Evaluating the Feasibility of Proposed Blockchain Use Cases

Blockchain Technology: An Emerging Issues Forum

September 13, 2018

Myles Stern, Ph.D., CMA
Department of Accounting, Mike Ilitch School of Business
Wayne State University

Copyright © 2018 by Myles Stern.
All rights reserved.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Bitcoin: a true breakthrough

- Satoshi Nakamoto's brilliance was his extremely clever combination of existing technologies to tightly meet the needs of a cryptocurrency.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

The tremendous interest in blockchain

- Many other sessions at this conference will cover this.
- A November 2017 report from Deloitte captures both the interest and the controversy.
  - GitHub is an open-source software development platform.
  - 86,034 blockchain projects
    - Only about 9,400 from organizations rather than individuals
    - 26,885 in 2016 alone
    - 92% have been abandoned.

What uses are being suggested at this conference?

- REA smart contracts
- Shared ledger system for financial accounting
- Automobile registration
- Food supply tracking

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Comparing proposed uses with Bitcoin

- Bitcoin is the "proof of concept" for blockchain.
- Many proposed uses have characteristics that differ greatly from Bitcoin.
- The requirements for those uses probably differ greatly from Bitcoin's requirements.

A fundamental question

- Can a technological solution designed to closely meet a cryptocurrency's needs work well with applications that are very different?

Does Bitcoin really work?

- "Bitcoin works in practice but not in theory."
- In 2015, Bonneau and others claimed: "We do not yet have sufficient understanding to conclude with confidence that Bitcoin will continue to work well in practice . . ."

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Does Bitcoin really work?

- This remains an open question in the computer science literature.
- Perhaps Bitcoin works only because its participants believe it works, regardless of any underlying fatal flaw!

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

A suggested approach

- Identify the requirements of a specific application.
- Explain how the proposed technological solution meets those requirements.
- This has been accepted IT practice for decades.

Matching the solution to the requirements

- We must deeply understand how the technologies used in blockchain work.
  - A superficial understanding can lead to incorrect conclusions.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

What we will cover

- Bitcoin's requirements
- An overview of the technologies in blockchain
  - There's likely a very wide range of understanding among the conference participants.
- Blockchain structure and data retrieval
  - A stumbling block (*pardon the pun*) for many proposed uses.
- What about SegWit, Ethereum, and Hyperledger Fabric?

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

The cypherpunks

- Started in 1992 by Eric Hughes, Tim May, and John Gilmore.
  - Hughes wrote “A Cypherpunk’s Manifesto” in 1993.
- Led to monthly meetings at Gilmore’s company, Cygnus Solutions.
- Created mailing list with hundreds of subscribers.
  - Use of then-novel encryption methods ensured complete privacy. Ideas were shared freely.
  - Personal privacy and personal liberty were paramount.
- Based on principles in the manifesto, several proposals were made for digital cash.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

The cypherpunks

- Bitcoin is part of the cypherpunk "heritage."
  - Strong resistance to government or any other central authority
- A digital currency *could* be issued by a central authority.
- Much of the technological foundation of blockchain exists specifically to avoid having a central authority in Bitcoin.
- Many proposed uses of blockchain involve government or some other central authority.
  - Does this give you pause?

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Requirements for Bitcoin

- Scarcity to provide value
- No central authority
  - Cypherpunk legacy
- No need to trust individual participants
- Privacy through anonymity
- Prevent double-spending.
- Units must be divisible.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

How blockchain meets these requirements

- Peer-to-peer network
- Public/private key encryption
- Fully consuming the original bitcoin and providing "change"
- Hashing
- Linked blocks of transactions
- Merkle tree
- Proof of work
- Game theory and group consensus

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

How does blockchain meet these requirements?

- This is an extraordinarily complex topic.
- In an attempt to simplify, many explanations of blockchain present some wrong information!
- We don't have nearly enough time to do a deep dive into all the technical details.
  - These details are covered in the first half of my three-credit course: about twenty class hours.

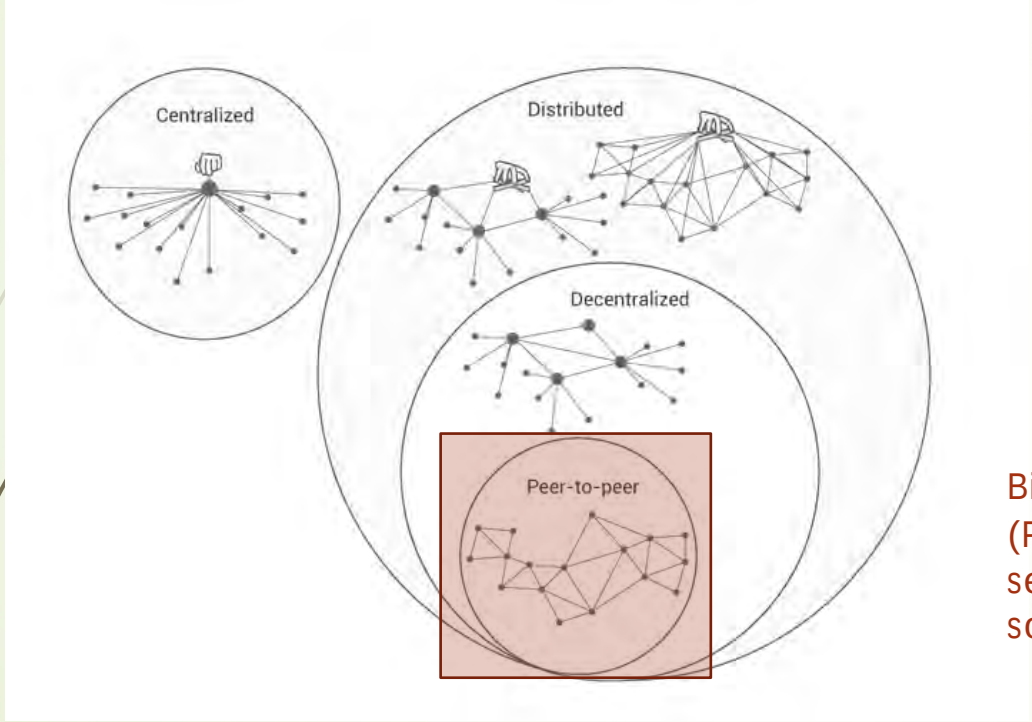
WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

How does blockchain meet these requirements?

- A high-level overview will help frame the argument.
- I will do a “deep dive” in one specific area.
- Warning: frustration ahead!
  - I won’t have time today to answer questions about details of these technologies.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Types of networks



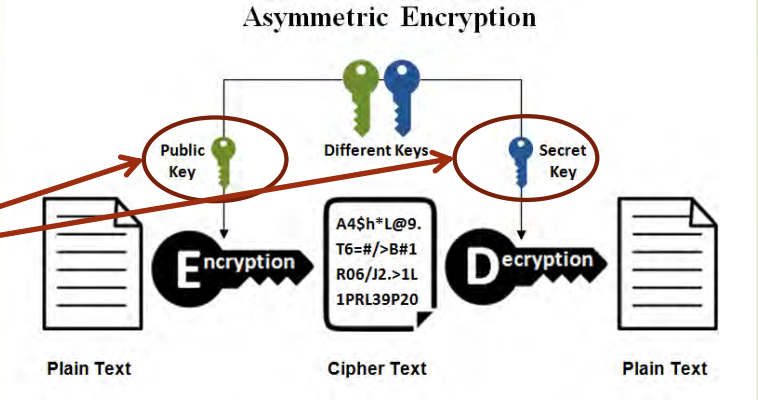
Source: https://medium.com/safenetwork/evolving-terminology-with-evolved-technology-decentralized-versus-distributed-7f8b4c9eacb

Bitcoin uses a peer-to-peer (P2P) network with no servers. All nodes are in some sense equal (peers).

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Public/private key encryption

- Invented in the 1970s
- Also called asymmetric encryption.
- Create two mathematically-related keys.
  - It's impossible to determine the private key from the public key.
- Alice publishes her public key to be used by anyone who wants to send her a secure message.
- Alice uses her private key to decrypt the message.

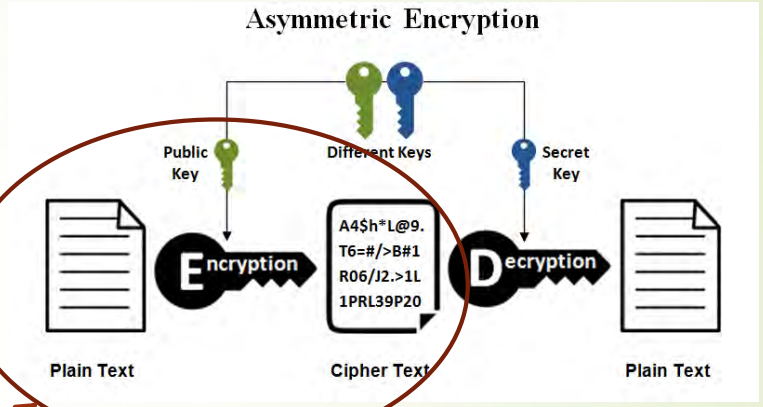


Source: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Public/private key encryption

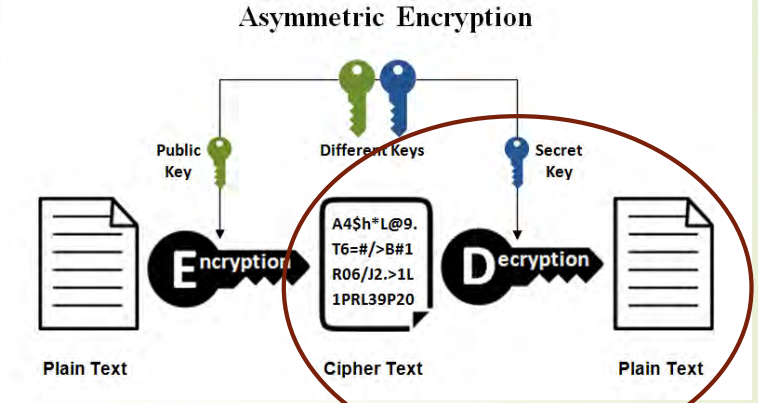
- Invented in the 1970s
- Also called asymmetric encryption.
- Create two mathematically-related keys.
  - It's impossible to determine the private key from the public key.
- Alice publishes her public key to be used by anyone who wants to send her a secure message.
- Alice uses her private key to decrypt the message.



Source: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Public/private key encryption

- Invented in the 1970s
- Also called asymmetric encryption.
- Create two mathematically-related keys.
  - It's impossible to determine the private key from the public key.
- Alice publishes her public key to be used by anyone who wants to send her a secure message.
- Alice uses her private key to decrypt the message.

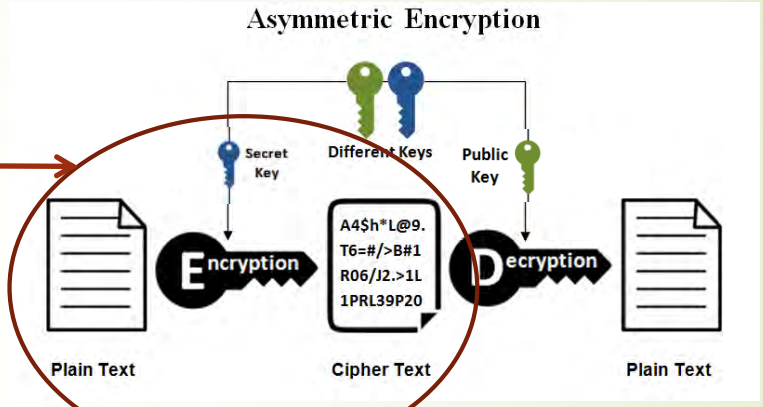


Source: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Public/private key encryption

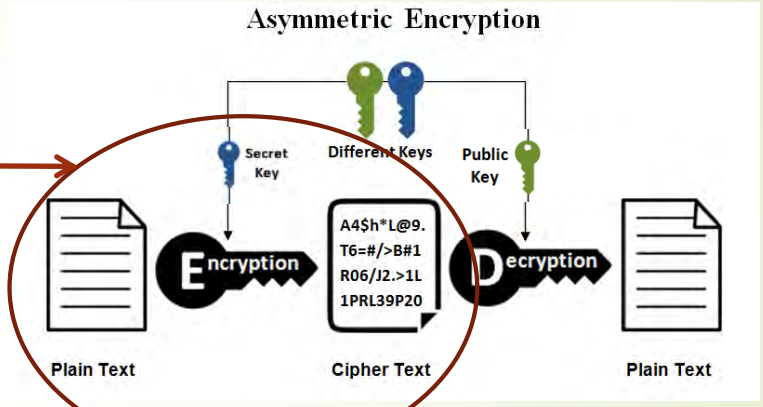
- Alice can also encrypt a message with private key and decrypt it with public key.
- Why would Alice do this? Anyone with the freely available public key can decrypt the message!



Based on: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Public/private key encryption

- Alice can also encrypt a message with private key and decrypt it with public key.
- Why would Alice do this? Anyone with the freely available public key can decrypt the message!
- Allows Alice to securely sign a document, proving that it came from her.

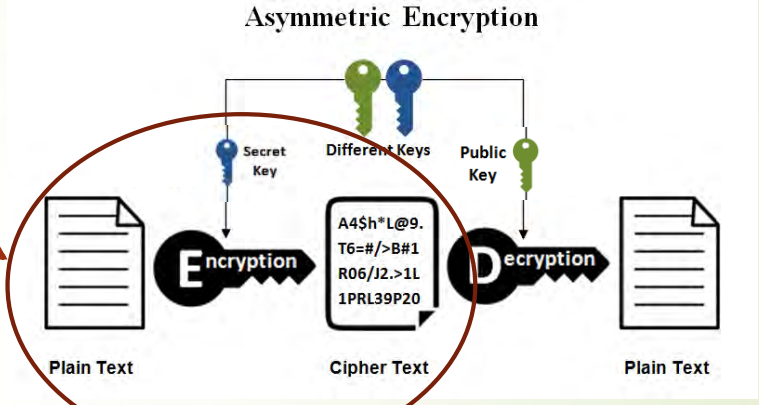


Based on: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Public/private key encryption

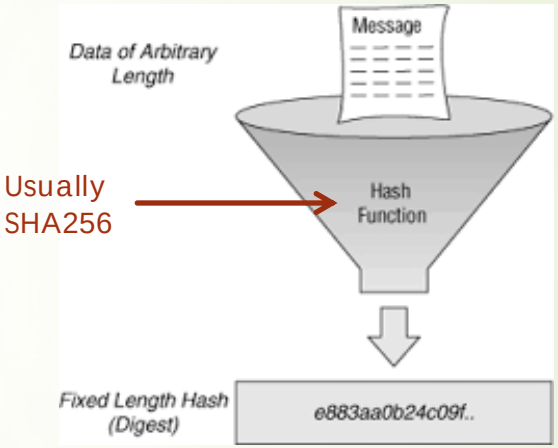
- Alice uses her private key to securely sign a transaction to move her bitcoin to someone.



Based on: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Hashing

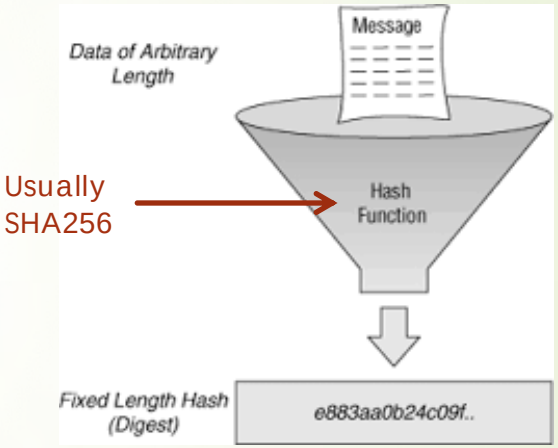
- Take a message (string of bits) of arbitrary length.
- Mathematically transform it into a digital "fingerprint" (hash) of shorter and fixed length.
- Used in many places in Bitcoin.
- Bitcoin primarily uses a hash known as "SHA256."



WAYNE STATE UNIVERSITY
MIKE ILITCH SCHOOL OF BUSINESS

Hashing

- Hashing is irreversible.
- There are 2^256 possible hashes. This makes a collision (two different messages with the same hash) exceedingly unlikely in practice.
- Used in multiple places in Bitcoin.
- SHA256 is not predictable: there's no short-cut to obtaining the hash.



WAYNE STATE UNIVERSITY
MIKE ILITCH SCHOOL OF BUSINESS

Bitcoin transactions

- Most transactions move bitcoin from one or more input transactions to one or more output "addresses."
- Alice wants to send Bob 5 BTC.
  - She will take this amount from a previous transaction that moved bitcoin to her.
- Bob generates a private/public key pair.
- Bob hashes the public key and sends the hash to Alice as the "address" to which the bitcoin should be sent.
- Alice signs the transaction with her private key corresponding to the previous transaction.
  - If Alice looses the private key, she can never spend the bitcoin!

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

A simple transaction: Alice sends bitcoin to Bob

- Input: pointer to an output of an earlier transaction
  - Transaction 123456, index 1
  - That output had delivered 8 BTC to Alice pseudonymously at "address" xxxxxx.
- Outputs
  - 5 BTC to Bob at address yyyyyy.
  - 2.99999 BTC "change" to Alice at a new address zzzzzz.
  - The remaining 0.00001 BTC is a transaction fee.
- Alice signs the input using her private key that corresponds to address xxxxxx.
- Note that Alice's original 8 BTC were consumed.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Bitcoin transactions

- Average size is about 250 bytes.
  - Very rarely over 900 bytes.
- Some other proposed uses would need to store much more data.
- This is yet another issue to consider.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Bitcoin wallets

- Transactions are generally initiated through client "wallet" software.
  - The wallet holds bitcoin addresses and corresponding private keys (proof of ownership)
  - Wallets can be a significant potential point of weakness in the Bitcoin structure.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Blockchain

- Shared public ledger that contains all verified Bitcoin transactions
  - Only wallet clients maintain spendable *balances*. They are not stored on the blockchain.
- The integrity of the blockchain is enforced by cryptography and group consensus among the nodes on the network.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Adding transactions to the blockchain

- A miner is a full node on the Bitcoin network.
  - Not all full nodes are miners.
- Miners assemble transactions into blocks.
- Miners compete to add the next block of transactions to the blockchain.
  - Until August 2017, there was a 1 MB limit on block size.
  - May ignore a transaction if its fee is too low.
  - By design, a new block is added about every ten minutes.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Adding transactions to the blockchain

- Miner collects a reward (12.5 BTC since July 9, 2016) and any transaction fees.
  - Reward was initially 50 BTC.
  - Reward is halved every 210,000 blocks or about every four years.
  - A “satoshi” is the smallest unit of bitcoin that currently can be spent.
    - 1 BTC = 100,000,000 satoshis
  - Estimate is that reward will go to zero in 2140, because you can’t have less than one satoshi as the reward.
- 21 million BTC will have been mined by 2140.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

What's in a block?

- Header
  - Hash of previous block
  - Hash of "all transactions" in the block
  - Other fields
- Transactions
- Hash of this block that incorporates
  - Hash of previous block
  - Hash of "all transactions"
  - Proof of work: solution to a difficult puzzle

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Adding transactions to the blockchain

- Proof of work: solving a difficult puzzle
  - Find a number, called a “nonce.”
  - Hash the nonce, the hash of the prior block, some other header data, and the hash of all transactions in the current block.
  - The resulting hash has must have a numeric value less than a number called the “difficulty” of the proof of work.
    - The difficulty is adjusted periodically to keep the time between successive blocks about ten minutes.
  - Requires enormous computing power.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Adding transactions to the blockchain

- When a miner solves the puzzle, it broadcasts the new block to the network.
- Each other full node verifies the entire block.
  - Verifies each transaction in the block.
  - Verifies the hash for the new block.
  - If verified, adds the block to its local copy of the blockchain and rebroadcasts the block.
  - If verification fails, the node simply ignores the new block.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

How a miner creates new bitcoins

- "Coinbase" transaction
  - First transaction in a block
  - Created by miner to collect the block reward (new bitcoin, currently 12.5 BTC) and transaction fees
  - No inputs
  - Includes arbitrary data

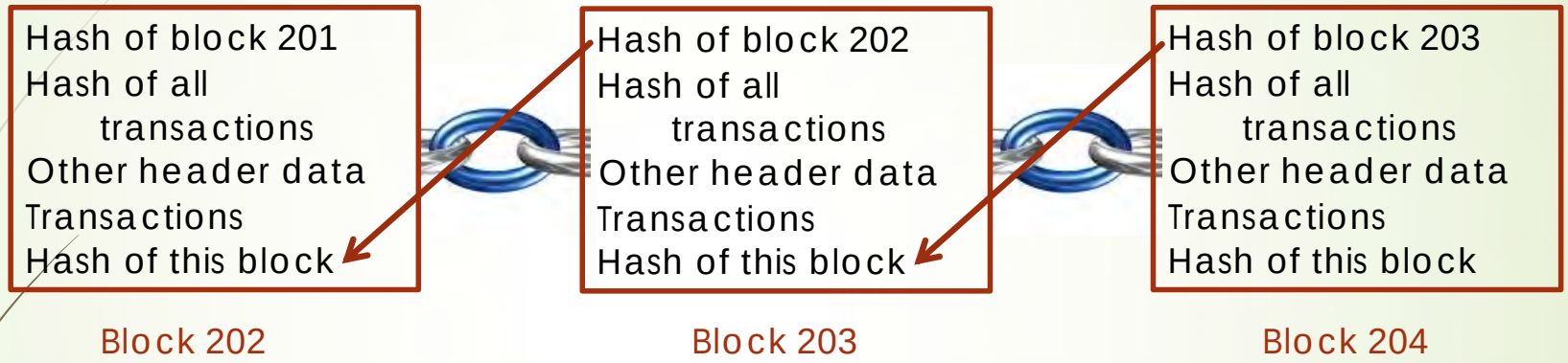
WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Genesis block

- First block in the blockchain
- Created by Satoshi Nakamoto
- Has only a single, coinbase transaction
- Refers to a January 3, 2009 article in the *London Times*: "Chancellor on brink of second bailout for banks."
- The first 50 bitcoins are unspendable.
  - 16 additional bitcoins have since been sent to this unspendable address as tributes to Satoshi Nakamoto.

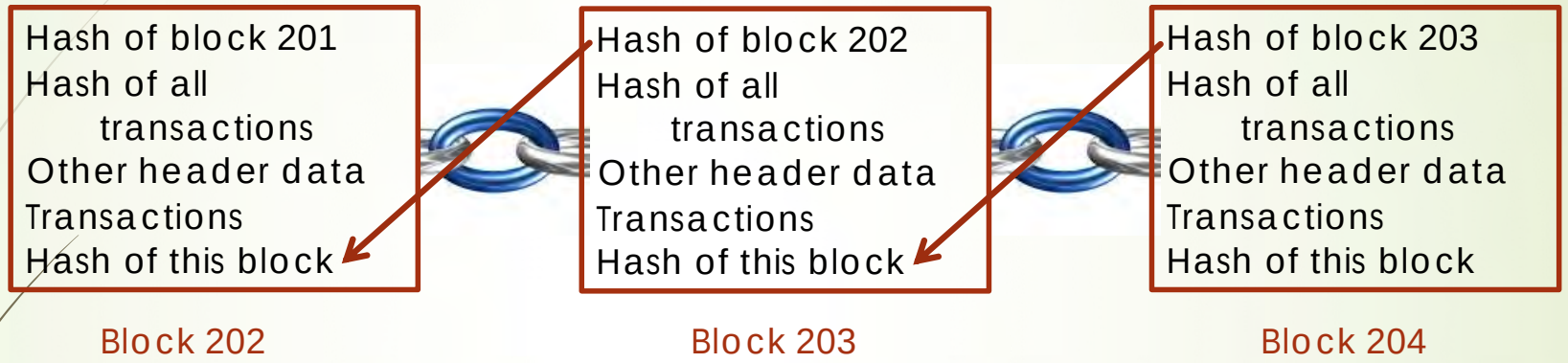
WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

How blockchain works



WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

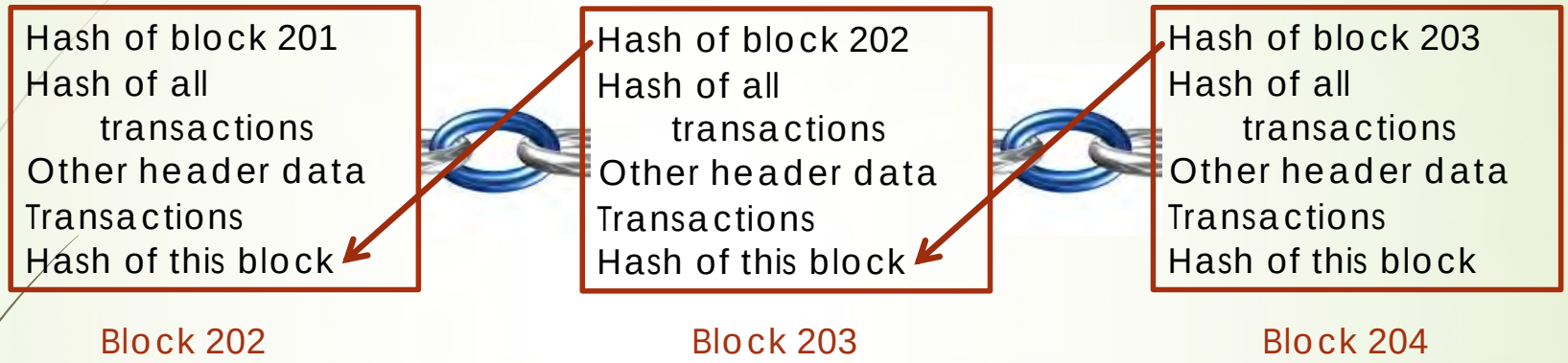
How blockchain works



A transaction is changed in block 202. ➡ The hash of all transactions in block 202 won't match. ➡ The hash of block 202 is wrong. ➡ The hash of block 203 is wrong. ➡ The hash of every subsequent block is wrong.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

How blockchain works



A transaction is changed in block 202. ➡ The hash of all transactions in block 202 won't match. ➡ The hash of block 202 is wrong. ➡ The hash of block 203 is wrong. ➡ The hash of every subsequent block is wrong.

How will the transaction change be detected?

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

How will the transaction change be detected?

- The blockchain is *not* immutable. Rather, any change is readily detectable.
- But will the change actually be detected?
- Heads up: This is an important question that should be considered further.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Gee, blockchain is really fast!

- Here's the hash of an old transaction. This hash is used as the transaction ID (txid).
  - 287d49a84bef4eeb087d6288b3cc63543243bb81dd614be8f0d7c51b1598deae
- Let's find this transaction on blockchain.info.
- Transaction details come up immediately.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

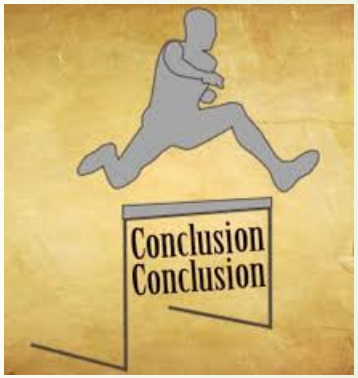
Gee, blockchain is really fast!

- When a new transaction is broadcast to the network, all full nodes verify it.
  - One step is checking to make sure the bitcoin in the input has not already been spent.
- This verification appears to happen quickly.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

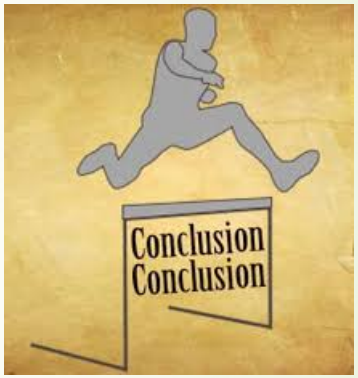
Jumping to a conclusion

- If we can quickly find a transaction by its txid and if we can quickly determine whether a new transaction is a double-spend, then we can quickly retrieve any data from the blockchain.



Jumping to a conclusion

- If we can quickly find a transaction by its txid and if we can quickly determine whether a new transaction is a double-spend, then we can quickly retrieve any data from the blockchain.
- Hold on! Is this conclusion justified?



WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Structure of the Bitcoin database

- Currently, about 180 GB
- Contains four types of data
  - The actual blocks of data
  - blocks/index: metadata about each known block, including a pointer to where the block is stored
    - Optionally includes an index to all transactions in the block
  - chainstate: compact representation of all current utxo's and some metadata about the transactions that created them.
    - Utxo: Unspent transaction output
    - Sufficient to check for double-spending
  - blocks/rev: undo data to remove a block from the chain

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Why the database structure matters to us

- We're doing a deep dive here.
- Technical details are important when evaluating proposed blockchain use cases.
  - There are so many technical details.
  - It's a challenge to know which details might impact suitability for a specific application.
    - You have to understand *all* the details.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Why the database structure matters to us

- "Blocks/index" lets you quickly locate a specific transaction by its txid.*
  - *Transaction indexing is optional.
- "Chainstate" lets you quickly determine whether a new transaction is a double-spend.
- Searching through the block history for other purposes is probably very time-consuming.
  - Locating non-indexed data can be very slow.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Consider using Bitcoin to maintain vital statistics

- Births, deaths, marriages
- Accept for now that this application is possible on Bitcoin's blockchain.
- Consider this query: How many people born after January 1, 1998 have been married?
  - How this query would be processed using the blockchain?
  - Modern databases have evolved to process such queries efficiently.
    - Physical data storage techniques
    - Multiple index tables

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Consider using Bitcoin to maintain vital statistics

- Consider this query: How many people born after January 1, 1998 have been married?
- It would be very time-consuming to run this query on the blockchain.
  - You'd have to go through every block starting with the first block that has data from 1998.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

You need a strong understanding of how blockchain works to evaluate proposed use cases.

- My current research
  - How does SegWit ("Segregated Witness"), adopted in August 2017, impact this discussion?
    - Effectively allows a larger block size
    - Supports "second layer protocols
      - Smart contracts
      - Lightning Network: small, recurring payments off-chain

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

You need a strong understanding of how blockchain works to evaluate proposed use cases.

- My current research (continued)
  - What other characteristics of Bitcoin's blockchain may limit its suitability for other uses?
  - Do other versions of blockchain, specifically Ethereum and Hyperledger Fabric, overcome these limitations?

Keep a healthy skepticism.

- Blockchain was designed to meet the specific needs of a cryptocurrency.
  - The “cypherpunk” distrust of central authority is fundamental.
  - Many proposed uses differ significantly from Bitcoin.
- Many proposed uses would need efficient querying of the blockchain database.
  - That’s not how blockchain in Bitcoin was designed.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Is blockchain mostly hype?

- *The need exists for a shared, trusted ledger that supports processing smart transactions.*
- This probably will happen and be hugely impactful.
- But blockchain is just one possible approach to meeting this need.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS

Evaluating the Feasibility of Proposed Blockchain Use Cases

Thanks for participating!

Myles Stern, Ph.D., CMA
Department of Accounting, Mike Ilitch School of Business
Wayne State University

Copyright © 2018 by Myles Stern.
All rights reserved.

WAYNE STATE UNIVERSITY
MIKE ILITCH
SCHOOL OF BUSINESS