Security Challenges in Blockchain

Thirumani Solaiappan, CISM

Email: thirumani.solaiappan@gmail.com

https://www.linkedin.com/in/thirumanisolaiappan/

http://thirumani.blogspot.in/

ISACA®
Trust in, and value from, information systems
Bangalore Chapter

Disclaimer

- All the material presented here are done in my personal capacity. None of it has any implication whatsoever to the company I work for. This presentation is my effort to share my own thoughts with the larger ISACA community and to have some intellectual conversations with all of you.

Agenda

- Security Challenges in Blockchain
- Some ways to improve Security of Blockchain
- Focus areas for Security Processes used with Blockchain

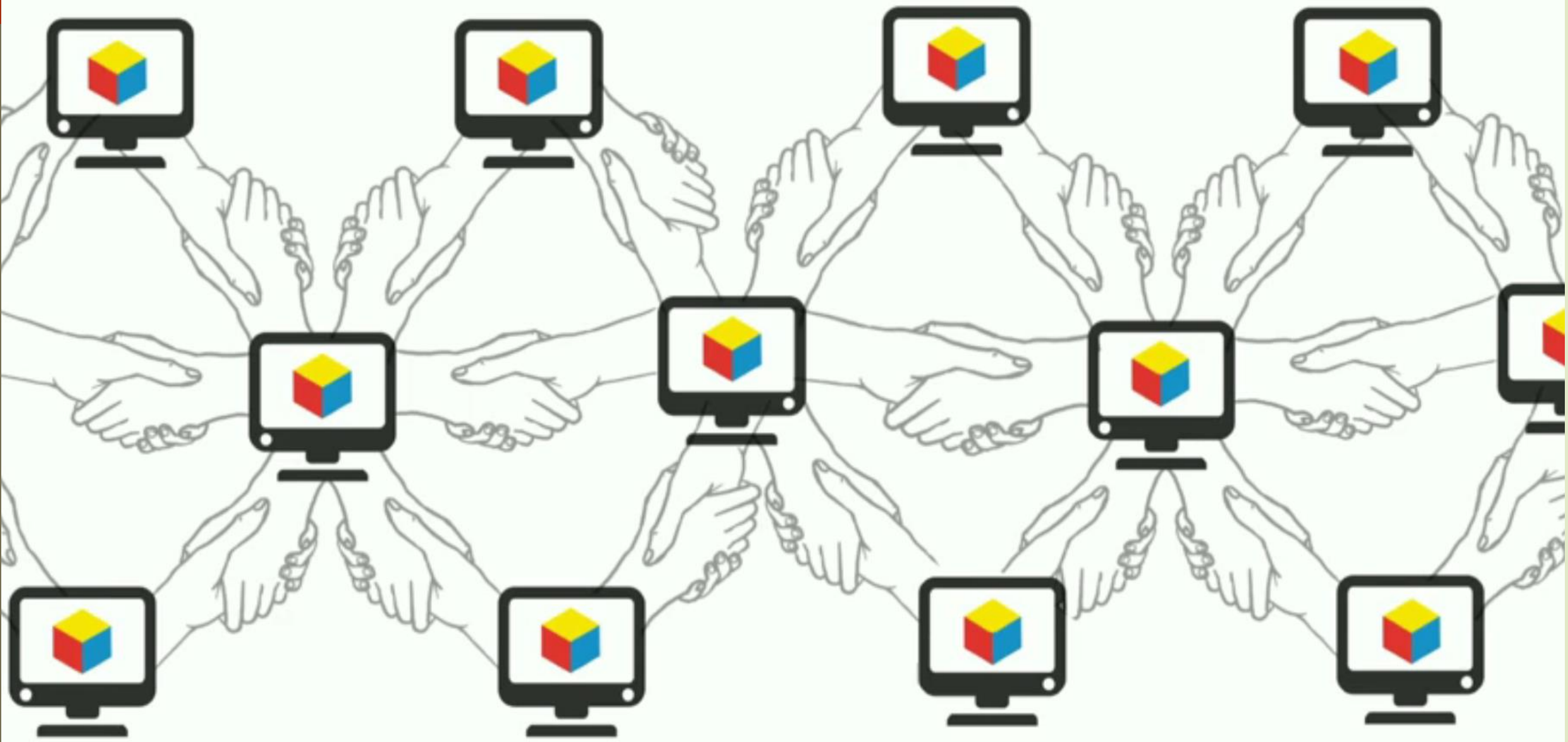
Boundaries for this presentation

- Mostly talk about Permissioned Blockchain
- No talk about legal aspects
- Not comprehensive

What is Blockchain

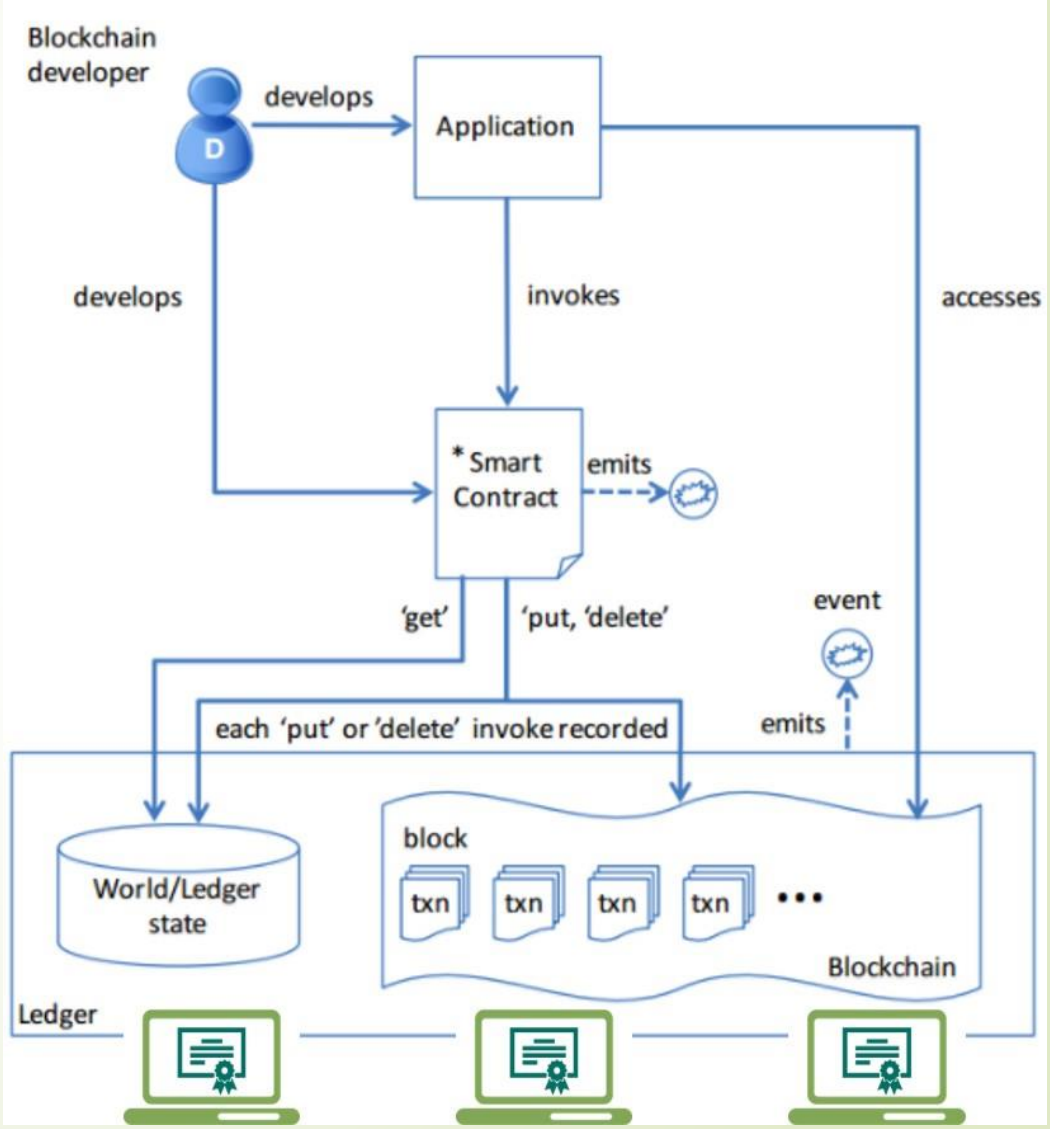
- A distributed peer-to-peer data store for all kinds of data
- It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way".
- Blockchain is a decentralized database that stores a registry of assets and transactions across a peer-to-peer network
- A Blockchain is a system for maintaining distributed ledgers in a way that allows organizations who might not fully trust each other to agree on ledger updates.
- Blockchain is the next generation of Internet – internet of value

THE TRUST PROTOCOL



Key Components of Blockchain

- Applications
  - Deals with User
  - Query Blockchain
  - Invoke Smart contracts
  - Handle events
- Smart Contracts
  - Business Logic
  - Emits events
- Blockchain Infrastructure
  - Ledger
  - Nodes
  - Administration



Challenges in Blockchain Implementations

- Complexity of the technology is a risk – one misstep, the entire infrastructure falls apart
- There is strength in numbers – more nodes make it more secure – corruption and other human factors can play against this
- As the system grows, data storage and transaction speed issues gain prominence
- Safeguarding crypto keys is important – hackers focus on stealing keys

Challenges in Blockchain Implementations

- Endpoint vulnerabilities – risks while accessing the Blockchain data.
- Vendor risks - security of 3rd-party Blockchain apps and platforms are no greater than the trustworthiness of their vendor - especially when using smart contracts
- Untested code – like in the case of DAO attack
- Power required per transaction is far higher than any other technology

Security Challenges in Blockchain Implementations

- Human error – vast majority of breaches
- Network security is the weakest link
- Inherent Security Concerns - Attacks like the '51% attack'
- No standards or regulatory guidelines defined
- Storage security

Improving the Security Posture

- Make sure you keep both AV and operating systems updated
- Use a good antivirus for Windows and Android devices
- Run anti-malware scans regularly
- Never store your Blockchain keys in a text file, Word Document, or other file
- Never include either of your keys in the body of any email to anyone for any purpose

Improving the Security Posture

- Dealing with lack of standards
  - Forced regulation and standards where required
  - Self-imposed regulation and standardization among consortiums in areas where innovation is necessary
  - No regulation or standardization for internal stuff – ie)Blockchains built in-house and only used internally within the organization.

Improving the Security Posture

- Dealing with DAO attacks
  - Heavy peer-review of code before deployment.
  - Smart contract testing performed by independent testing facilities.

Focus Areas for Security Processes

- Confidentiality
  - Integrate with identity management system
  - Certificate revocation management
  - Data protection at rest
- Availability
  - Ledger check-pointing
  - Archiving and pruning process
  - Backup and recovery process

Focus Areas for Security Processes

- Private Key handling process
  - Different admins for key and systems storing keys
  - Change private keys when admins leave organization
  - Securing private keys – use of HSMs can improve security
- Membership management process
  - Include approval flow
  - Innovative proof mechanisms improve robustness
- Configuration management
  - Smart contract
  - Application Code

Q & A