The ABC's of Healthcare with Blockchain

The Reality Today and How to Make it Work For You Tomorrow.

HIMSS
CENTRAL & SOUTHERN OHIO *Chapter*

Speakers

David Houlding CISSP CIPP
Principal Healthcare Lead | Microsoft
Chair | HIMSS Blockchain Task Force
Advisor | British Blockchain Association
David.Houlding@Microsoft.com
LinkedIn/In/DavidHoulding
@DavidHoulding

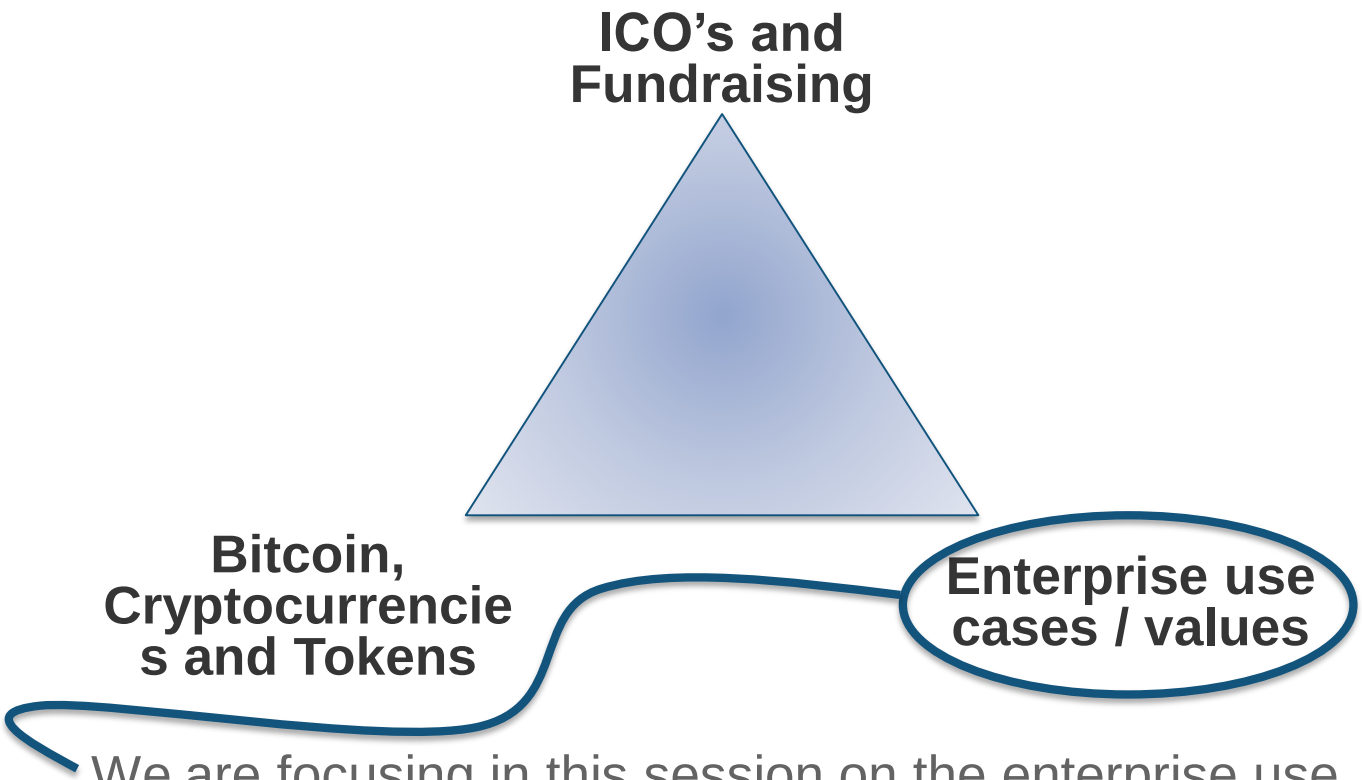
Mitch Parker CISSP
Executive Director,
Information Security and Compliance,
Indiana University Health
Mitchell.Parker@IUHealth.org
LinkedIn/In/MitchParkerCISO

Blockchain in Healthcare

- What is it?
- Use cases and business values
- Where we are as an industry, next steps, evolution

HIMSS
CENTRAL & SOUTHERN OHIO *Chapter*

3 Facets of Blockchain

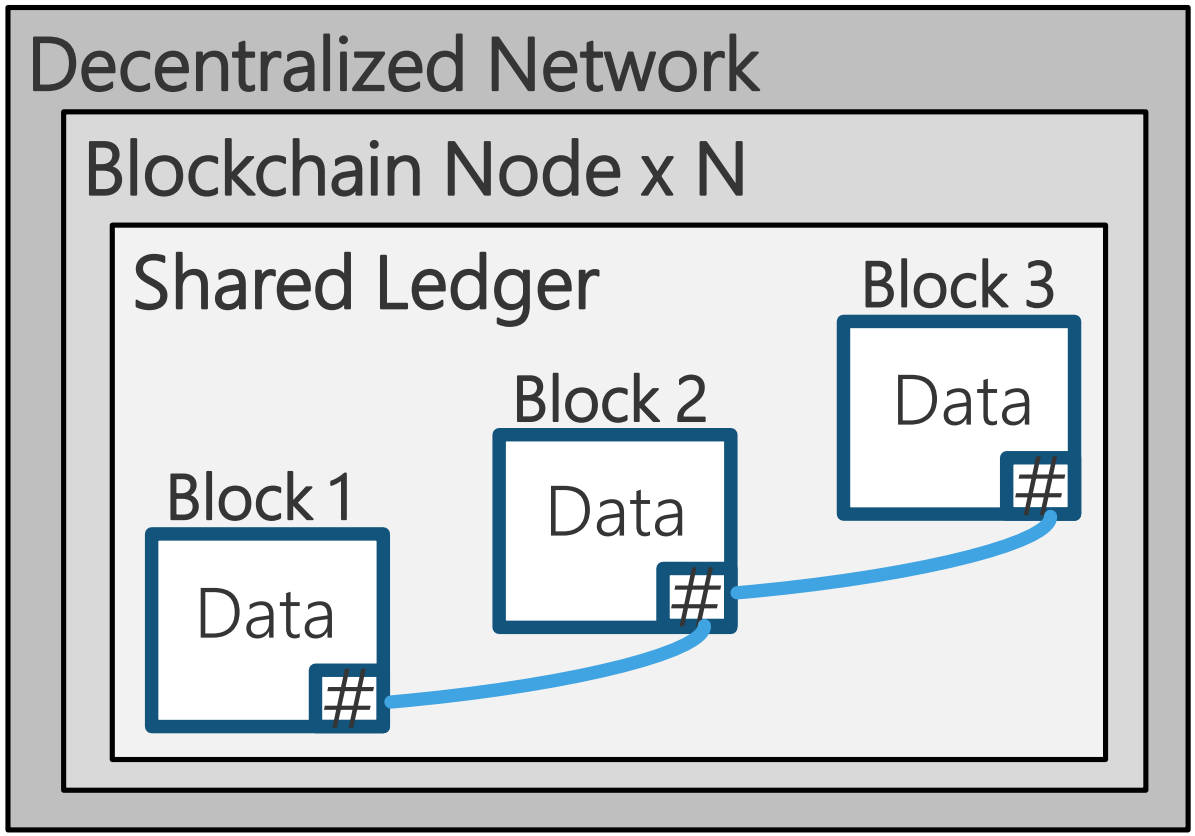


We are focusing in this session on the enterprise use cases and associated business values of blockchain

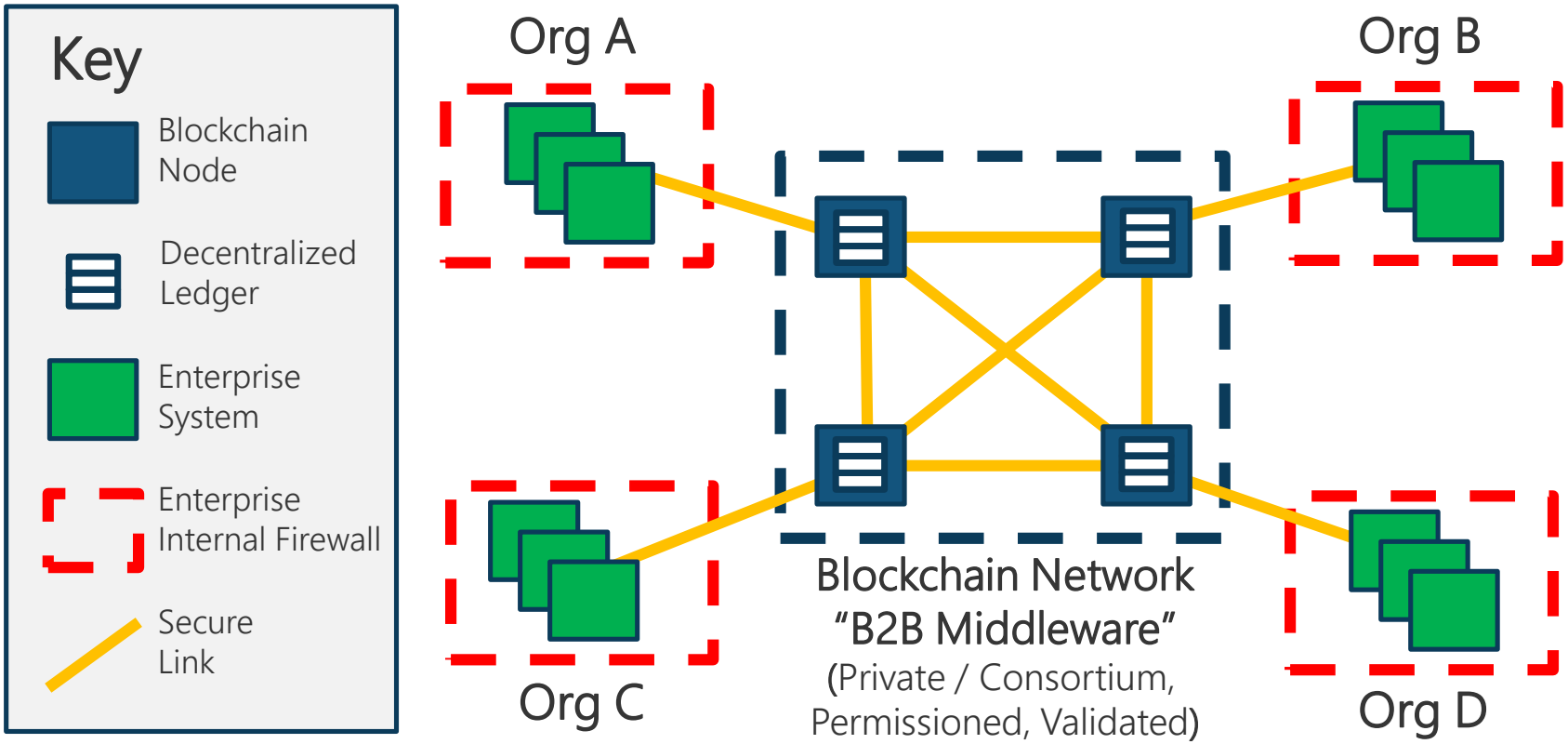
Blockchain in Healthcare
A Layered View

Layer 4	**Artificial Intelligence and Machine Learning** Enable Major New Insights, Values
Layer 3	**Cryptocurrencies, Tokens** Enable New Incentives, Marketplaces, Commerce
Layer 2	**Smart Contracts** Increasingly Automates Transactions, Improving Efficiency
Layer 1	**Blockchain** Enables Secure Sharing of Healthcare Data Across B2B Networks
Layer 0	Healthcare Data Mostly in **Silos**, Little Sharing, Massive Untapped Potential

Blockchain and Distributed Ledger Technology

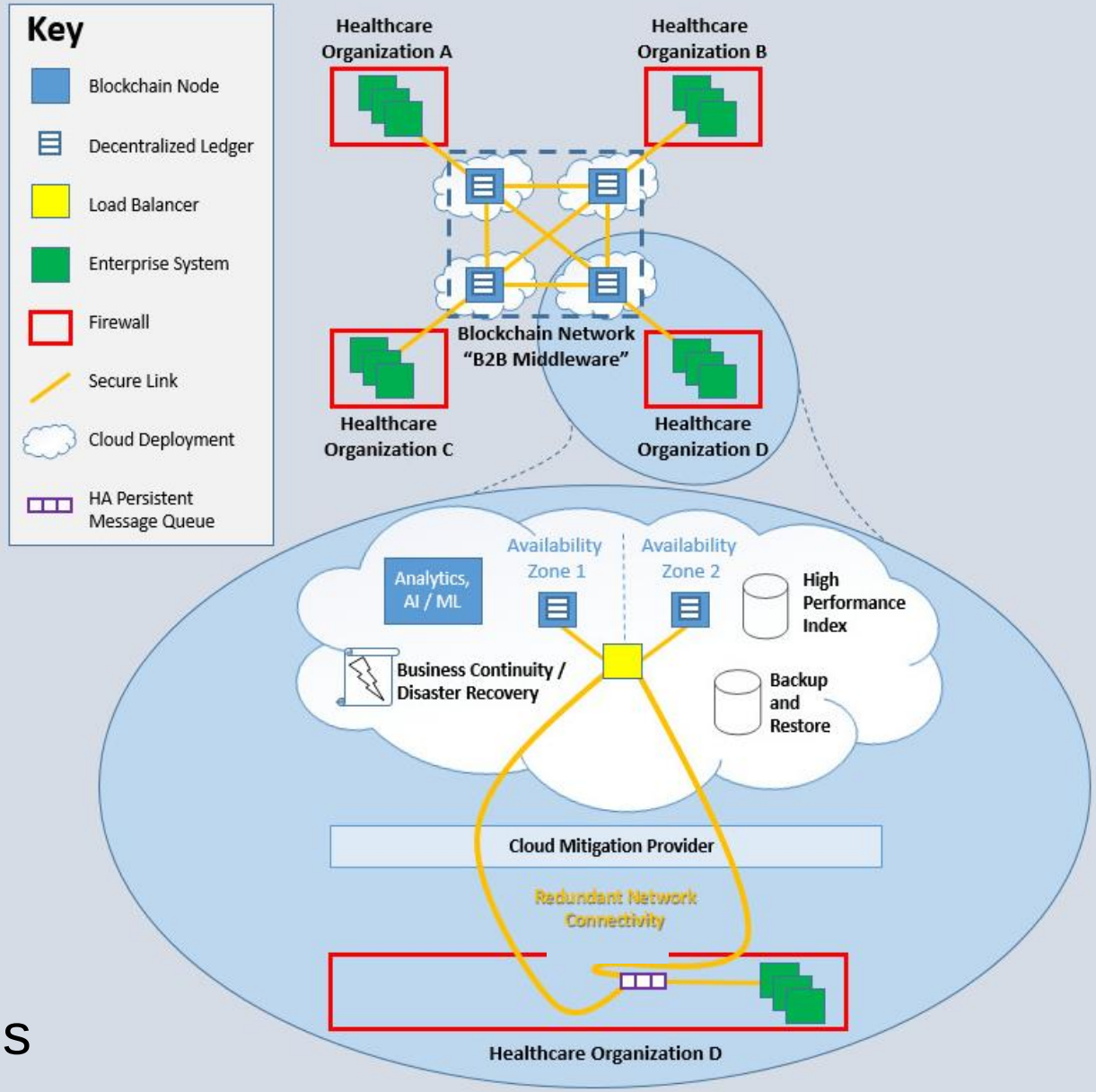


Blockchain Architecture

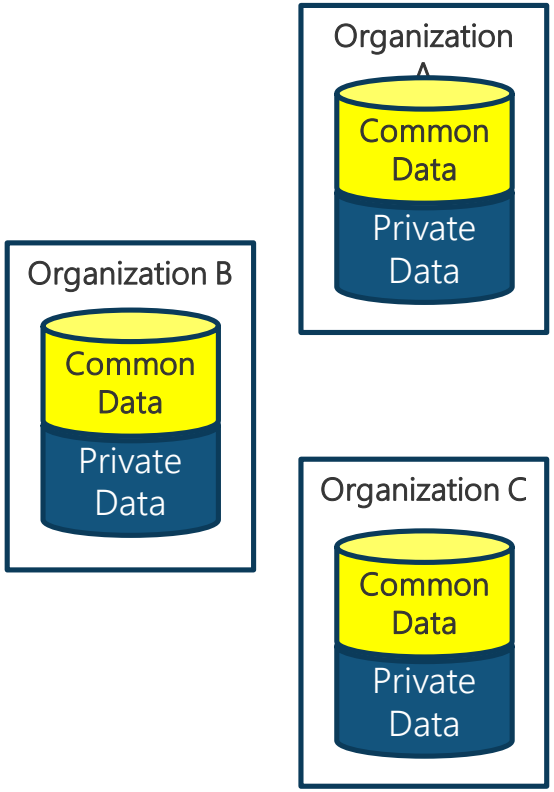


Blockchain in the Cloud

- On premises
- In cloud
- Heterogeneous deployment options
- Consistent consensus

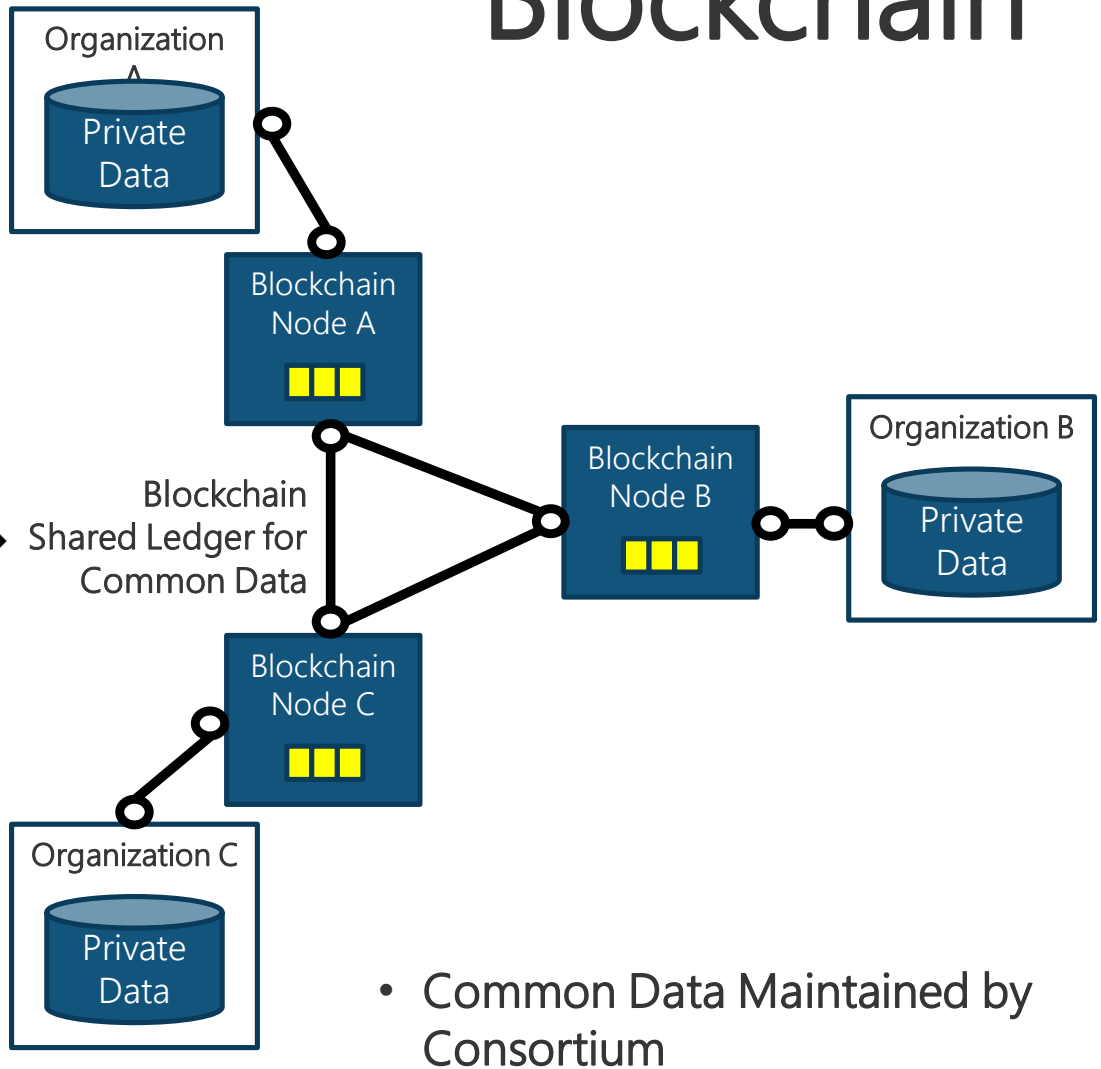


Today



- Redundant Maintenance of Common Data
- Inconsistencies, Causing Friction

Blockchain



- Common Data Maintained by Consortium
- Update Once, Near Realtime Visibility Across

Blockchain Strengths

- Secure, targeted sharing of data, where it makes business sense
- Data integrity
- Transparency
- Decentralization, resilience, availability of the network
- Anti-fraud

Identifying Use Cases and Business Value Propositions

- Its about the **network** of organizations, not a database
- Collaboration around shared data for business value
  - Reducing healthcare **costs**
  - Improving patient **outcomes**
  - Improving patient **engagement**, experience
  - Improving healthcare professional **experience**
- **Existing healthcare B2B networks** are near term opportunities

Delivering Value with Blockchain Healthcare Examples

Use Case	Reduce Cost	Improve Patient Outcomes	Engage Patients, Enhance Experience	Enhance Healthcare Professional Experience
Provider Directory	✓			
Drug Supply Chain	✓	✓	✓	✓
Medical Device Track and Trace	✓	✓	✓	✓
Health Information Exchange	✓	✓	✓	
Provider Credentialing	✓			✓
Anti-Fraud	✓		✓	

Pilot, Case Study with Attestations, Scale

- Multiple blockchain pilots in progress, ending in 2019
- Consortiums of recognizable, respected organizations
- Centered on use cases and business value(s)
  - Provider Directory
  - Provider Credentialing
  - Etc

- Results and case studies with attestations of business values, and areas to improve are imminent
- Establish a solid foothold to scale consortiums, use cases

Blockchain Reality vs Hype

1. Security
Hype: blockchain fixes security
Reality: security strengths, limitations. Must augment for effective security

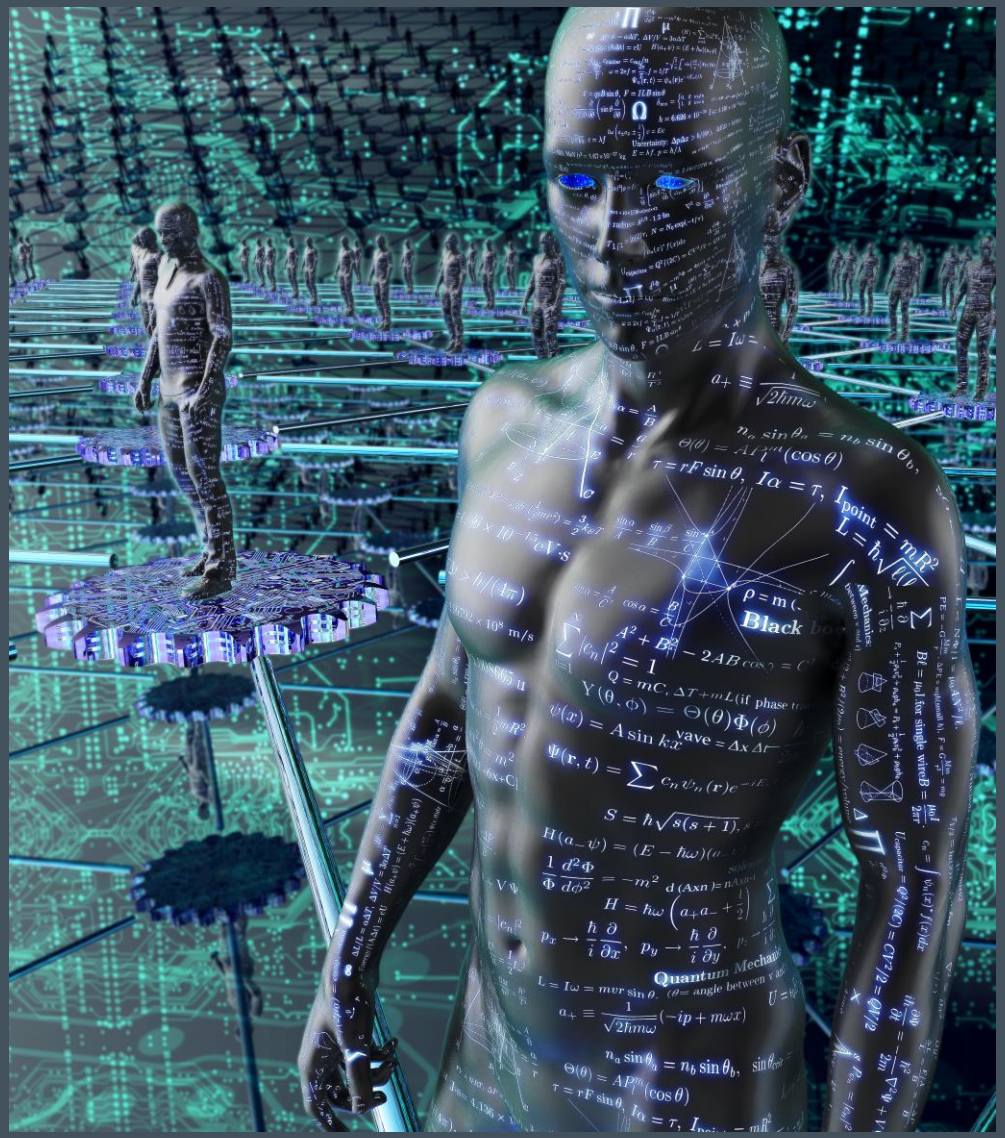
2. Replacing Enterprise Systems
Hype: blockchain will replace enterprise systems
Reality: blockchain will co-exist with enterprise systems, where it makes business sense

3. Public vs Private Blockchains
Hype: only public blockchain is truly blockchain
Reality: with focus on value, the vast majority of use cases are using private / consortium blockchains

Blockchain Evolution, Opportunities, Barriers

- Mostly private / consortium blockchains
- An archipelago of blockchain islands
- Interoperability challenge
- Pilots, case studies, attestations
- Natural selection
- Winners scale in size, use cases, network effect
- Gradual move over time to larger islands
- Pave way for richer smart contracts, DAOs

Blockchain Ethical Considerations



- Patients Own Data
- Patients Monetize Data
- Disintermediation, and Disruption
- Hyper-Efficiency, Job Loss
- Environmental Impacts
- Anonymity, Cryptocurrency, and Crime

Blockchain Challenges, Strategies

- Building consortium,
- Provenance,
- Privacy, Security, Compliance,
- Integration and Interoperability,
- Performance

HIMSS
CENTRAL & SOUTHERN OHIO *Chapter*

Building Consortium

- Where do we start? Good rules of the road
- The operative word is Co-opetition
- We are doing business with our rivals
- We need to work together with others to protect ourselves and our trading partners
- Consortia do not work without establishing minimum standards for privacy, security, compliance, integration and interoperability, performance, change management, dispute resolution (esp for smart contracts), and data provenance

Value Added Network (VAN) 2.0

- These standards need to be codified with a centralized controlling organization and agreements/contracts to establish these relationships
- Like the old Value Added Networks for Electronic Data Interchange, but with a decentralized network approach
- Difference: instead of one organization controlling and storing all of the transaction records and data, participants cross-verify and validate them
- We will go over the VAN 2.0 standards in order

Data Provenance

- According to Springer:
  - The term “data provenance” refers to a record trail that accounts for the origin of a piece of data (in a database, document or repository) together with an explanation of how and why it got to the present place
  - This is something a lot of AI vendors cannot explain
  - This is something that many have not proven
  - A lot of work in the Blockchain space to prove this (Rymedi and supply chain vendors)
    - Pharmaceutical Supply Chain is a big use case
    - AI for clinical decision making is another

Data Provenance

- We need to understand where the data came from and how it got there
- What good is interoperability if you have bad data?
- We need to establish provable forward data provenance from the systems of record to the Blockchain
- We also need to establish provable reverse data provenance from the Blockchain back to the systems of record
- Emphasis on provable and auditable - demonstrate that proper processes are being followed
- The technology is not fully able yet to do reporting and analytics at the same level of performance as current reporting and analytics platforms - this will change however we need to address for now

Data Provenance

- We also need to be able to integrate into existing systems using stable, supported APIs
- Don’t want to make the same mistakes we made with customizations , Enterprise Resource Planning, and Electronic Medical Records
    - This is where we hacked systems to bits to customize for business logic and built islands of data that we’re still addressing now with historical medical data
- If we don’t address this we will repeat these same mistakes and Blockchain will immortalize them for us

Privacy

- We need to have in the agreements what data elements will be used to transact business, how they will be used, and how we will use the minimum necessary information to do so in transactions
- Transactions can be tied to identities and wallet addresses - therefore while in public Blockchains one can be pseudonymous, in private ones there will be tie back to a specific person.
- The issue is that all participants can see all transactions and their source and destinations.
- This is part of how Silk Road was taken down. The FBI got really good at mining Blockchain for transactions and were able to trace back transactions.

Privacy – Zero Knowledge Proofs

- First implemented as zk-Snarks by zCash
- Also integrated into Ethereum by Consensys
- Allows the use of “notes” as a way of transferring assets between two parties without others knowing and protecting their privacy
    - Computationally Complex to generate- takes 48 seconds and 3GB RAM on a high end server
    - Cannot be created on mobile devices (yet) or older computers
    - Can be quickly verified (6ms)

Privacy – Zero Knowledge Proofs

- EY, however, has demonstrated Zero Knowledge Proofs for Ethereum on Public Ethereum - EY Ops Chain Public Edition
- In beta now with full release at the end of the year
- Allows for transaction privacy on public Ethereum blockchains
- Brings us one step closer to Blockchain as a utility
- Addresses the concerns of companies that want to use Blockchain but want transactions protected
- Addresses the use of Blockchains in consortia by protecting transactions from consortia members that are also competitors

Caveats of Zero Knowledge Proofs

- Will require excellent data provenance to verify and validate data against source systems
- The issue is that when you implement this:
  - You put together an excellent system to use Blockchain to transact data
  - However you put the onus of verifying and validating transaction data back on source systems
- Data provenance and provable validation is key to addressing this issue
- Zero Knowledge Proofs, Minimum Necessary Data, and Data Provenance are key to implementing Privacy in Blockchains

Security

- Blockchain puts an emphasis on network security
    - Routing (Border Gateway Protocol)
    - Domain Names/Domain Name Services
    - Anti-Spoofing Algorithms
    - Security-focused development activities
    - Strong Identity management
    - Strong Vulnerability management
    - Segmentation of transactional systems like Credit Card Processing
    - Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI)

- As we learned a few weeks ago with Ethereum private keys, we have issues with key generation as wallets have been robbed due to weak keys
- Public/Private key encryption is supposed to rely on keys that are mathematically significantly complex to reverse (called NP-complete)
- Weak implementations of key generation can cause easy impersonation and compromise of integrity of the Blockchain

Public Key Infrastructure (PKI)

- Satoshi (whoever they are) used good key generation because it's been impossible for anyone to forge the key signatures used to prove his identity
- This leads us to being able to verify and validate the process by which the public and private keys are generated to do two things:
    - Issue provably strong keys
    - Identify weak keys when a vulnerability is found in the key generation algorithm implementation (see Heartbleed)

Dispute Resolution

- Need to have an agreed upon method to settle disputes and amend transactions
- There will always be disputes - need a neutral agreed upon method to settle disputed transactions
- You cannot have consortia or cooperation without this

Integration and Interoperability

- Need to have ability to securely transfer data to and from systems using known data elements, structures, and APIs
- Required for compliance with 21st Century CURES Act and Trusted Exchange Framework
- Also required to interchange data between your source systems, EMRs, and ERP systems

Change Management

- Change and evolution are inevitable
- Due to security, functionality, and privacy requirements, there will need to be coordinated upgrades and changes to the infrastructure to support new needs and requirements
- Esp. Encryption - always assume that within 5 years someone will present a way to completely invalidate your implementation at DEFCON or Black Hat
- Changes will need to be coordinated amongst consortium members to prevent adverse effects

Performance

- You need strict service level agreements for transaction times, consensus, and API response
- You also need strict SLAs on vulnerability management and patching - restrict it to a strict number of days to prevent potential issues
- You also need to monitor performance to make sure that there are no potential upstream or downstream issues with systems causing longer transaction times

Compliance

- You’re not going to have strong regulatory compliance without:
  - Strong privacy
  - Security
  - Data provenance
  - Auditability
  - Change management
  - Integration,
  - Interoperability and dispute resolution
  - It’s not about the specific regulations.
  - Most of them focus on these core items: HIPAA PCI-DSS HITECH GAAP

What business value does this bring us?

- The ability to effectively move this toward privacy-focused and decentralized consortia
- The tools we need to build a repeatable strategy based on Blockchain
- The ability to do so while meeting regulatory requirements

Questions

David Houlding CISSP CIPP
Principal Healthcare Lead | Microsoft
Chair | HIMSS Blockchain Task Force
Advisor | British Blockchain Association
David.Houlding@Microsoft.com
LinkedIn/In/DavidHoulding
@DavidHoulding

Microsoft

Mitch Parker CISSP
Executive Director,
Information Security and Compliance,
Indiana University Health
Mitchell.Parker@IUHealth.org
LinkedIn/In/MitchParkerCISO

HEALTH