UNT®

UNIVERSITY
OF NORTH TEXAS®

EST. 1890

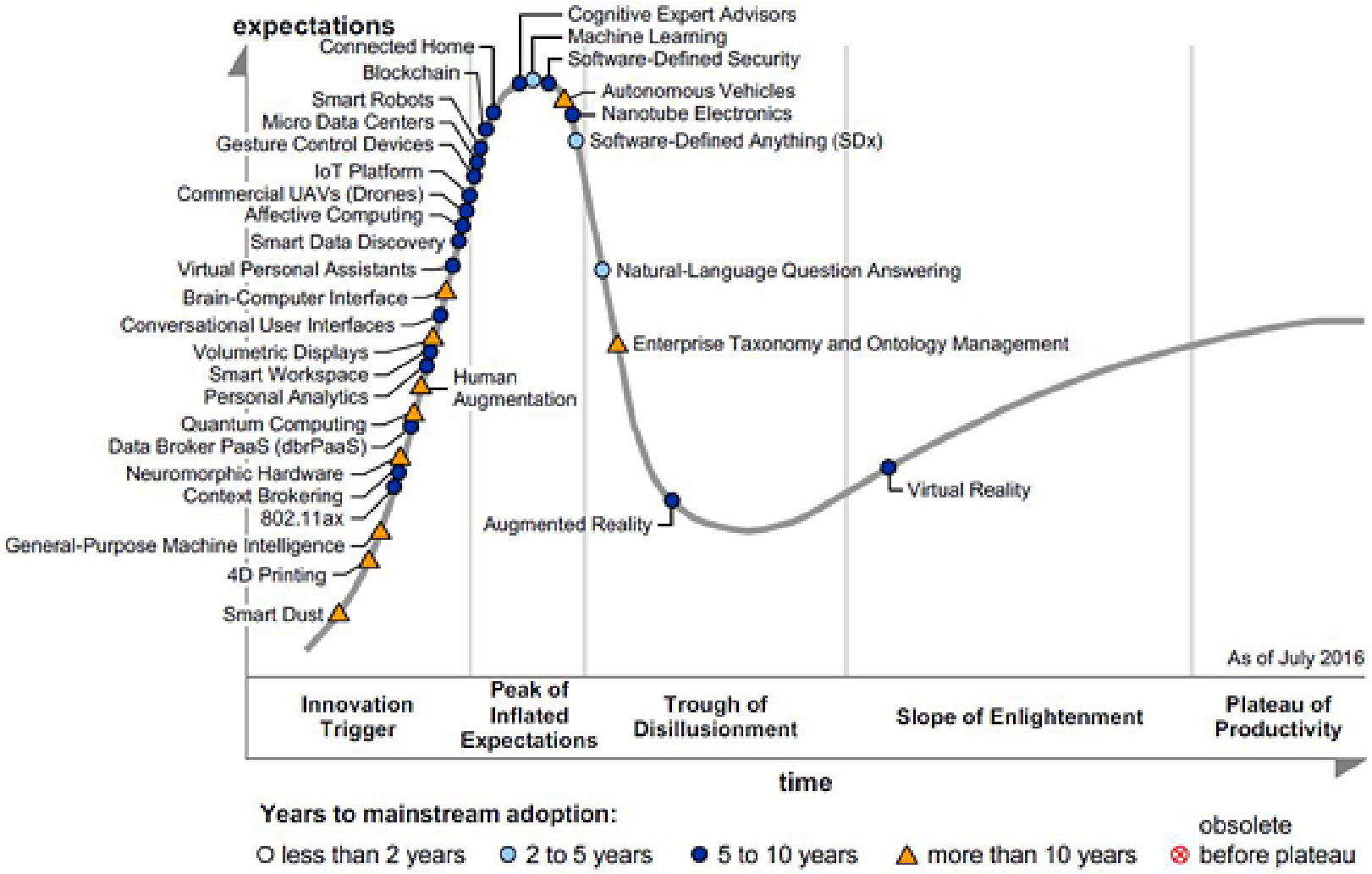
Blockchain: Where are We and Where are We Heading?

Objectives

- Define the underlying technologies of blockchain
- Describe some shortcomings of blockchain
- Describe the accounting profession's interest in blockchain
- Examples of current and early adoption
- Considerations for adoption within your organization

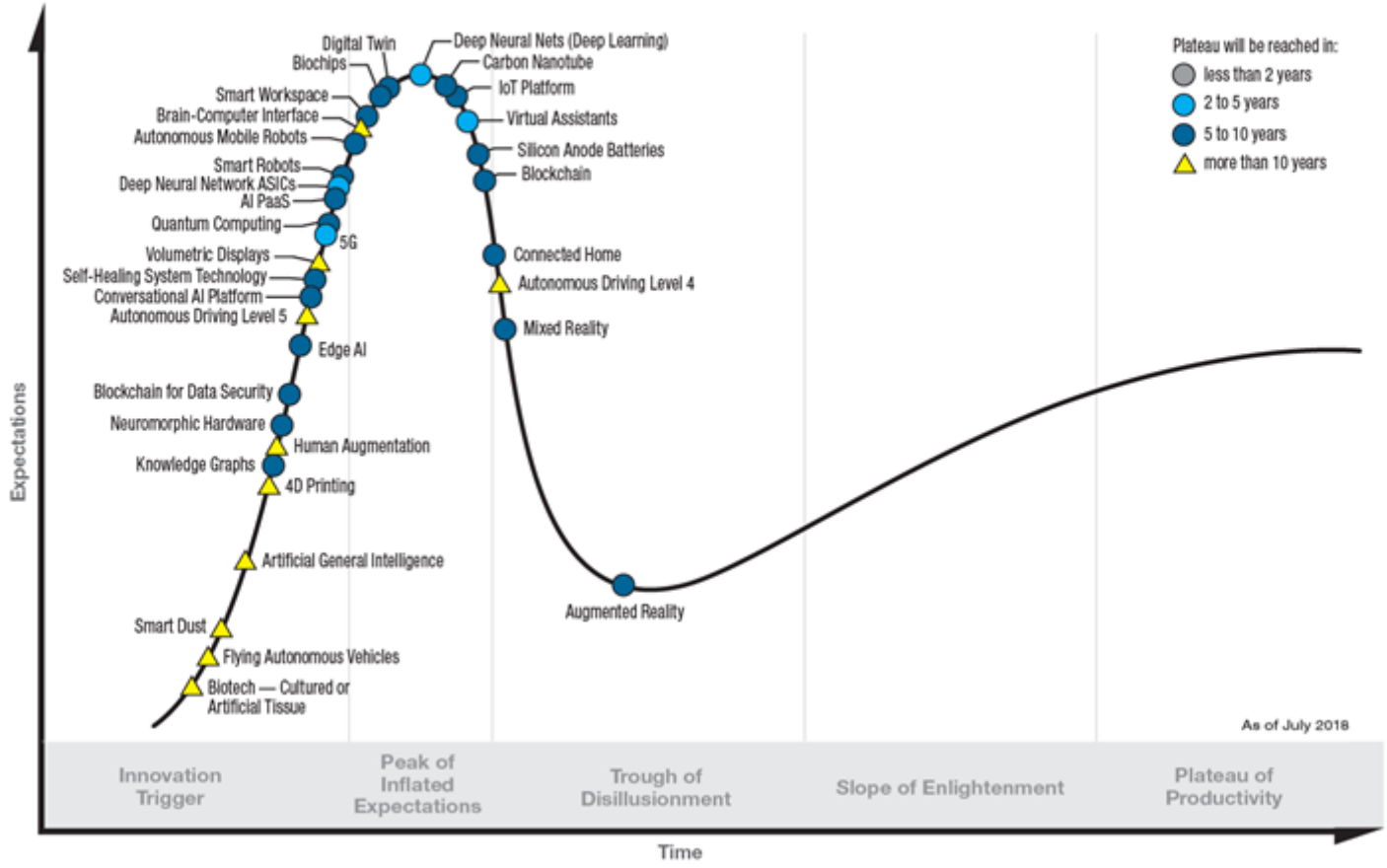
What is Blockchain?

- "…[blockchain] offers a sweeping vista of opportunity to reimagine how the financial system can and should work in the Internet era…" (Marc Andreesen 2014)
- "Blockchain technology will revolutionise far more than money: it will change your life." (Dominic Frisby 2016)
- "Blockchain technology is the most significant Invention since the internet and electricity" (Mark Metry 2017)
- "There are no good uses for blockchain" (Kai Stinchcombe 2018)
- "[O]ne of the most overhyped technologies ever" (Nouriel Robini 2018)



Source: Gartner (July 2016)

Hype Cycle for Emerging Technologies, 2018



Let's Talk About Bitcoin

- Suppose I want to transact with a seller, but I don't necessarily trust the seller
  - If I give you my credit card information you might steal it
  - May want to keep my identity anonymous
- Solution: Exchange through an intermediary! (such as PayPal)
  - May even be able to protect my identity from the seller
  - However, I lose the ability to interact with the seller directly (e.g., lost efficiency)
- Alternative: Pay in cash
  - Totally anonymous
  - No need for approval from a third-party
  - However, not nearly as convenient as a credit card (online transactions)
  - Second issue: Virtual cash can be copied and spent more than once
    - Double-spend problem
    - Solution: Create a unique serial number for each virtual dollar. However, we arrive at the problem again of having a central authority who must verify that serially numbered dollar has not yet been spent.

Let's Talk About Bitcoin

- Bitcoin
  - Solves the problem of anonymity (e.g., allows you to transact pseudo anonymously)
  - Allows you to transact directly without third-parties (e.g., no central authority)
- Accomplishes this with…

How does Blockchain Work?

- Bitcoin blockchain: aggregates transactions into blocks and chains them together.
- Original idea from Haber and Stornetta (1991) – Secure timestamping of digital documents.
  - Each certificate ensures the validity of the transaction
- Sophisticated application of several existing technologies.
  - Public key – private key (asymmetric) encryption
  - Hashing
  - Distributed ledger
  - Peer-to-peer consensus

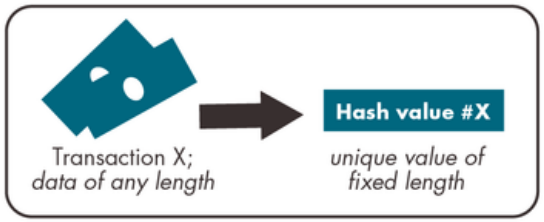
Asymmetric Encryption

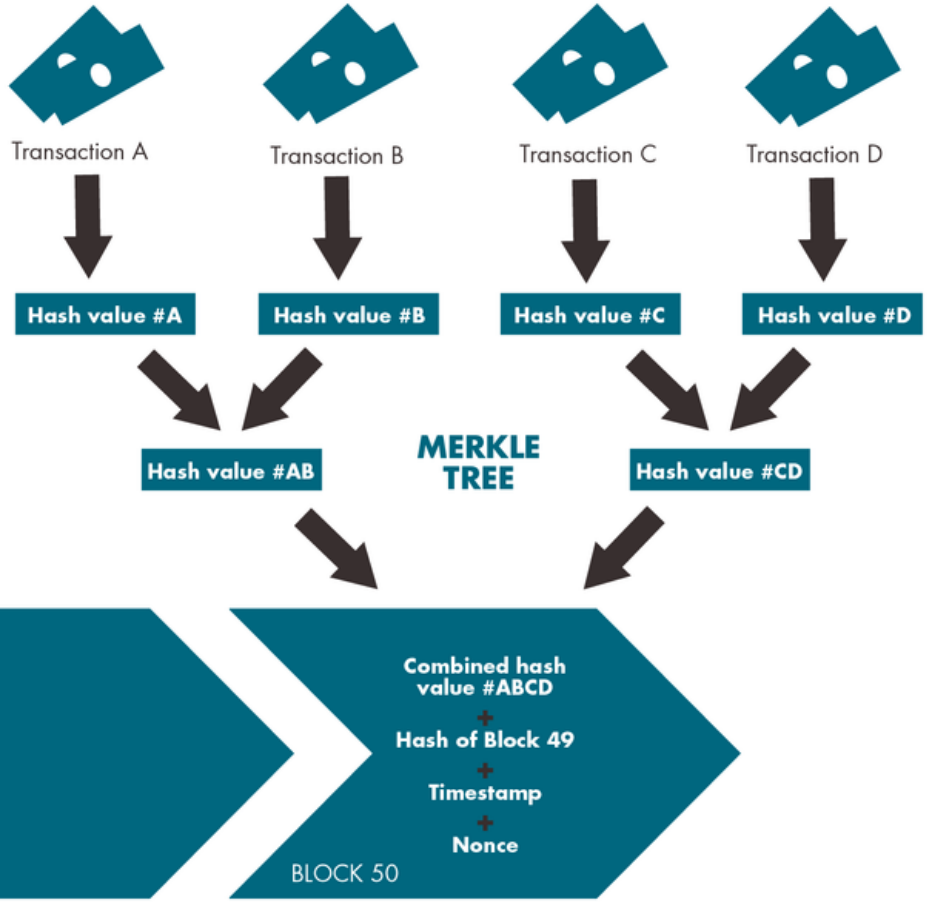
- Suppose we have two parties: Alice and Bob
- Alice enters a blockchain and wants to transact with Bob.
  - Alice has a private key and public key pair.
  - The public key is shared with every party in the blockchain network (including Bob).
    - Private key is kept (spoiler alert!) private.
  - Alice broadcasts a message across the network that she is sending $100.00 to Bob. She signs the message with her private key.
    - Four necessary conditions: (1) The asset is valid (e.g., the cash exists), (2) the asset has not be consumed/used in a previous transaction, (3) total value that comes in is the same that went out (e.g., not creating or destroying an asset), (4) the transaction is validly signed by the owner's private key
  - Members of the network, including Bob, can use the public key distributed by Alice to verify the above conditions
- Digital signature must be:
  - Verifiable
  - Infeasible to forge

Cryptographic Hash Function

- What if Alice transmits a message that she has paid Bob $100.00, but she decides she wants to change the entry to show she paid the $100.00 to Chad?
- Adopt a cryptographic hash function
- For a hash to be cryptographically secure it must satisfy three conditions:
  - Collision resistant – it is infeasible to find two values that result in the same hash
    - If $x \neq y$ and $H(x) = H(y)$, not collision resistant
  - Hiding – given the hash of a nonce and a message, it is infeasible to determine the message.
  - Puzzle friendliness – there is no strategy better than trying random values to solve for the nonce.

HOW THE BLOCKCHAIN WORKS



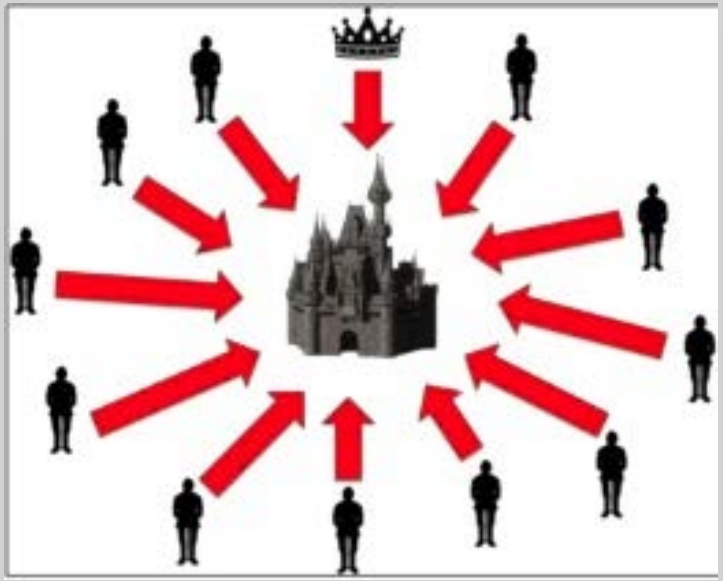


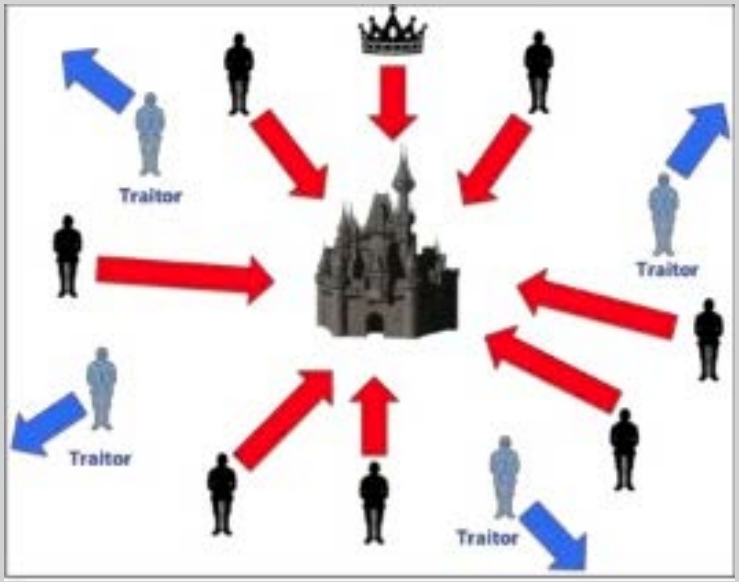
Cryptographic Hash Function

- If any value is altered within the blockchain and transmitted to other nodes, will result in an “avalanche effect”
- Examples:
  - Hello North Texas ISACA!
    - CFCCF4991C3C982AFEE33C8AFEEAD048F74BCAC2B876097231E23889A61441F4
  - Hello North Texas ISACA
    - 11CBFF72E7A824A32D0C8AE8C15FB2D7A1B0283B2246783B5F6EDCCA83CFB6BA
  - Hello north Texas ISACA!
    - FF2FD95CACA29EE452607DD18970E6CD31E802141653A149D91182DA424B0874
- Gives the blockchain the property of immutability
  - Not tamper-proof, but tamper-evident

Distributed Consensus Protocol

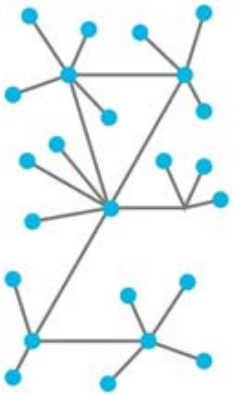
- Permissioned and permissionless blockchains
- Attempts to solve the Byzantine General Problem.





Centralized

Decentralized



Distributed Ledgers

Distributed Consensus Protocol

- The protocol must have two properties:
  - It must terminate with all honest nodes in agreement on a value.
  - The value must have been generated by an honest node.
- But what does “honesty” mean when we don’t have perfect information?
  - Impossible to know which transactions are morally legitimate.
  - How do we incentivize “honest” behavior?

Distributed Consensus Protocol

- 1. New transactions are broadcast to all nodes.
- 2. Each node collects new transactions into a block
- 3. In each round, a *random* node gets to broadcast its block
  - Probability is proportional to some resource in a PoW system
  - Bitcoin blockchain uses a hash puzzle to proxy for computing power
    - (1) Must be difficult to compute (e.g., puzzle friendliness)
    - (2) Parametizable
    - (3) Trivial to verify
- 4. Other nodes accept the block only if all transactions in it are valid (unspent assets, valid signatures).
- 5. Nodes express their acceptance of the block by including its hash in the next block they create.
  - Newly created block is added to the longest chain

Distributed Consensus Protocol

- Other consensus protocols include:
  - Proof of Stake
    - Avoids energy expenditure of PoW
    - Randomly assigns block leadership to participants proportional to their stake in the system
    - Vulnerable to gaming through forking
  - Proof of Elapsed Time
    - Nodes are required to wait for a randomly determined time period (determined by a trusted code), and the first one to complete the designated waiting period wins the new block.
  - Proof of Importance
    - Similar to PoS, but attempts to discourage gaming by randomly assigning block leadership to participants proportional to their activity (e.g., number of transactions, amount spent, etc.).
  - Proof of Activity
    - Hybrid of PoW and PoS

Is Blockchain Invincible?

- Several vulnerabilities, including:
- 51% attacks
  - Targets smaller cryptocurrency
  - Usually requires a “hard fork”
- Transactional Malleability
  - Input address (where is it coming from), output address (where is it going), the asset being sent, and the cryptographic signature of the sender
    - Can’t change the transaction semantics without subverting the cryptography
    - However, can make amendments that change the transaction ID or the hash
  - If the amended transaction is accepted by the network first, the original transaction will not be accepted
  - Mt. Gox - $473 million
- Ethereum Decentralized Autonomous Organization
  - Code vulnerability. Could refund DAO tokens for Ether cryptocurrency recursively
- Bitfinex
  - Flawed code with multi-signature wallets

Applications for Accounting and Industry

- Audit – Immutable audit trail
  - However, need to be careful about ownership and existence.
  - Who controls data entry?
- Financial Services – Decreased settlement times
- Tax Authorities – Immutable ledger
  - Again, need controls around data input. Cannot verify ownership and existence
- Supply Chain Management – Complete Record
- Smart Contracts – Boolean Logic
  - Voter registration, proxy voting

Considerations moving from the bitcoin blockchain

- Inefficiency and scalability of the proof-of-work consensus protocol
  - Bitcoin blockchain allows 3.3 to 7 transactions a second
    - Visa processes 1,700 transactions a second and could process 24,000 transactions a second!
  - Bitcoin blockchain consumes 61.4 terawatts annually.
    - The same energy consumed as the entire country of Ireland.
  - Several alternative cryptocurrencies are investigating different consensus mechanisms to address shortcomings of bitcoin.
- Private (permissioned) blockchains
  - Vulnerable to Byzantine General problem
- Side deals
  - No presence on the blockchain

Considerations moving from the bitcoin blockchain

- Digital presence
  - Assets (mostly) exist in the physical world
  - To represent the physical world on a blockchain, need to input data
  - How to we verify ownership? Existence?
- Privacy
  - Users may adopt an alias (e.g., public key), but…
    - If I can see every transaction you've ever been involved in, it becomes possible that I can identify you.
- Regulatory requirements
  - Financial services industry needs to comply with anti-money laundering and know your customer laws/regulations

Examples of blockchain in practice

- Walmart
  - Prototype blockchain to identify where food-borne illnesses originated in the supply chain
- Republic of South Africa
  - Blockchain used for proxy voting
- NASDAQ
  - LINQ – Pre-IPO trading on the private market
- Overstock.com
  - Land registry joint venture hosted on blockchain

Examples of blockchain in practice

- Kodak
  - Created KodakCoin on its blockchain for photographers to license their works and receive payments
- IBM
  - Global Consent Ledger allows you to sell your personal data on a blockchain.
- Dubai
  - Blockchain powered government
  - Visa, utility bills, shipping manifests all maintained on blockchain

What Should I Consider Before Adoption?

- **Trust -** Do I trust this firm? What information do I want to share with others?
- **Consensus Models –** What consensus protocol is best suited for your business network?
- **General Controls –** Blockchains were designed to be decentralized. What entities are permitted to do what? If there is an anomaly who will spearhead the remedial process?

What Should I Consider Before Adoption?

- **Digital Asset Generation –** Who creates an asset on the blockchain? Who governs ownership? Who actually owns the shared data?
- **Authority for Issuance –** If the system is truly decentralized and distributed, how is authority assigned? Who is responsible for governance, culpability, and regulations?
- **Change Controls –** How are new members added? If members leave, do they no longer have access to shared data? How do we remove the shared information from their devices?

References for Future Reading

- Narayanan, A., J. Bonneau, E. Felten, A. Miller, S. Goldfeder (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.
- O'Dowd, A., V. Ramakrishna, P. Novotny, N. Gaur, L. Desrosiers, S. Baset (2018). *Hand-On Blockchain with Hyperledger*. Packt Publishing.

UNT®

UNIVERSITY
OF NORTH TEXAS®

EST. 1890

Thank You!

Peter Kipp, CPA, Ph.D.
peter.kipp@unt.edu