BLOCKCHAIN

How Blockchain works;
Case studies using private Blockchains

Chris Carroll
Associate Teaching Professor, Drexel University

DREXEL UNIVERSITY
College of
Computing &
Informatics

Drexel University

Comprehensive Coverage of Computing and Informatics

Computer Science

Data Science

Software Engineering

Information Systems

Computing & Security Technology

Computing Theory Programming

Computing Application Client Needs

Cipher Methods

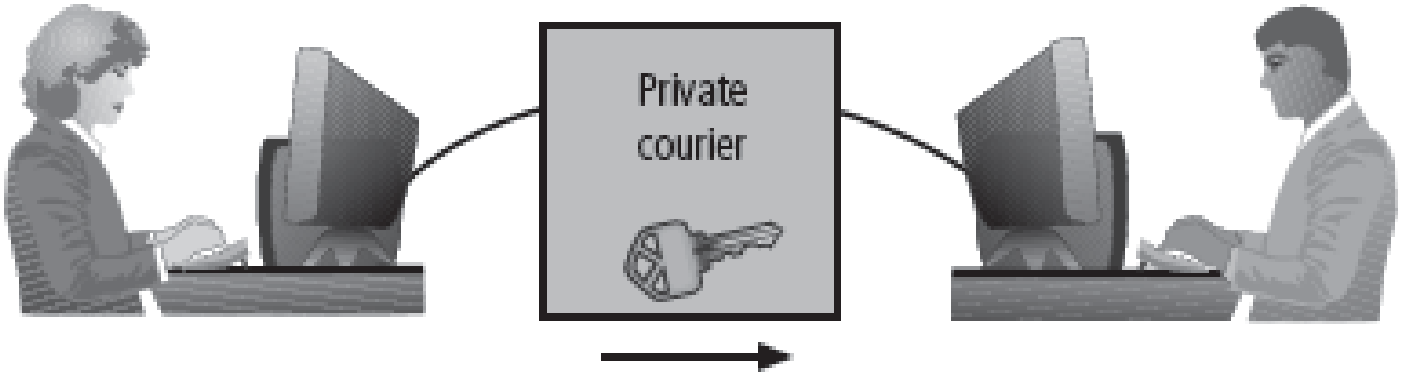
- At the lowest level encryption algorithms use mathematics to manipulate the numeric representations of data.
- Plaintext can be encrypted through bit stream or block cipher method
- Bit stream: each plaintext bit transformed into cipher bit one bit at a time
- Block cipher: message divided into blocks (e.g., sets of 8- or 16-bit blocks) and each is transformed into encrypted block of cipher bits using algorithm and key

Cryptographic Algorithms

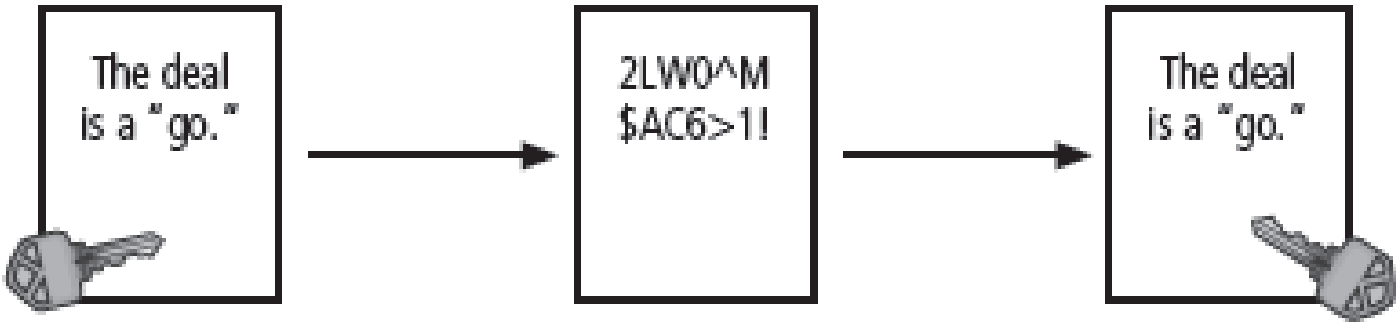
- Often grouped into two broad categories, symmetric and asymmetric
  - Today's popular cryptosystems use hybrid combination of symmetric and asymmetric algorithms
- Symmetric and asymmetric algorithms distinguished by types of keys used for encryption and decryption operations

Symmetric Encryption

- Uses same "secret key" to encipher and decipher message
  - Encryption methods can be extremely efficient, requiring minimal processing
  - Both sender and receiver must possess encryption key
  - If either copy of key is compromised, an intermediate can decrypt and read messages



Rachel at ABC Corp. generates a secret key. She must somehow get it to Alex at XYZ Corp. out of band. Once Alex has it, Rachel can use it to encrypt messages, and Alex can use it to decrypt and read them.



Example of Symmetric Encryption

Symmetric Encryption (cont'd.)

- Here are the names of some commonly used Symmetric algorithms:
- Encryption Standard (DES): one of most popular symmetric encryption cryptosystems
- Triple DES (3DES): created to provide security far beyond DES
- Advanced Encryption Standard (AES): developed to replace both DES and 3DES

Asymmetric Encryption

- Also known as public-key encryption
- Uses two different but related keys
  - Either key can encrypt or decrypt message
  - If Key A encrypts message, only Key B can decrypt
  - Highest value when one key serves as private key and the other serves as public key
- RSA algorithm

Man-in-the-Middle Attack

- Designed to intercept transmission of public key or insert known key structure in place of requested public key
- From victim's perspective, encrypted communication appears to be occurring normally, but in fact, attacker receives each encrypted message, decodes, encrypts, and sends to originally intended recipient
- Establishment of public keys with digital signatures can prevent traditional man-in-the-middle attack

Encrypting Passwords

- Server administrators can access every file on a server including the file that stores passwords
- Problem:
  - Administrators can see passwords in the password file
- Solution:
  - Encrypt passwords before they are stored
  - Use a “one-way” encryption algorithm

Hash Functions

- Mathematical algorithms that generate message summary/digest to confirm message identity and confirm no content has changed
- Hash algorithms: publicly known functions that create hash value
- Use of keys not required
  - Message authentication code (MAC), however, may be attached to a message
- Used in password verification systems to confirm identity of user

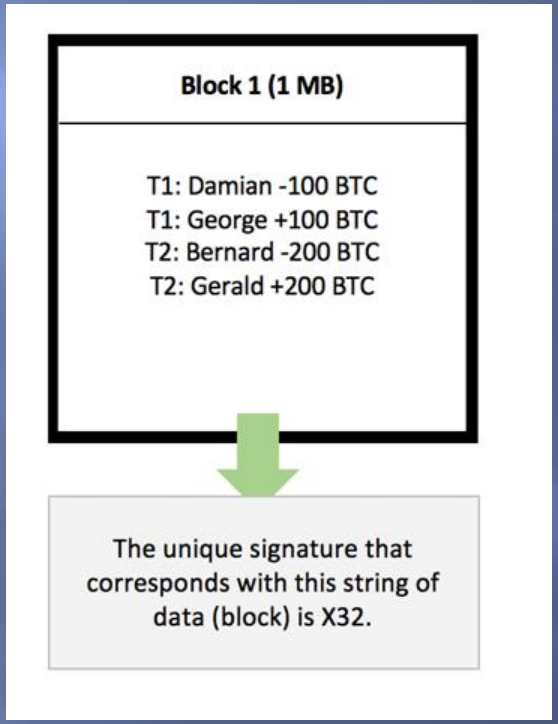
Hash Functions

- Message authentication code (or digest) must be unique and not repeat for more than one letter combinations or patterns.
- If two different patterns generate the same message digest, it is called a collision
- There are many Hash functions because:
  - Earlier functions produced collisions.
  - More sophisticated hash functions are difficult to compute and match a password to a stored hash

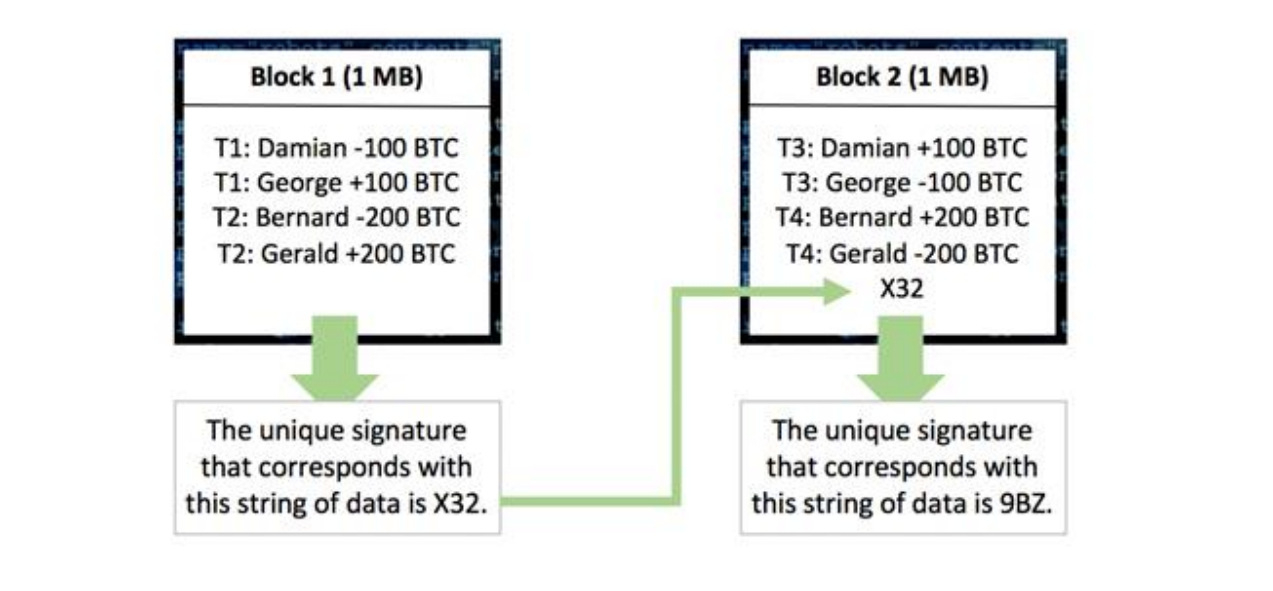
How does Blockchain use encryption?

- Blockchain uses the SHA-256 hash function to protect information in the chain
- Let's Examine a sample blockchain with transaction data
  - Block 1 registers two transactions, transaction 1 and transaction 2
  - Block 2 registers two transactions, transaction 3 and transaction 4
- Let Tn represent transaction n so T1 represents transaction 1, T2 represents transaction 2, …

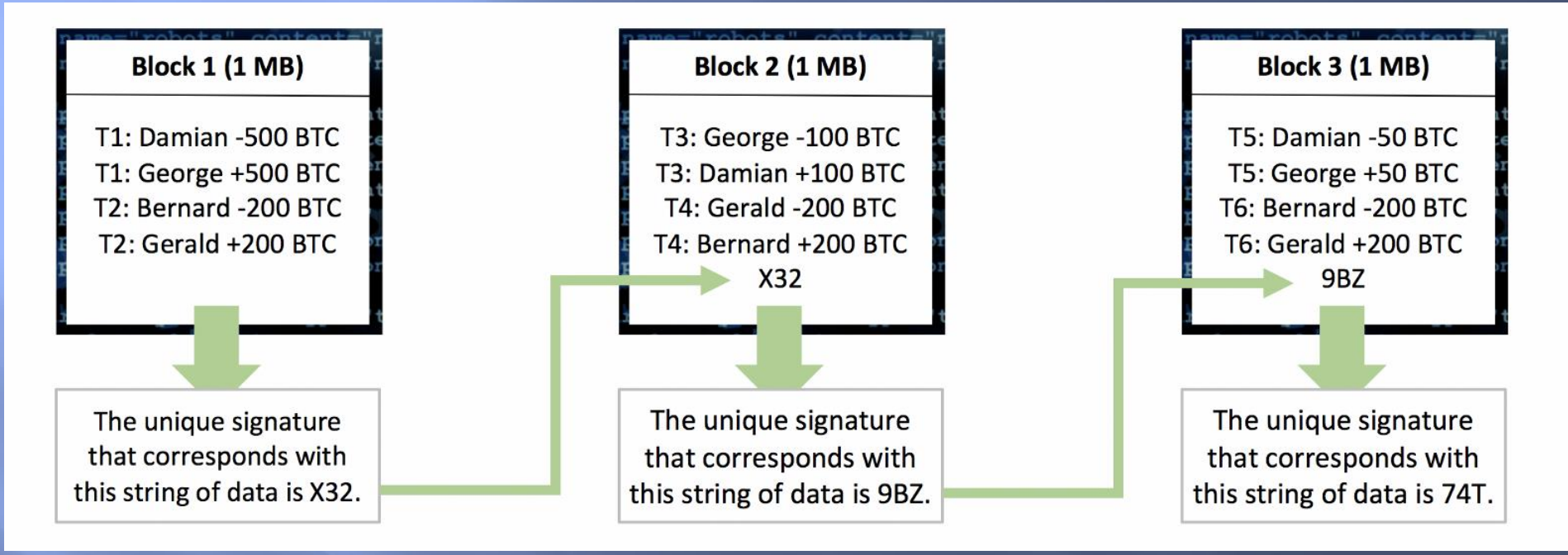
Blockchain – Linking the blocks



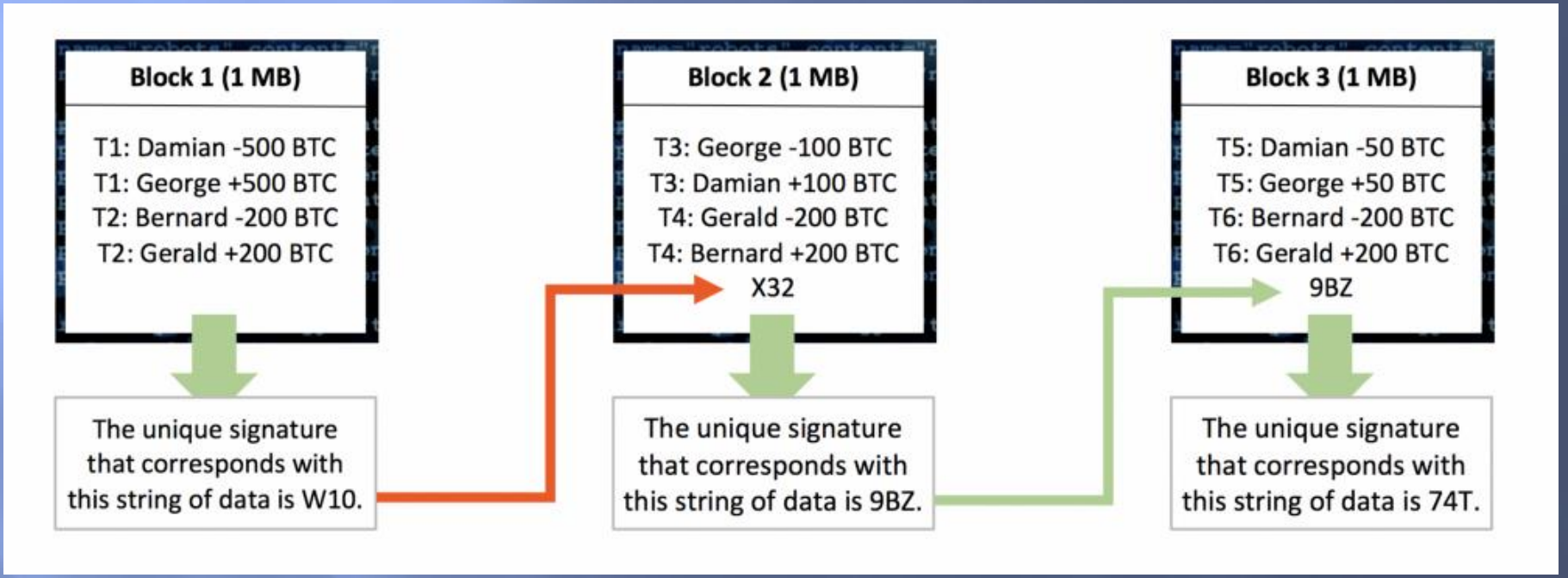
Blockchain – Linking the blocks



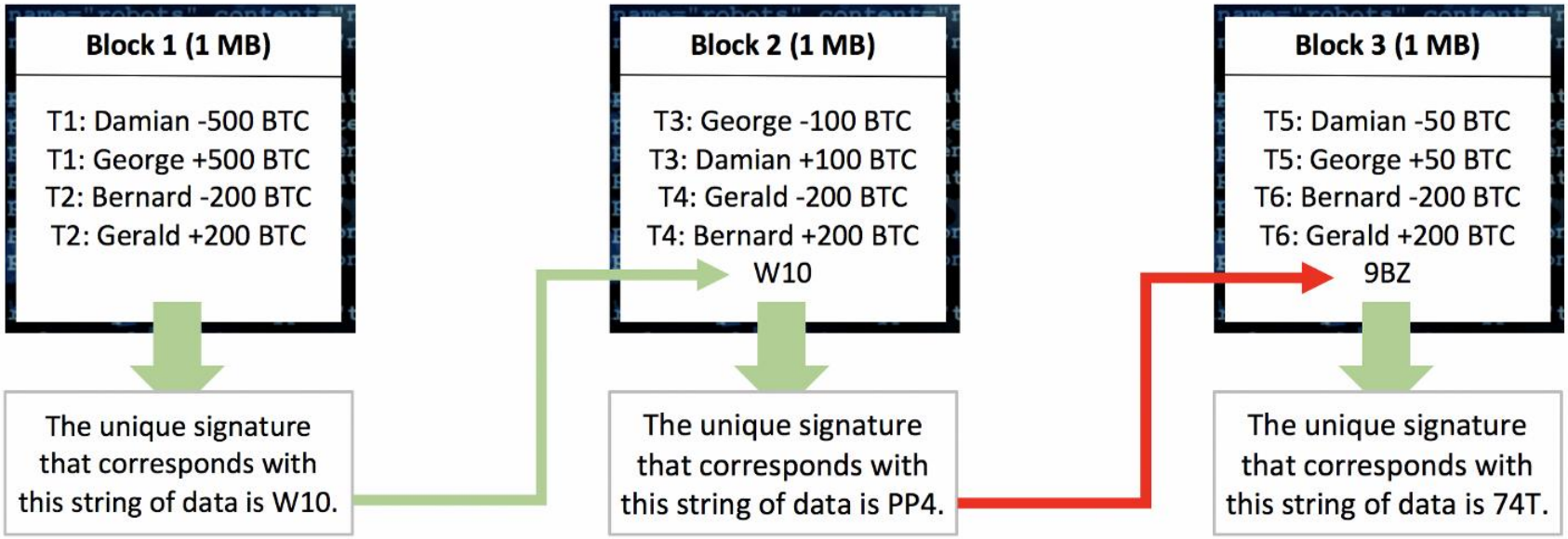
Blockchain – Linking the blocks



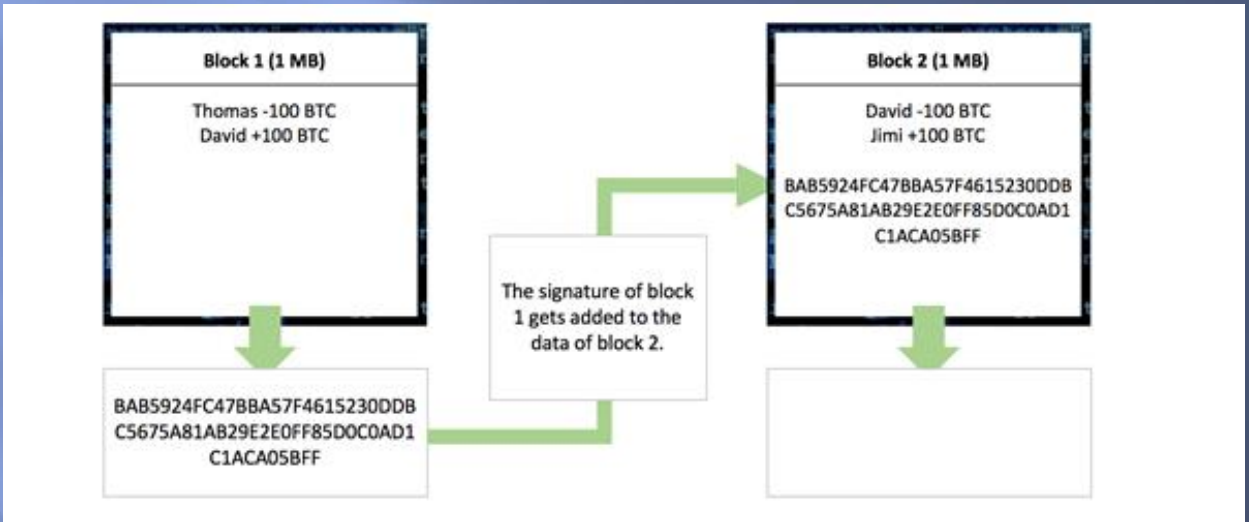
Blockchain – Linking the blocks



Blockchain – Linking the blocks



Blockchain - Example with a more realistic hash



Blockchain

- The blocks holding transactions get *linked* (aka chained) together.
- To do this, every block gets a unique (digital) signature that corresponds to exactly the string of data in that block
- If anything inside a block changes, even just a single digit change, the block will get a new signature
- The signature of block 2 is now partially based on the signature of block 1, because it is included in the string of data in block 2 and so on …

Blockchain

- Adding the previous blocks digest signature to the data of the next block before creating its digest makes the chain immutable
- Immutable: not subject or susceptible to change

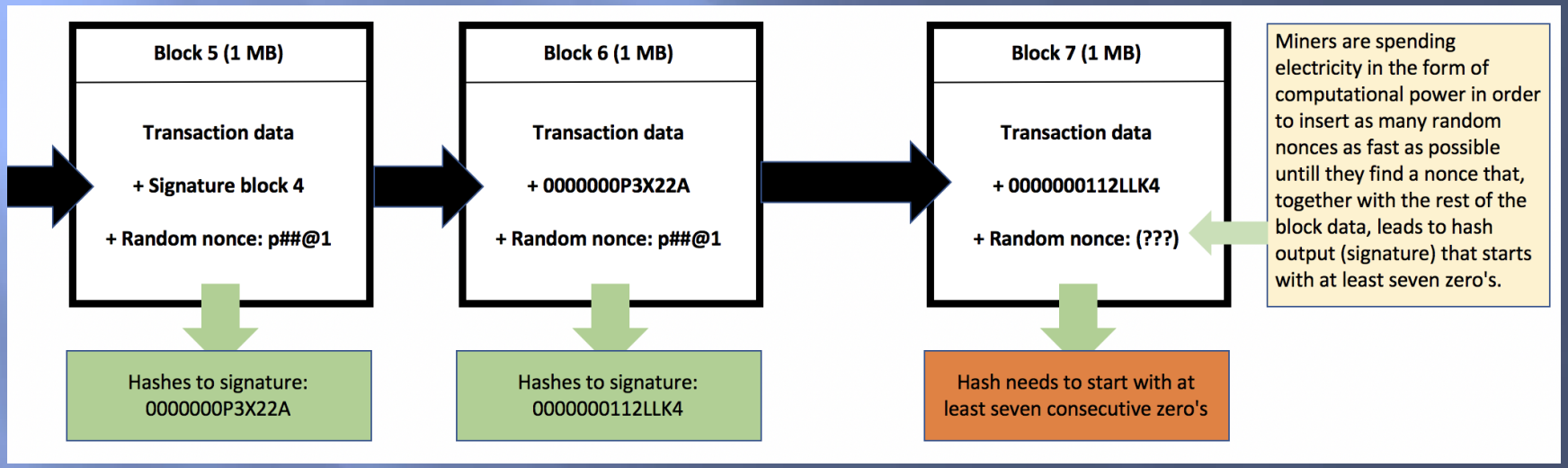
Blockchain – Adding difficulty

- In order to make it more difficult to generate a valid hash for a given block, blockchain uses a nonce
  - A nonce is a number used once
- Miners find a nonce value that when used in the hash function, generates an output that meets certain requirements such as a leading number of zeros
- Brute force trial and error is required to compute the nonce. Miners compete to compute nonces to collect a transaction fee.

Blockchain

- To summarize what was just explained, a block now contains;
  - 1) transaction data,
  - 2) the signature of the previous block, and
  - 3) a nonce.
- The process of repeatedly changing the nonce and hashing the block's data to find an eligible signature is called *mining* and is what *miners* do. Miners spend electricity in the form of computational power by constantly changing the block composition (nonce) and hashing it until they find an eligible signature (output).

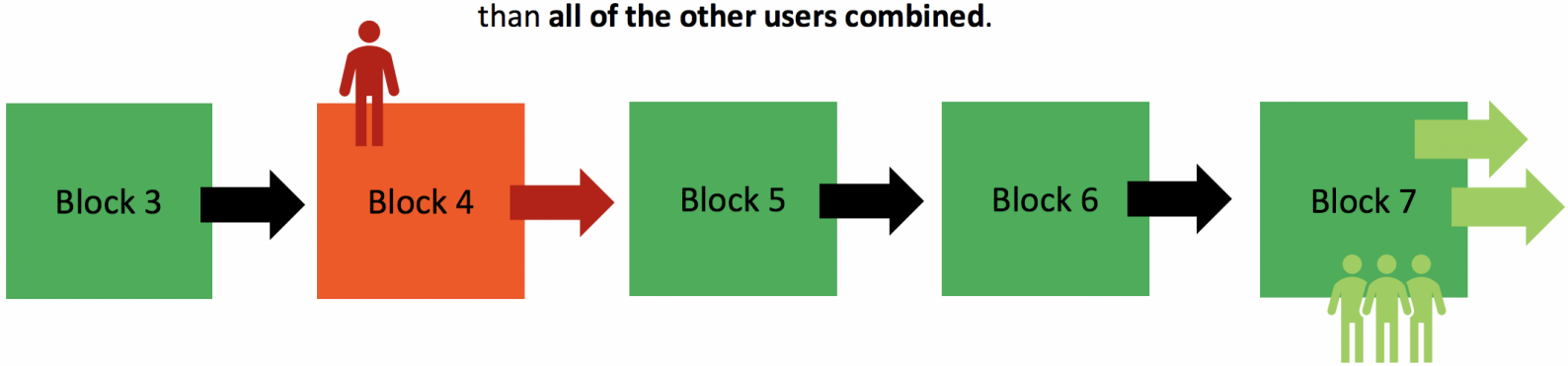
Blockchain - Mining



Blockchain - Mining

- Due to the computational capacity required for mining blocks, this prevents a corrupt miner from modifying blocks on the chain.

The malicious miner calculates new signatures much slower than the rest of the network combined because they have way more computational power together. His change can never catch up with the rest of the network and will be ignored forever. The only way to catch up is to calculate signatures faster than **all of the other users combined**.



Blockchain - Mining

- As you can see, the *hash* (signature) of this block and the hash of the previous block both start with a number of zeroes. Finding a hash like that is not easy, it requires a lot of computational power and time, or a lot of *luck*.
- From time to time a miner with a small amount of computational power will compute the nonce first.

Blockchain - Governance

- Democratic model
- Requires the *majority* of the computational power to create the longest version of the blockchain.
- On the Bitcoin blockchain, all transaction history and wallet balances are public (blockchain.info)

Blockchain – Bitcoin

- Bitcoin is the most infamous public Blockchain
- Anyone can participate in a the Bitcoin blockchain
  - Decentralized - no one entity is in charge
  - Self governed
  - Immutable
- Anyone can start mining the Bitcoin Blockchain
- Anyone can make transactions
- Anyone can review/audit the Bitcoin Blockchain

Bitcoin - Wallet

- Bitcoin wallets
  - Desktop
  - Web
  - Hardware
    - USB drive, Smart card type of device (2 factor authentication)
  - Mobile wallet
    - Most similar to a traditional wallet
    - A wallet that you can use along with an Internet connection for Bitcoin transactions
- Making Bitcoin transactions use Public-key, (Asymmetric), encryption
  - Cryptocurrency wallet only holds a person's private key

Bitcoin - Wallet

- The number of Bitcoins a person owns is recorded on the Blockchain
- So a wallet's public and private key are used to make transactions as follows:
  - Sign and verify transactions:
    - use private key to make a digital signature on a transaction
    - use public key to verify signature of the wallet that owns the transaction

Blockchain – Bitcoin

- Satoshi Nakamoto is the original fictitious name used by the person or group of people who developed bitcoin and authored the bitcoin white paper
- Capable of providing anonymous transactions.
- Many governments consider Bitcoin hostile or contentious
- Considered a currency/commodity
  - especially for tax purposes

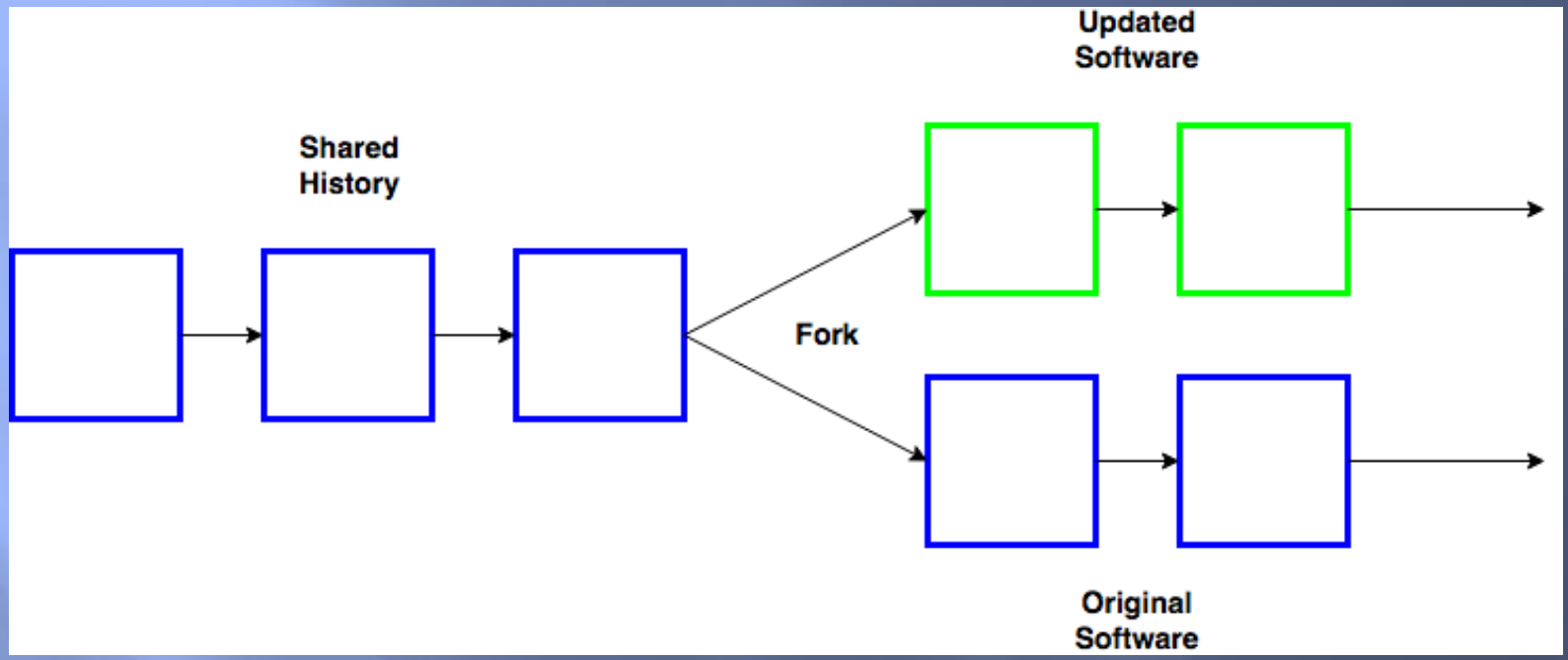
Blockchain – 51 % attack

- A new block can only be added to the blockchain if a Miner computes the correct nonce
- Distributed ledger so the new block can only be accepted if it is valid.
- Corrupt miner does the following:
  - Gets more computing power than all of the other miners combined
  - Builds a longer second Blockchain
  - Gets other miners to accept the second chain as the legitimate chain
  - All transactions not included on the second chain reversed
  - Corrupt miners transactions become refunded bitcoins meaning they can double spend these coins
- There are recorded successful 51% attacks on smaller crypto currencies:
  - Zencash
  - Verge
  - MonaCoin

Blockchain – forks

- Blockchain relies on decentralized groups of computers all working collaboratively; often referred to as full nodes
- These full nodes need to run the same version of software that reads and verifies the Blockchain's ledger
  - Bitcoin Core for Bitcoin
- Soft fork – software updates that are compatible with older versions of the software
- Hard fork – new version of software not compatible with older versions. So full nodes running older software may continue to create blocks.

Blockchain – forks



- Hard fork – new version of software not compatible with older versions. So full nodes running older software may continue to create blocks.

PRIVATE BLOCKCHAINS

Case studies using Blockchain

Blockchain – IoT

- IoT – Internet of Things – Sensors that attach to the Internet
- Supply chain, Blockchain and IoT
  - Track the journey of raw materials used to manufacture products when many different suppliers, processors and couriers come in contact with the materials
  - For materials
    - that are temperature sensitive
    - that must be sourced from a particular location
    - Use an IoT sensor to record temperature and gps data into the Blockchain

Blockchain – Issues

- Issues related to:
  - Humans
  - IoT devices
  - The amount of data stored in each block
  - Software
  - Transparent transactions
  - Transparency between separate entities
  - Encrypting data placed on a Blockchain
    - Managing keys for duration of the Blockchain
  - Write to erasure laws
  - Decisions regarding Blockchains
  - Advances in technology

Blockchain

- Many businesses are examining uses for private Blockchains for transactions with partners
- A private Blockchain normally entails more than one business or supplier that all have an interest in solving a common problem
- Speed up the process for transactions between different entities

Blockchain – Private Case Study

- Situation: Businesses that provide food products purchase food from many different farmers. Bacteria identified in a particular food product causes discarding that food product from all stores. Time to locate the source of the food with the bacteria contamination takes weeks.
- Target: Trace the source of contamination and the specific stores, (individual packages), that may be contaminated. Discard only the food from the contaminated source. Avoid discarding the food product from all stores.
- Solution: Use a private Blockchain to record the path from farmer to courier to processor back to the food business for each package of food.

- Pilot using IBM's Blockchain technology in the cloud underway with these food supply companies: Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestle, Tyson Foods, Unilever and Walmart.

Blockchain – Private Case Study

- Situation: Sanctions in place between two countries. Detecting sanction violations is often done by financial institutions examining deposits. This verifies the one transaction may follow a sanction, but it is difficult to reject a transaction if that financial intuition has evaded sanctions with other institutions.
- Target: Know the identity of the other institutions a financial institution does business with for all their transactions
- Solution: Use a private Blockchain to record the identity of all financial transactions transparent to all financial institutions
  - Pilot projects underway in Asia

- How could Bitcoin help evade sanctions?

References

- Principles of Information Security, 6th Edition, by Michael Whitman, Cengage 2017
  - 4th edition of this text book available in the Drexel Library (Chapters 1 and 8)
- https://blog.goodaudience.com/blockchain-for-beginners-what-is-blockchain-519db8c6677a