OHIOERC BLOCKCHAIN COMPARISONS

This document provides various comparisons that can be used when determining whether Blockchain technology might be a good fit for a particular project, or, whether existing database technology will serve the purpose. It contains the following comparisons:

- Blockchain Advantages v. Disadvantages
- Blockchain versus Database
- Public v. Private v. Federated Blockchains

Blockchain features and functionalities mentioned throughout this document are explained in more detail in the OhioERC companion document, *Blockchain Basics: Introduction to Blockchain Concepts*.

DEFINITIONS

Blockchain: A consensus digital ledger comprised of unchangeable, digitally recorded data in packages called blocks. Each block is 'chained' to the next block using a cryptographic signature. This allows blockchains to act like a ledger, which can be shared with and accessed by anyone with the appropriate permissions. Blockchains are maintained across multiple computers, or nodes, that are linked in a peer-to-peer network.	**Database:** An organized collection of structured data, typically stored electronically, and controlled by an administrator. Data in databases can be accessed, managed, modified, updated, controlled, queried, and organized.

BLOCKCHAIN ADVANTAGES V. DISADVANTAGES (BY FEATURE)

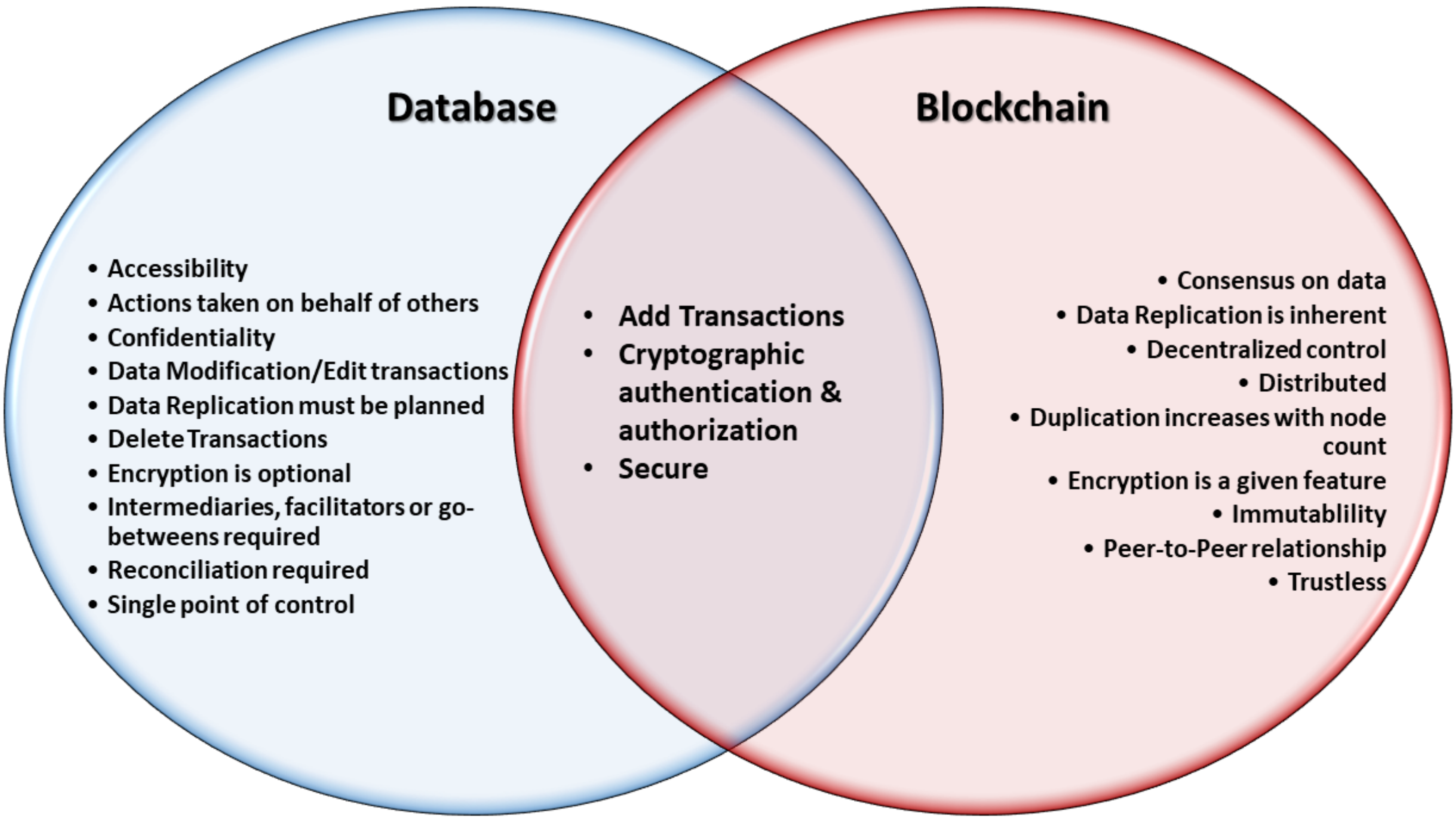
ADVANTAGES	DISADVANTAGES
Immutability	
Less risk of fraud	Incorrectly entered data cannot be fixed
Transactions are irreversible – each change is a separate transaction	Transactions are irreversible
Audit trail	Records disposition cannot be applied
Hackers have to compromise at least 51% of the nodes to be successful in altering data	Data privacy concerns since information cannot be deleted
Trustlessness	
Reduces number of parties involved in a transaction	Potential loss of jobs or need to retrain employees in industries that serve as 3rd parties
Does not require a trusted, single 3rd party intermediary	
Removing 3rd parties reduces costs of transactions	
Security	
Transaction not accepted and added to block until validated	Lacks confidentiality since anyone with a node can see the transactions
Private Keys	If private key lost, information not recoverable (no "password reset")
The more nodes that join the blockchain, the more secure it becomes	Private security keys could slow access to public records
	Vulnerable to attacks if a single party gets control of a majority of nodes
Distributed (not Centralized)	
No single point of failure (system not affected if one node goes offline)	Speed of transactions may slow as the chain gets larger since each node has a full replica of the data, which is never reduced
Multiple copies exist	May become too large for a party to store, creating risk of losing nodes
Transactions verifiable by a large peer-to-peer network	Energy inefficient – as storage requirements increase, the energy necessary to operate increases, as does environmental ramifications Technology too new to demonstrate permanence or migration if necessary

DATABASE V. BLOCKCHAIN

Database	Blockchain
Reconciliation required	Consensus on data
Add, delete, edit	Only add new transactions
Rely on one or only a few servers, which leave it vulnerable to technical failure or cyber attack	Distributed across nodes, no single point of failure
Single point of control. Administrators and designated users determine who has access and what level of access is assigned.	Decentralized control (public blockchains)
Gateways & middlemen involved for external transactions	Peer-to-Peer relationship (removes middleman)
Encryption is optional	Encryption is a given feature
Actions can be taken on behalf of others	Authentication & authorization
Backups must be provided for manually	Resiliency and availability increase with node count
More scalable, faster speed of transactions	Slower speed of transaction (compared to a database) due to ever growing number of blocks and nodes for verification and consensus to run through
Sufficient if everyone with access has authority to write or edit data	Useful if you can't trust everyone adding to the node
Create, Read, Update, and Delete (CRUD) operations means that data can be updated or replaced	Only Read and Write operations available
Able to be deleted per retention schedule	No ability to delete per retention schedule
Public access. Compliance with public records law more feasible over time.	More difficult to provide public access[1], upon request and over time, due to private keys or potential of keys being lost.
More seasoned technology may be easier to implement and maintain	May be harder to implement and maintain since it is new technology and may not be able to be integrated or "added on" to existing technology as easily.

[1] The word "transparency" has a different meaning in reference to blockchain than in reference to public records. In the realm of public records, transparency refers to the availability of records, which lend insight into the organization. Whereas in blockchain, transparency refers to the openness, or control of, the technology process. The OhioERC feels that documents stating that blockchain aids in transparency is confusing, even contradictory, to public records use of the term. Therefore, while other documents may use the word transparent when discussing blockchain, the OhioERC has removed the word all together to avoid potential confusion.

DATABASE V. BLOCKCHAIN (VISUALIZED)



PUBLIC V. PRIVATE V. FEDERATED BLOCKCHAIN

Public Blockchain: Anyone can read it or write to a public blockchain. All participants follow the blockchain protocol (rules) that have been pre-defined and built into the structure.	**Private Blockchain:** Participants need to have access permissions, and what they can do with the blockchain can also be limited by permissions. A single organization makes these decisions.	**Federated/Consortium Blockchain:** These blockchains are private, but have participation from multiple organizations who all agree on permission rules. Nodes are spread across the member organizations.

PUBLIC V. PRIVATE V. FEDERATED BLOCKCHAIN (CONTINUED)

Feature	Public Blockchain	Private Blockchain	Federated/Consortium Blockchain
Computational/validation time - Faster (i.e. cost-effective)		✓	✓
Computational/validation time - Slower	✓		
Consensus protocol	✓	✓	✓
Data redundancy - High	✓		
Data redundancy - Low		✓	
Data redundancy - Mid-level			✓
Immutability	✓	✓	✓
Levels of access and operation - All participants have equal read/write authority	✓		
Levels of access and operation - Different levels and functionality can be set		✓	✓
Network of nodes - Decentralized, peer-to-peer	✓		
Network of nodes - Governed by a single entity		✓	
Network of nodes - Partially decentralized, multiple permissioned organizations			✓
Permissions - Administrator needed to join the network, identities known		✓	✓
Permissions - Anyone can join the network, anonymous	✓		
Privacy - Lack of privacy	✓		
Privacy - Permissioned access to data, increased privacy compliance		✓	✓
Security - Increased security because multiple entities agree to rules and create stronger consensus			✓
Security - Less secure because it is owned and controlled by a single entity, which can make alterations		✓	
Security - Stronger due to larger network, more consensus (harder to hack)	✓		
Transactional cost - Higher	✓		
Transactional cost - Lower		✓	
Transactional cost - Mid-level			✓

PUBLIC V. PRIVATE V. FEDERATED BLOCKCHAIN (VISUALIZED)