the HIPAA Security Rule

Areas of concern (cont.)

- No recommended protection against network-based attacks that hijack networks and Domain Name Services (DNS)
- No recommended controls over enterprise-level Internetworking using BGP and DNS
  - No recommended controls over network monitoring for anomalies
  - No recommended controls over service level agreements for anomaly resolution

Areas of concern (cont.)

Due to this risk analysis, we are implementing:

- Cisco BGPMon – Proactive monitoring of Border Gateway Protocol, the prevalent Routing algorithm for the Internet, for BGP Hijacking
- 3rd Party DNS Monitoring and OpenDNS - Proactive monitoring of DNS for:
  - Malware using DNS to communicate
  - Phishing attacks using similar domain names
  - Attempted DNS hijacking
  - Attempted DNS spoofing

Areas of Concern (cont.)

- No right to monitor for all participants the system health and connectivity of all participants
- No right to monitor for all participants of all vulnerability types
- No right to terminate non-compliant participants after 7 days

Areas of concern (cont.)

- No provisions for strong identity management backed by cryptographic keys that use verifiable cryptographic processes
  - Your crypto is only as strong as the process used to manage it!
  - As healthcare system security evolves, cryptographic management and ID management need to support innovation
  - Get very smart with ID management and certificate provisioning to support current and future security standards

Areas of concern (cont.)

- Need for backward and forward validation and verification of data
  - Verify that data being used as part of system is valid
  - Reconcile transactions with transactions stored in your local systems
  - Trace back transactions to verified and validated identities
  - Reconcile all cryptographically verified identities to legal entities

Areas of Concern (7)

- Documented method and process for appending records to the system in case of a correction
- Governance process for arbitrating disputed transactions and posting amendments, especially for consortia – A C-suite “must have”

Where do things stand now?

- Amended existing Business Associate Agreement and Master IT Contract Documentation (Appendix B):
  - Specifies contractual protections for Distributed Verification and Validation, e.g. blockchain
  - Addresses these 20 key core areas
  - Provides enforceable methods for ensuring strong security processes
- Established as starting point for vendor engagements: “If they’re not written down and shared, they don’t exist.”

What can you do?

- Consider our Appendix B (Available to whomever asks)
- Address these areas and think critically
- Think about your entire network and security program, not just about the latest technology
  - Avoid FUD
  - No technology is secure by default
  - Need for constant attention, care and feeding