What is Blockchain?

- Database shared across a network of computers.
- Data uploaded to the blockchain is validated by other computers in the shared network.
- When data is added to the blockchain, it is converted to a complex string of code and is nearly impossible to forge, alter, or erase.
- Blockchain databases can be publicly viewable or private networks accessed by coded key.
Types of Distributed Ledgers

“Blockchain”

Permissionless, Public, Shared Systems

Permissioned, Public, Shared Systems

Permissioned, Private, Shared Systems

Derived from “Blockchain Beyond the Hype,” World Economic Forum, April 2018
How Blockchain Works

Someone requests a transaction to upload or modify data.

The requested transaction is broadcast to a shared network consisting of different computers.

The shared network of computers validates the transaction and the user’s status.

Once verified, the transaction is combined with other transactions to create a new block of data.

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

The transaction is complete.
Blockchain Opportunities

- **Structural Security**
  - The network’s structure of data validation through consensus of a majority of computers in the network means a hacker would need to break into not one computer, but multiple computers.

- **Eliminates a Single Point of failure**
  - No single function or part of the database can take down the entire network.

- **Redundancy**
  - Multiple file copies mean that data are less likely to get lost or irrevocably altered.
  - Blockchain creates an immutable record of all past data transactions. Even if data is modified, past versions will still permanently exist on the network.

- **Collaboration**
  - Large numbers of participants can collaborate on a blockchain in a decentralized manner.
Blockcchain Challenges

- **Privacy**
  - All data is viewable to anyone who can access the database

- **Data Theft, Corruption and Authentication Issues**
  - Wherever users interface with the blockchain, there are vulnerabilities
  - Cryptographic keys are kept on users’ computers and vulnerable to theft

- **Stewardship and Governance**
  - Who owns and has access to the data?

- **Vendor Stability and Experience**
  - New industry lacks trusted, experienced vendors and support services

- **Performance and Cost**
  - Energy requirements can be expensive and create latency and scaling issues

- **Complexity**
  - Can be difficult for non-technical personnel to understand new technology
Blockchain Considerations

- Are you trying to remove intermediaries or brokers?
- Do you intend to store a large amount of non-transactional data?
- Do you want/need to rely on a trusted third-party?
- Are you managing contractual relationships or value exchange?
- Do you required shared write access?

Derived from “Blockchain Beyond the Hype,” World Economic Forum, April 2018
Applicability to Elections

- **Pre-Election**
  - Estonia uses blockchain keyless signature infrastructure (KSI) with its Oracle cloud database to store citizens’ records and verify identification
    - National Electronic ID: links to encrypted files that identify the owner and allow access to online banking, digital contracts, and voter registration
    - Verifies voter eligibility digitally through computer card reader, or via mobile phone and specialized SIM card

- **Election Day**
  - West Virginia: First state to allow online voting via blockchain in May 8, 2018 pilot test
  - Utah Republican Party: Used blockchain to vote in its caucuses in 2016

- **Post-Election**
  - In Sierra Leone, Swiss-based company Agora logged and verified paper ballots digitally using blockchain technology. Audit reflected official results
For more information visit:
www.dhs.gov/office-cyber-infrastructure-analysis