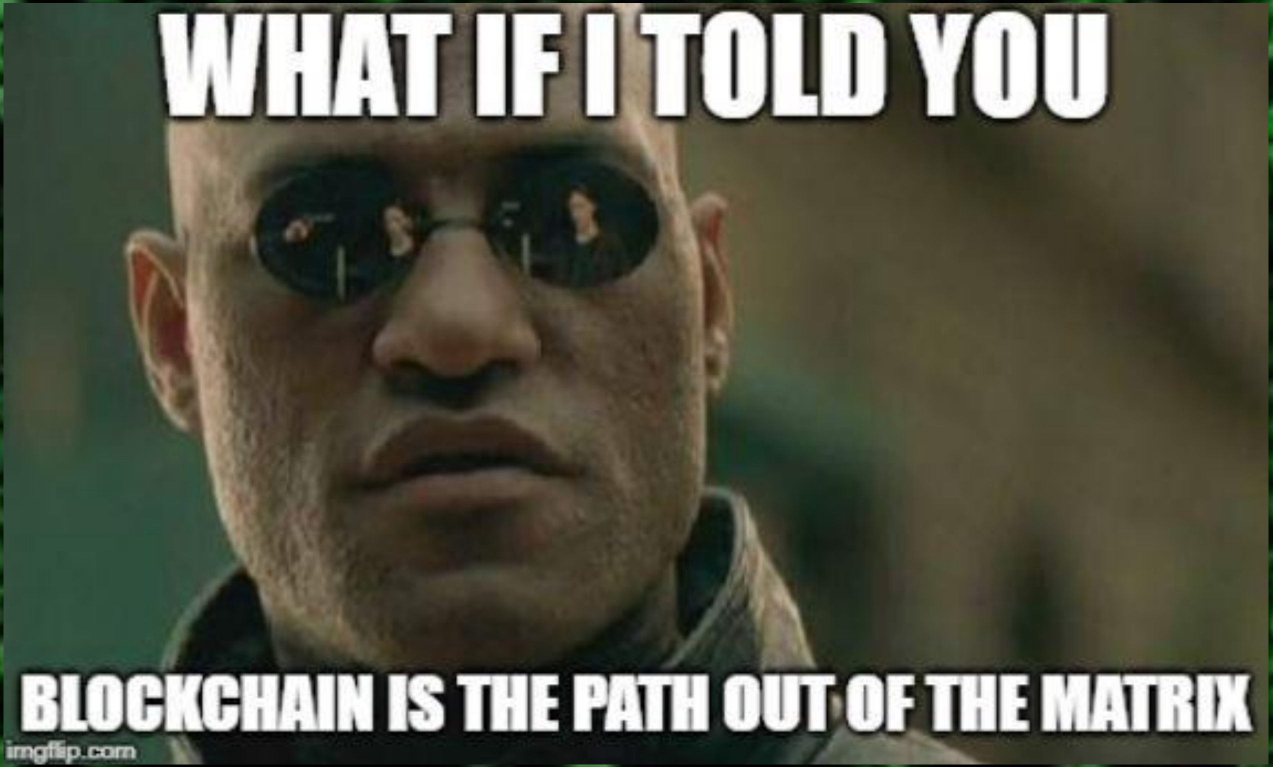
Introduction to Blockchain and Blockchain Development at Forensecure 2018

April 13, 2018

William Favre Slater, III, M.S., MBA, PMP, CISSP, CISA, SSCP, Security+
Adjunct Industry Instructor

ILLINOIS INSTITUTE OF TECHNOLOGY


WHAT IF I TOLD YOU
BLOCKCHAIN IS THE PATH OUT OF THE MATRIX
imgflip.com

***** CAUTION *****

- Blockchain and Bitcoin are sophisticated applied technologies that work together to provide trusted computing.
- They are built on complex rules with the objective of providing reliable, trusted, anonymous transactions on decentralized distributed ledgers via the Internet.
- It took the time, experience, knowledge and hard work of many geniuses to mature the technology.
- It takes time, energy, patience and many hours of study to just begin to wrap your head around it.
- If you are lazy or have a short attention span, or are overwhelmed after this presentation these topics are probably not a good career direction for you.
- This path will not be easy, but it will be worthwhile if you are up for investing your time and energy to learn it.
- **As of February 2018, there are 14 open positions for every single Blockchain engineer who is looking for a job.**

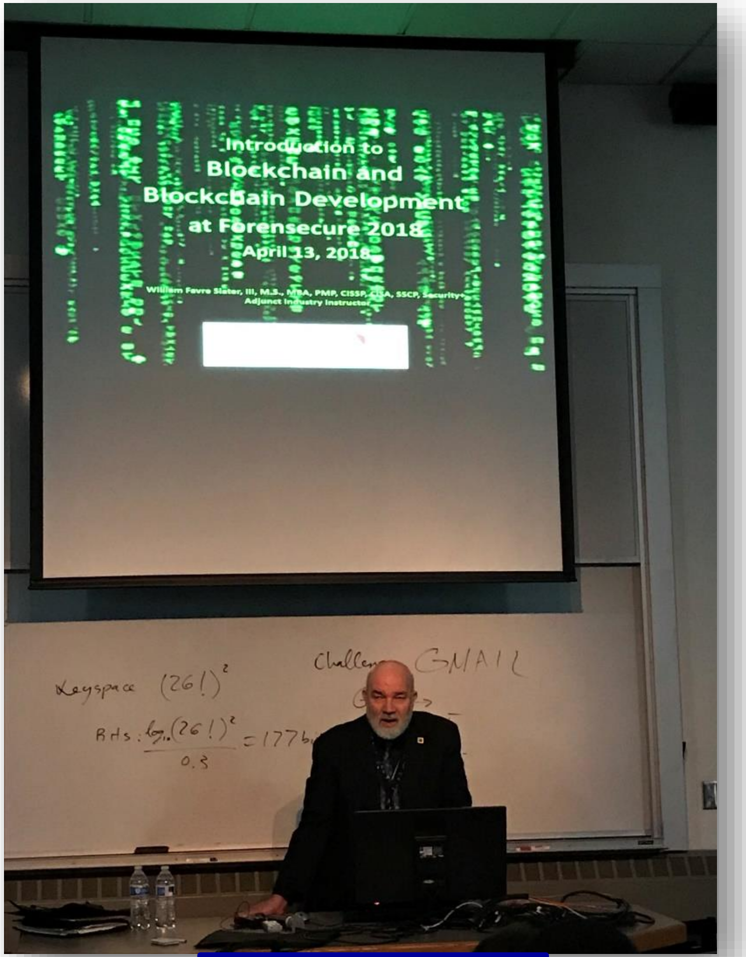
Two More Important Notes

- This presentation is not about CRYPTOCURRENCY, only BLOCKCHAIN
- Please clear your mind about everything you thought you knew about BLOCKCHAIN before this presentation.
- BLOCKCHAIN MUCH bigger than you think.

ILLINOIS INSTITUTE OF TECHNOLOGY

Agenda

- Introduction
- Some Important Terms
- Cryptography
- What is Blockchain?
- Types of Blockchains
- Hash Puzzle
- Merkle Trees
- Authentication in the Blockchain
- How does Blockchain work?
- Blockchain Architecture
- Blockchain Accomplishments
- Blockchain Uses
- Blockchain Limitations
- Blockchain Development
- How Can You Accelerate Your Blockchain Understanding, Knowledge and Skills?
- Conclusion
- Questions
- Practical Exercises
- References



William Favre Slater, III
Forensecure 2018

ILLINOIS INSTITUTE OF TECHNOLOGY

Introduction

- Since the emergence of Bitcoin in 2009 as the world's leading "cryptocurrency" it has been met internationally with extreme reactions ranging from skepticism to fanaticism. It has also gotten the attention of governments and law enforcement agencies, as people have used Bitcoin's attributes to undermine legal controls.
- The really surprising and amazing thing about Bitcoin is the BLOCKCHAIN technology that makes it work.
- Smart people and companies are now using Blockchain to create trusted computing environments that are reliable, efficient, time-saving, and cost-effective. It's no longer just "cool", it's now practical and becoming widely adopted.
- Some are calling this explosion of new Blockchain-enabled applications, the ***Era of the Trusted Internet***.
- This presentation will explain the Blockchain, how it works, why it is useful, and what it means for the future of the global economy.

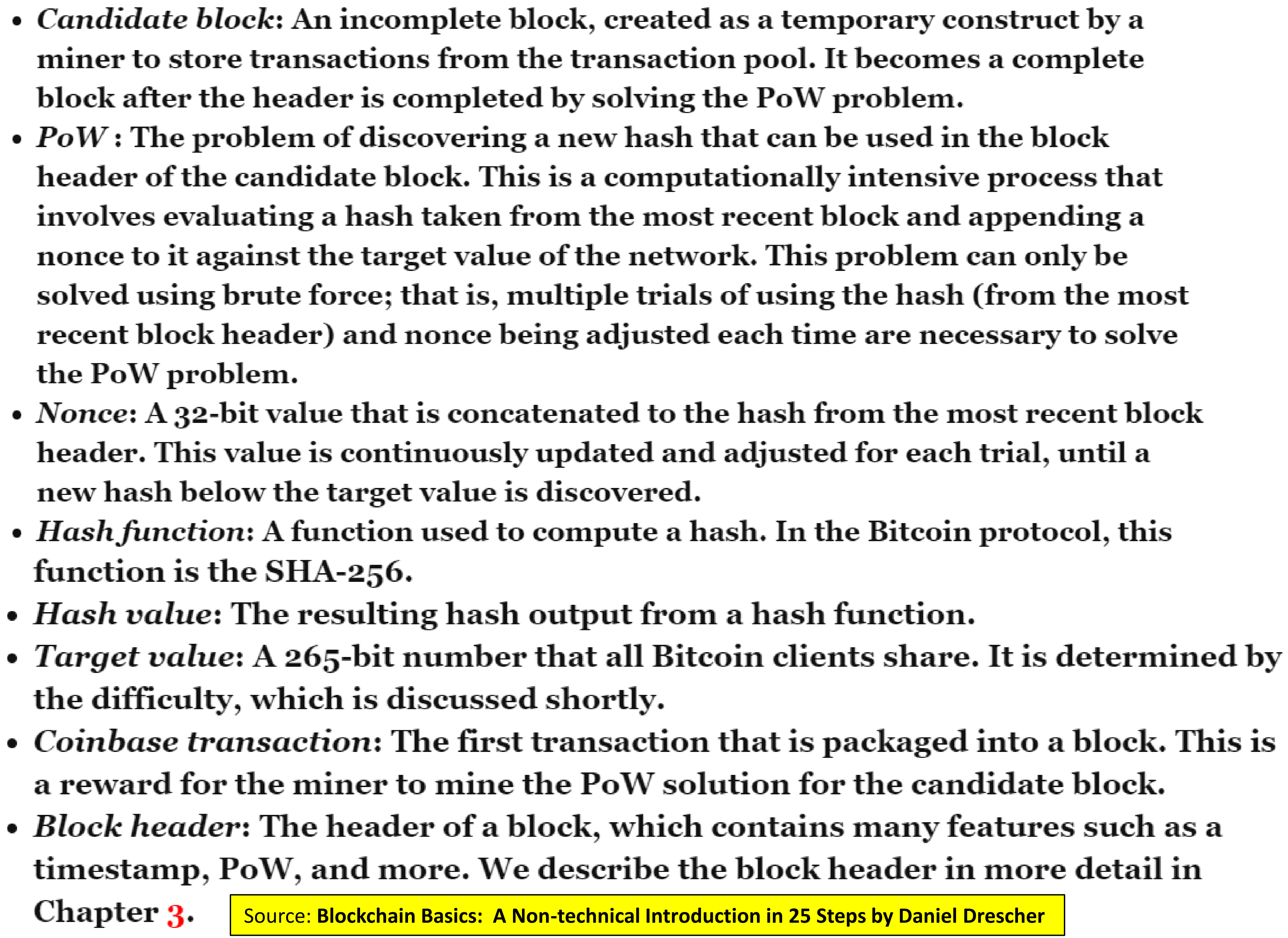
ILLINOIS INSTITUTE OF TECHNOLOGY

SOME IMPORTANT TERMS

Some Important Terms

Term	Explanation
AES SHA-256	The 256-bit encryption algorithm that is AES standard used for Bitcoin keys.
Bitcoin Network	The Internet-connected network comprised of the software and data that supports Bitcoin transactioms
Blockchain	The Bitcoin ledger of past transactions.
Difficulty	The measure of how difficult it is to find a new block compared to the easiest it can ever be
Exchange	A place that sells can buys Bitcoins, like a stock exchange.
Hash	It is a standard cryptographic algorithm function for the generation and verification of currency
Mining	Bitcoin mining serves 2 purposes, it creates the general ledger of Bitcoin transactions and it provides security.
Private Key	The secret cryptographic key that is used to protect your Bitcoin account
Proof of Work	An economic time-stamped measure to deter service abuses on a network by requiring some work from the service requester, usually meaning processing time by a computer.
Public Key	The public (shared) cryptographic key that is used to protect your Bitcoin account
Transaction	Use of the Bitcoin to purchase good or services, or the purchase of sale of a Bitcoin, or fractional part of Bitcoin
Wallet	A service that will safely store your Bitcoin account for you.

ILLINOIS INSTITUTE
OF TECHNOLOGY



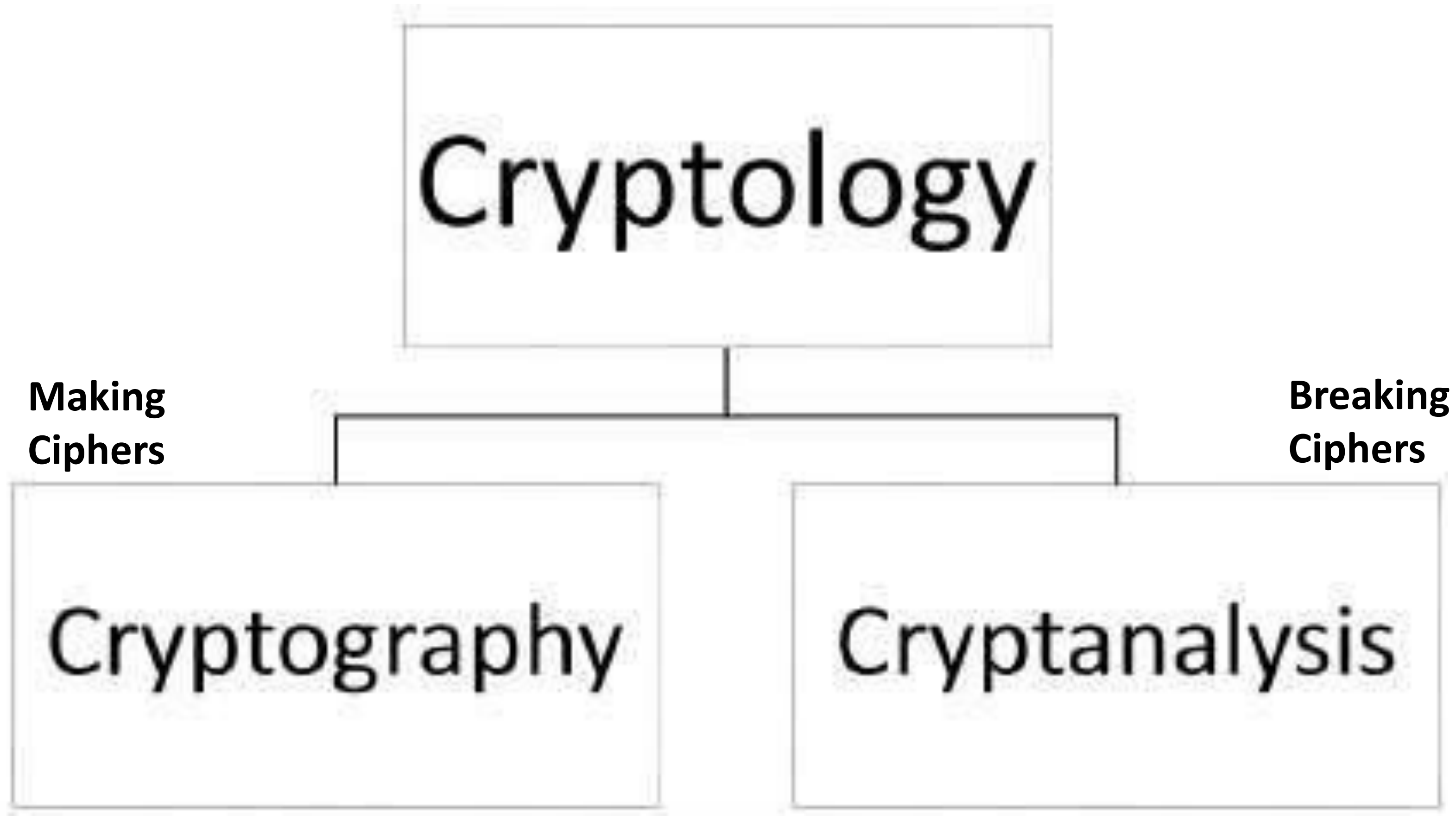
- *Candidate block*: An incomplete block, created as a temporary construct by a miner to store transactions from the transaction pool. It becomes a complete block after the header is completed by solving the PoW problem.
- *PoW* : The problem of discovering a new hash that can be used in the block header of the candidate block. This is a computationally intensive process that involves evaluating a hash taken from the most recent block and appending a nonce to it against the target value of the network. This problem can only be solved using brute force; that is, multiple trials of using the hash (from the most recent block header) and nonce being adjusted each time are necessary to solve the PoW problem.
- *Nonce*: A 32-bit value that is concatenated to the hash from the most recent block header. This value is continuously updated and adjusted for each trial, until a new hash below the target value is discovered.
- *Hash function*: A function used to compute a hash. In the Bitcoin protocol, this function is the SHA-256.
- *Hash value*: The resulting hash output from a hash function.
- *Target value*: A 265-bit number that all Bitcoin clients share. It is determined by the difficulty, which is discussed shortly.
- *Coinbase transaction*: The first transaction that is packaged into a block. This is a reward for the miner to mine the PoW solution for the candidate block.
- *Block header*: The header of a block, which contains many features such as a timestamp, PoW, and more. We describe the block header in more detail in Chapter 3.

Source: **Blockchain Basics: A Non-technical Introduction in 25 Steps by Daniel Drescher**

GY

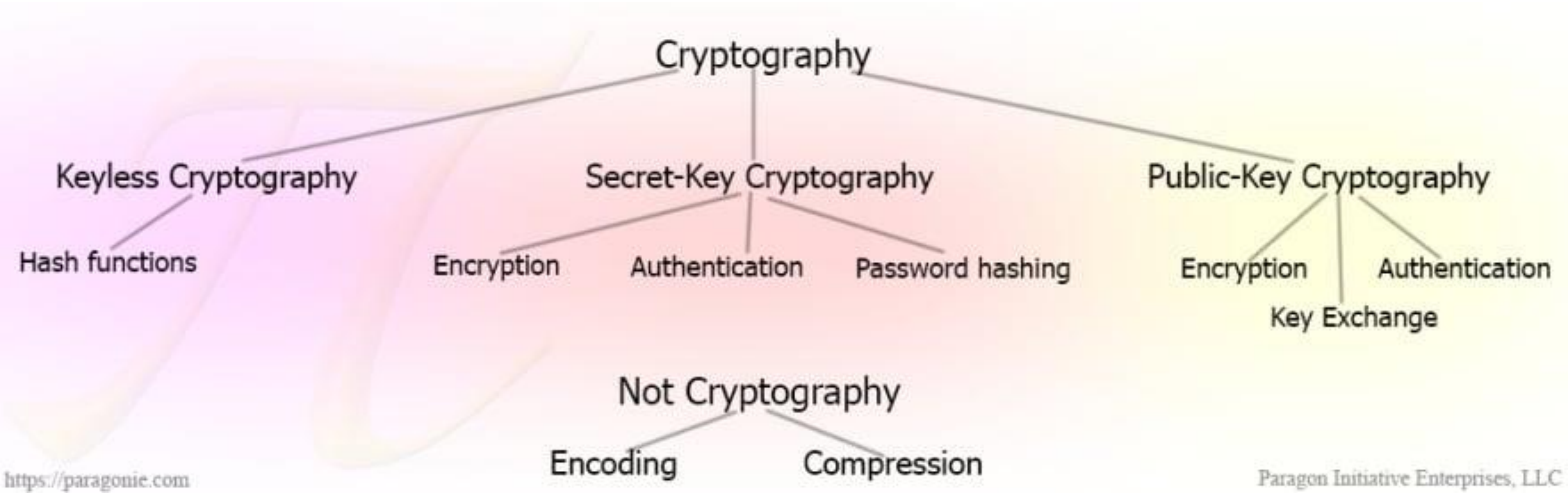
CRYPTOGRAPHY

Cryptography



ILLINOIS INSTITUTE OF TECHNOLOGY

Cryptography



Cryptography

Keyless Cryptography

Hash functions

Secret-Key Cryptography

Encryption

Authentication

Password hashing

Public-Key Cryptography

Encryption

Authentication

Key Exchange

Not Cryptography

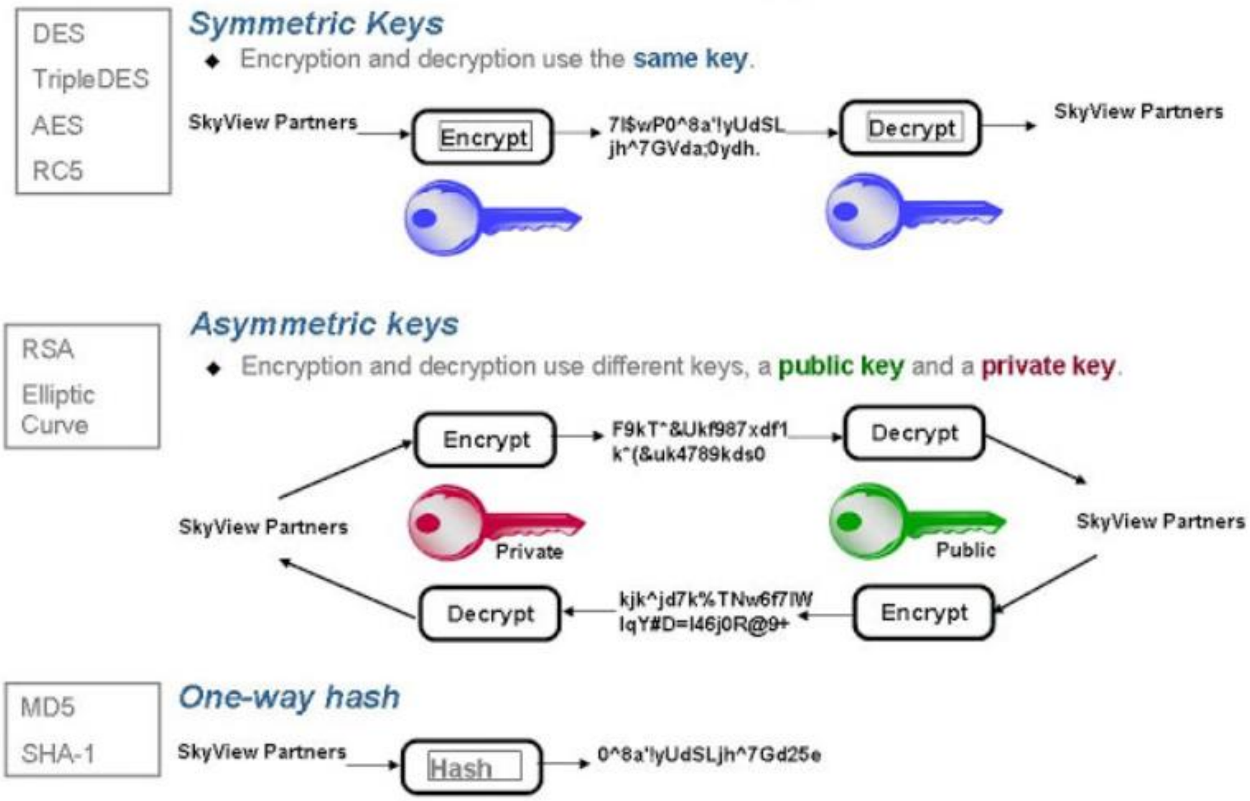
Encoding

Compression

https://paragonie.com

Paragon Initiative Enterprises, LLC

Types of Encryption



Symmetric Keys

- Encryption and decryption use the **same key**.

Asymmetric keys

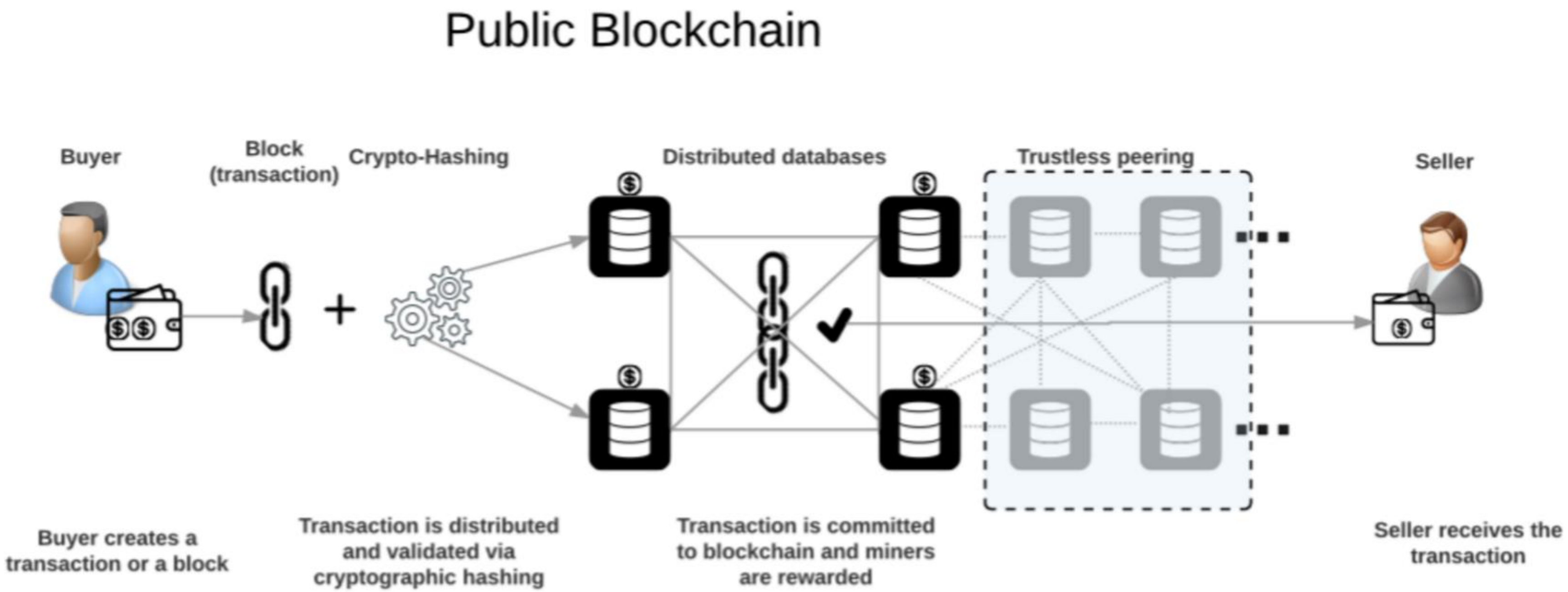
- Encryption and decryption use different keys, a **public key** and a **private key**.

One-way hash

http://computer-trickster.blogspot.tw/2015/11/encryption.html

ILLINOIS INSTITUTE OF TECHNOLOGY

Hashing in Blockchain



Public Blockchain

Buyer creates a transaction or a block

Transaction is distributed and validated via cryptographic hashing

Transaction is committed to blockchain and miners are rewarded

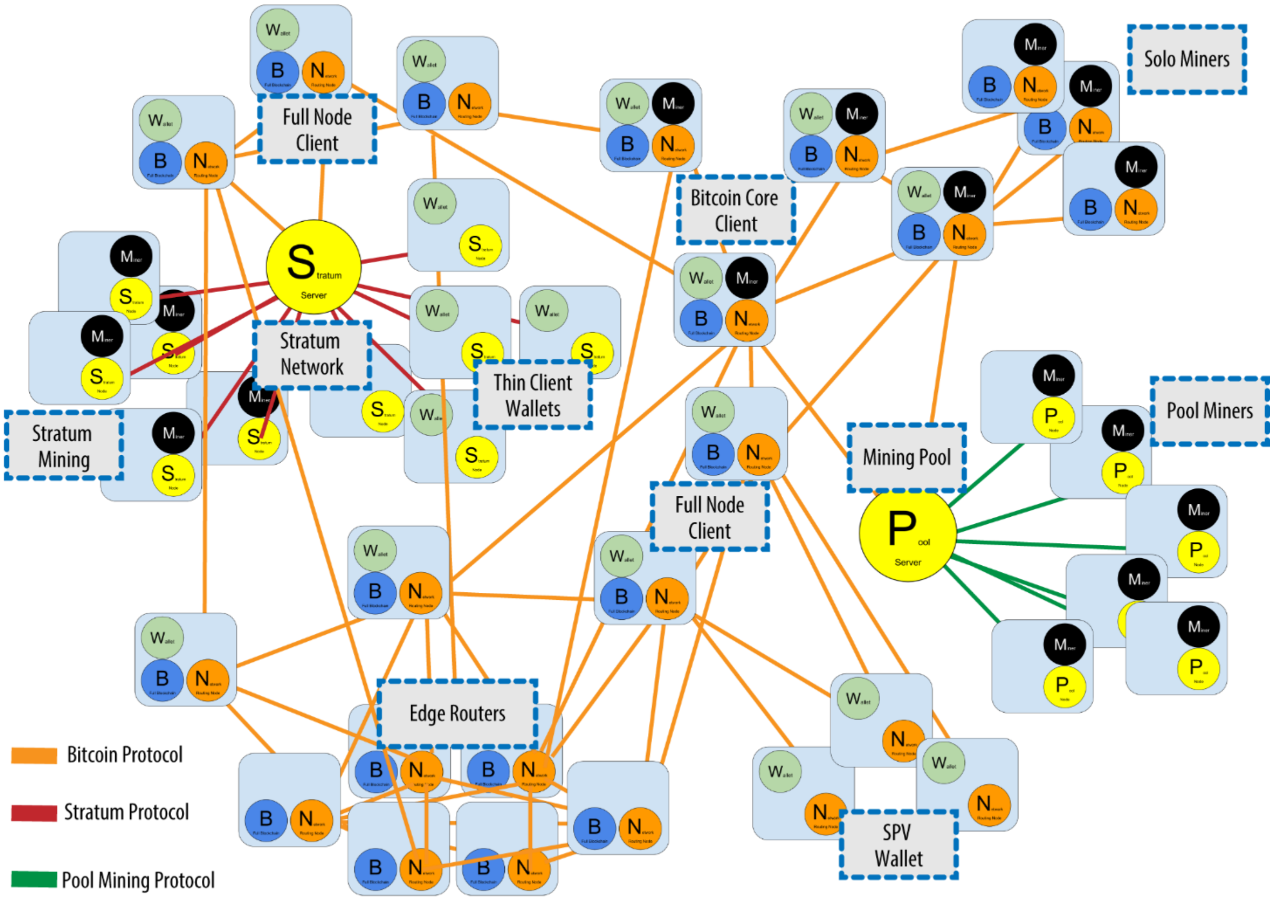
Seller receives the transaction

ILLINOIS INSTITUTE OF TECHNOLOGY

WHAT IS BLOCKCHAIN?

ILLINOIS INSTITUTE OF TECHNOLOGY

A Logical Diagram of a Blockchain Network



This Photo by Unknown Author is licensed under CC BY-SA

ILLINOIS INSTITUTE OF TECHNOLOGY

What Is Blockchain?

- Distributed Ledger
- Decentralized
- Popularized by Satoshi Nakamoto
- Uses Cryptography and Hashing
- Append-only Transactions
- The Code already exists in Github
- Immutable
- First discussed in 1991

ILLINOIS INSTITUTE
OF TECHNOLOGY

What Is Blockchain?

- Blockchain Consensus Protocol guide. A blockchain is a decentralized peer-to-peer system with no central authority figure. While this creates a system that is devoid of corruption from a single source, it still creates a major problem.
  - How are any decisions made?
  - How does anything get done?
  - Think of a normal centralized organization.
- All the decisions are taken by the leader or a board of decision makers. This isn’t possible in a blockchain because a blockchain has no “leader”. For the blockchain to make decisions, they need to come to a consensus using “consensus mechanisms”.

What is Blockchain?

- A Decentralized, Distributed Ledger
- Updated using software, messaging and databases with Append-only transactions
- Records are immutable.
- There are multiple copies
- Updated by miners, and synchronized using Proof of Work, and Consensus
- The foundation technology for Cryptocurrency
- The Future of Trusted Computing Transactions on the Internet and in public and private networks
- First described by Satoshi Nakamoto in his 9-page January 2009 paper: https://bitcoin.org/bitcoin.pdf
- The world's largest Blockchain Database is the Bitcoin Blockchain Database, with 160 GB (it doesn't scale very well)

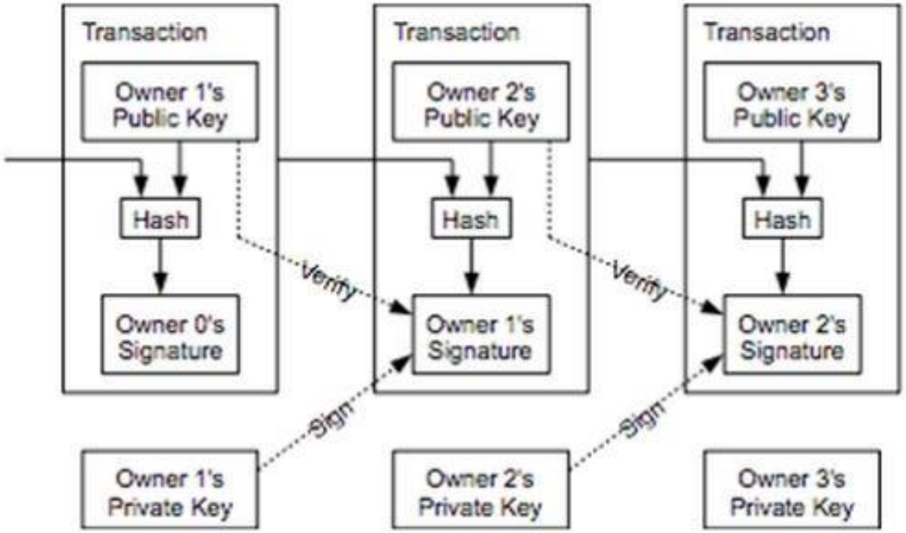


Image: Satoshi Nakamoto

ILLINOIS INSTITUTE OF TECHNOLOGY

The Term Blockchain

- Name for a data structure
- Name for an algorithm
- Name for a suite of Technologies
- An umbrella term for purely distributed peer-to-peer systems with a common application area
- A peer-to-peer-based operating system with its own unique rule set that utilizes hashing to provide unique data transactions with a distributed ledger

ILLINOIS INSTITUTE OF TECHNOLOGY

Blockchain – Simplified View

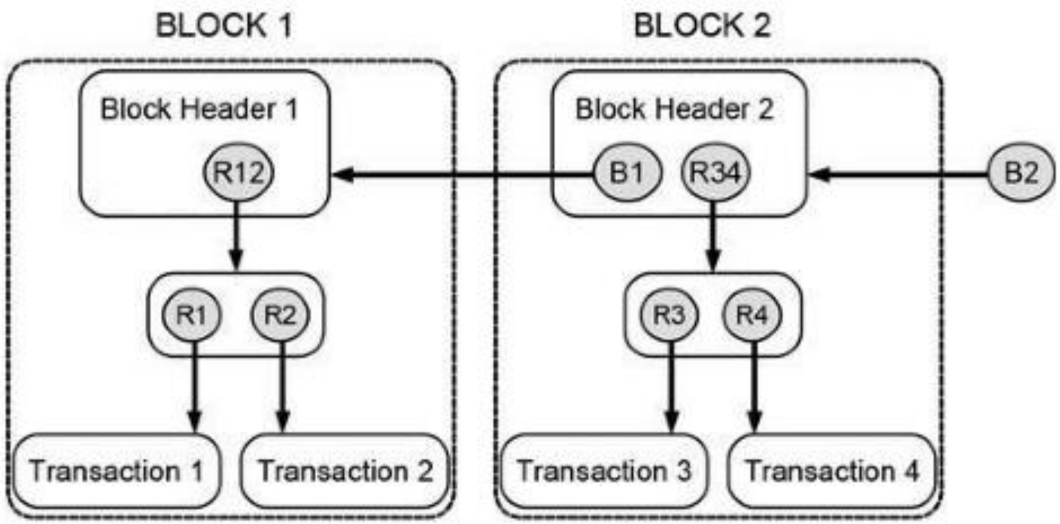
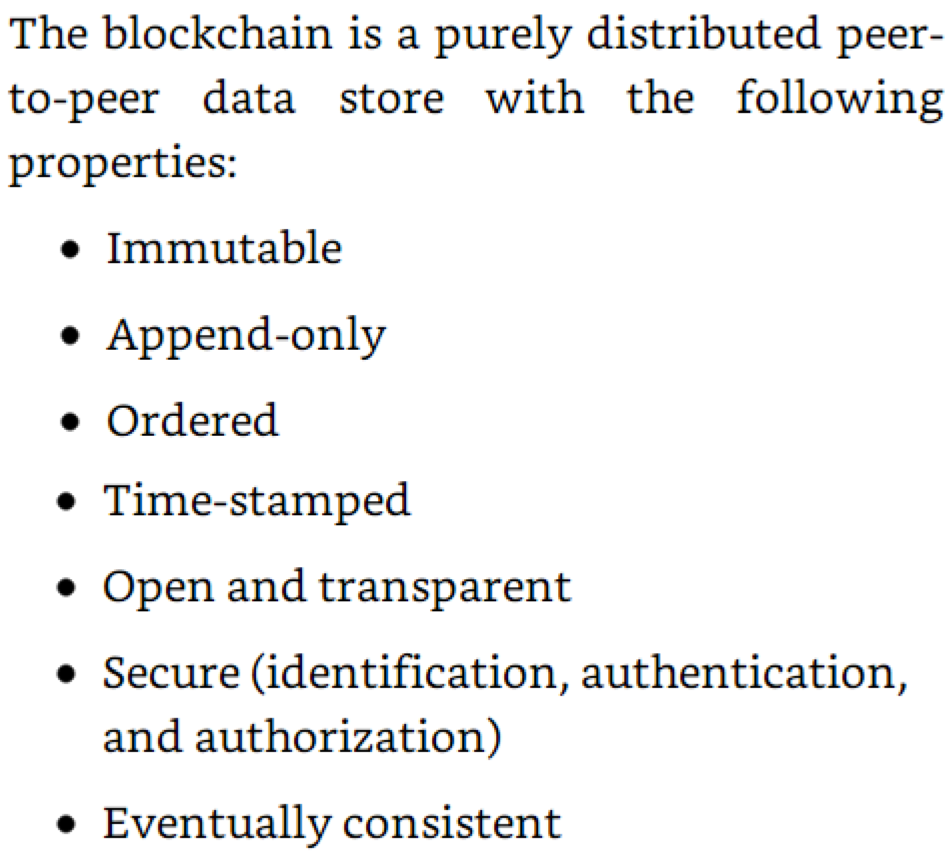


Figure 14-5. A simplified blockchain-data-structure containing four transactions

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Characteristics of the Blockchain



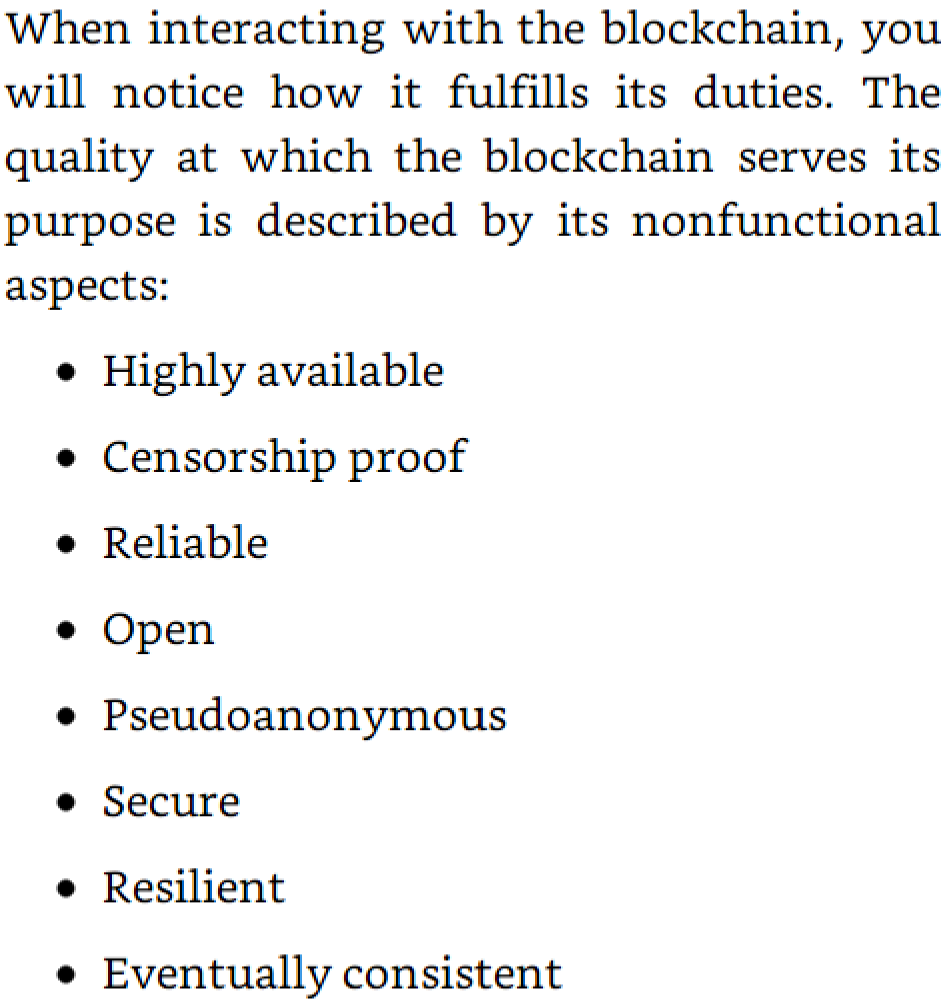
The blockchain is a purely distributed peer-to-peer data store with the following properties:

- Immutable
- Append-only
- Ordered
- Time-stamped
- Open and transparent
- Secure (identification, authentication, and authorization)
- Eventually consistent

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

Properties of the Blockchain Non-functional Aspects



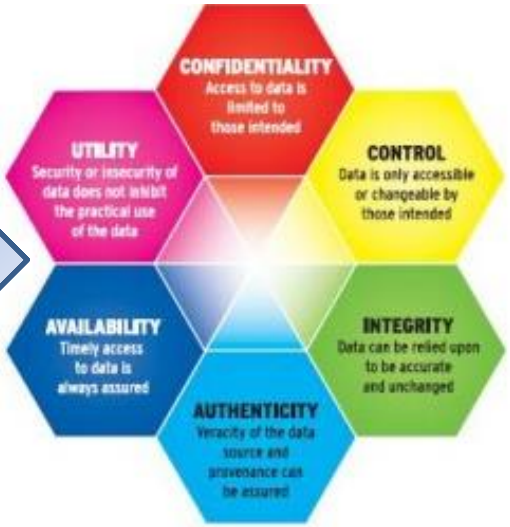
When interacting with the blockchain, you will notice how it fulfills its duties. The quality at which the blockchain serves its purpose is described by its nonfunctional aspects:

- Highly available
- Censorship proof
- Reliable
- Open
- Pseudoanonymous
- Secure
- Resilient
- Eventually consistent

ILLINOIS INSTITUTE OF TECHNOLOGY

Why Is Blockchain Important?

- Accessible
- Open source
- Easily provides three challenging elements of the **Parkerian Hexad** model for security:
  - **Authenticity**
  - **Control**
  - **Utility**
- It WORKS!
- Business enabler
- Reduces risk of computer fraud
- It is being widely adopted for trusted computing
- Blockchain developers and architects are in great demand: for every Blockchain professional there are 14 open positions


CONFIDENTIALITY
Access to data is limited to those intended
UTILITY
Security or insecurity of data does not inhibit the practical use of the data
CONTROL
Data is only accessible or changeable by those intended
AVAILABILITY
Timely access to data is always assured
INTEGRITY
Data can be relied upon to be accurate and unchanged
AUTHENTICITY
Veracity of the data source and provenance can be assured

Donn B. Parker

ILLINOIS INSTITUTE OF TECHNOLOGY

Blockchain Transactions: Satoshi Nakamoto's Vision

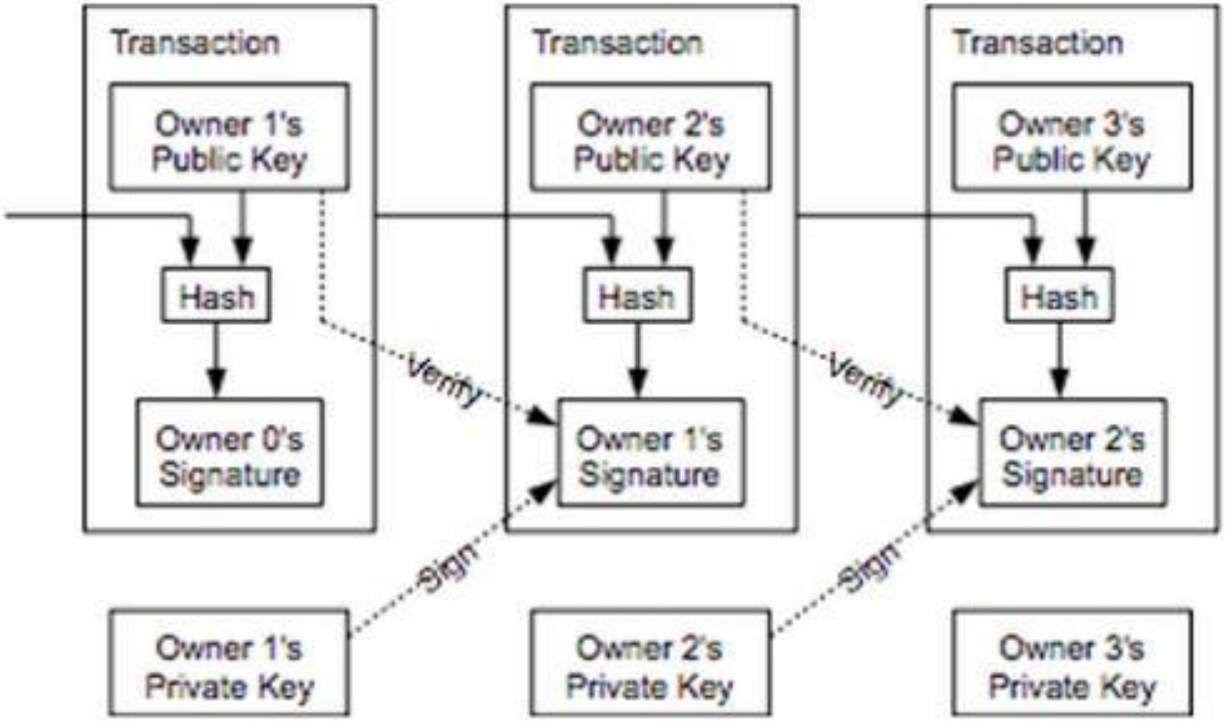
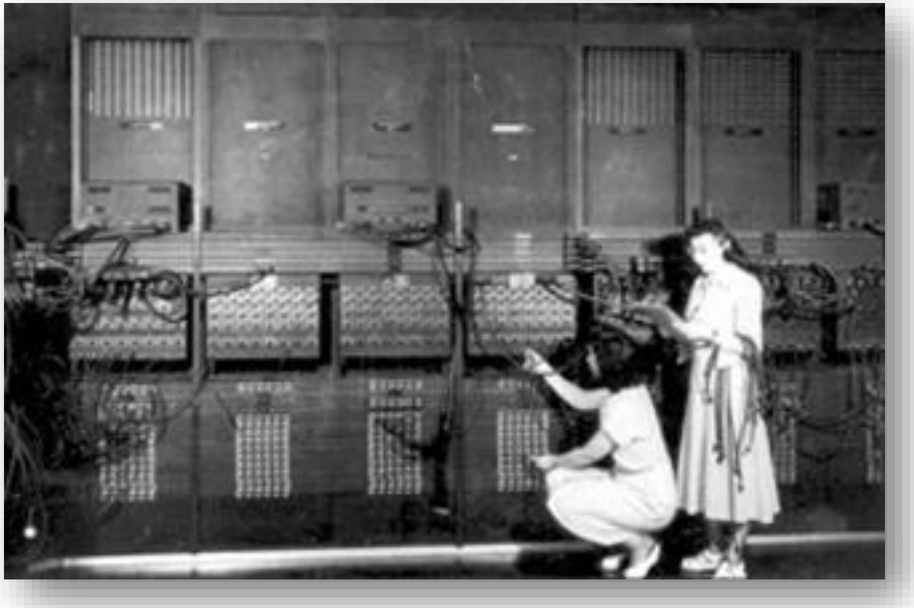


Image: Satoshi Nakamoto

Source: **Bitcoin: A Peer-to-Peer Electronic Cash System**. By Satoshi Nakamoto. Retrieved from https://bitcoin.org/bitcoin.pdf

Technologies and Events that Led to the Creation of Bitcoin and Blockchain

- Cryptography
- Transistors
- Digital Computers
- Databases
- Silicon Chips
- Programming
- Applied Cryptography
- Computer Networks
- Transaction Processing
- TCP/ IP and The Internet
- The World Wide Web
- Evolution of Security and Privacy Thought
- The Great 2008 Economic Recession



ILLINOIS INSTITUTE OF TECHNOLOGY

Blockchain Technologies

Technology	Source
The Internet (TCP/IP)	Built into every modern OS
Cryptography	Cryptography software
Bitcoin software	Github
Blockchain Database	MongoDB or BigchainDB

ILLINOIS INSTITUTE
OF TECHNOLOGY

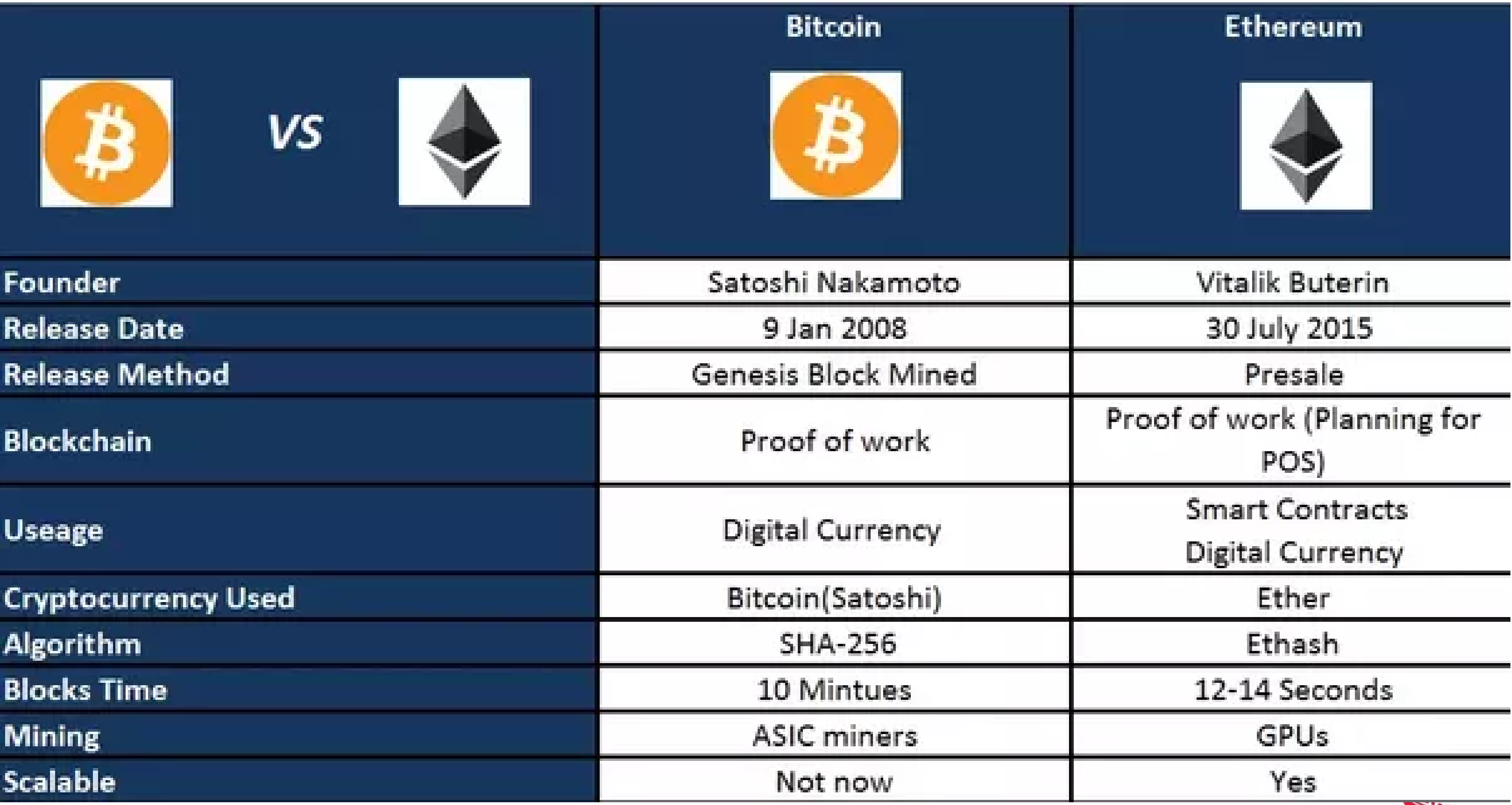
TYPES OF BLOCKCHAINS

ILLINOIS INSTITUTE OF TECHNOLOGY

Types of Blockchains

- Bitcoin vs. Ethereum vs, Hyperledger (Linux and IBM)
- Public vs. Private
- Permissioned (private) vs. Permissionless

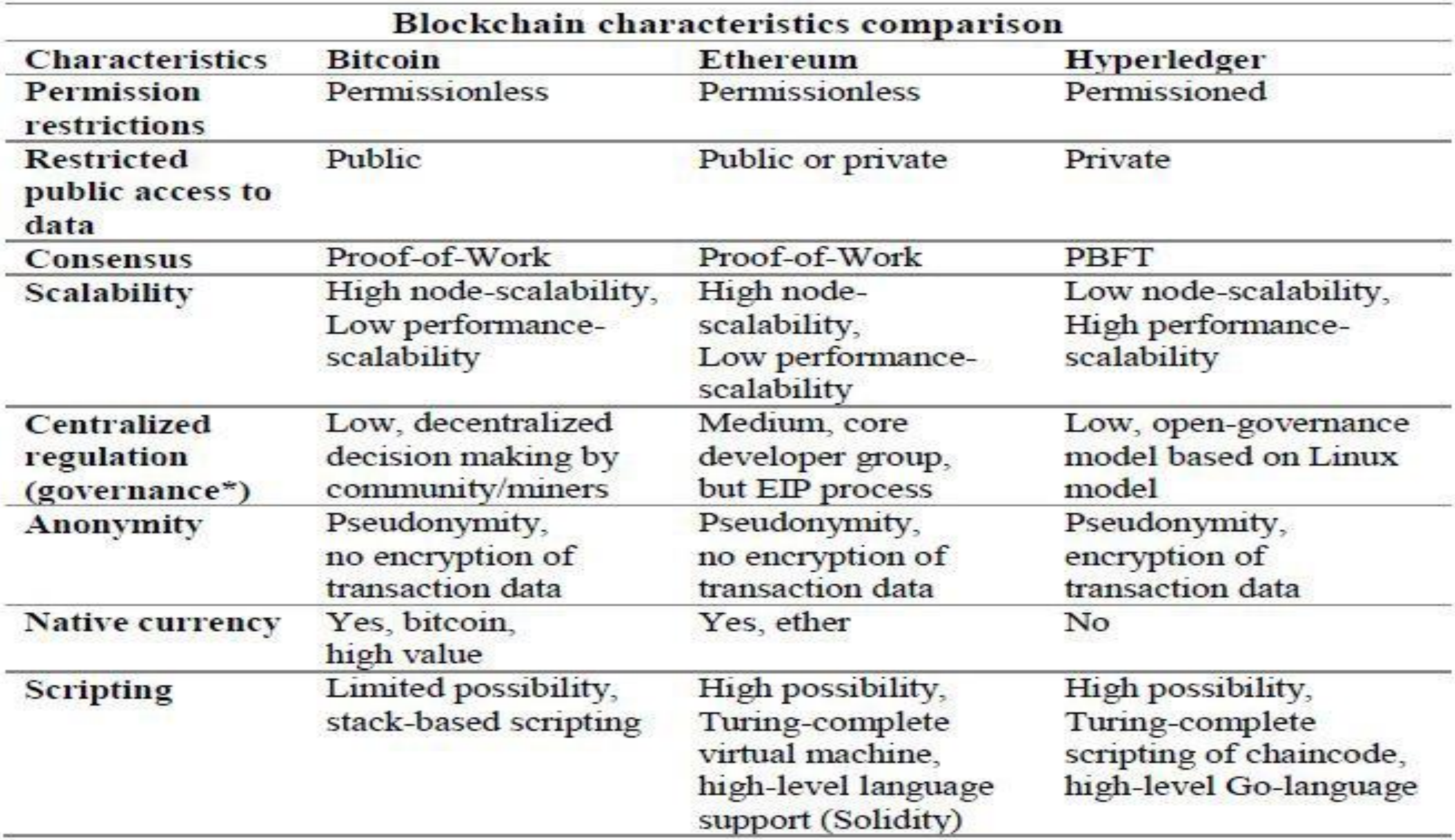
Bitcoin vs. Ethereum



VS	Bitcoin	Ethereum
Founder	Satoshi Nakamoto	Vitalik Buterin
Release Date	9 Jan 2008	30 July 2015
Release Method	Genesis Block Mined	Presale
Blockchain	Proof of work	Proof of work (Planning for POS)
Useage	Digital Currency	Smart Contracts Digital Currency
Cryptocurrency Used	Bitcoin(Satoshi)	Ether
Algorithm	SHA-256	Ethash
Blocks Time	10 Mintues	12-14 Seconds
Mining	ASIC miners	GPUs
Scalable	Not now	Yes

Bitcoin vs. Ethereum vs. Hyperledger

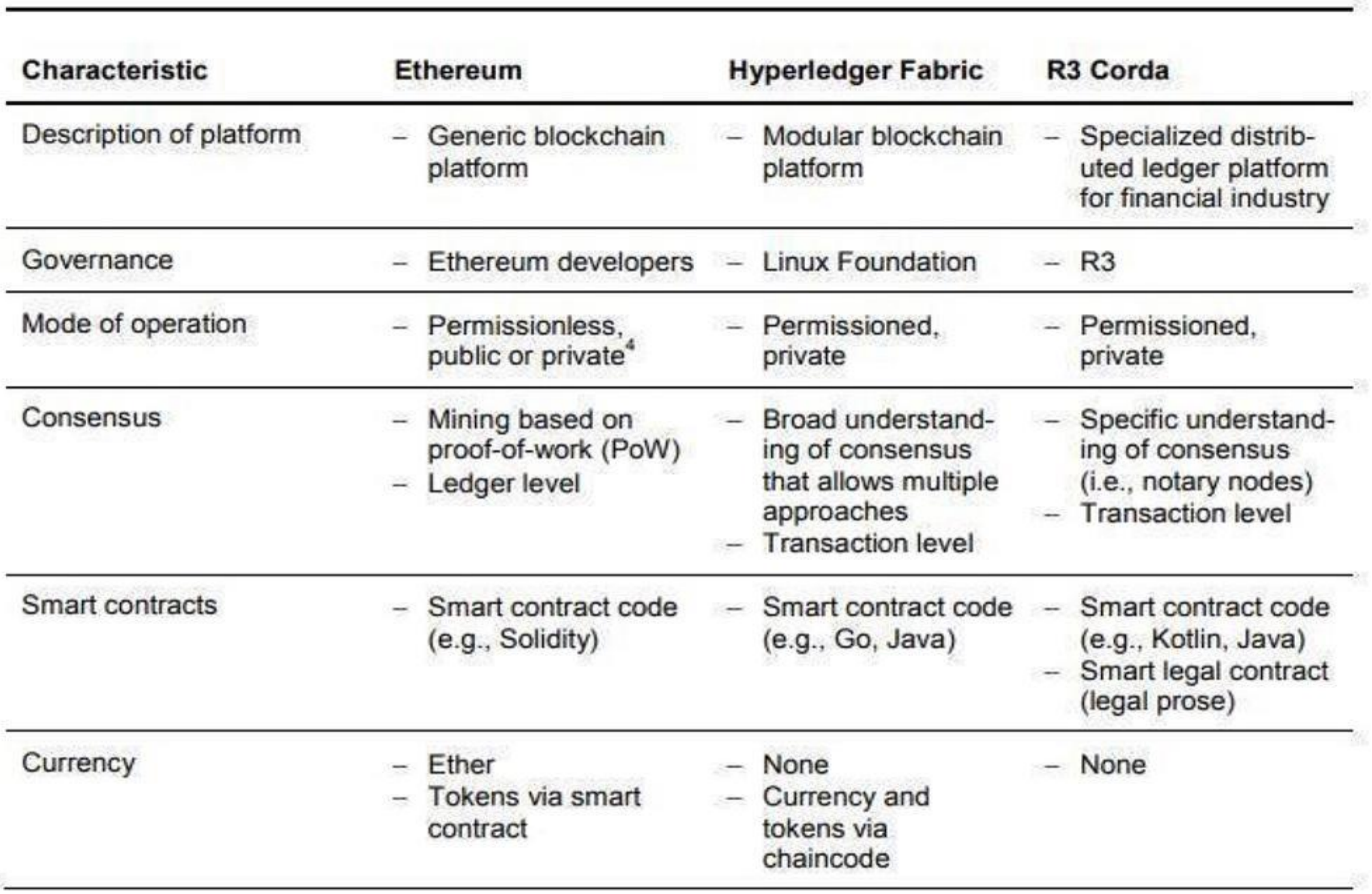
bitcoin ethereum HYPERLEDGER



Blockchain characteristics comparison

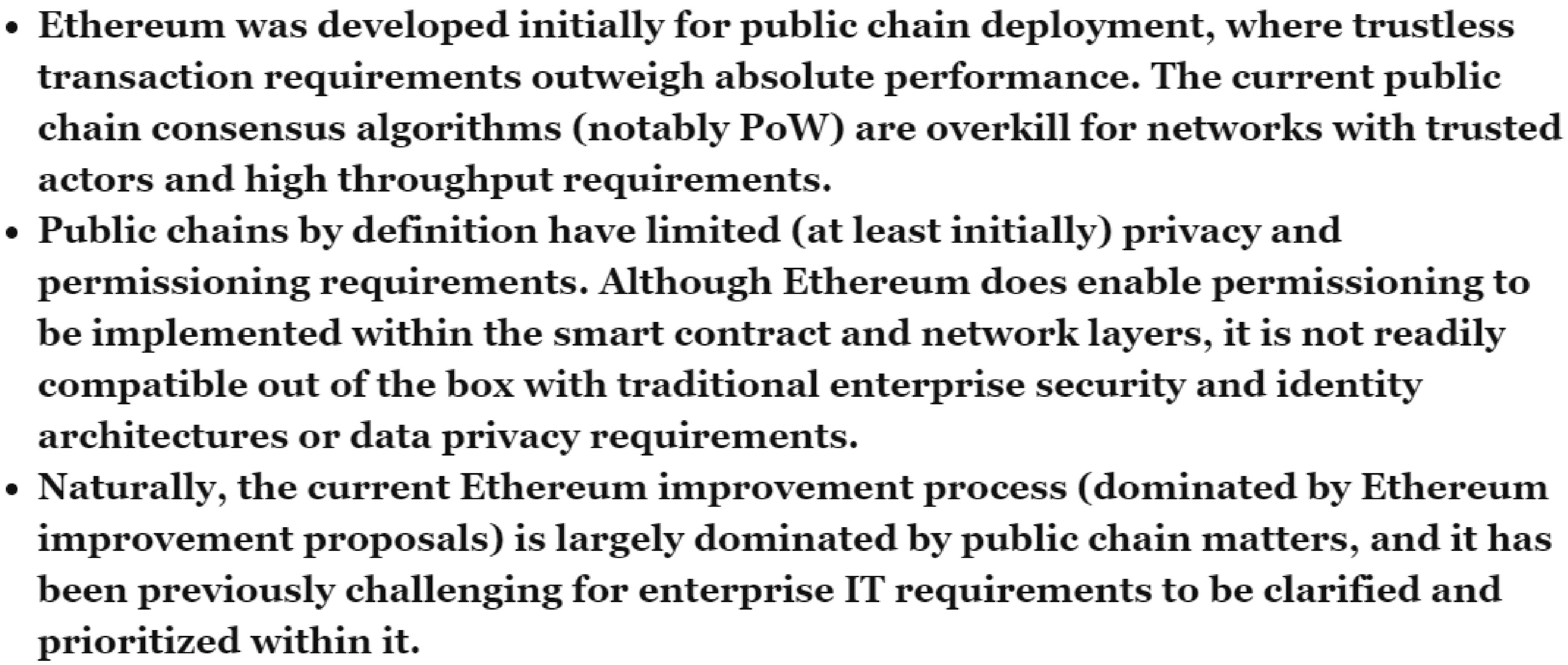
Characteristics	Bitcoin	Ethereum	Hyperledger
Permission restrictions	Permissionless	Permissionless	Permissioned
Restricted public access to data	Public	Public or private	Private
Consensus	Proof-of-Work	Proof-of-Work	PBFT
Scalability	High node-scalability, Low performance-scalability	High node-scalability, Low performance-scalability	Low node-scalability, High performance-scalability
Centralized regulation (governance*)	Low, decentralized decision making by community/miners	Medium, core developer group, but EIP process	Low, open-governance model based on Linux model
Anonymity	Pseudonymity, no encryption of transaction data	Pseudonymity, no encryption of transaction data	Pseudonymity, encryption of transaction data
Native currency	Yes, bitcoin, high value	Yes, ether	No
Scripting	Limited possibility, stack-based scripting	High possibility, Turing-complete virtual machine, high-level language support (Solidity)	High possibility, Turing-complete scripting of chaincode, high-level Go-language

Comparison of Ethereum, Hyperledger Fabric and Corda



Characteristic	Ethereum	Hyperledger Fabric	R3 Corda
Description of platform	– Generic blockchain platform	– Modular blockchain platform	– Specialized distributed ledger platform for financial industry
Governance	– Ethereum developers	– Linux Foundation	– R3
Mode of operation	– Permissionless, public or private[4]	– Permissioned, private	– Permissioned, private
Consensus	– Mining based on proof-of-work (PoW) – Ledger level	– Broad understanding of consensus that allows multiple approaches – Transaction level	– Specific understanding of consensus (i.e., notary nodes) – Transaction level
Smart contracts	– Smart contract code (e.g., Solidity)	– Smart contract code (e.g., Go, Java)	– Smart contract code (e.g., Kotlin, Java) – Smart legal contract (legal prose)
Currency	– Ether – Tokens via smart contract	– None – Currency and tokens via chaincode	– None

Ethereum Public Blockchain

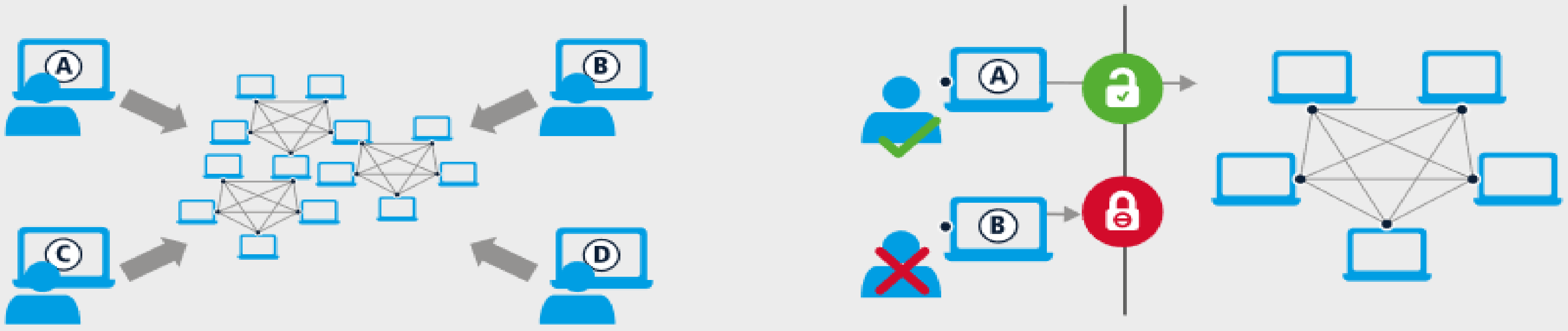


- Ethereum was developed initially for public chain deployment, where trustless transaction requirements outweigh absolute performance. The current public chain consensus algorithms (notably PoW) are overkill for networks with trusted actors and high throughput requirements.
- Public chains by definition have limited (at least initially) privacy and permissioning requirements. Although Ethereum does enable permissioning to be implemented within the smart contract and network layers, it is not readily compatible out of the box with traditional enterprise security and identity architectures or data privacy requirements.
- Naturally, the current Ethereum improvement process (dominated by Ethereum improvement proposals) is largely dominated by public chain matters, and it has been previously challenging for enterprise IT requirements to be clarified and prioritized within it.

Source: **Blockchain Basics: A Non-technical Introduction in 25 Steps**
by Daniel Drescher

Public vs. Private

PUBLIC VS. PRIVATE BLOCKCHAINS



PUBLIC, PERMISSIONLESS BLOCKCHAINS

- Anyone can join the network and submit transactions
- Anyone can contribute computing power to the network and broadcast network data
- All transactions are broadcast publicly

PRIVATE, PERMISSIONED BLOCKCHAINS

- Only safelisted (checked) participants can join the network
- Only safelisted (checked) participants can contribute computing power to the network and broadcast network data
- Access privileges determine the extent to which each safelisted participant can contribute data to the network and access data from the network

Key differences between public, permissionless blockchains and private, permissioned blockchains; **Source:** Accenture

ILLINOIS INSTITUTE
OF TECHNOLOGY

Four Functional Versions of Blockchain Distributed Ledgers

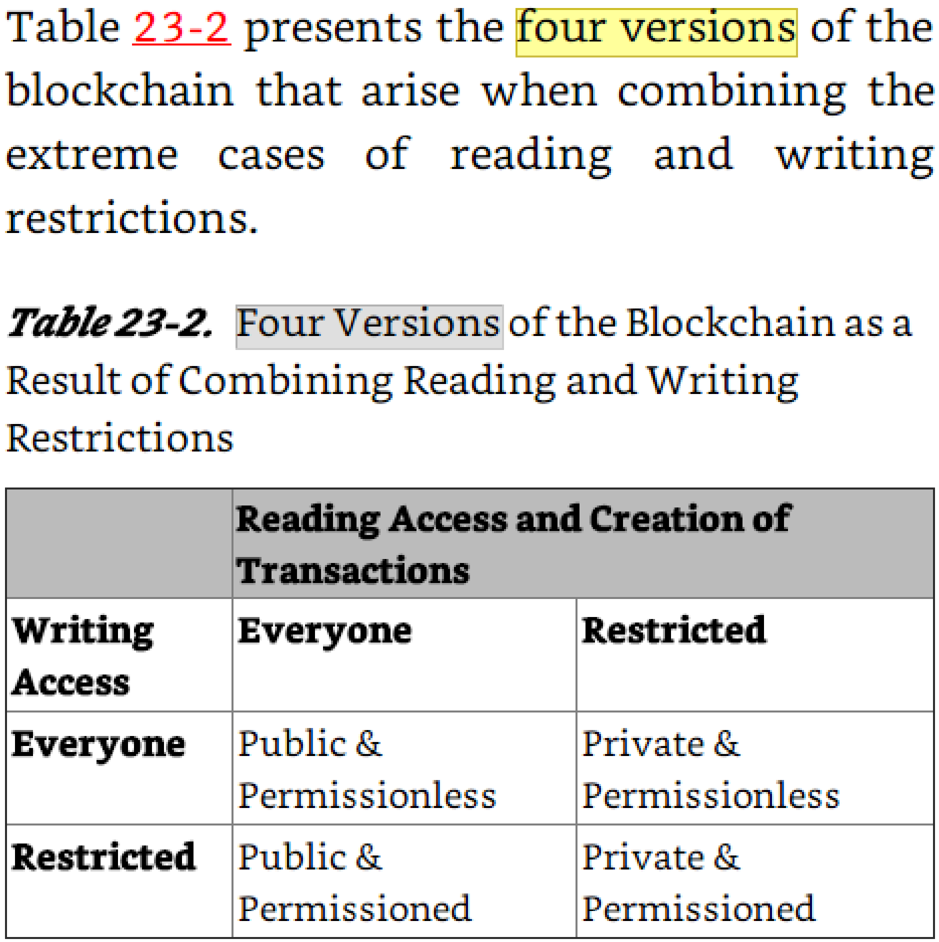


Table 23-2 presents the four versions of the blockchain that arise when combining the extreme cases of reading and writing restrictions.

Table 23-2. Four Versions of the Blockchain as a Result of Combining Reading and Writing Restrictions

	Reading Access and Creation of Transactions	
Writing Access	**Everyone**	**Restricted**
Everyone	Public & Permissionless	Private & Permissionless
Restricted	Public & Permissioned	Private & Permissioned

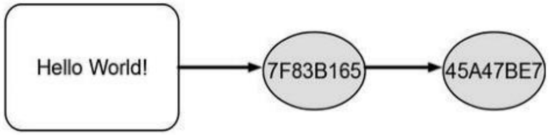
Source: **Blockchain Basics: A Non-technical Introduction in 25 Steps** by Daniel Drescher

HASH PUZZLE

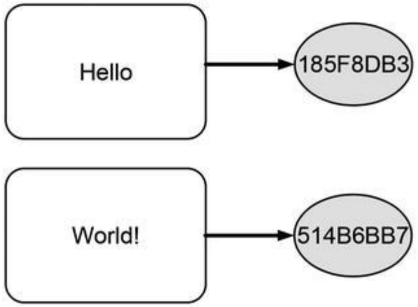
ILLINOIS INSTITUTE OF TECHNOLOGY

Hashing Data

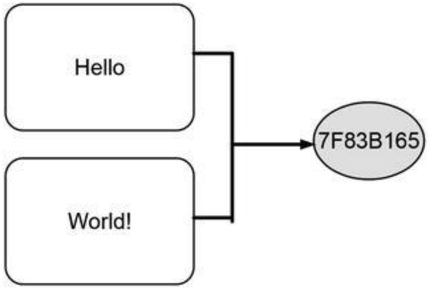
- Hash functions transform any kind of data into a number of fixed length, regardless of the size of the input data.
- There are many different hash functions that differ among others with respect to the length of the hash value they produce.
- Cryptographic hash functions are an important group of hash functions that create digital fingerprints for any kind of data.
- Cryptographic hash functions exhibit the following properties:
  - Provide hash values for any kind of data quickly
  - Deterministic
  - Pseudorandom
  - One-way usage
  - Collision resistant
- Application of hash functions to data can be accomplished by using the following patterns:
  - Repeated hashing
  - Independent hashing
  - Combined hashing
  - Sequential hashing
  - Hierarchical hashing



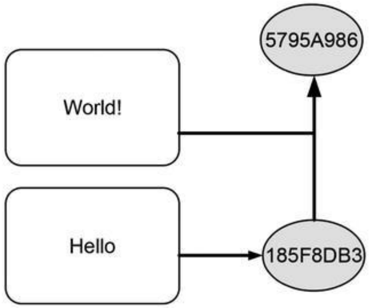
Repeated Hashing



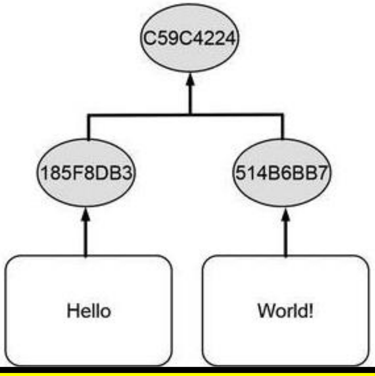
Independent Hashing



Combined Hashing



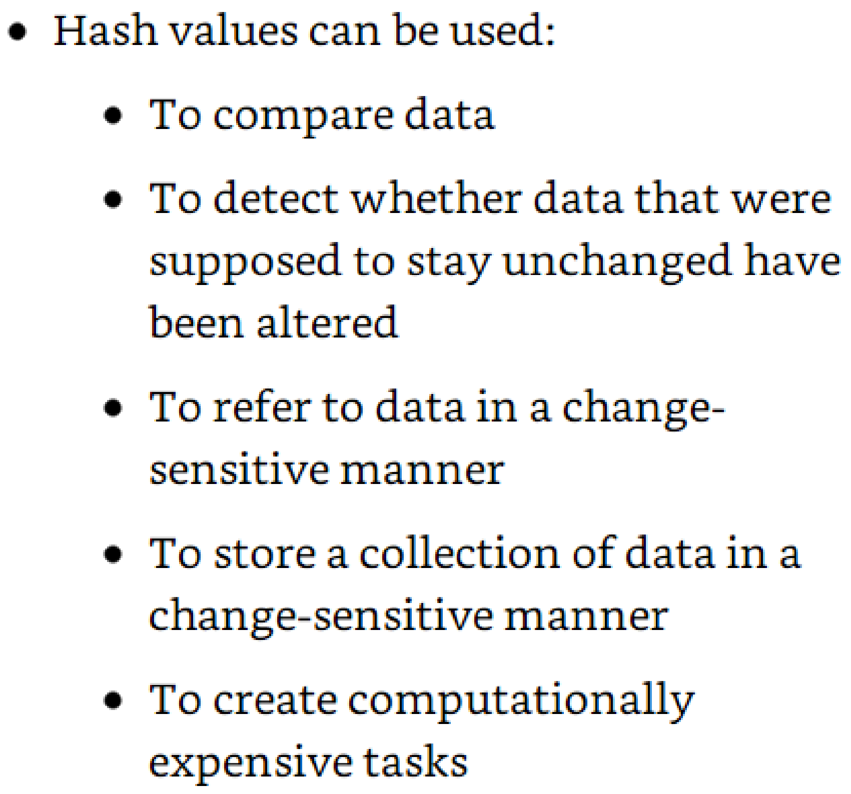
Sequential Hashing



Hierarchical Hashing

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Hashing in the Real World



- Hash values can be used:
  - To compare data
  - To detect whether data that were supposed to stay unchanged have been altered
  - To refer to data in a change-sensitive manner
  - To store a collection of data in a change-sensitive manner
  - To create computationally expensive tasks

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

Hashing in the Real World

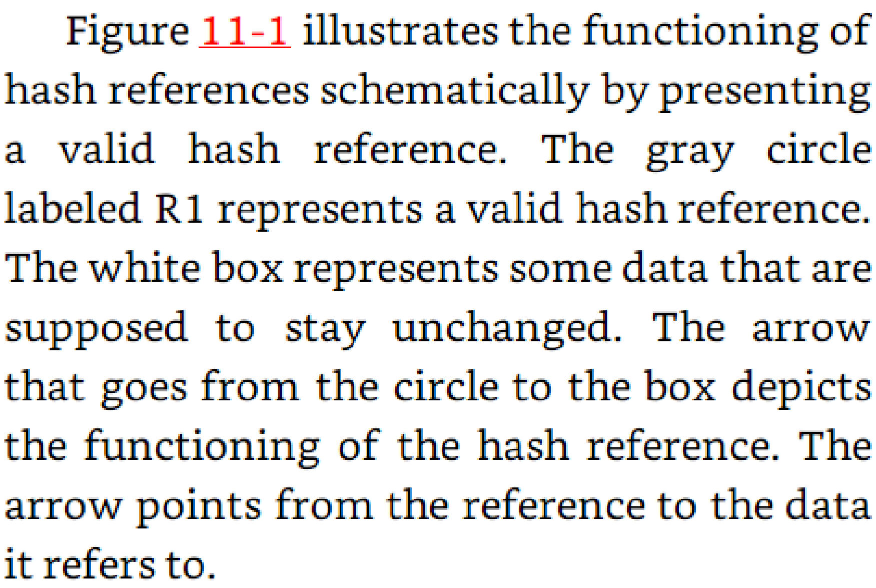
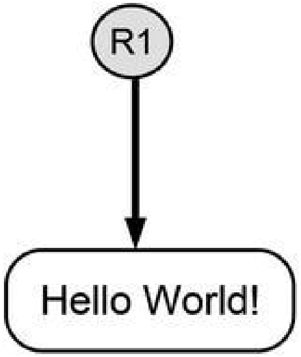


Figure 11-1 illustrates the functioning of hash references schematically by presenting a valid hash reference. The gray circle labeled R1 represents a valid hash reference. The white box represents some data that are supposed to stay unchanged. The arrow that goes from the circle to the box depicts the functioning of the hash reference. The arrow points from the reference to the data it refers to.



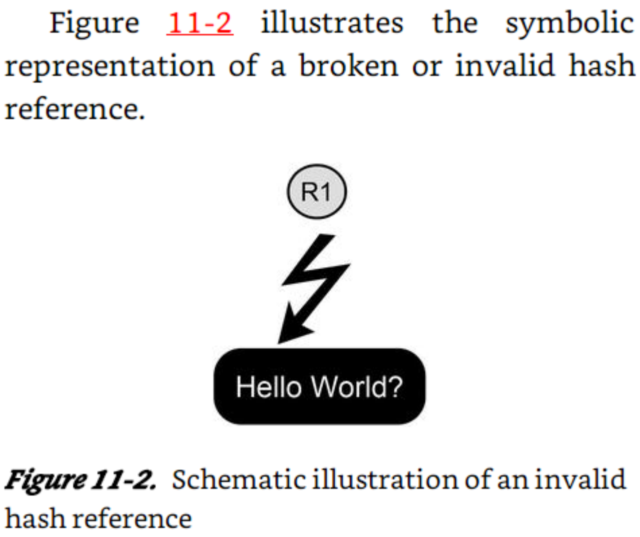


Figure 11-2 illustrates the symbolic representation of a broken or invalid hash reference.

R1
Hello World?

Figure 11-2. Schematic illustration of an invalid hash reference

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Hashing in the Real World

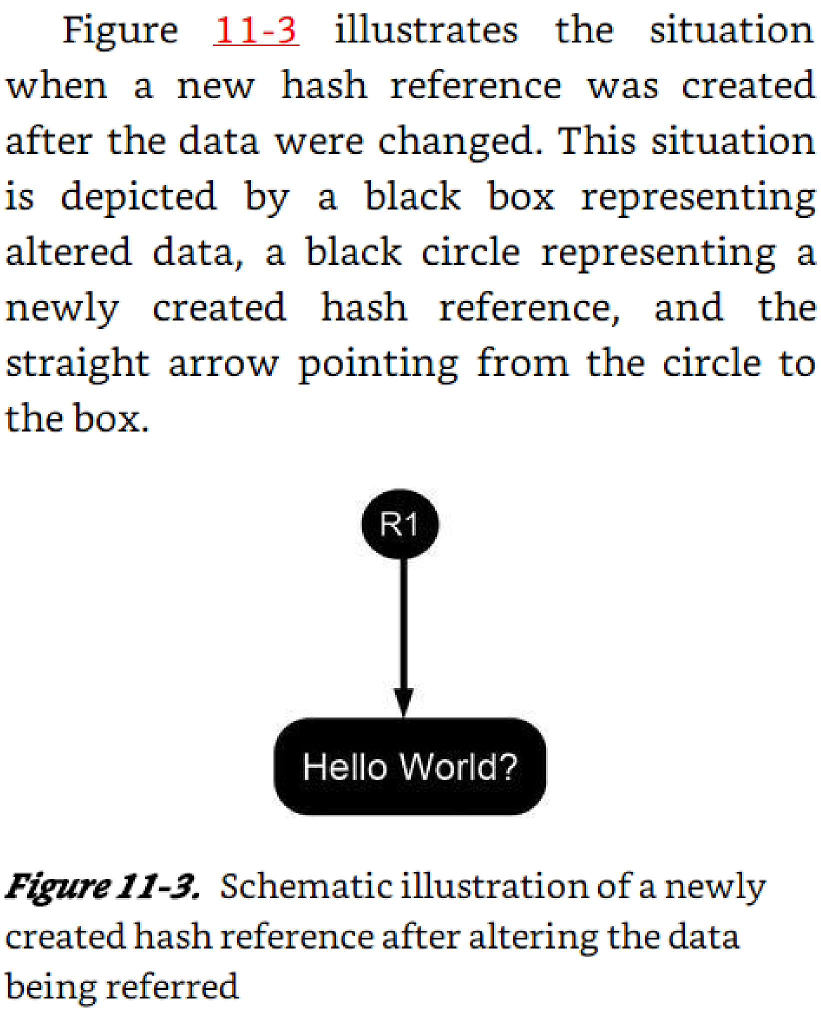


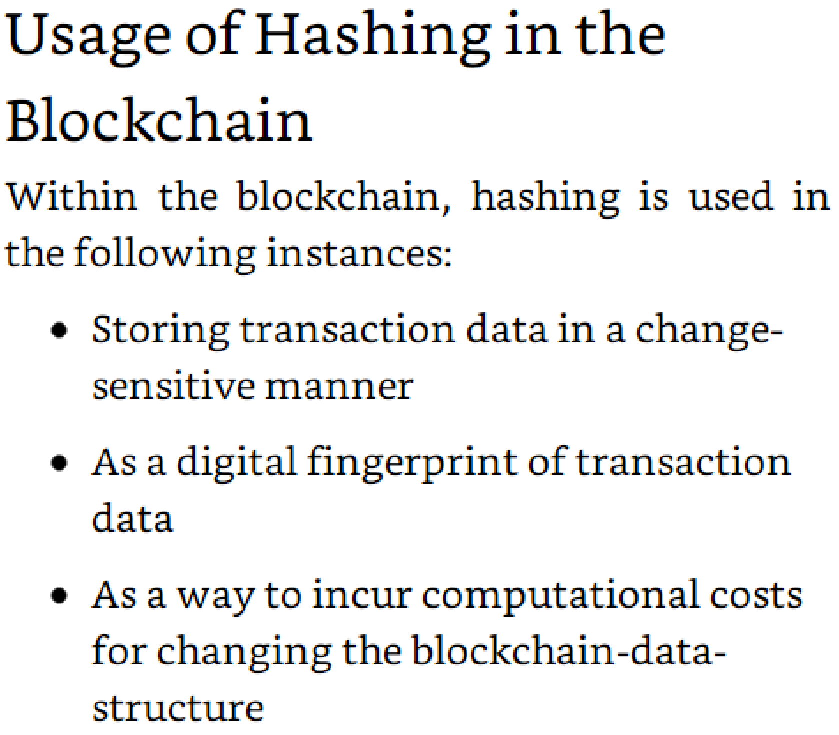
Figure 11-3 illustrates the situation when a new hash reference was created after the data were changed. This situation is depicted by a black box representing altered data, a black circle representing a newly created hash reference, and the straight arrow pointing from the circle to the box.

R1
Hello World?

Figure 11-3. Schematic illustration of a newly created hash reference after altering the data being referred

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

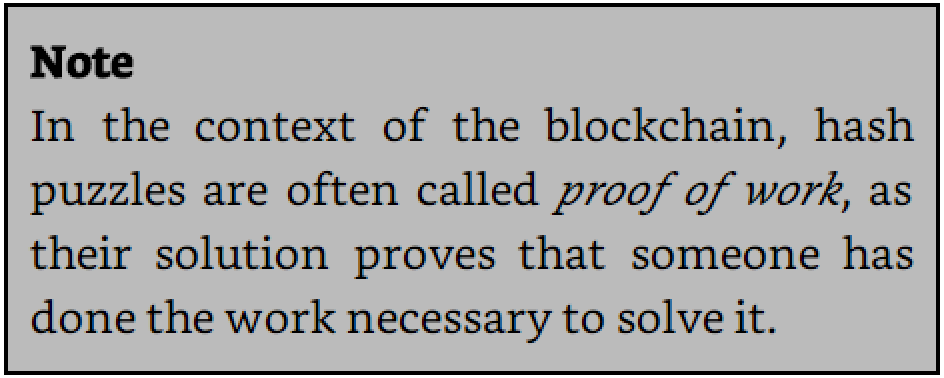
Hashing in the Real World



Usage of Hashing in the Blockchain

Within the blockchain, hashing is used in the following instances:

- Storing transaction data in a change-sensitive manner
- As a digital fingerprint of transaction data
- As a way to incur computational costs for changing the blockchain-data-structure



Note

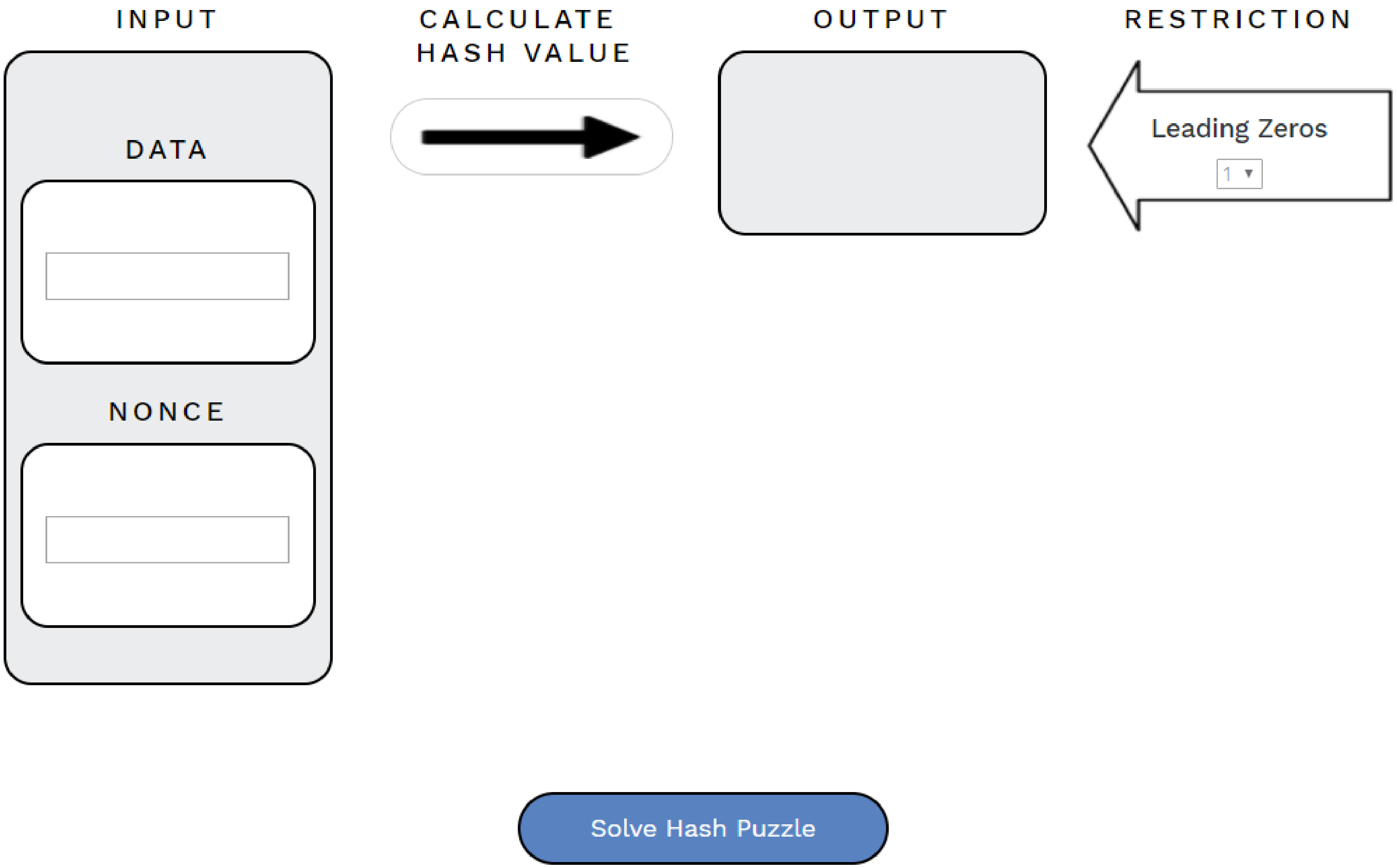
In the context of the blockchain, hash puzzles are often called *proof of work*, as their solution proves that someone has done the work necessary to solve it.

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

Hash Puzzle

Before

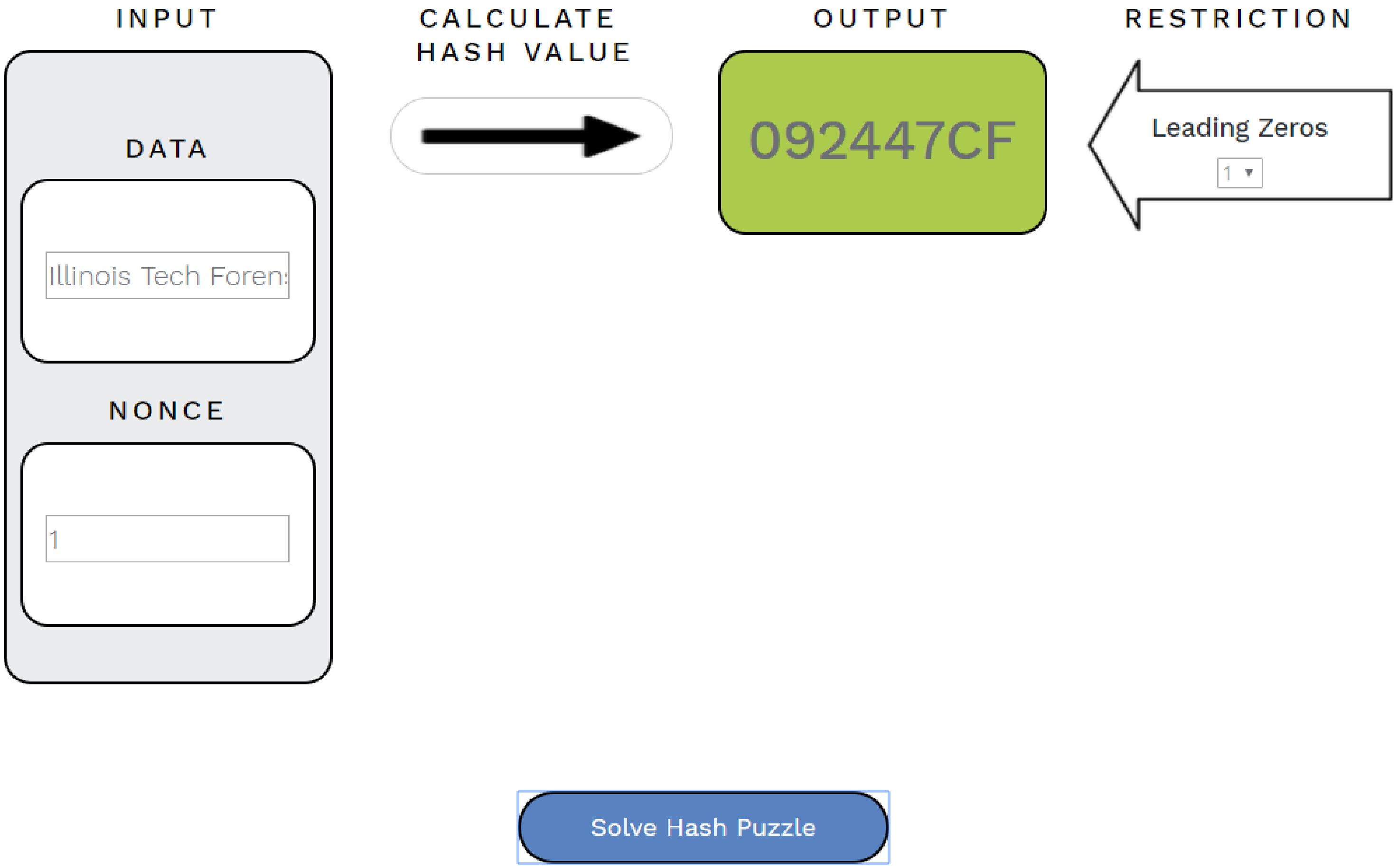


Source: http://www.blockchain-basics.com/HashPuzzle.html

ILLINOIS INSTITUTE OF TECHNOLOGY

Hash Puzzle

Test



DATA
Illinois Tech Foren

NONCE
1

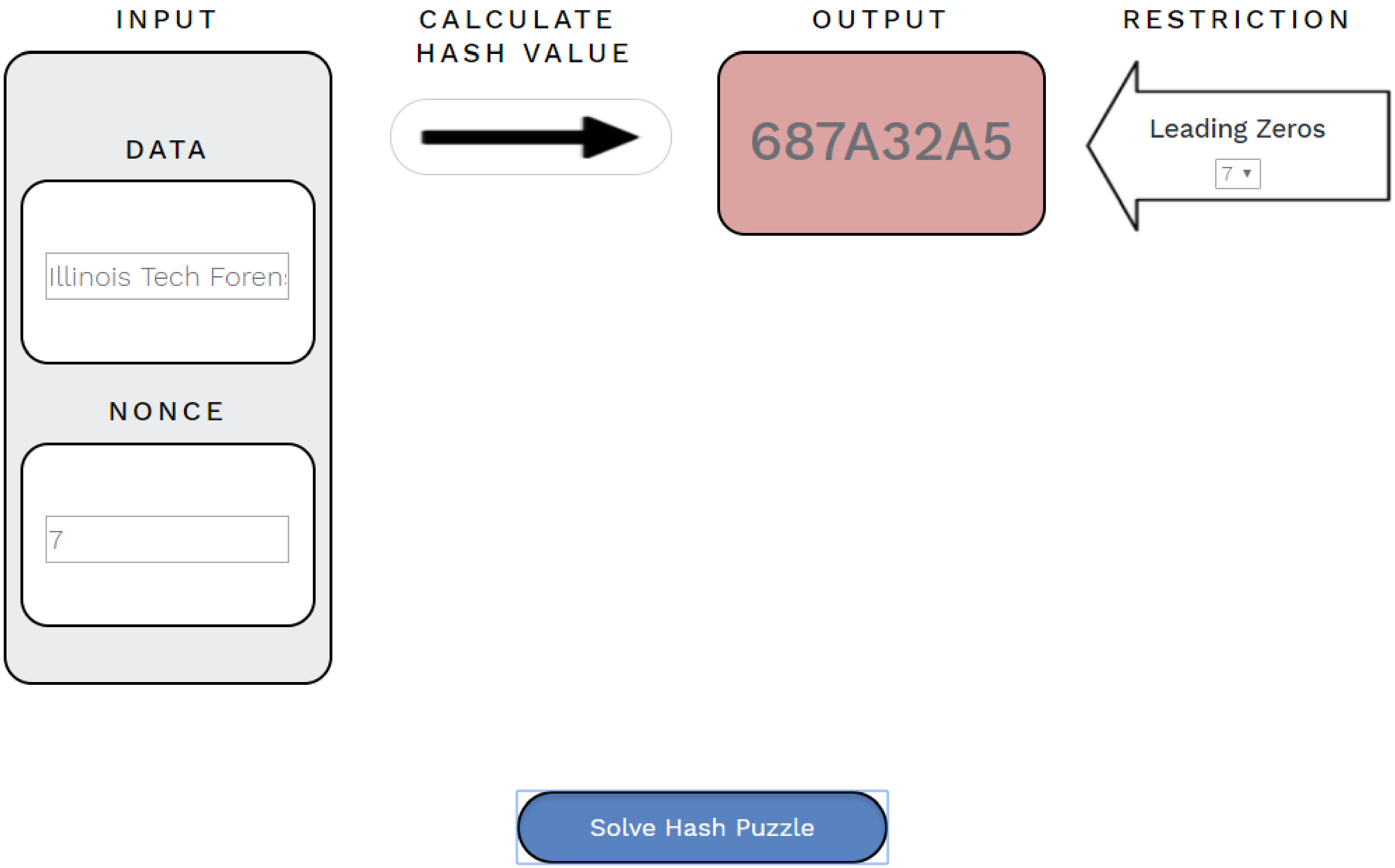
OUTPUT
092447CF

Leading Zeros
1

Source: http://www.blockchain-basics.com/HashPuzzle.html

Hash Puzzle

Test



DATA: Illinois Tech Foren:

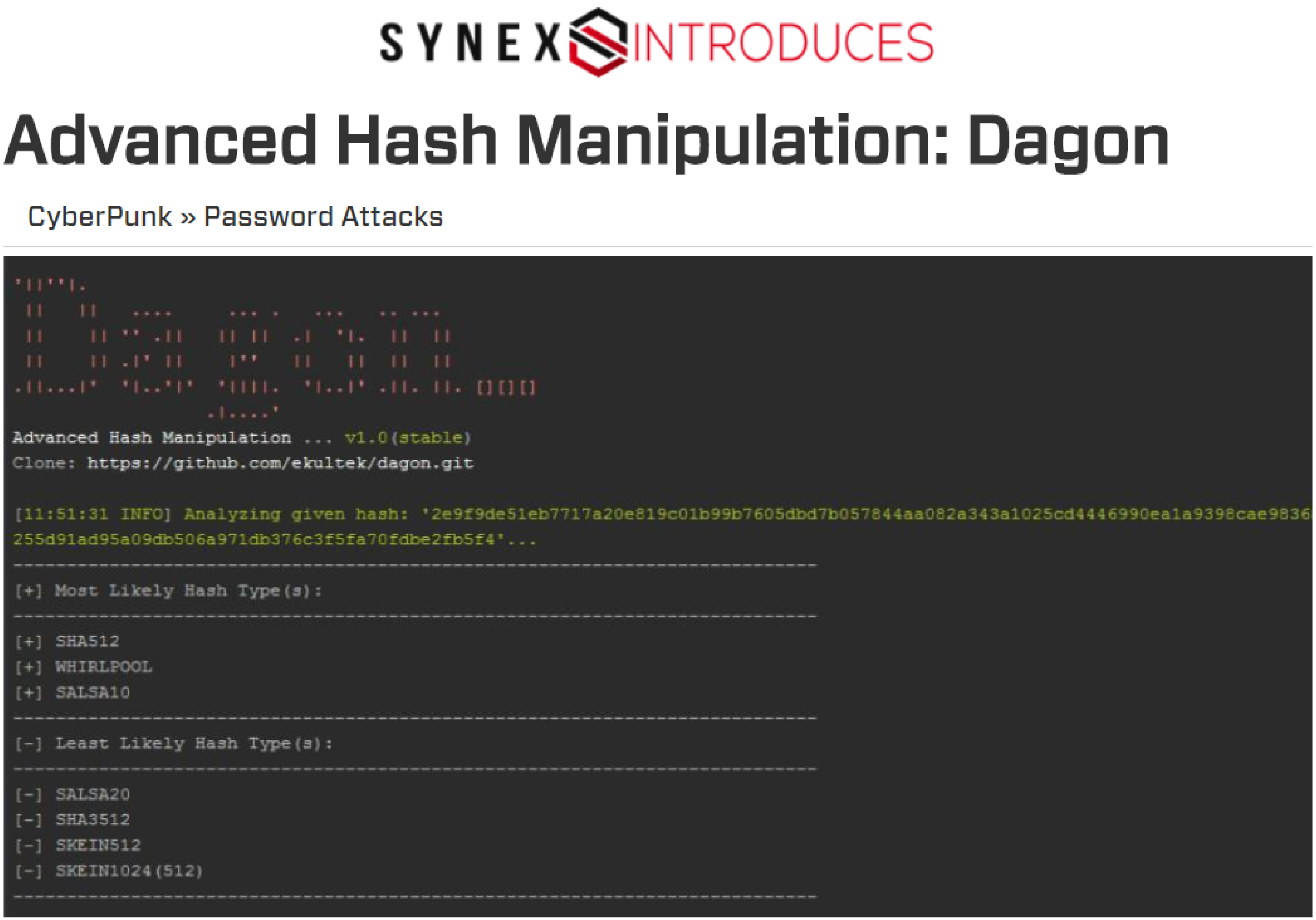
NONCE: 7

687A32A5

Leading Zeros: 7

Source: http://www.blockchain-basics.com/HashPuzzle.html

Advanced Hash Tool



SYNEX INTRODUCES

Advanced Hash Manipulation: Dagon

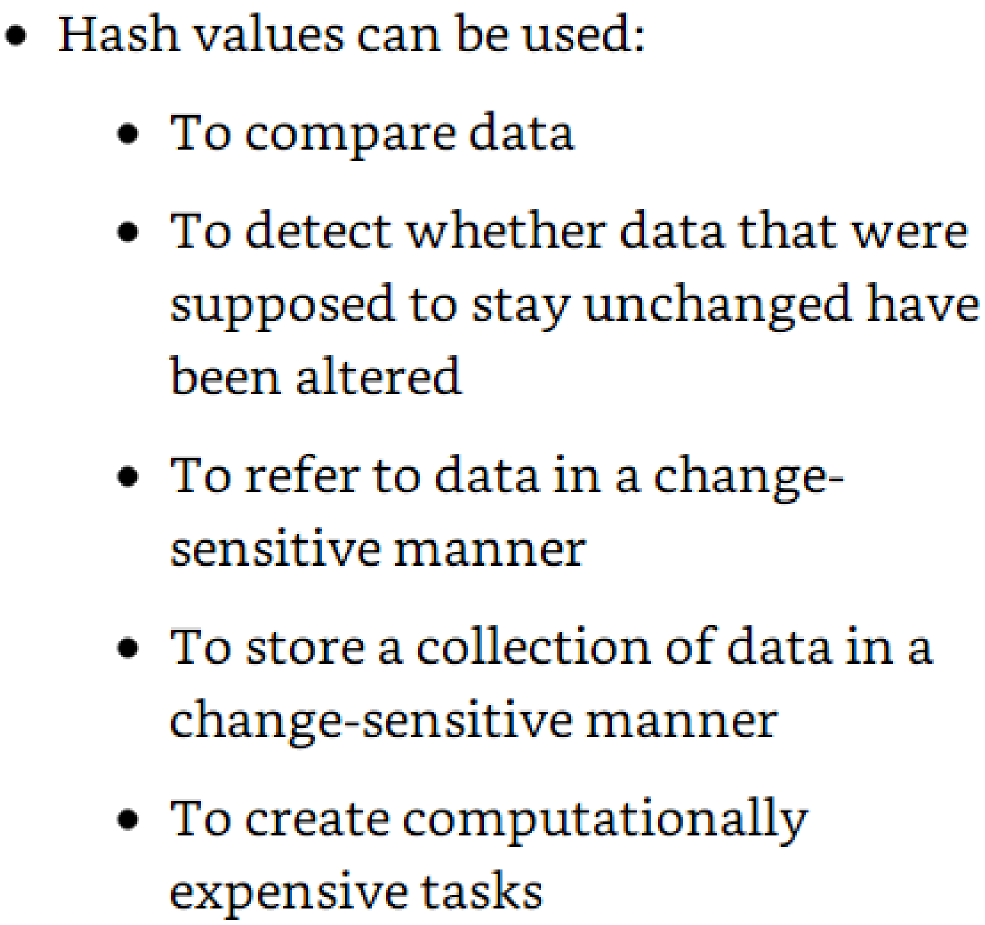
CyberPunk » Password Attacks

```
'||''|.
 ||   ||   ....     ... .   ...   .. ...
 ||    || '' .||   || ||  .|  '|.  ||  ||
 ||    || .|' ||    |''   ||   ||  ||  ||
.||...|'  '|..'|'  '||||.  '|..|' .||. ||. [][][]
                  .|....'
Advanced Hash Manipulation ... v1.0(stable)
Clone: https://github.com/ekultek/dagon.git

[11:51:31 INFO] Analyzing given hash: '2e9f9de51eb7717a20e819c01b99b7605dbd7b057844aa082a343a1025cd4446990ea1a9398cae9836
255d91ad95a09db506a971db376c3f5fa70fdbe2fb5f4'...
---------------------------------------------------------------------------
[+] Most Likely Hash Type(s):
---------------------------------------------------------------------------
[+] SHA512
[+] WHIRLPOOL
[+] SALSA10
---------------------------------------------------------------------------
[-] Least Likely Hash Type(s):
---------------------------------------------------------------------------
[-] SALSA20
[-] SHA3512
[-] SKEIN512
[-] SKEIN1024(512)
---------------------------------------------------------------------------
```

Source: https://n0where.net/advanced-hash-manipulation-dagon

Hash Use Summary



- Hash values can be used:
  - To compare data
  - To detect whether data that were supposed to stay unchanged have been altered
  - To refer to data in a change-sensitive manner
  - To store a collection of data in a change-sensitive manner
  - To create computationally expensive tasks

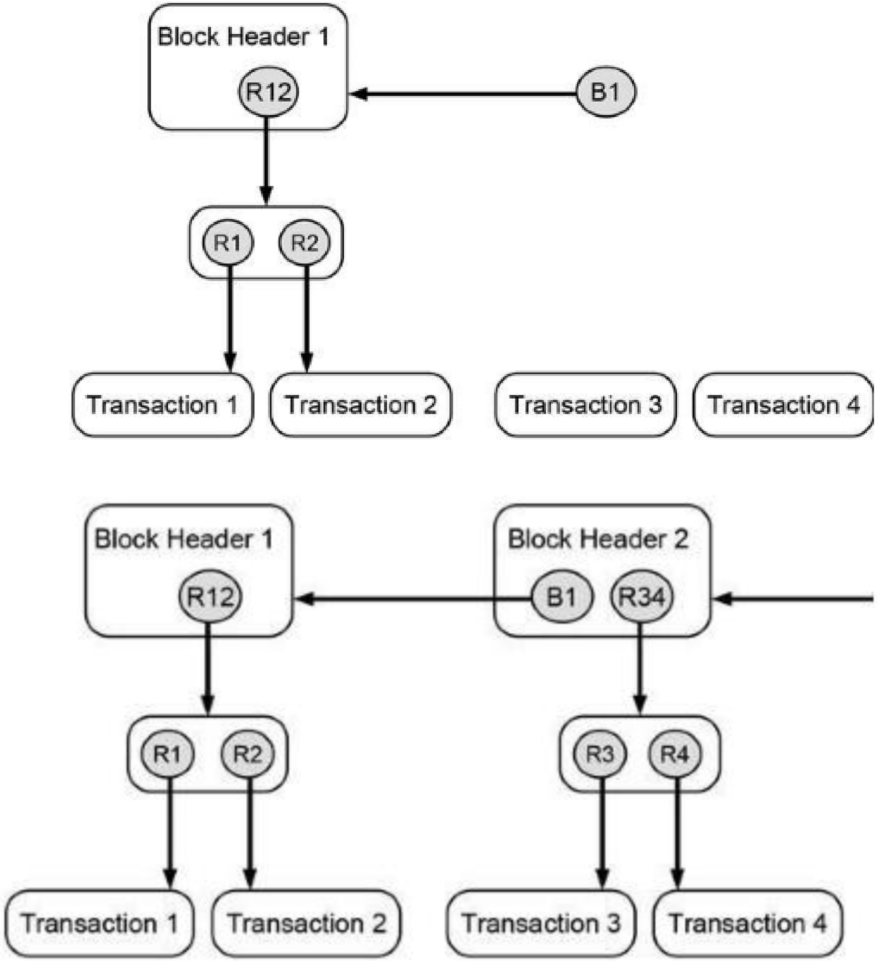
Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

MERKLE TREES

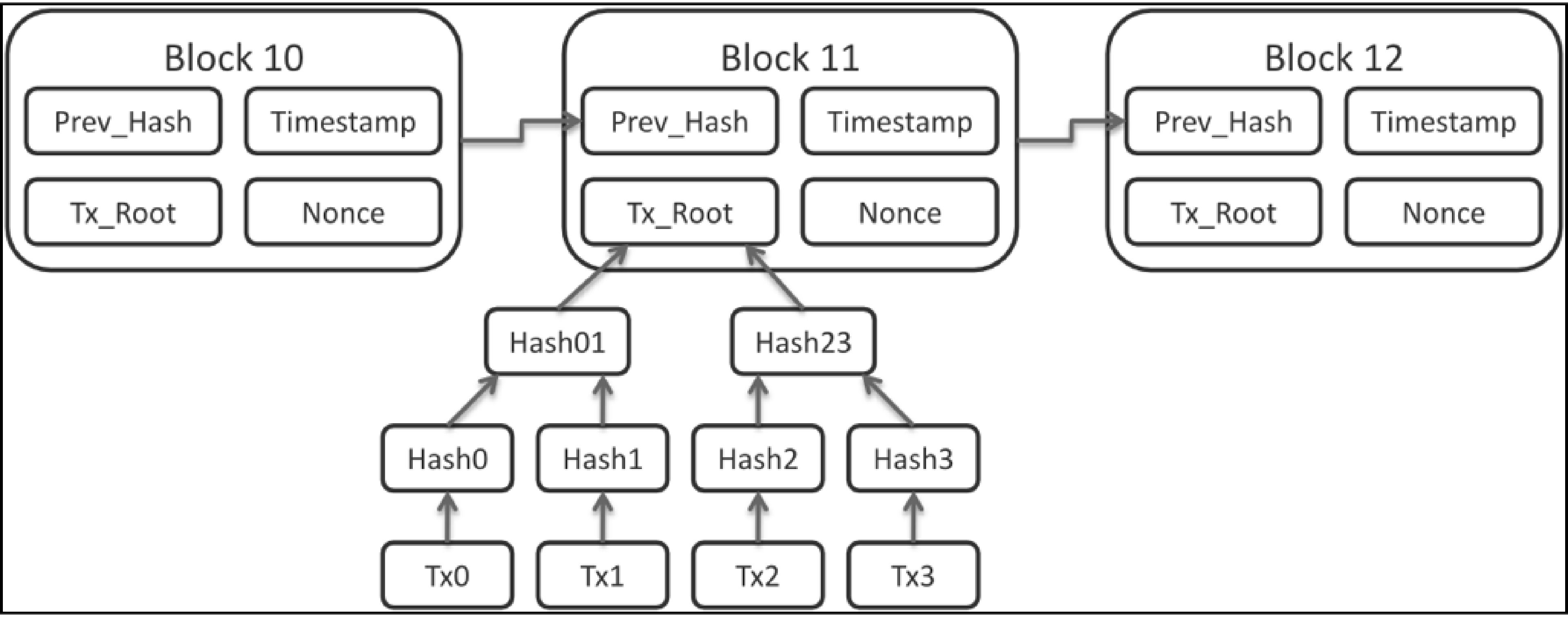
Merkle Trees

- Merkle Trees are used to add transactions to Blocks in Bitcoin Blockchains



Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Merkle Tree

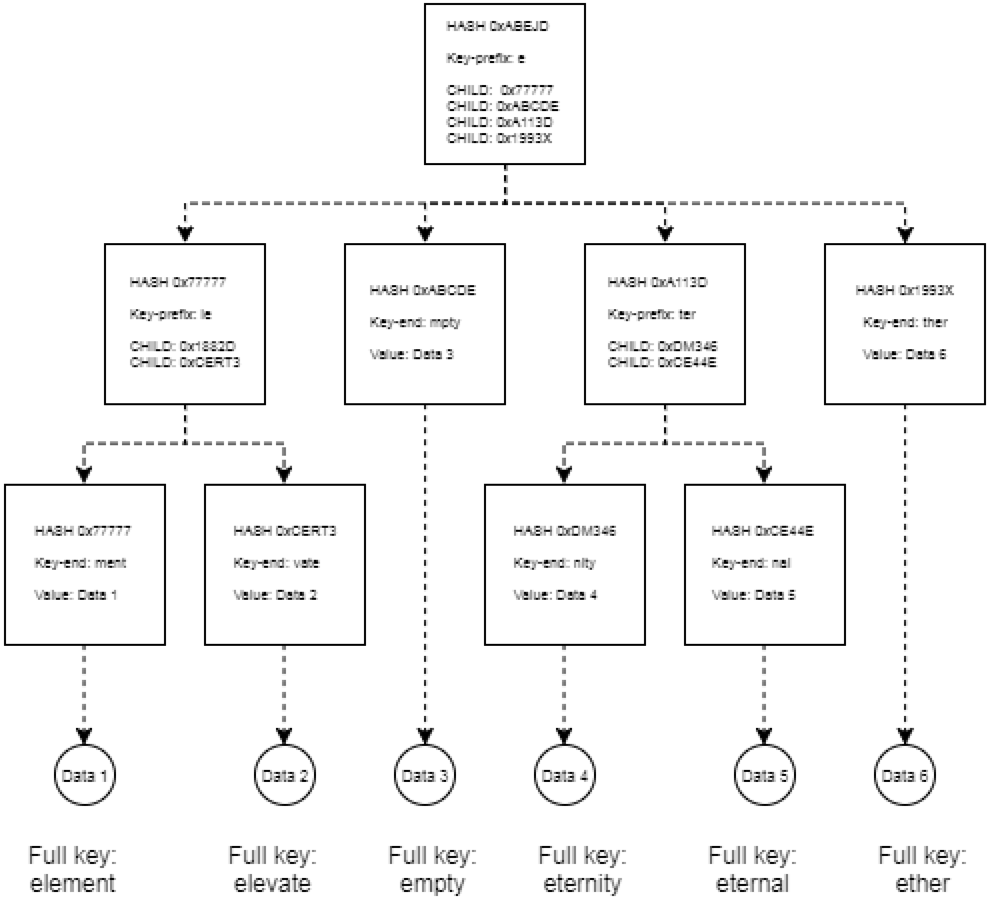


Source: Nakamoto, S. (2008).

ILLINOIS INSTITUTE
OF TECHNOLOGY

Merkle Trees

- Merkle Patricia Trees (MPT) data structures are used to add transactions to Blocks in Ethereum Blockchains to permit the use of Smart Contracts
- MPTs use private and public keys to authenticate
- The Ethereum Blockchain is categorized as “Turing Complete” because it can be programmed using languages, like Solidity and Java, and Javascript that contain looping and testing capabilities.



Source: Peterson, O. (2018). An Introduction of Programmable Smart Contracts in Ethereum (Pt 1). Retrieved from https://www.linkedin.com/pulse/introduction-programmable-smart-contracts-ethereum-p1-%CE%BE%CE%BE%CE%BE-oliver/

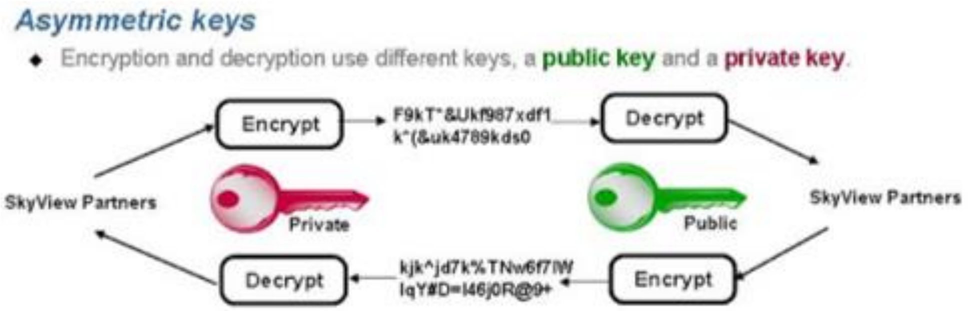
ILLINOIS INSTITUTE OF TECHNOLOGY

AUTHENTICATION IN THE BLOCKCHAIN

ILLINOIS INSTITUTE OF TECHNOLOGY

Authentication in the Blockchain

- Blockchain uses asymmetric cryptography for two purposes
  - Identification of actors
  - Authorization of transactions



Asymmetric keys

- Encryption and decryption use different keys, a **public key** and a **private key**.

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Authentication in the Blockchain

- Identifying accounts: User accounts are public cryptographic keys.
- Authorizing transactions: The owner of the account who hands off ownership creates a piece of cypher text with the corresponding private key. This piece of cypher text can be verified by using the corresponding public key, which happens to be the number of the account that hands off ownership.

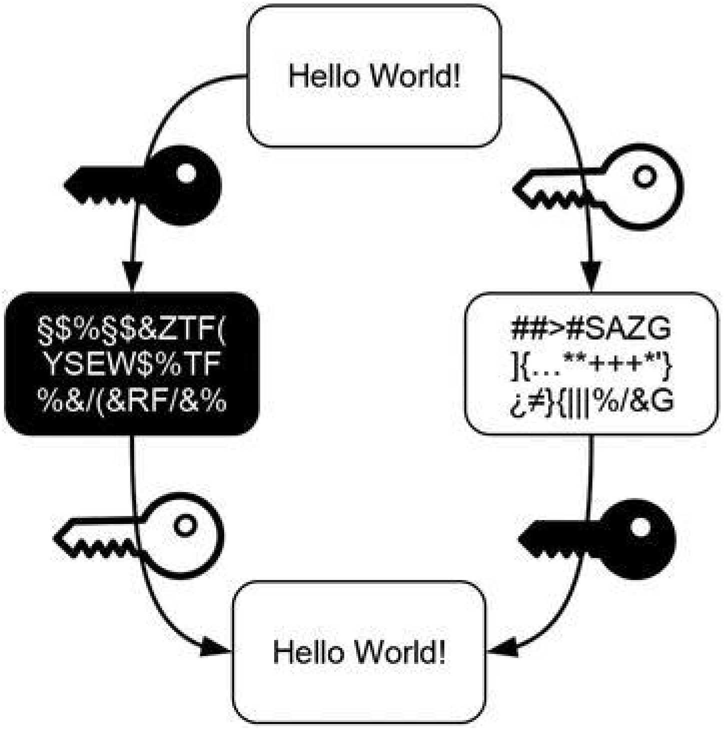


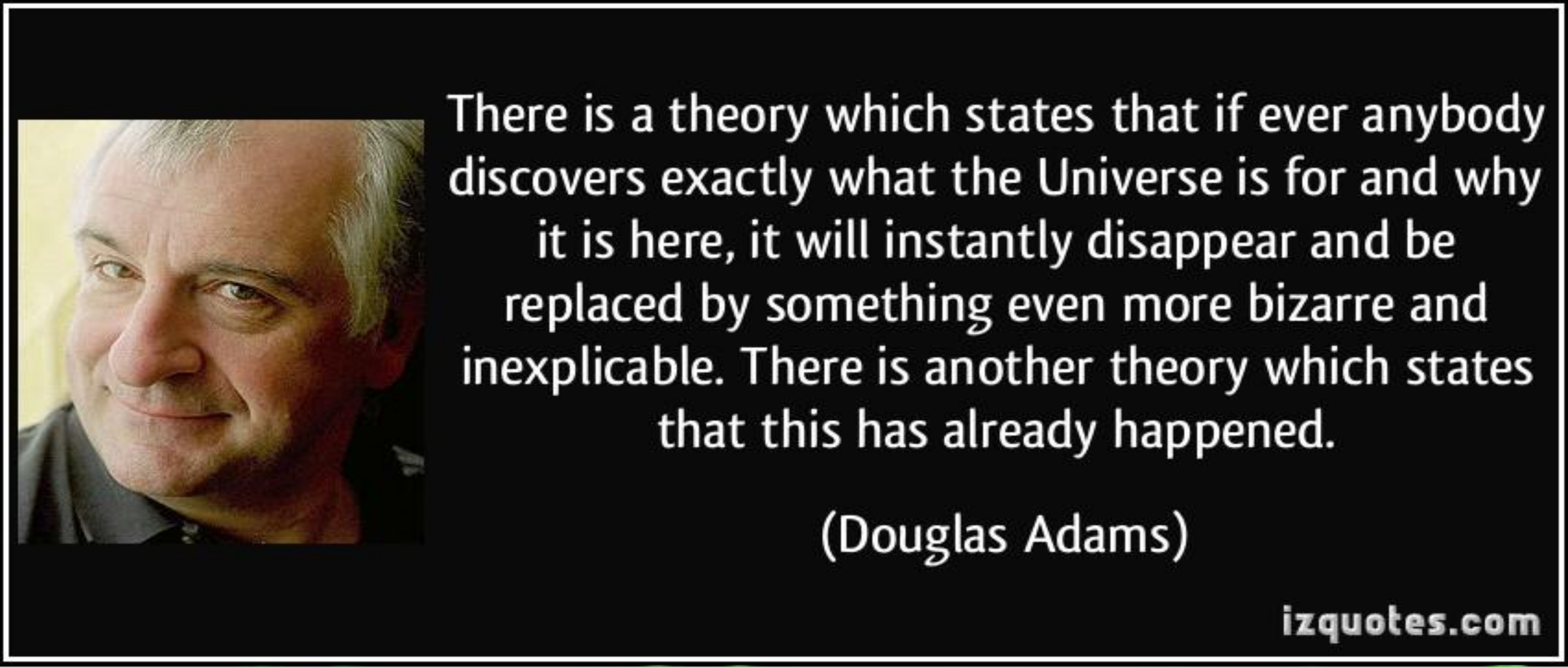
Figure 12-3. Schematic illustration of asymmetric cryptography

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

HOW DOES BLOCKCHAIN WORK?

The Great and Beautiful News… Everything you are about to see already works and works well, right now, and it is in Open Source on Git at https://github.com/bitcoin/

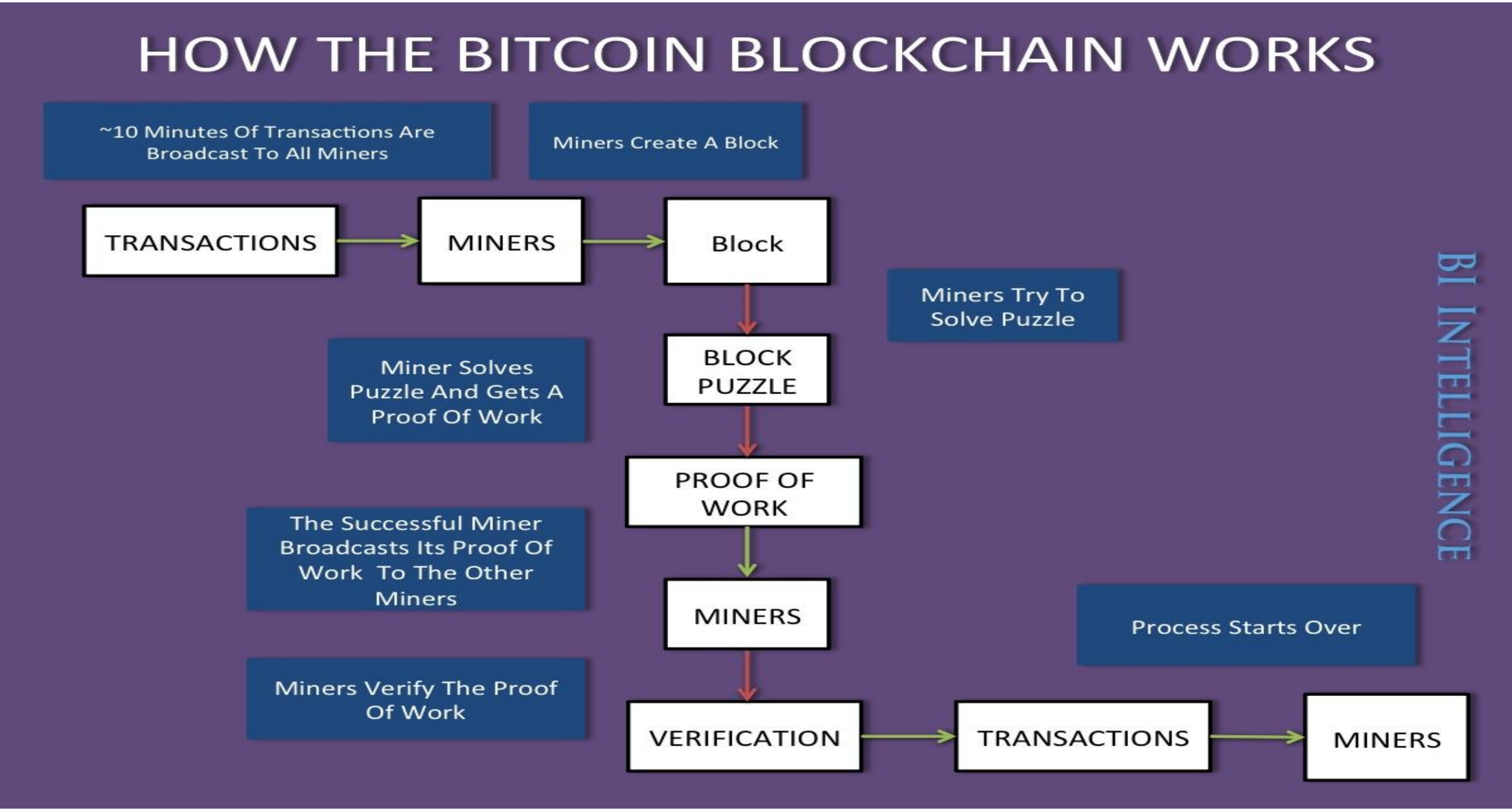


There is a theory which states that if ever anybody discovers exactly what the Universe is for and why it is here, it will instantly disappear and be replaced by something even more bizarre and inexplicable. There is another theory which states that this has already happened.

(Douglas Adams)

izquotes.com

How Does Blockchain Work?



HOW THE BITCOIN BLOCKCHAIN WORKS

~10 Minutes Of Transactions Are Broadcast To All Miners

Miners Create A Block

Miners Try To Solve Puzzle

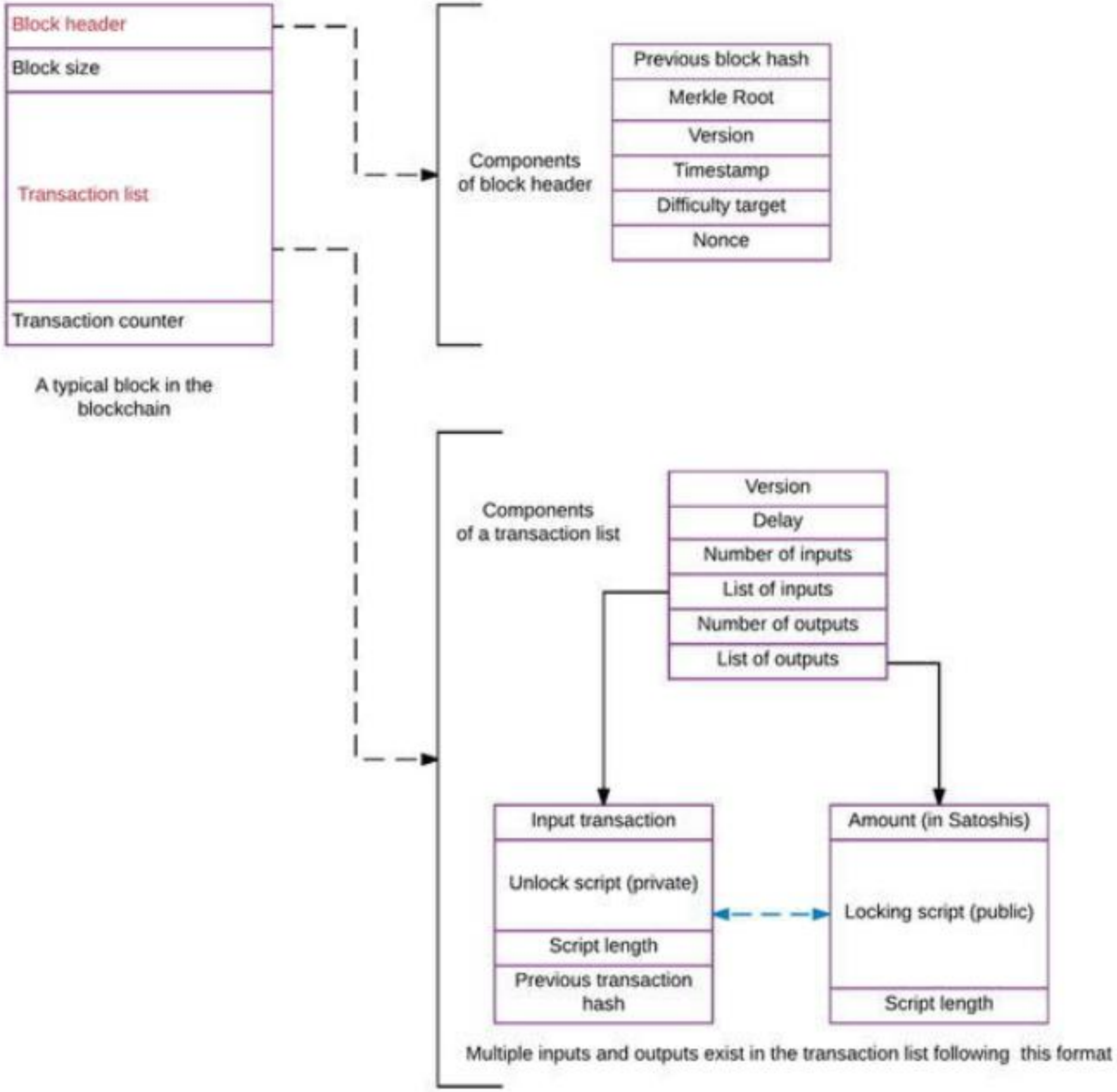
Miner Solves Puzzle And Gets A Proof Of Work

The Successful Miner Broadcasts Its Proof Of Work To The Other Miners

Miners Verify The Proof Of Work

Process Starts Over

ILLINOIS INSTITUTE OF TECHNOLOGY



Typical Block Composition:

Block Header
Block Transactions

Source: **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You** by Vikram Dhillon, David Metcalf, Max Hooper

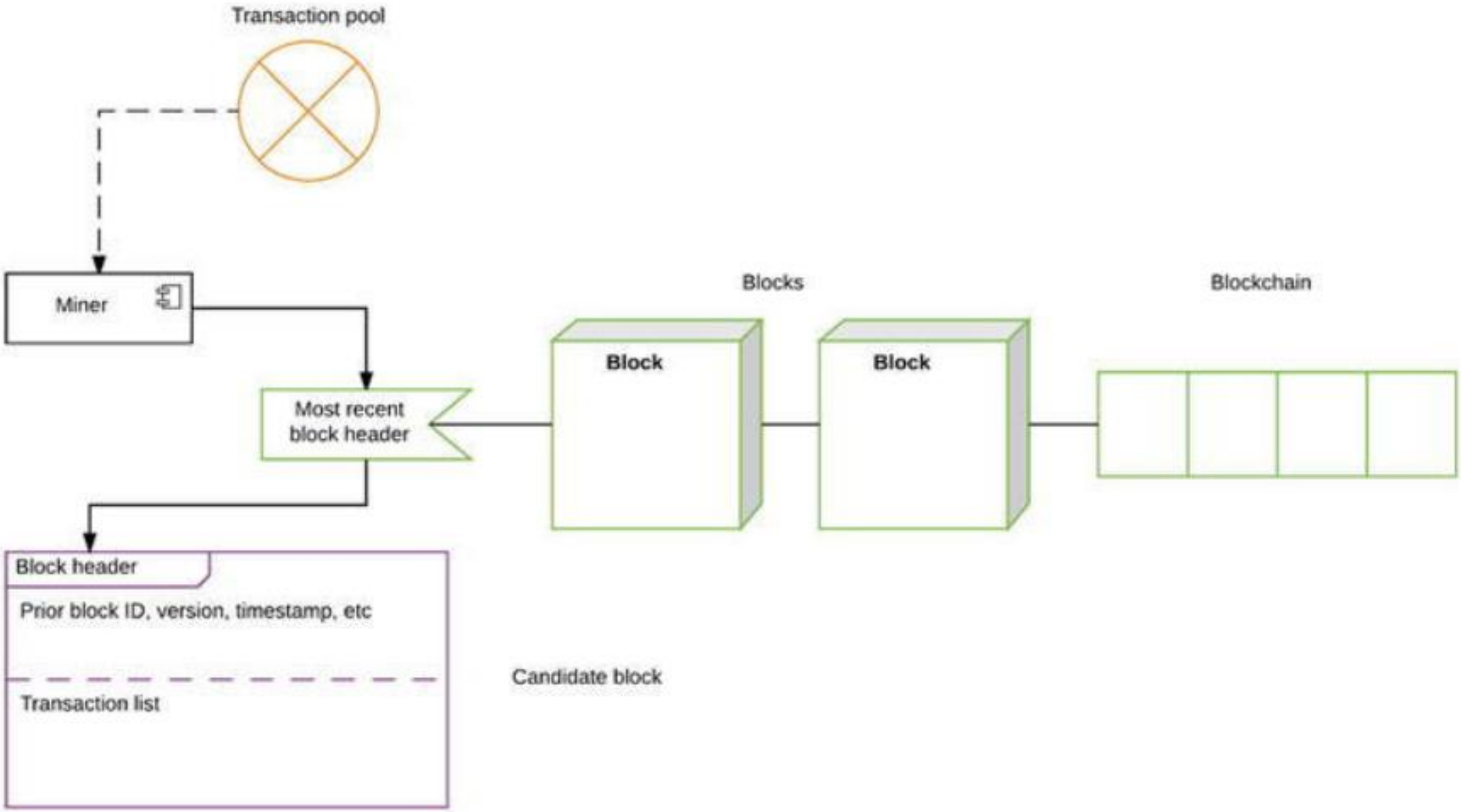


Figure 2-1.

A simplified overview of the mining process

Source: **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You** by Vikram Dhillon, David Metcalf, Max Hooper

ILLINOIS INSTITUTE OF TECHNOLOGY

Bitcoin Mining Principles

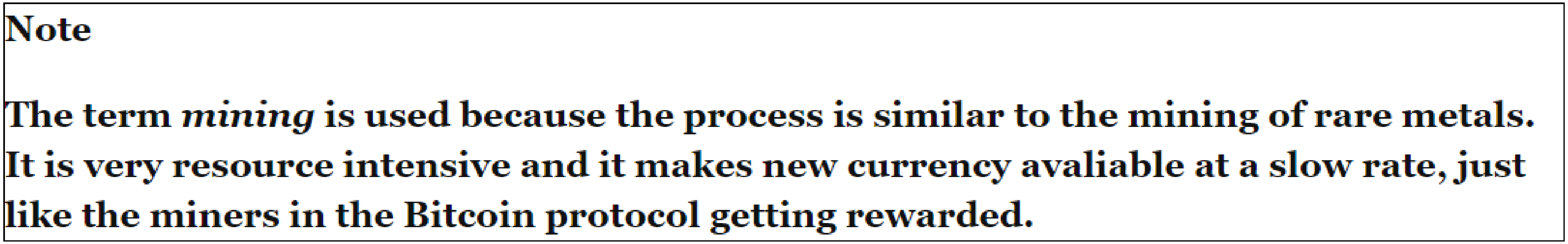
1. 1.
An increase in mining difficulty causes a decrease in the target value to compensate for the mining time.

2. 2.
An increase in the number of miners joining the network causes an increase in the rate at which PoW is solved, decreasing the mining time. To adjust for this, mining difficulty increases and the block creation rate returns to normal.

3. 3.
The target value is recalculated and adjusted every 2,016 blocks created, which happens in approximately two weeks.

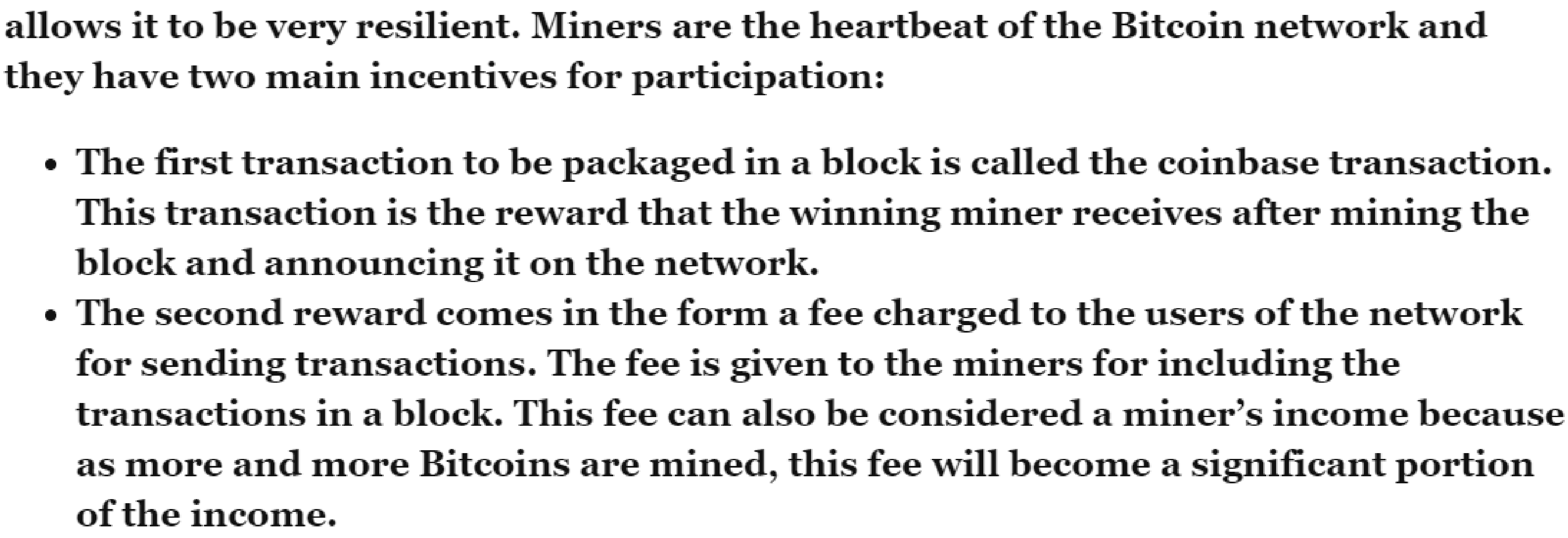
Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

More on Bitcoin Blockchain Mining



Note

The term *mining* is used because the process is similar to the mining of rare metals. It is very resource intensive and it makes new currency avaliable at a slow rate, just like the miners in the Bitcoin protocol getting rewarded.



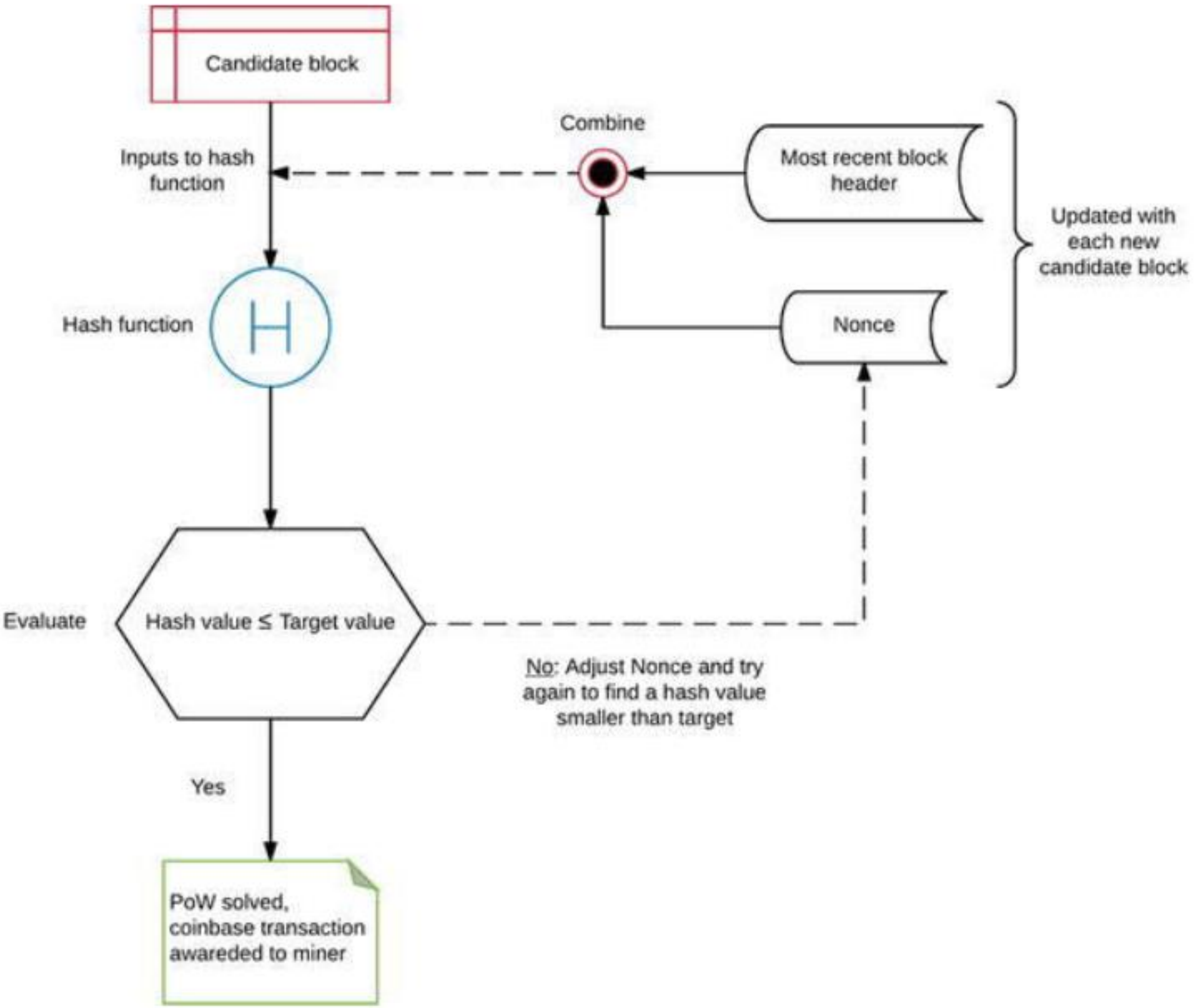
allows it to be very resilient. Miners are the heartbeat of the Bitcoin network and they have two main incentives for participation:

- The first transaction to be packaged in a block is called the coinbase transaction. This transaction is the reward that the winning miner receives after mining the block and announcing it on the network.
- The second reward comes in the form a fee charged to the users of the network for sending transactions. The fee is given to the miners for including the transactions in a block. This fee can also be considered a miner's income because as more and more Bitcoins are mined, this fee will become a significant portion of the income.

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE
OF TECHNOLOGY

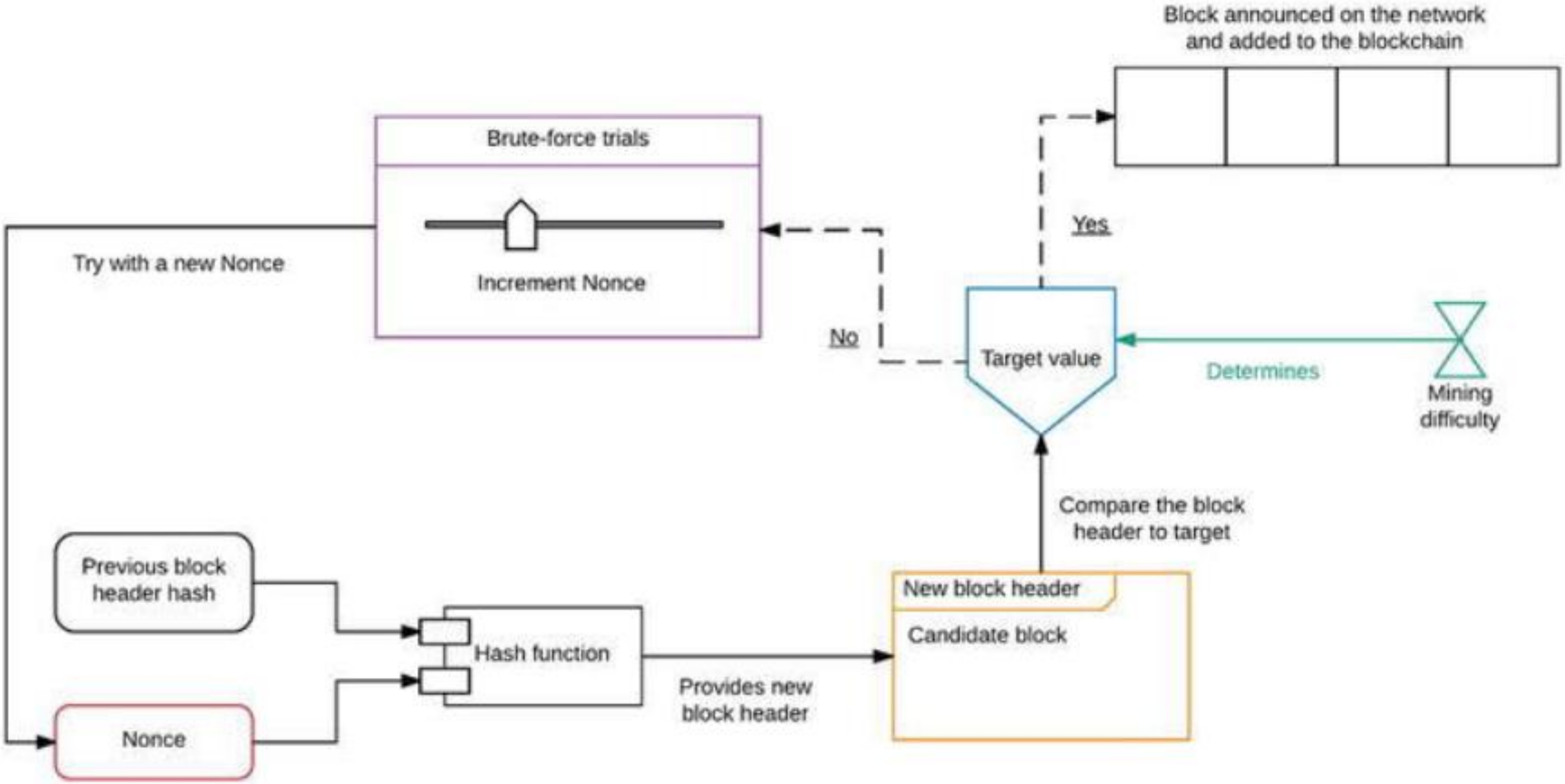
Proof of Work


Candidate block
Inputs to hash function
Combine
Most recent block header
Updated with each new candidate block
Hash function
H
Nonce
Evaluate
Hash value ≤ Target value
No: Adjust Nonce and try again to find a hash value smaller than target
Yes
PoW solved, coinbase transaction awareded to miner

Source: **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You** by Vikram Dhillon, David Metcalf, Max Hooper

ILLINOIS INSTITUTE OF TECHNOLOGY

Solving the Proof of Work Problem



Source: **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You** by Vikram Dhillon, David Metcalf, Max Hooper

ILLINOIS INSTITUTE OF TECHNOLOGY

Block Creation

1. Get the root of the Merkle tree that contains the transaction data to be added.
2. Create a hash reference to the header of that block that will be the predecessor from the new block header's point of view.
3. Obtain the required difficulty level.
4. Get the current time.
5. Create a preliminary block header that contains the data mentioned in points 1 to 4.
6. Solve the hash puzzle for the preliminary block header.
7. Finish the new block by adding the nonce that solves the hash puzzle to the preliminary header.

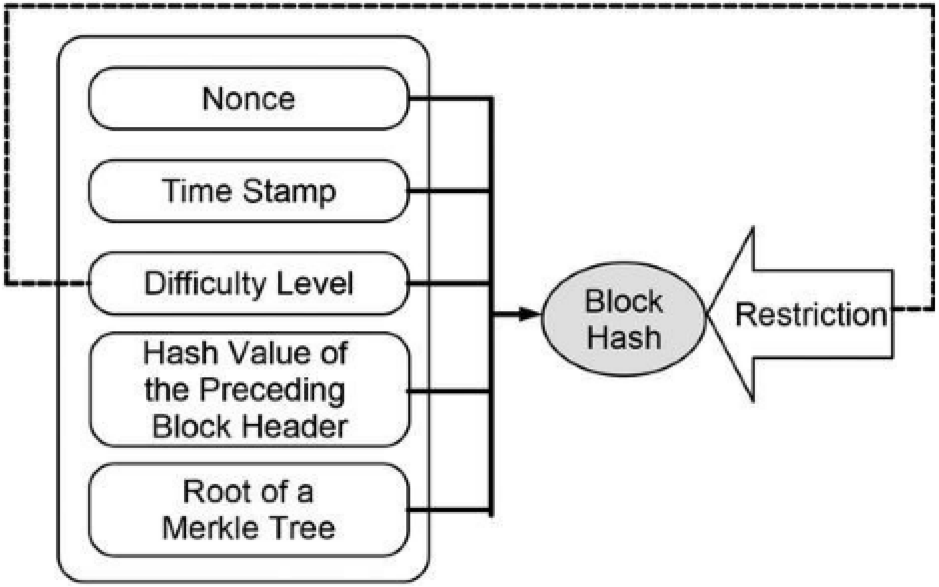
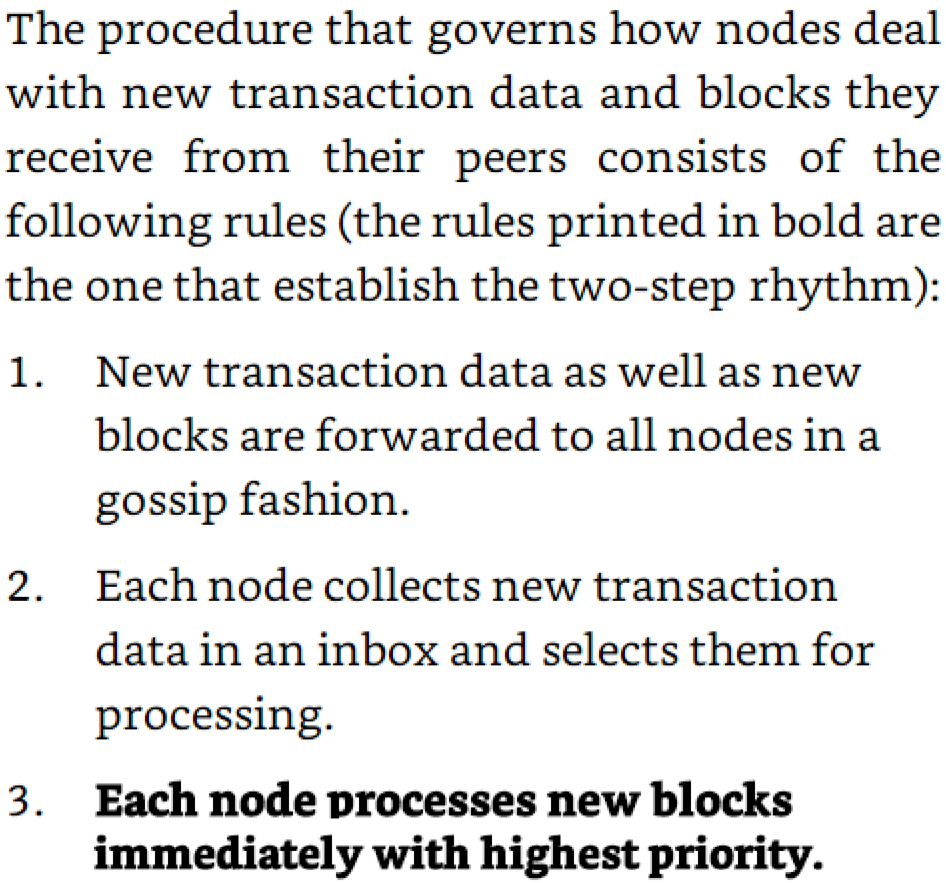


Figure 16-1. *Schematic illustration of the hash puzzle required to be solved when adding a new block to the blockchain-data- structure*

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

How Blockchain Works – In Detail (part 1)

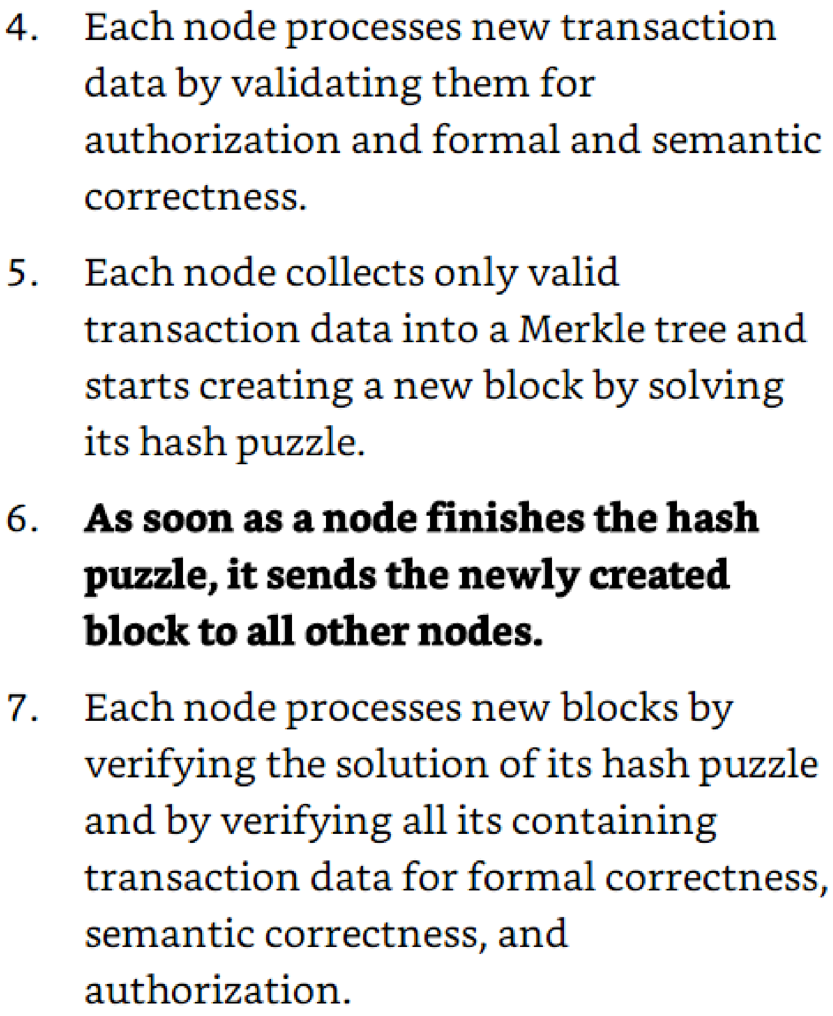


The procedure that governs how nodes deal with new transaction data and blocks they receive from their peers consists of the following rules (the rules printed in bold are the one that establish the two-step rhythm):

1. New transaction data as well as new blocks are forwarded to all nodes in a gossip fashion.
2. Each node collects new transaction data in an inbox and selects them for processing.
3. **Each node processes new blocks immediately with highest priority.**

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

How Blockchain Works – In Detail (part 2)

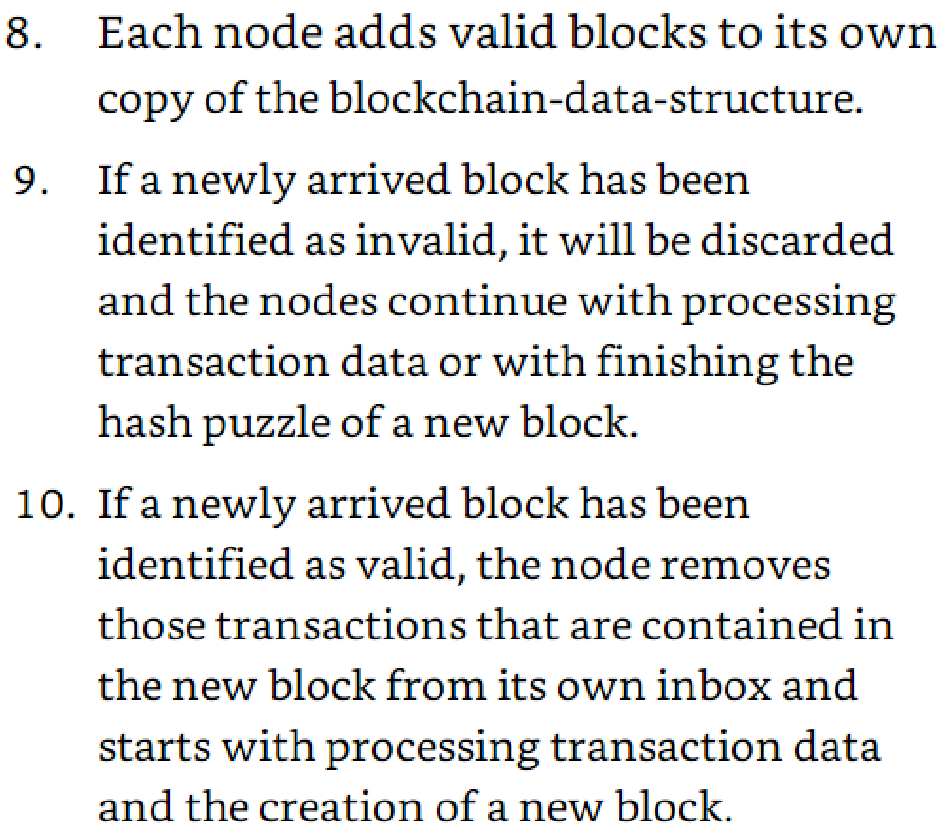


4. Each node processes new transaction data by validating them for authorization and formal and semantic correctness.
5. Each node collects only valid transaction data into a Merkle tree and starts creating a new block by solving its hash puzzle.
6. **As soon as a node finishes the hash puzzle, it sends the newly created block to all other nodes.**
7. Each node processes new blocks by verifying the solution of its hash puzzle and by verifying all its containing transaction data for formal correctness, semantic correctness, and authorization.

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

How Blockchain Works - In Detail (part 3)

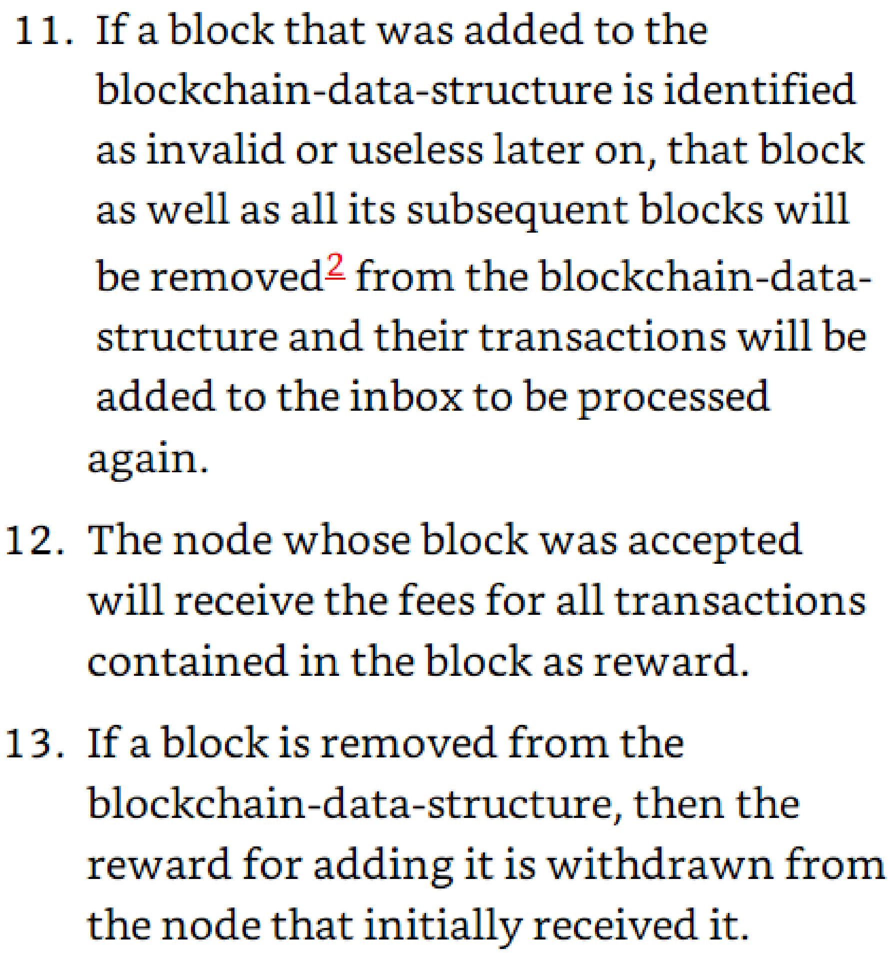


8. Each node adds valid blocks to its own copy of the blockchain-data-structure.
9. If a newly arrived block has been identified as invalid, it will be discarded and the nodes continue with processing transaction data or with finishing the hash puzzle of a new block.
10. If a newly arrived block has been identified as valid, the node removes those transactions that are contained in the new block from its own inbox and starts with processing transaction data and the creation of a new block.

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

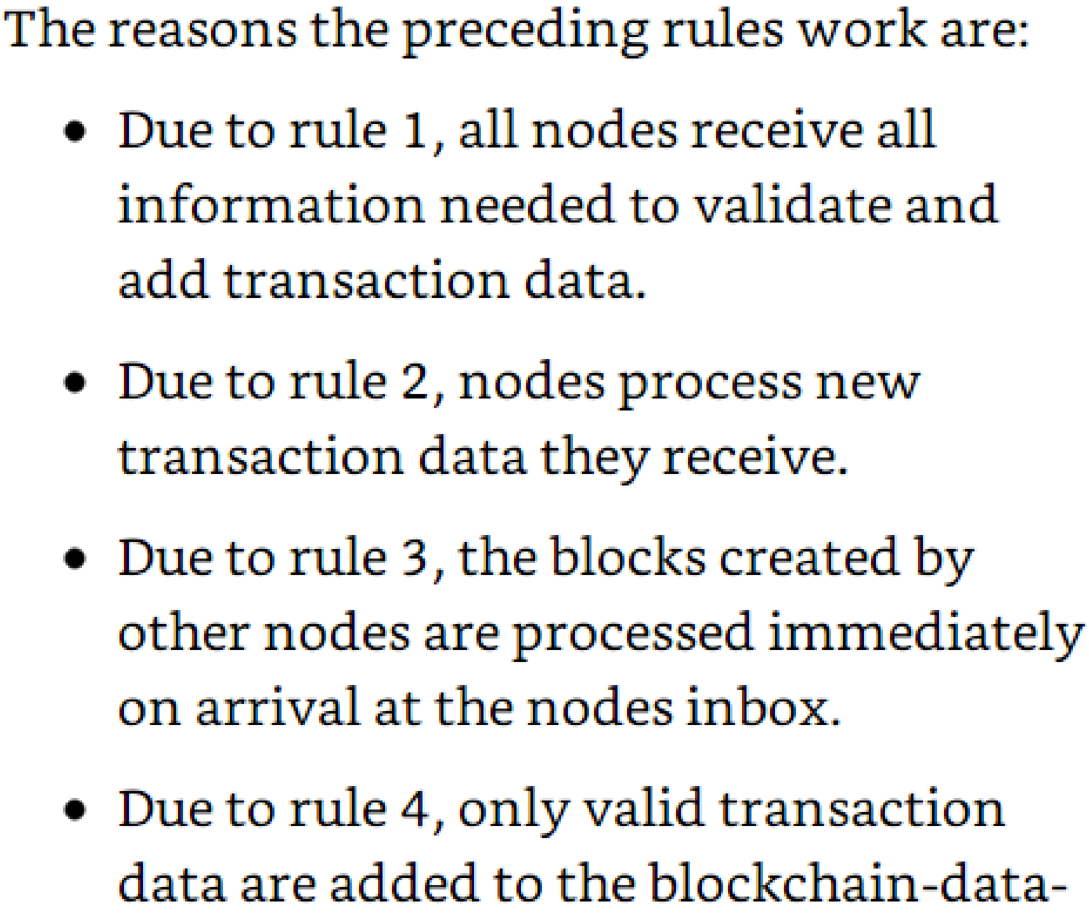
How Blockchain Works - In Detail (part 4)



11. If a block that was added to the blockchain-data-structure is identified as invalid or useless later on, that block as well as all its subsequent blocks will be removed[2] from the blockchain-data-structure and their transactions will be added to the inbox to be processed again.
12. The node whose block was accepted will receive the fees for all transactions contained in the block as reward.
13. If a block is removed from the blockchain-data-structure, then the reward for adding it is withdrawn from the node that initially received it.

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Why It Works – Part 1



The reasons the preceding rules work are:

- Due to rule 1, all nodes receive all information needed to validate and add transaction data.

- Due to rule 2, nodes process new transaction data they receive.

- Due to rule 3, the blocks created by other nodes are processed immediately on arrival at the nodes inbox.

- Due to rule 4, only valid transaction data are added to the blockchain-data-structure

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

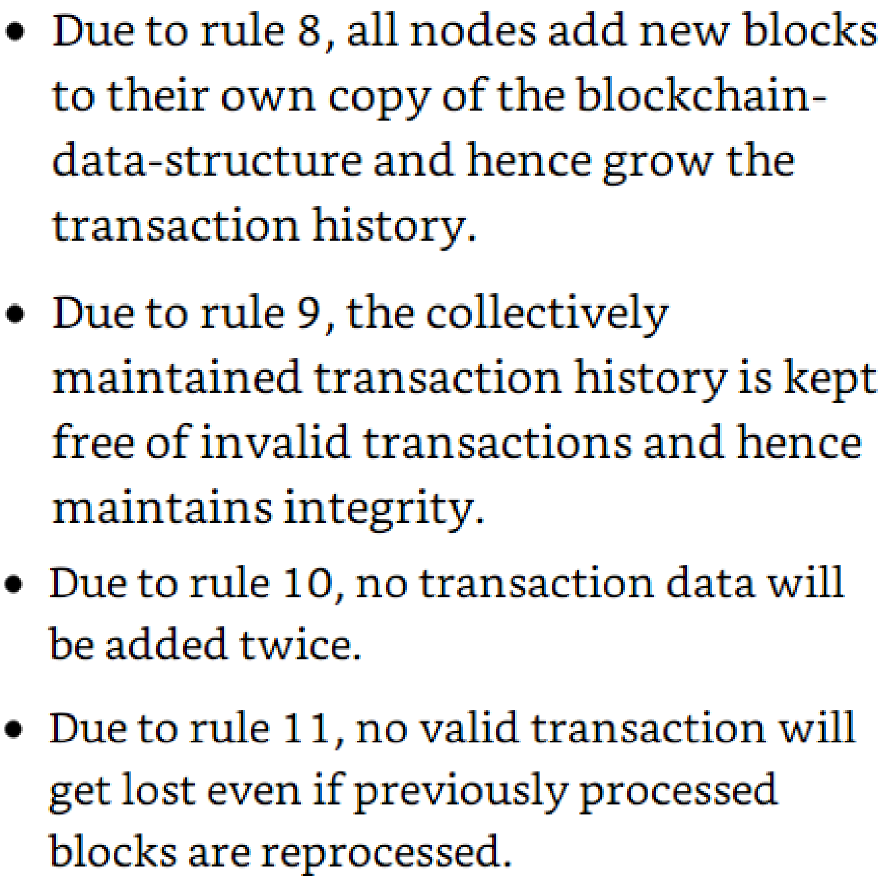
Why It Works – Part 2

- Due to rule 5, all nodes take part in a race for solving the hash puzzle. Due to the nature of the hash puzzle it is unpredictable which node will solve it first.
- Due to rule 6, all nodes are informed when a node solves the hash puzzle of a new block.
- Due to rules 6 and 3, all nodes receive the newly created block and recognize the winner of the race for solving the hash puzzle.
- Due to rule 7, all nodes of the system review and verify newly created blocks and ensure that only correct blocks are accepted.

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE
OF TECHNOLOGY

Why It Works – Part 3



- Due to rule 8, all nodes add new blocks to their own copy of the blockchain-data-structure and hence grow the transaction history.
- Due to rule 9, the collectively maintained transaction history is kept free of invalid transactions and hence maintains integrity.
- Due to rule 10, no transaction data will be added twice.
- Due to rule 11, no valid transaction will get lost even if previously processed blocks are reprocessed.

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Why It Works – Part 4

- Due to rule 11, the system is able to perform ex post validity checks on the transaction history and correct it retrospectively.
- Due to rule 12, nodes have an incentive to process transactions and to create new blocks quickly.
- Due to rule 12, all nodes have an incentive to inform all other nodes about a new block because earning a reward depends on having transactions examined and accepted by all other nodes.
- Due to rule 13, nodes have an incentive to work correctly, to avoid accepting any invalid transaction data, or producing invalid blocks.
- Due to rule 13, nodes have an incentive to review and revalidate blocks and transactions in a retrospective way.

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

BLOCKCHAIN ARCHITECTURE

Microsoft Windows NT Software Architecture – Circa 1996

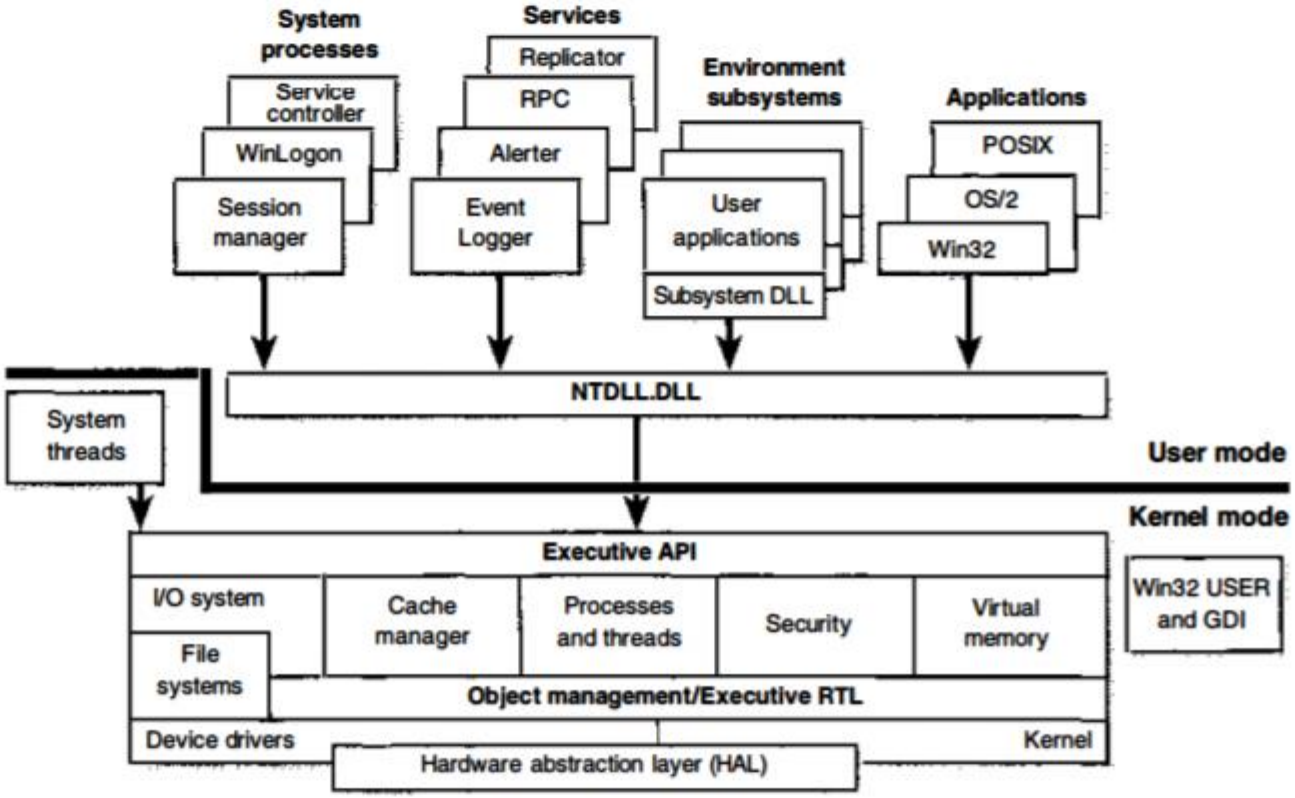


Figure 2-5
Windows NT architecture

Source: Solomon, D. (1998). Inside Windows NT, 2nd Edition. Redmond, WA: Microsoft Press.

ILLINOIS INSTITUTE OF TECHNOLOGY

Blockchain Architecture

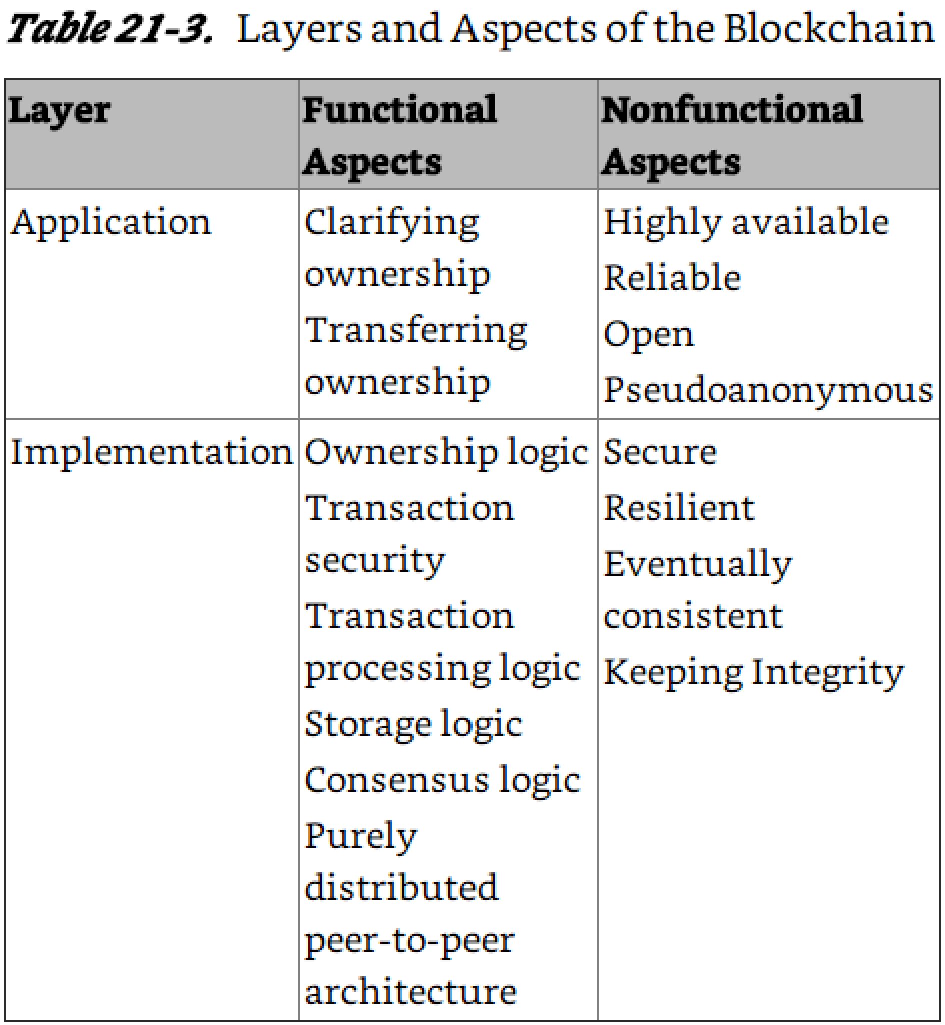
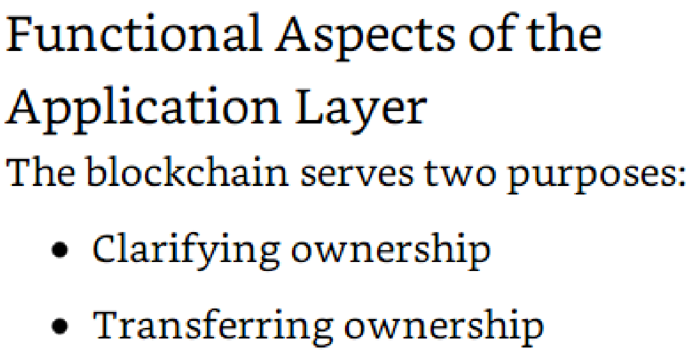


Table 21-3. Layers and Aspects of the Blockchain

Layer	Functional Aspects	Nonfunctional Aspects
Application	Clarifying ownership Transferring ownership	Highly available Reliable Open Pseudoanonymous
Implementation	Ownership logic Transaction security Transaction processing logic Storage logic Consensus logic Purely distributed peer-to-peer architecture	Secure Resilient Eventually consistent Keeping Integrity

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

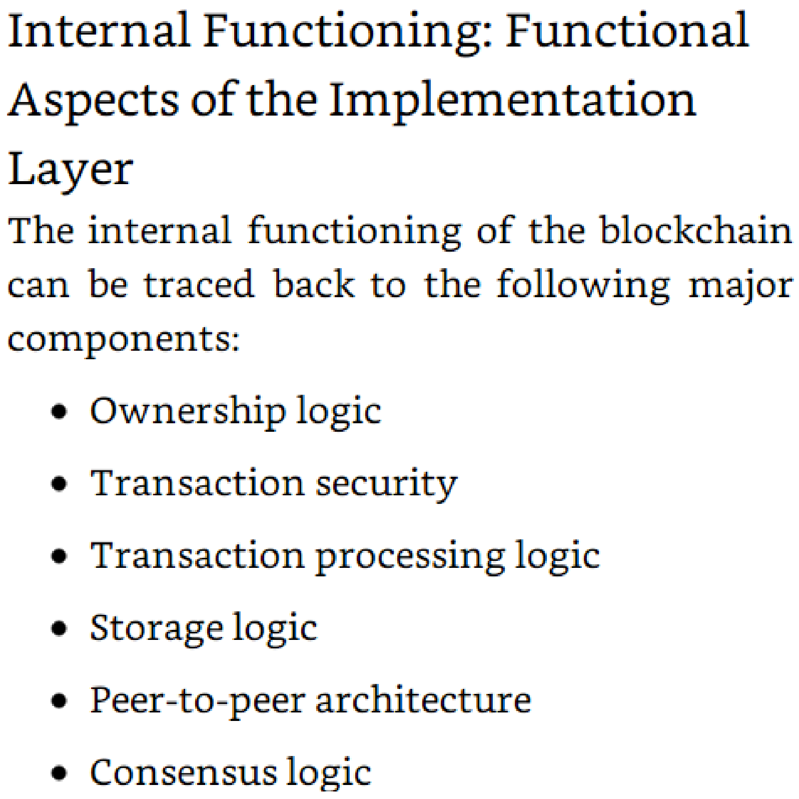
Blockchain Architecture



Functional Aspects of the Application Layer

The blockchain serves two purposes:

- Clarifying ownership
- Transferring ownership



Internal Functioning: Functional Aspects of the Implementation Layer

The internal functioning of the blockchain can be traced back to the following major components:

- Ownership logic
- Transaction security
- Transaction processing logic
- Storage logic
- Peer-to-peer architecture
- Consensus logic

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Blockchain Architecture

- The architecture of a software system determines how its components are organized and related to one another.
- Centralized and distributed software architectures can be seen as antipodes.
- A distributed system consists of a number of independent computers that cooperate with one another by using a communication medium in order to achieve a specific objective without having any centralized element of control or coordination.
- As a rule of thumb, one can state that as soon as a system has a single component that could bring down the whole system it is not distributed, regardless of how complex its architecture looks.
- The blockchain is part of the implementation layer of a distributed software system.
- The purpose of the blockchain is to ensure a specific nonfunctional aspect of a distributed software system that is: achieving and maintaining its integrity.

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

Blockchain Software Architecture

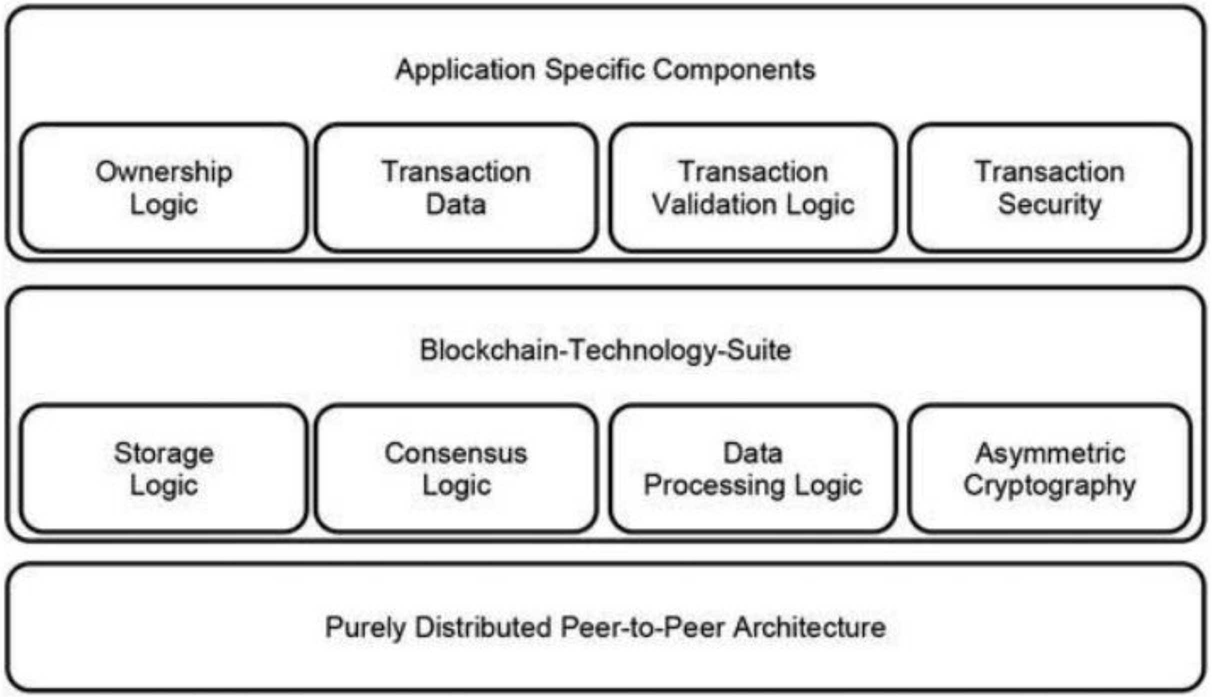
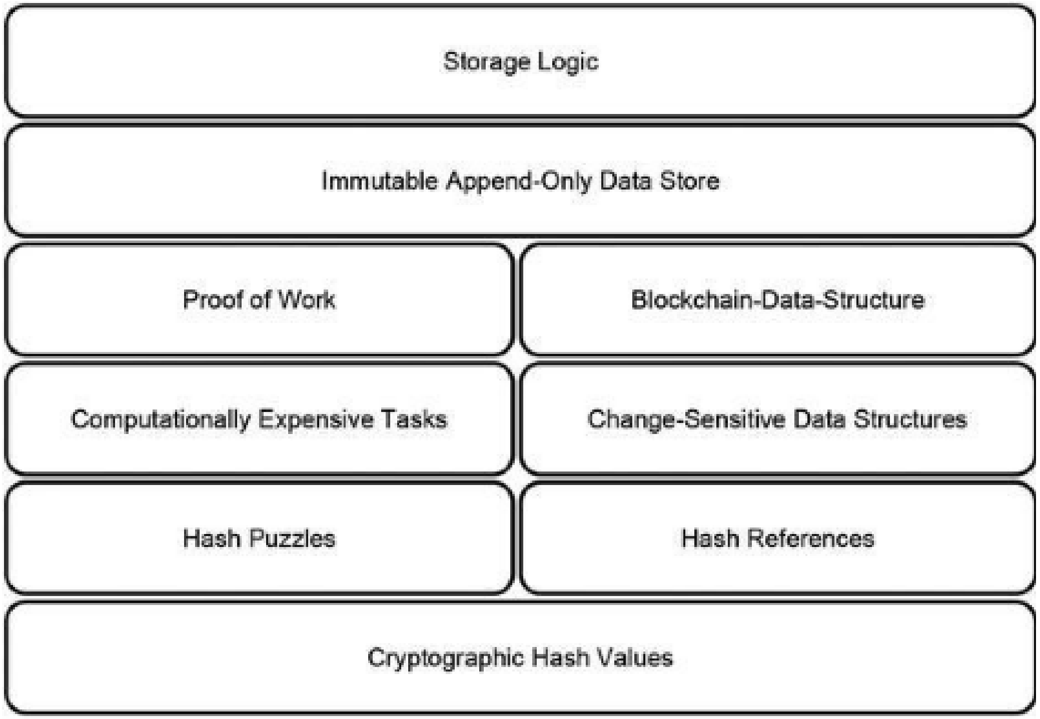

Application Specific Components
Ownership Logic
Transaction Data
Transaction Validation Logic
Transaction Security
Blockchain-Technology-Suite
Storage Logic
Consensus Logic
Data Processing Logic
Asymmetric Cryptography
Purely Distributed Peer-to-Peer Architecture

Figure 21-7.
The blockchain-technology-suite within the blockchain

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

Blockchain Software Architecture - Storage Logic Components



Storage Logic

Immutable Append-Only Data Store

Proof of Work

Blockchain-Data-Structure

Computationally Expensive Tasks

Change-Sensitive Data Structures

Hash Puzzles

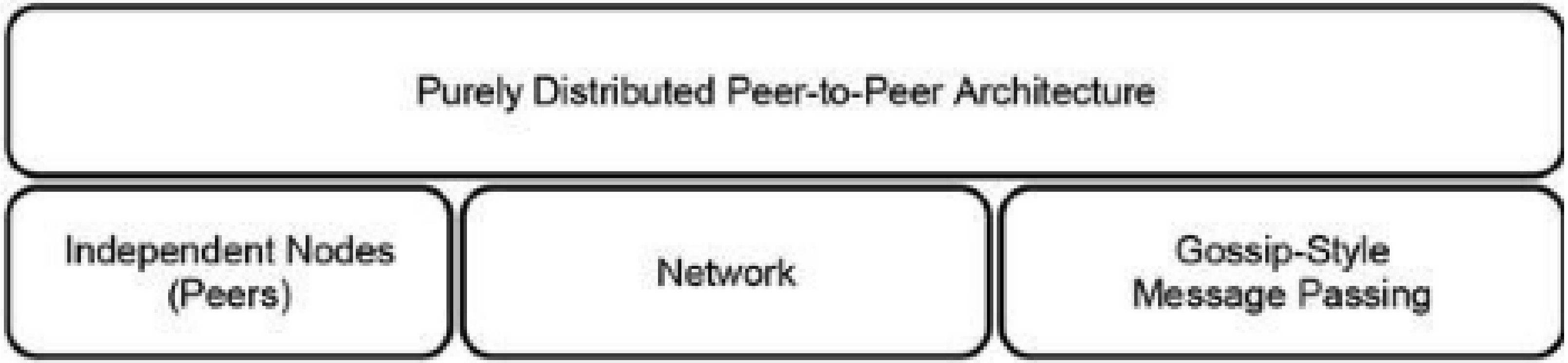
Hash References

Cryptographic Hash Values

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

Blockchain Software Architecture - Peer-to-Peer Components



Purely Distributed Peer-to-Peer Architecture

Independent Nodes (Peers)

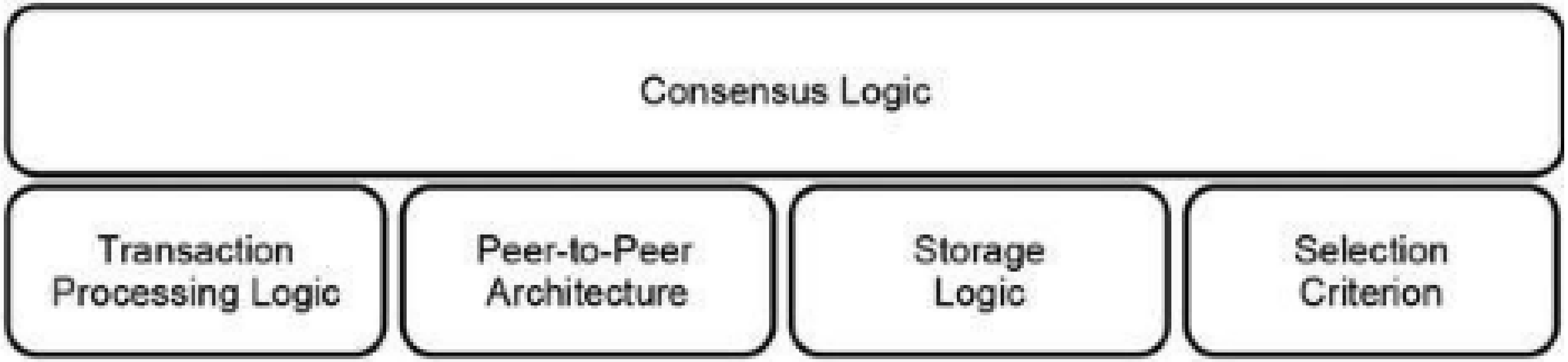
Network

Gossip-Style Message Passing

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

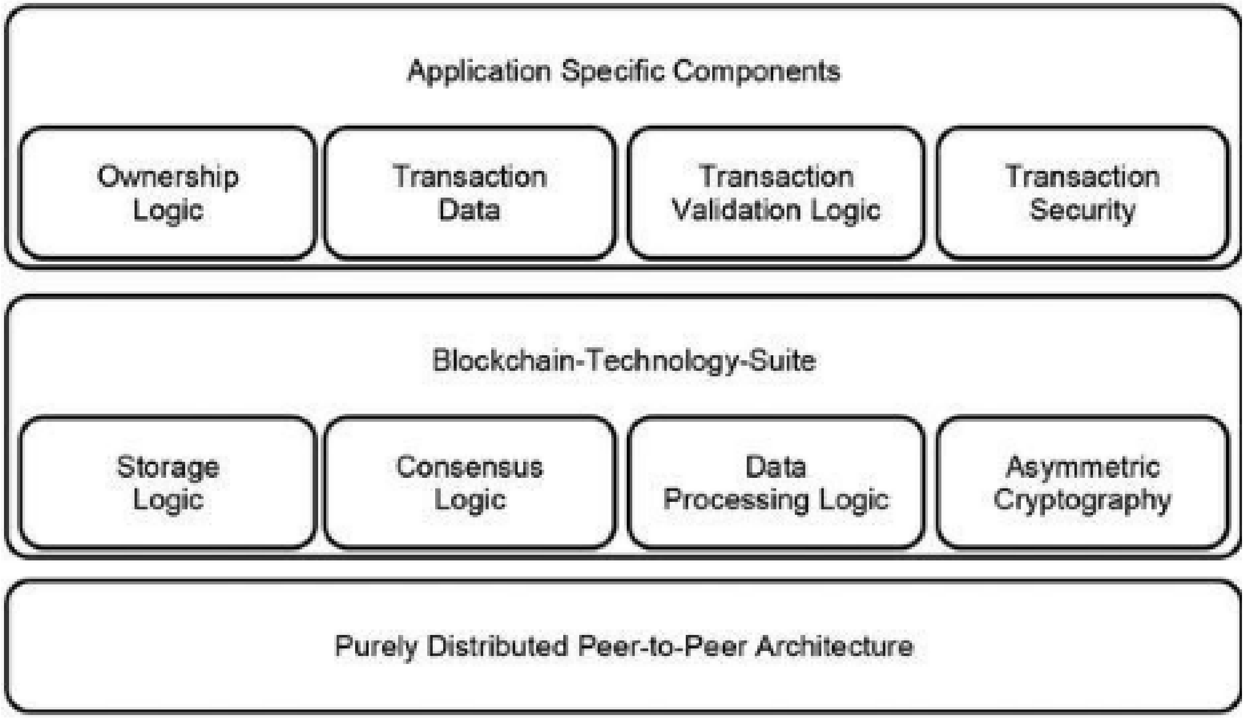
Blockchain Software Architecture - Consensus Components



Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

Blockchain Software Architecture - Application Specific Components


Application Specific Components
Ownership Logic
Transaction Data
Transaction Validation Logic
Transaction Security
Blockchain-Technology-Suite
Storage Logic
Consensus Logic
Data Processing Logic
Asymmetric Cryptography
Purely Distributed Peer-to-Peer Architecture

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

Blockchain Database Nodes are Peer-to-Peer

Peer-to-Peer Architecture

The architecture determines how the components or nodes of the system are related and connected with one another. As illustrated in Figure 21-5, the blockchain utilizes a purely distributed peer-to-peer system that consists of independent peers called nodes. These nodes are connected with one another via a network that serves as a medium for communication. Each of the peers maintains its own copy of the blockchain-data-structure containing the whole history of transaction data. The peers communicate with one another by utilizing a gossip-style message-passing protocol that ensures that eventually each peer will receive all of the information.

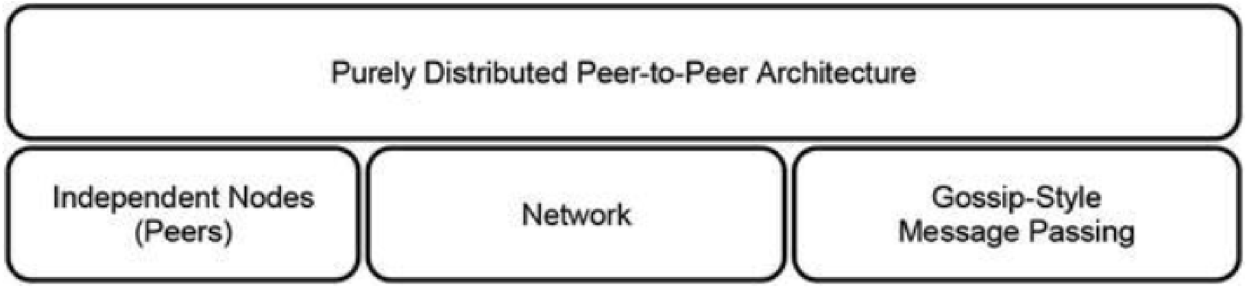

Purely Distributed Peer-to-Peer Architecture
Independent Nodes (Peers)
Network
Gossip-Style Message Passing

Figure 21-5.

Architecture and its underlying concepts

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

Consensus Logic – What Makes Blockchain Trusted

Consensus Logic

Since all the nodes of the distributed system maintain their history of transaction data independently, their content can differ due to delays or other adversities of passing messages through a network. As a result, the data store that was meant to form a straight line of linked data blocks actually forms a three-shaped data structure where each branch represents a conflicting version of the transaction history. The consensus logic as depicted in Figure 21-6 makes all nodes of the system eventually consistent by making them choose the identical version of the transaction history that unites the most collective effort.

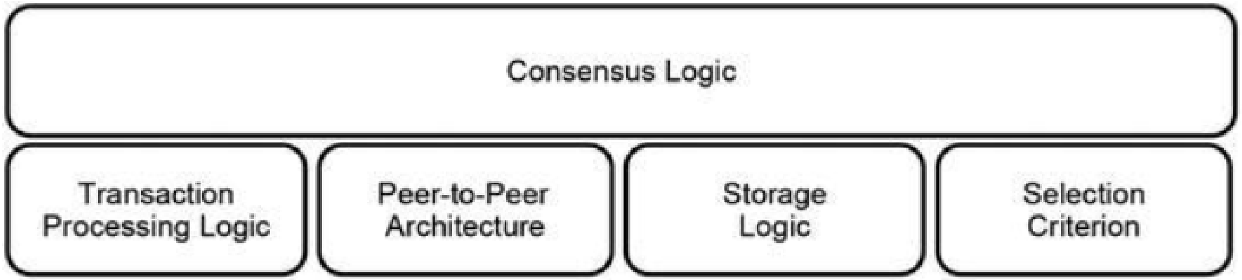
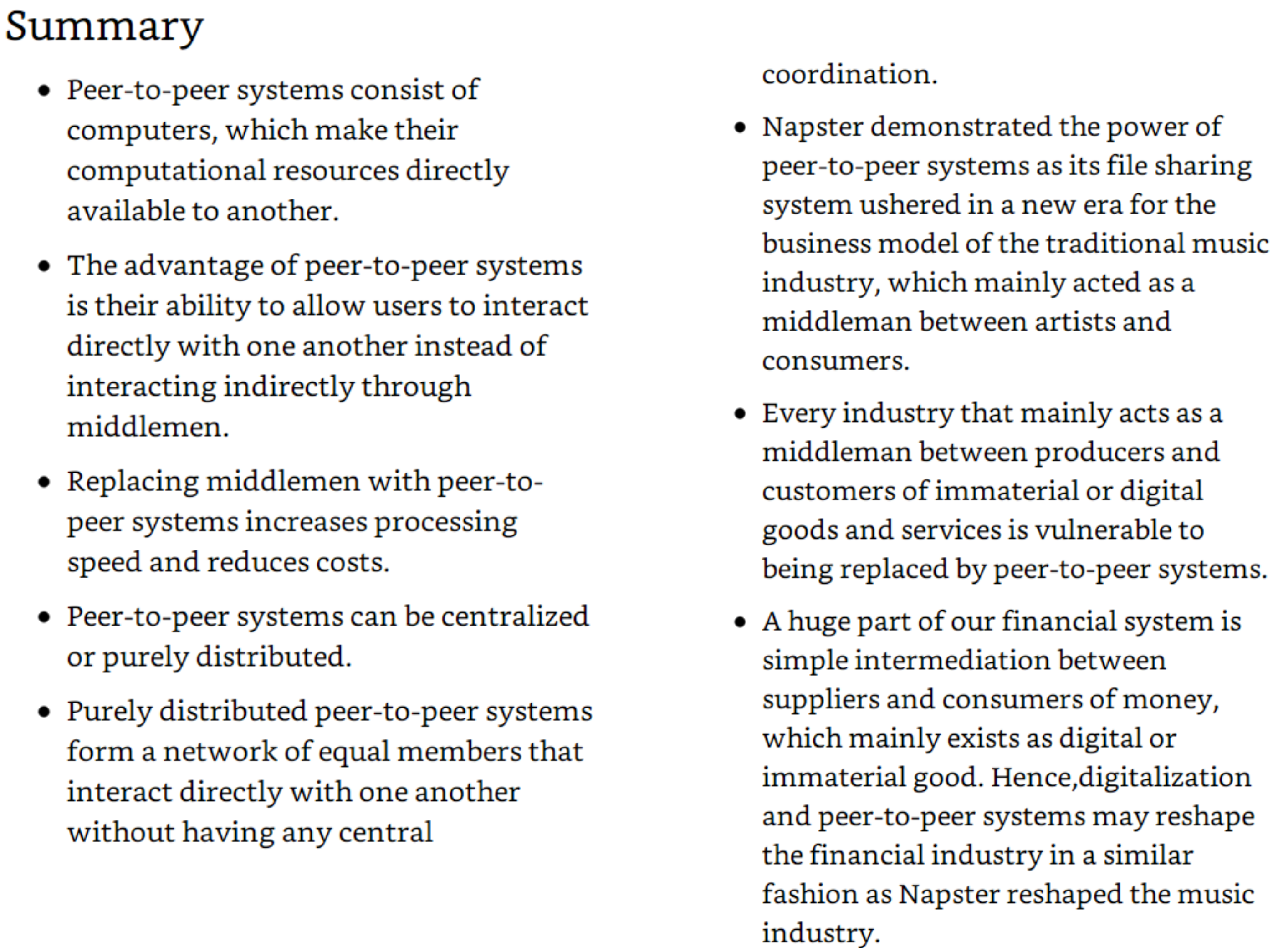


Figure 21-6.

Consensus logic and its underlying concepts

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Architecture Summary



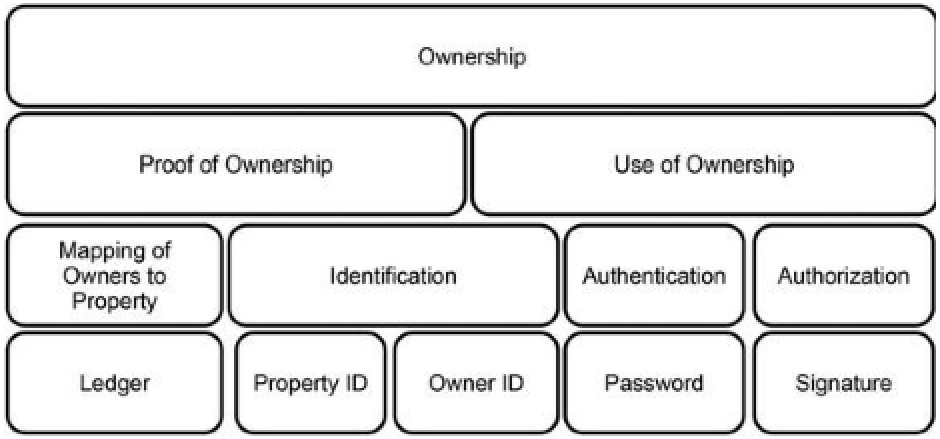
Summary

- Peer-to-peer systems consist of computers, which make their computational resources directly available to another.
- The advantage of peer-to-peer systems is their ability to allow users to interact directly with one another instead of interacting indirectly through middlemen.
- Replacing middlemen with peer-to-peer systems increases processing speed and reduces costs.
- Peer-to-peer systems can be centralized or purely distributed.
- Purely distributed peer-to-peer systems form a network of equal members that interact directly with one another without having any central coordination.
- Napster demonstrated the power of peer-to-peer systems as its file sharing system ushered in a new era for the business model of the traditional music industry, which mainly acted as a middleman between artists and consumers.
- Every industry that mainly acts as a middleman between producers and customers of immaterial or digital goods and services is vulnerable to being replaced by peer-to-peer systems.
- A huge part of our financial system is simple intermediation between suppliers and consumers of money, which mainly exists as digital or immaterial good. Hence,digitalization and peer-to-peer systems may reshape the financial industry in a similar fashion as Napster reshaped the music industry.

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Ownership

Figure 6-1 depicts the relation of the different concepts involved when designing software for managing ownership.



Ownership

Proof of Ownership

Use of Ownership

Mapping of Owners to Property

Identification

Authentication

Authorization

Ledger

Property ID

Owner ID

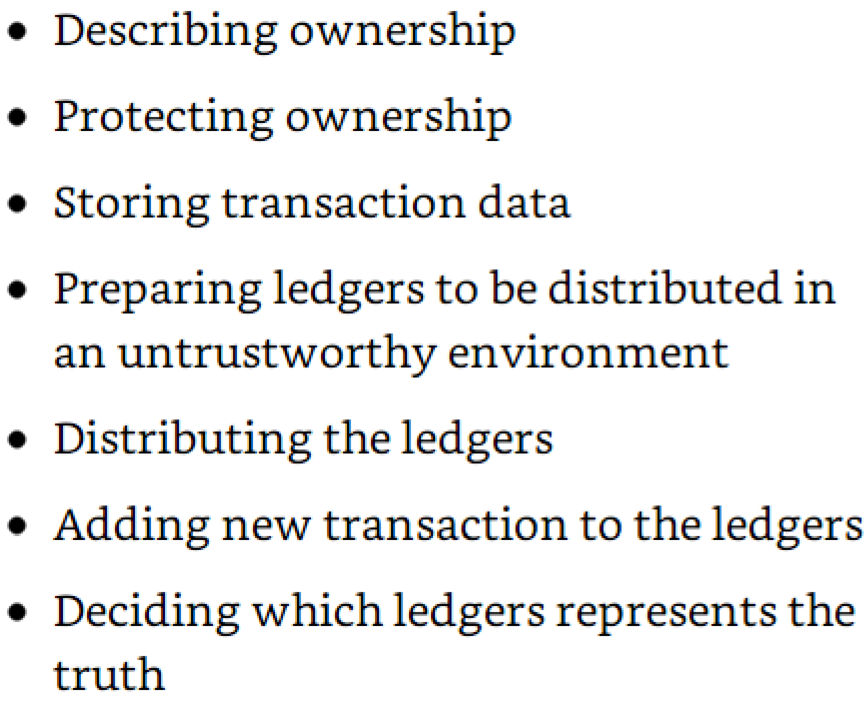
Password

Signature

Figure 6-1. Concepts of ownership

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Major Tasks Involved in Designing a System that Manages Ownership



- Describing ownership
- Protecting ownership
- Storing transaction data
- Preparing ledgers to be distributed in an untrustworthy environment
- Distributing the ledgers
- Adding new transaction to the ledgers
- Deciding which ledgers represents the truth

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Documenting Ownership with the Blockchain

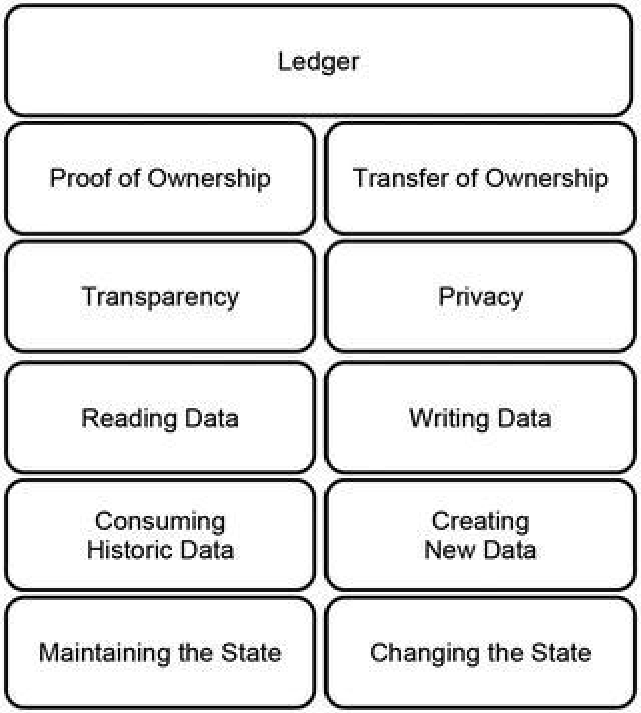
- Transaction data provide the following information for describing a transfer of ownership:
  - An identifier of the account who initiates the transaction and is to transfer ownership to another account
  - An identifier of that account that is to receive ownership
  - The amount of the goods to be transferred
  - The time the transaction is to be done
  - A fee to be paid to the system for executing the transaction
  - A proof that the owner of the account who hands off ownership agrees with that transfer
- The complete history of transaction data is an audit trail that provides evidence of how people acquired and handed off ownership.
- Any transaction not being part of that history is regarded as if it never happened.
- A transaction is executed by adding it to the history of transaction data and allowing it to influence the result of aggregating them.
- The order in which transaction data are added to the history must be preserved in order to yield identical results when aggregating these data.
- In order to maintain integrity, only those transaction data are added to the blockchain-data-structure that fulfill the following three criteria:
  - Formal correctness
  - Semantic correctness
  - Authorization

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

Purposes and Property of a Ledger

Figure 6-2 illustrates how the proof of ownership and transfer of ownership relate to the purpose and the properties of a ledger.



Ledger

Proof of Ownership | Transfer of Ownership

Transparency | Privacy

Reading Data | Writing Data

Consuming Historic Data | Creating New Data

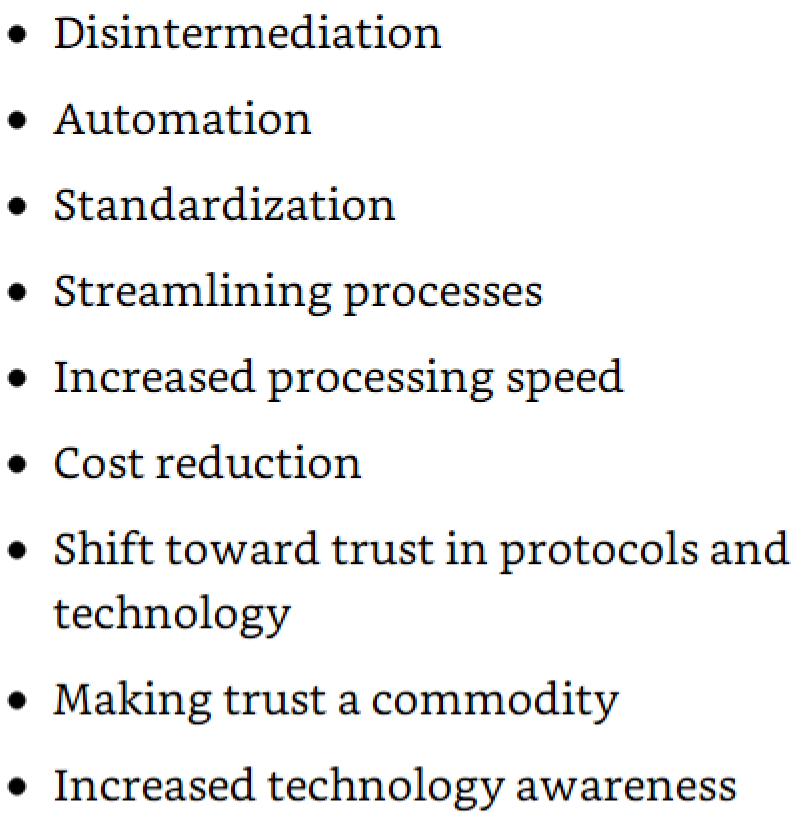
Maintaining the State | Changing the State

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

BLOCKCHAIN ACCOMPLISHMENTS

ILLINOIS INSTITUTE OF TECHNOLOGY

Major Accomplishments of the Blockchain



- Disintermediation
- Automation
- Standardization
- Streamlining processes
- Increased processing speed
- Cost reduction
- Shift toward trust in protocols and technology
- Making trust a commodity
- Increased technology awareness

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

The Core Problems Solved by Blockchain

- Integrity and trust are major concerns of peer-to-peer systems.
- People will join and continue to contribute to a peer-to-peer system if they trust it and if the results of interacting with the system on an ongoing basis confirm and reinforce that trust.
- As soon as people lose trust in a peer-to-peer system, they will abandon it, which in turn will cause the system to terminate eventually.
- Major integrity threats in peer-to-peer systems are:
    - Technical failures
    - Malicious peers
- Achieving integrity in a peer-to-peer system depends on:
    - The knowledge about the number of peers
    - The knowledge about the trustworthiness of the peers
- The core problem to be solved by the blockchain is achieving and maintaining integrity in a purely distributed peer-to-peer system that is comprised of an unknown number of peers with unknown reliability and trustworthiness.

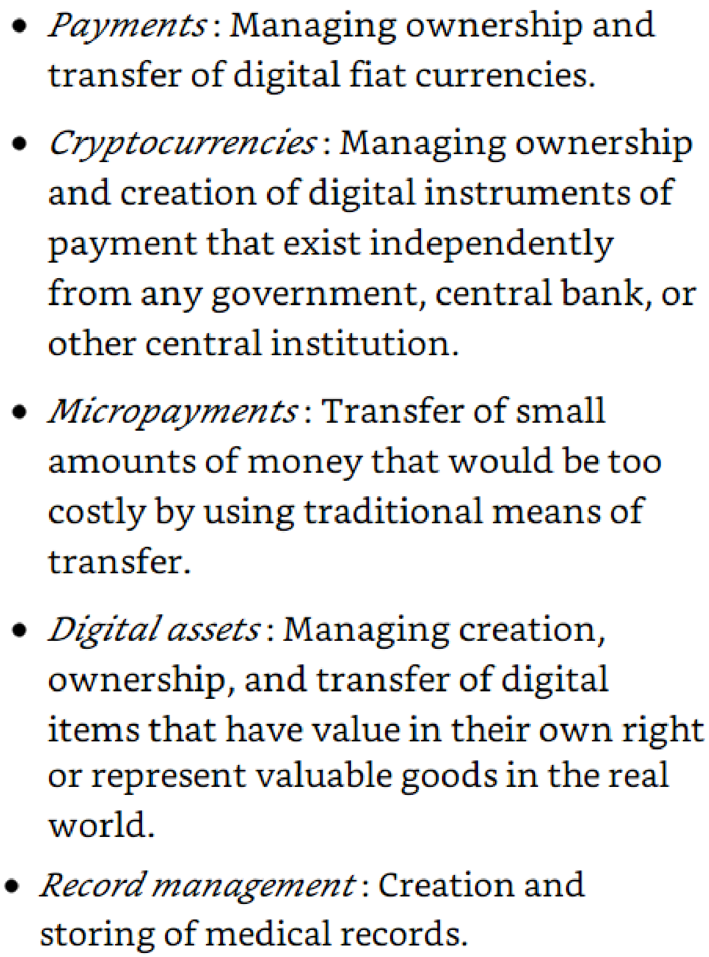
Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

BLOCKCHAIN USES

ILLINOIS INSTITUTE OF TECHNOLOGY

Small Selection of Actual Blockchain Applications

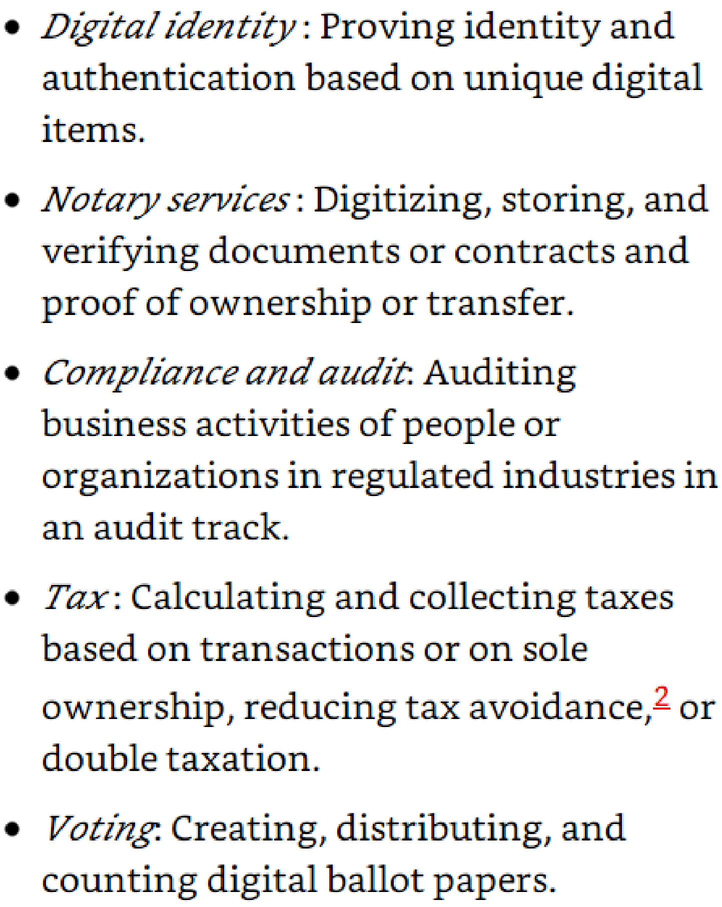


- *Payments*: Managing ownership and transfer of digital fiat currencies.
- *Cryptocurrencies*: Managing ownership and creation of digital instruments of payment that exist independently from any government, central bank, or other central institution.
- *Micropayments*: Transfer of small amounts of money that would be too costly by using traditional means of transfer.
- *Digital assets*: Managing creation, ownership, and transfer of digital items that have value in their own right or represent valuable goods in the real world.
- *Record management*: Creation and storing of medical records.

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

Small Selection of Actual Blockchain Applications

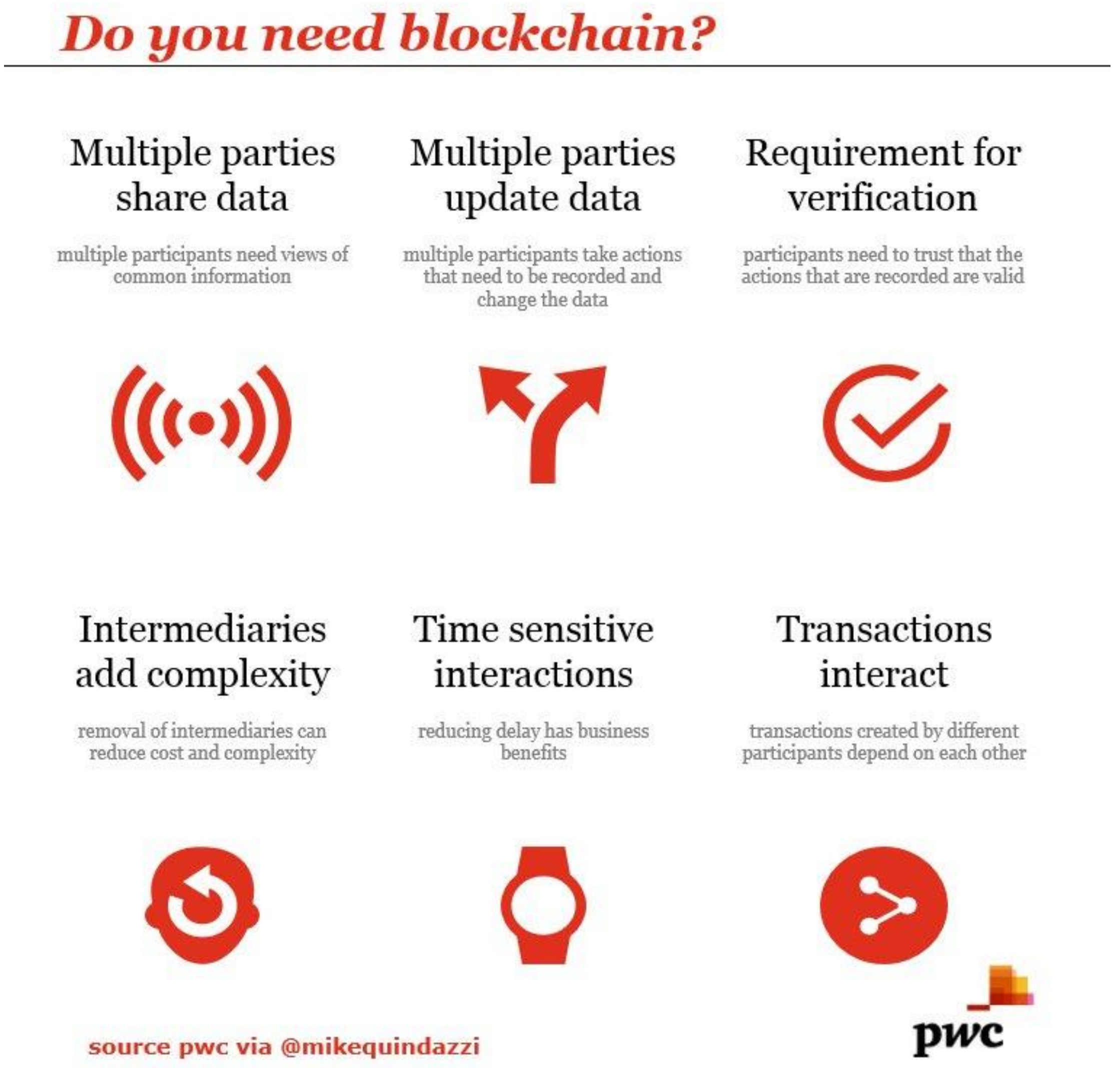


- *Digital identity* : Proving identity and authentication based on unique digital items.
- *Notary services* : Digitizing, storing, and verifying documents or contracts and proof of ownership or transfer.
- *Compliance and audit*: Auditing business activities of people or organizations in regulated industries in an audit track.
- *Tax* : Calculating and collecting taxes based on transactions or on sole ownership, reducing tax avoidance,[2] or double taxation.
- *Voting*: Creating, distributing, and counting digital ballot papers.

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

Do Need Blockchain?



Do you need blockchain?

Multiple parties share data

multiple participants need views of common information

Multiple parties update data

multiple participants take actions that need to be recorded and change the data

Requirement for verification

participants need to trust that the actions that are recorded are valid

Intermediaries add complexity

removal of intermediaries can reduce cost and complexity

Time sensitive interactions

reducing delay has business benefits

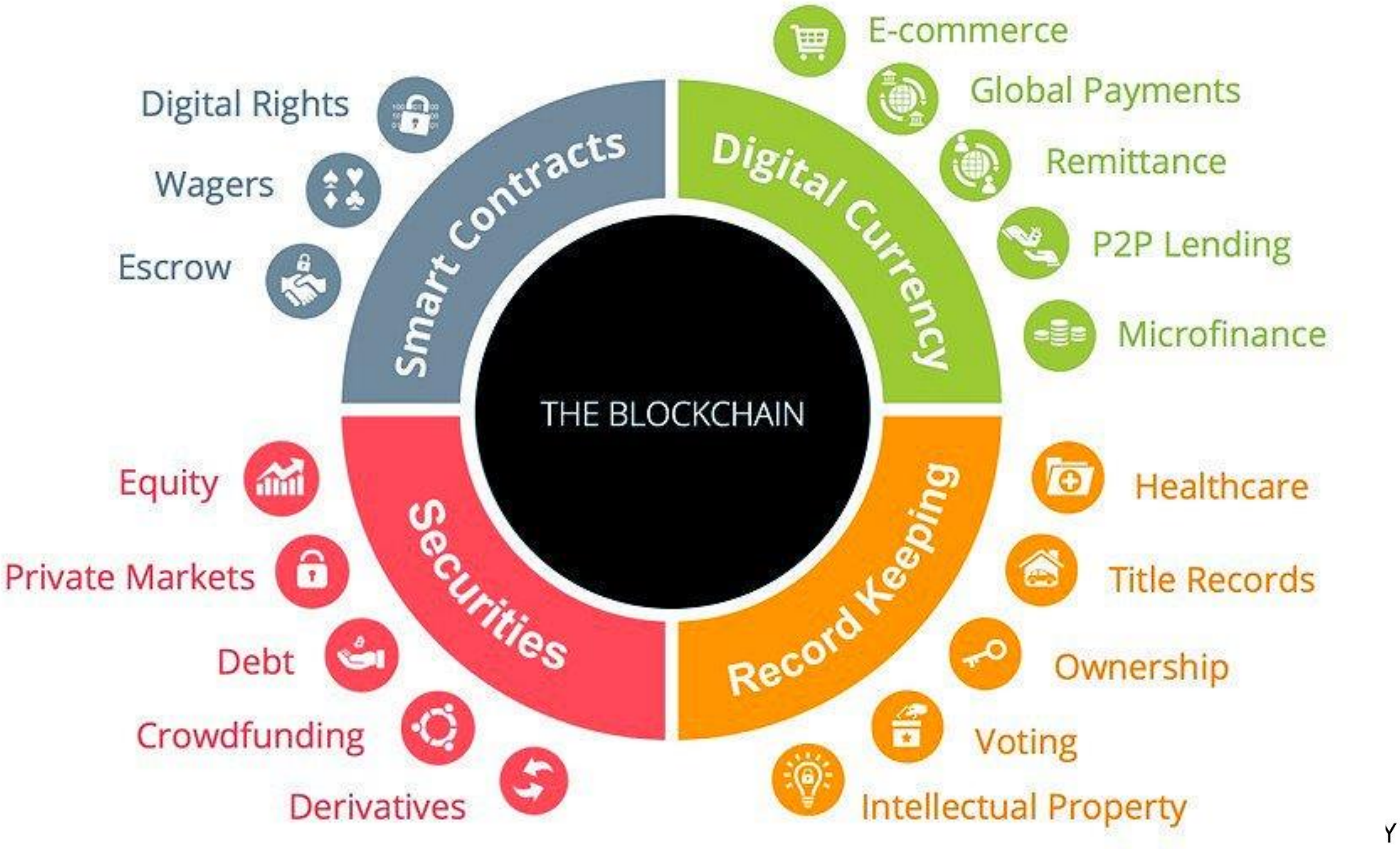
Transactions interact

transactions created by different participants depend on each other

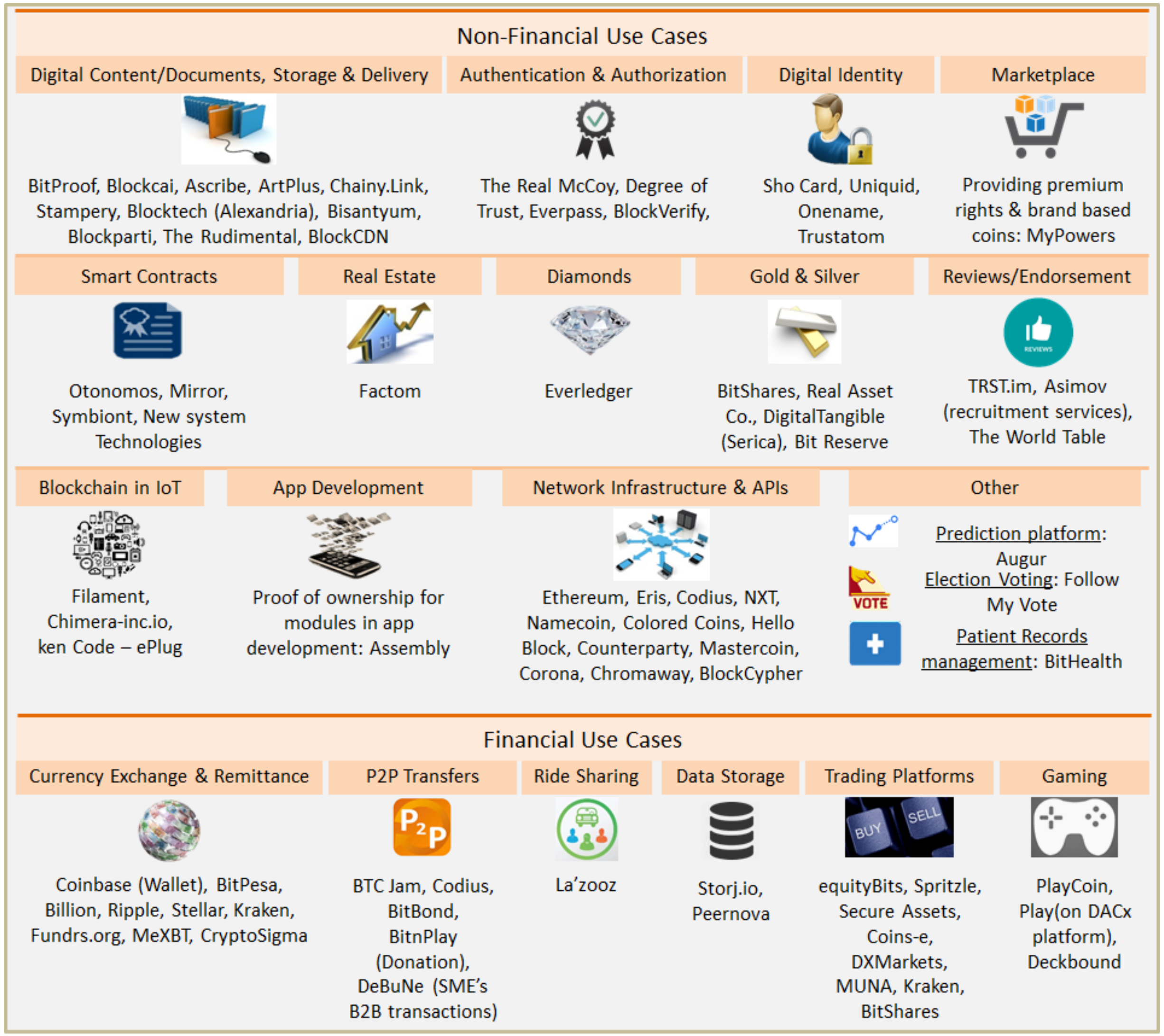
source pwc via @mikequindazzi

pwc

Blockchain Uses



Blockchain Uses



Non-Financial Use Cases

Digital Content/Documents, Storage & Delivery	Authentication & Authorization	Digital Identity	Marketplace
BitProof, Blockcai, Ascribe, ArtPlus, Chainy.Link, Stampery, Blocktech (Alexandria), Bisantyum, Blockparti, The Rudimental, BlockCDN	The Real McCoy, Degree of Trust, Everpass, BlockVerify,	Sho Card, Uniquid, Onename, Trustatom	Providing premium rights & brand based coins: MyPowers

Smart Contracts	Real Estate	Diamonds	Gold & Silver	Reviews/Endorsement
Otonomos, Mirror, Symbiont, New system Technologies	Factom	Everledger	BitShares, Real Asset Co., DigitalTangible (Serica), Bit Reserve	TRST.im, Asimov (recruitment services), The World Table

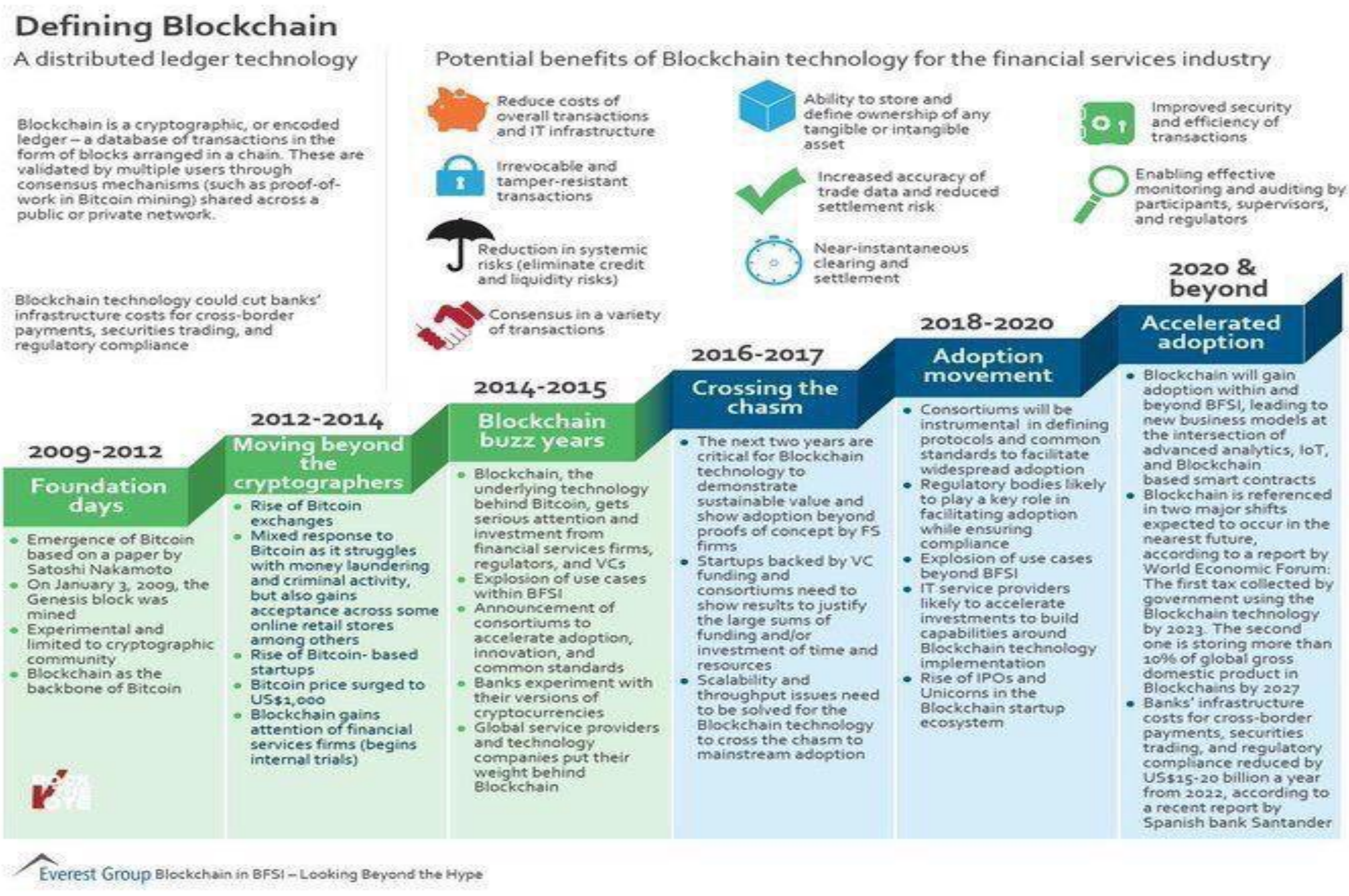
Blockchain in IoT	App Development	Network Infrastructure & APIs	Other
Filament, Chimera-inc.io, ken Code – ePlug	Proof of ownership for modules in app development: Assembly	Ethereum, Eris, Codius, NXT, Namecoin, Colored Coins, Hello Block, Counterparty, Mastercoin, Corona, Chromaway, BlockCypher	Prediction platform: Augur Election Voting: Follow My Vote Patient Records management: BitHealth

Financial Use Cases

Currency Exchange & Remittance	P2P Transfers	Ride Sharing	Data Storage	Trading Platforms	Gaming
Coinbase (Wallet), BitPesa, Billion, Ripple, Stellar, Kraken, Fundrs.org, MeXBT, CryptoSigma	BTC Jam, Codius, BitBond, BitnPlay (Donation), DeBuNe (SME's B2B transactions)	La'zooz	Storj.io, Peernova	equityBits, Spritzle, Secure Assets, Coins-e, DXMarkets, MUNA, Kraken, BitShares	PlayCoin, Play(on DACx platform), Deckbound

ILLINOIS INSTITUTE OF TECHNOLOGY

Blockchain Use Evolution



Defining Blockchain

A distributed ledger technology

Blockchain is a cryptographic, or encoded ledger – a database of transactions in the form of blocks arranged in a chain. These are validated by multiple users through consensus mechanisms (such as proof-of-work in Bitcoin mining) shared across a public or private network.

Blockchain technology could cut banks' infrastructure costs for cross-border payments, securities trading, and regulatory compliance

Potential benefits of Blockchain technology for the financial services industry

- Reduce costs of overall transactions and IT infrastructure
- Irrevocable and tamper-resistant transactions
- Reduction in systemic risks (eliminate credit and liquidity risks)
- Consensus in a variety of transactions
- Ability to store and define ownership of any tangible or intangible asset
- Increased accuracy of trade data and reduced settlement risk
- Near-instantaneous clearing and settlement
- Improved security and efficiency of transactions
- Enabling effective monitoring and auditing by participants, supervisors, and regulators

2009-2012 Foundation days

- Emergence of Bitcoin based on a paper by Satoshi Nakamoto
- On January 3, 2009, the Genesis block was mined
- Experimental and limited to cryptographic community
- Blockchain as the backbone of Bitcoin

2012-2014 Moving beyond the cryptographers

- Rise of Bitcoin exchanges
- Mixed response to Bitcoin as it struggles with money laundering and criminal activity, but also gains acceptance across some online retail stores among others
- Rise of Bitcoin- based startups
- Bitcoin price surged to US$1,000
- Blockchain gains attention of financial services firms (begins internal trials)

2014-2015 Blockchain buzz years

- Blockchain, the underlying technology behind Bitcoin, gets serious attention and investment from financial services firms, regulators, and VCs
- Explosion of use cases within BFSI
- Announcement of consortiums to accelerate adoption, innovation, and common standards
- Banks experiment with their versions of cryptocurrencies
- Global service providers and technology companies put their weight behind Blockchain

2016-2017 Crossing the chasm

- The next two years are critical for Blockchain technology to demonstrate sustainable value and show adoption beyond proofs of concept by FS firms
- Startups backed by VC funding and consortiums need to show results to justify the large sums of funding and/or investment of time and resources
- Scalability and throughput issues need to be solved for the Blockchain technology to cross the chasm to mainstream adoption

2018-2020 Adoption movement

- Consortiums will be instrumental in defining protocols and common standards to facilitate widespread adoption
- Regulatory bodies likely to play a key role in facilitating adoption while ensuring compliance
- Explosion of use cases beyond BFSI
- IT service providers likely to accelerate investments to build capabilities around Blockchain technology implementation
- Rise of IPOs and Unicorns in the Blockchain startup ecosystem

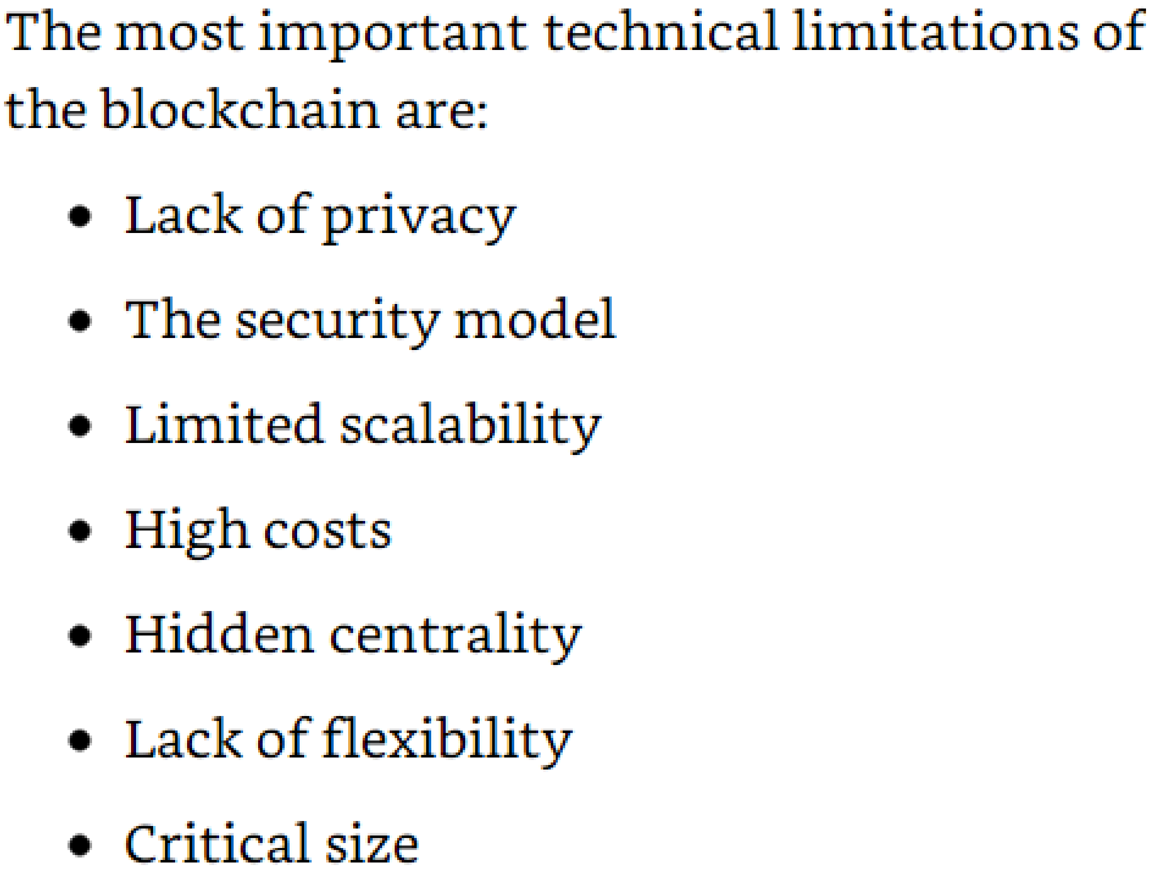
2020 & beyond Accelerated adoption

- Blockchain will gain adoption within and beyond BFSI, leading to new business models at the intersection of advanced analytics, IoT, and Blockchain based smart contracts
- Blockchain is referenced in two major shifts expected to occur in the nearest future, according to a report by World Economic Forum: The first tax collected by government using the Blockchain technology by 2023. The second one is storing more than 10% of global gross domestic product in Blockchains by 2027
- Banks' infrastructure costs for cross-border payments, securities trading, and regulatory compliance reduced by US$15-20 billion a year from 2022, according to a recent report by Spanish bank Santander

Everest Group Blockchain in BFSI – Looking Beyond the Hype

BLOCKCHAIN LIMITATIONS

Technical Limitations



The most important technical limitations of the blockchain are:

- Lack of privacy
- The security model
- Limited scalability
- High costs
- Hidden centrality
- Lack of flexibility
- Critical size

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE
OF TECHNOLOGY

Technical Limitations

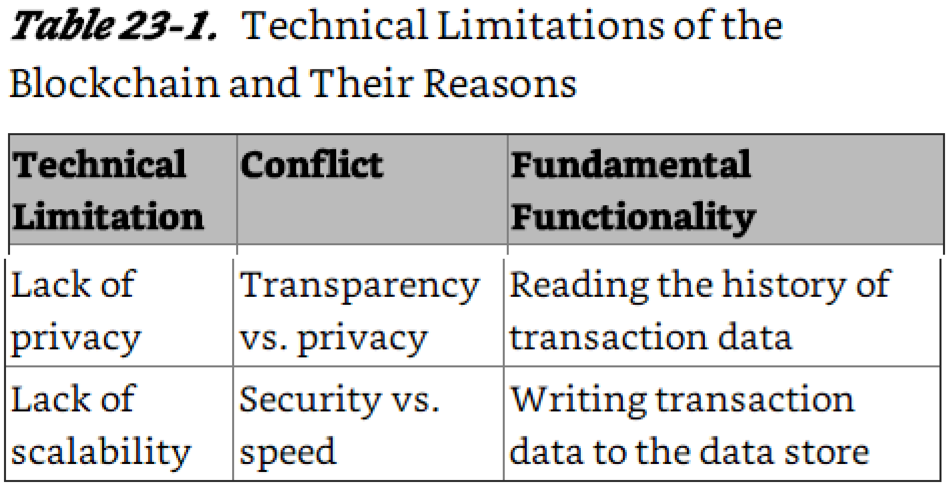


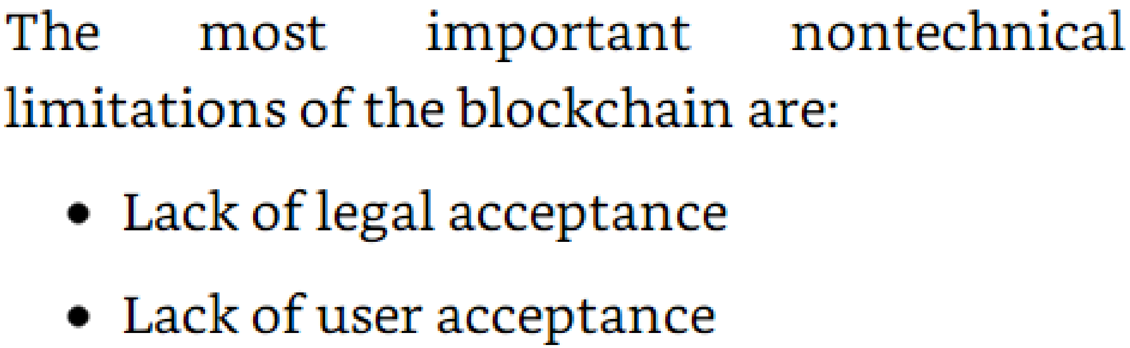
Table 23-1. Technical Limitations of the Blockchain and Their Reasons

Technical Limitation	Conflict	Fundamental Functionality
Lack of privacy	Transparency vs. privacy	Reading the history of transaction data
Lack of scalability	Security vs. speed	Writing transaction data to the data store

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

Nontechnical Limitations



The most important nontechnical limitations of the blockchain are:

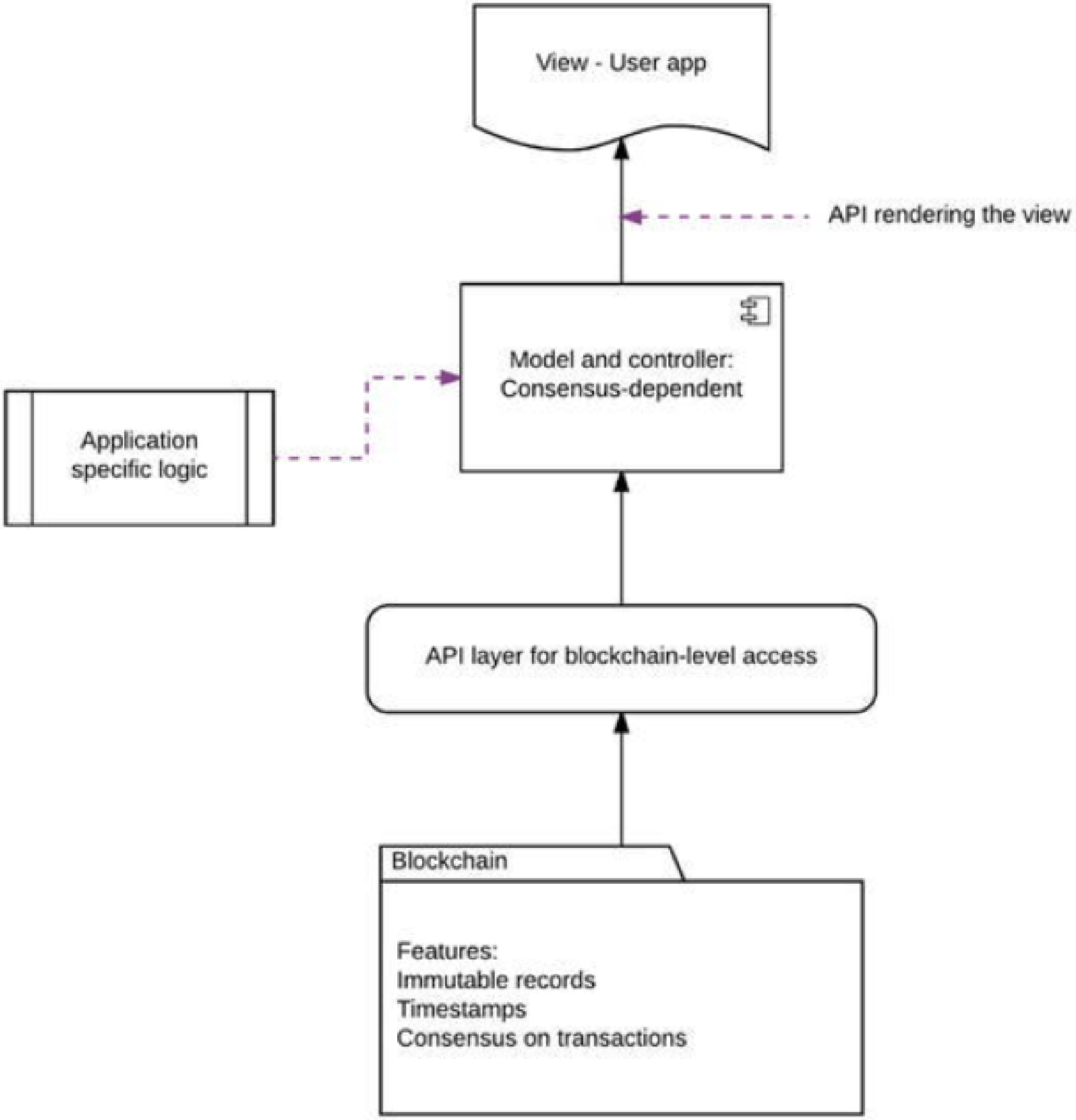
- Lack of legal acceptance
- Lack of user acceptance

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

BLOCKCHAIN DEVELOPMENT

ILLINOIS INSTITUTE OF TECHNOLOGY

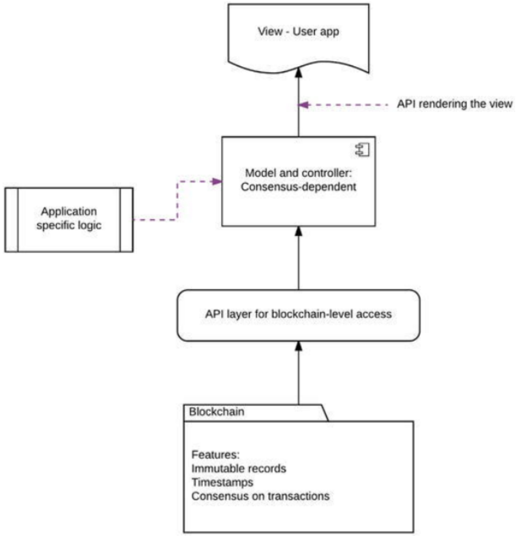
Simple Blockchain Application Model



Source: **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You** by Vikram Dhillon, David Metcalf, Max Hooper

ILLINOIS INSTITUTE
OF TECHNOLOGY

Simple Blockchain Application Model


View - User app
API rendering the view
Model and controller: Consensus-dependent
Application specific logic
API layer for blockchain-level access
Blockchain
Features:
Immutable records
Timestamps
Consensus on transactions

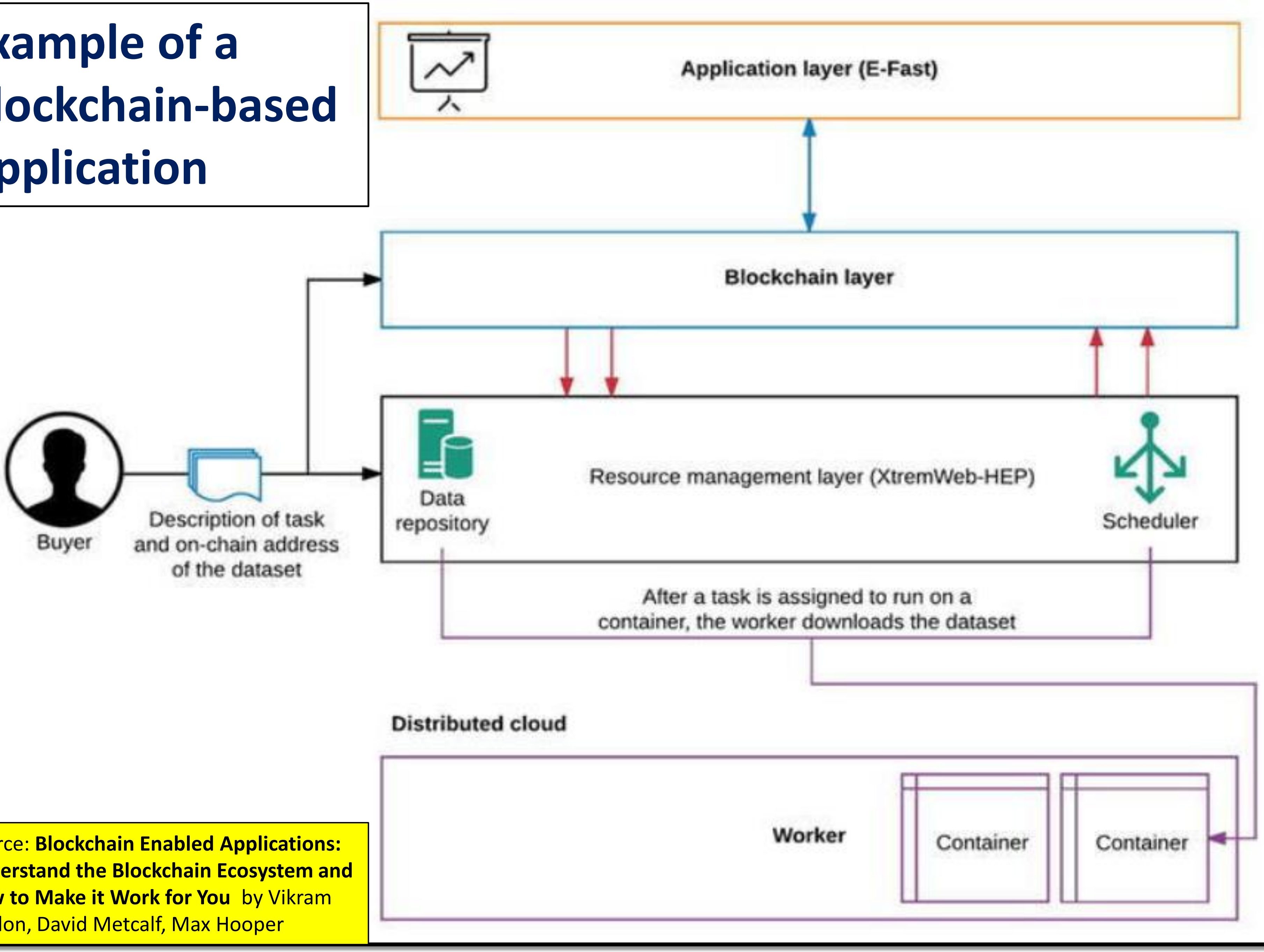
Source: **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You** by Vikram Dhillon, David Metcalf, Max Hooper

Figure 1-3.

Simple prototype of a decentralized application that interacts with the end user at the final steps

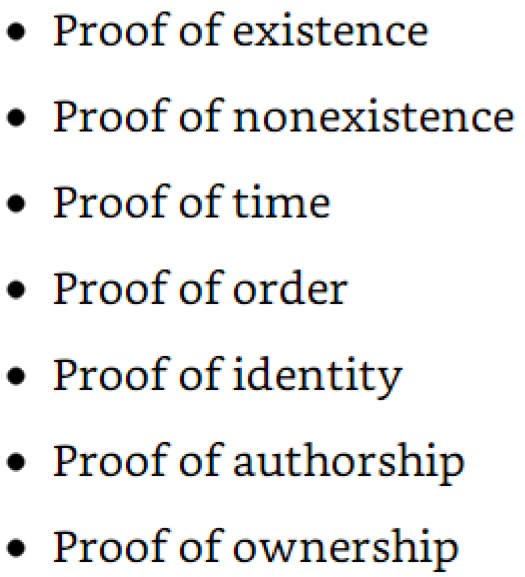
The model and controller here rely on the blockchain for data (data integrity and security) and accordingly update the view for the end user. The secret sauce in this prototype is the application programming interface (API), which works to pull information from the blockchain and provides it to the model and controller. This API provides opportunities to extend business logic and add it to the blockchain, along with basic operations that take blocks as input and provide answers to binary questions. The blockchain could eventually have more features, such as oracles that can verify external data and timestamp it on the blockchain itself. Once a decentralized app starts dealing with large amounts of live data and sophisticated business logic, we can classify it as a blockchain-enabled application.

Example of a Blockchain-based Application


Application layer (E-Fast)
Blockchain layer
Resource management layer (XtremWeb-HEP)
Data repository
Scheduler
Buyer
Description of task and on-chain address of the dataset
After a task is assigned to run on a container, the worker downloads the dataset
Distributed cloud
Worker
Container
Container

Source: **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You** by Vikram Dhillon, David Metcalf, Max Hooper

Generic
Blockchain Application Patterns



- Proof of existence
- Proof of nonexistence
- Proof of time
- Proof of order
- Proof of identity
- Proof of authorship
- Proof of ownership

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

12 Free Blockchain Resources

1. William Slater’s Blockchain Resource Page http://billslater.com/blockchain
2. Factom University http://www.factom.com/university
3. Ethereum 101 http://www.ethereum101.org
4. Build on Ripple http://ripple.com/build
5. Programmable money by Ripple https://goo.gl/g8vFPL
6. DigiKnow https://youtu.be/scr68zFddso
7. Blockchain University http://blockchainu.co
8. Bitcoin Core https://bitcoin.org
9. Blockchain Alliance http://www.blockchainalliance.org
10. Multichain Blog http://www.mutichain,com/blog
11. HiveMind http://bitcoinhivemind.com
12. Chicago Blockchain Project http://chicagoblockchainproject.com/
13. Chicago Bitcoin and Open Blockchain Meetup Group https://www.meetup.com/Bitcoin-Open-Blockchain-Community-Chicago/

Source: Laurence, T. (2017). Blockchain for Dummies. Hoboken, NJ: John Wiley & Sons, Inc.

The 10 Rules to Never Break on the Blockchain

1. Don’t use Cryptocurrency or Blockchain to Skirt the Law
2. Keep your contracts as simple as possible
3. Publish with great caution
4. Back Up, Back Up, Back Up Your Private Keys
5. Triple-check the Address Before Sending Currency
6. Take Care When Using Exchanges
7. Beware Wi-Fi
8. Identify Your Blockchain Dev
9. Don’t Get Suckered
10. Don’t Trade Tokens Unless You Know What You’re Doing

Source: Laurence, T. (2017). Blockchain for Dummies. Hoboken, NJ: John Wiley & Sons, Inc.

ILLINOIS INSTITUTE OF TECHNOLOGY

Top 10 Blockchain Projects

- The R3 Consortium http://www.r3cev.com
- T ZERO: Overstocking the Stock Market http://www.overstock.com
- Blockstream’s Distributed Systems http://www.blockstream.com
- OpenBazaar’s Blockchain http://www.openbazaar.com
- Code Valley: Find Your Coder http://www.codevalley.com
- Bitfury’s Digital Assets http://www.bitfury.com
- Any Coin Can Shapeshift http://www.shapeshift.io
- Machine-Payable Apps on 21 http://www.21.co
- Anonymous Transactions on Dash http://www.dash.org
- ConsenSys: Decentralized Applications: http://www.consensys.net

Source: Laurence, T. (2017). Blockchain for Dummies. Hoboken, NJ: John Wiley & Sons, Inc.

ILLINOIS INSTITUTE OF TECHNOLOGY

HOW CAN YOU ACCELERATE YOUR BLOCKCHAIN UNDERSTANDING, KNOWLEDGE AND SKILLS?

How Can You Accelerate Your Blockchain Understanding, Knowledge, and Skills?

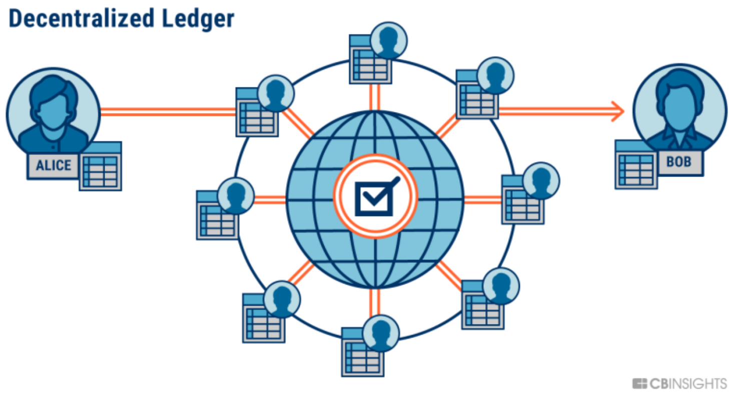
- Become obsessed with it because it’s the Future of Trusted, Decentralized, Distributed Computing
- The Internet
- Visit this link often: http://billslater.com/blockchain
- Self-study
- Hands-on (get a free tutorial)
- Join one or more Chicago Blockchain Meetup Groups
- Take one or more classes, either online or in a physical classroom

ILLINOIS INSTITUTE
OF TECHNOLOGY

CONCLUSION

Conclusion

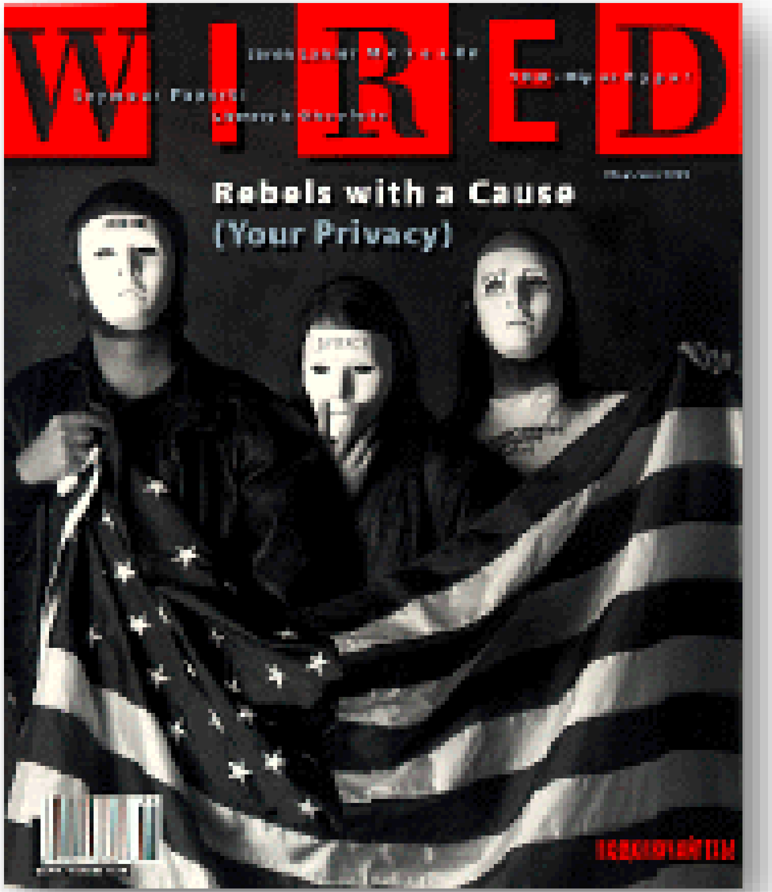
- Blockchain:
  - A technical marvel made possible by software, hardware, strong cryptography, and the Internet
  - Has made significant progress in only 100+ months
  - Has significant strengths and a few limitations too
  - Blockchain is starting to be widely used to automate trusted computing transactions and increase efficiencies in many industries
  - Has great potential because of popular support of talented nerds, and now major players in major industries
  - The excitement about the blockchain is based on its ability to serve as a tool for achieving and maintaining integrity in purely distributed peer-to-peer systems that have the potential to change whole industries due to disintermediation.



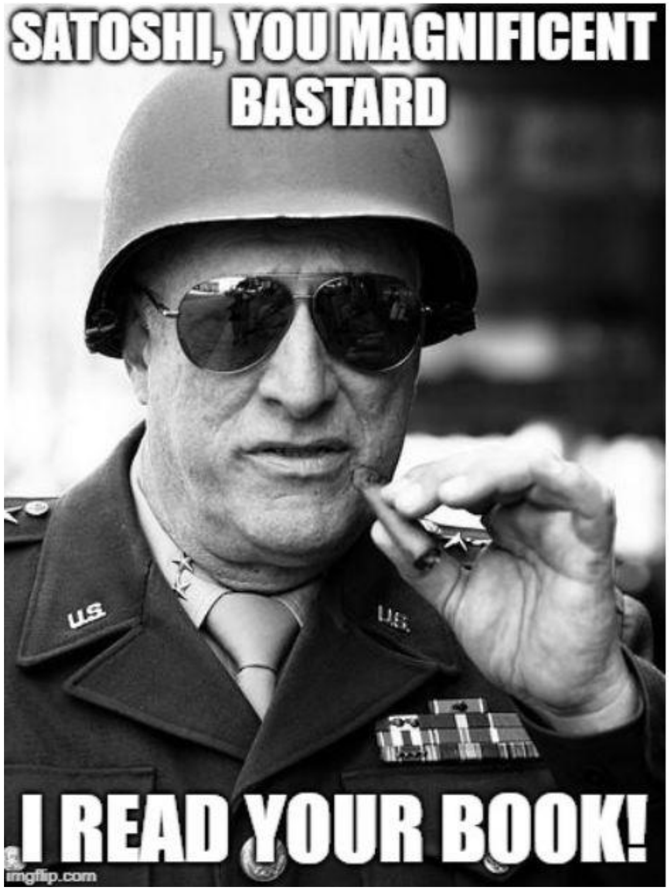
Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

ILLINOIS INSTITUTE OF TECHNOLOGY

Questions?



Wired Magazine, February 1993



General George S. Patton

ILLINOIS INSTITUTE OF TECHNOLOGY

PRACTICAL EXERCISES

ILLINOIS INSTITUTE OF TECHNOLOGY

Practical Exercises

1. Create and decode a hash
2. Decode a hash
3. Create a Blockchain record
4. Build a working Ethereum Blockchain Network

Practical Exercise 01

- Create a hash

1. Visit this website and type information about yourself or a message, and use the SHA 256 hash algorithm to create a hash http://www.hashemall.com/

2. Save the hash value.

3. Visit this website to decrypt your hash message: http://md5decrypt.net/en/Sha256/

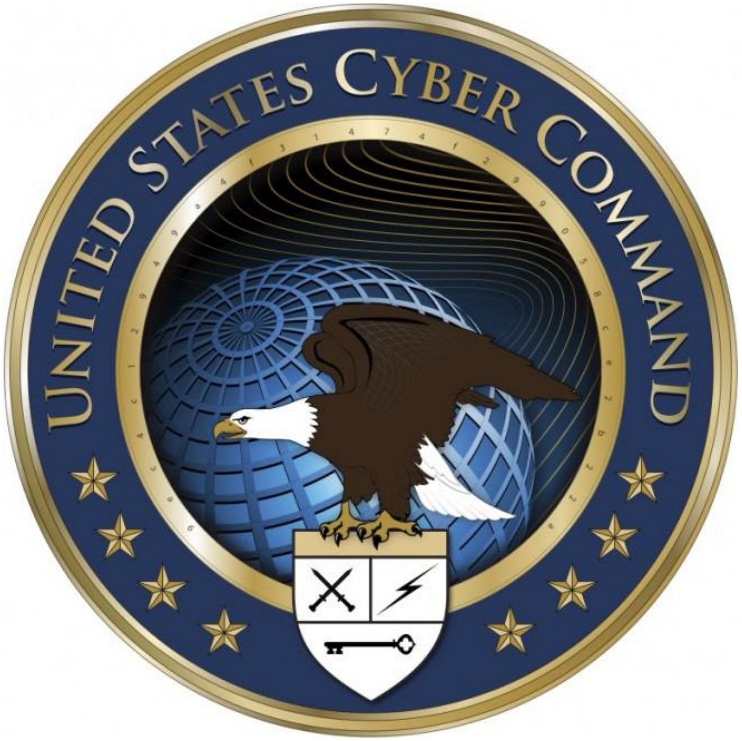
Practical Exercise 02

- Decode a hash

Hash:
9ec4c12949a4f31474f299058ce2b22a

This hash is found on the emblem of U.S. Cybercommand. It is a message that was hashed

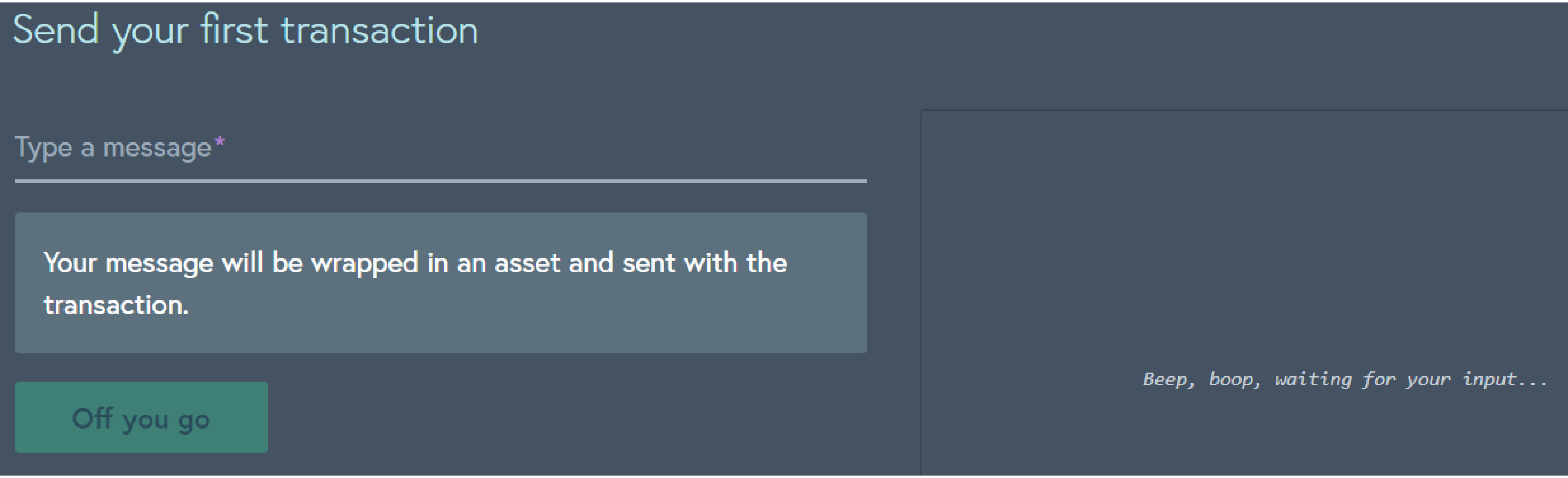
Using a commonly known hashing algorithm. Use this website to see if you can decrypt this Hash and see the message: http://www.hashemall.com/



Practical Exercise 03

- Create a Blockchain record

Visit this website and create your first Blockchain record:
https://www.bigchaindb.com/getstarted/
Copy and Save the results to a local text file named:
YYYY_ MMDD_FirstName_LastName_My_First_Blockchain_Transaction_.txt



Send your first transaction

Type a message*

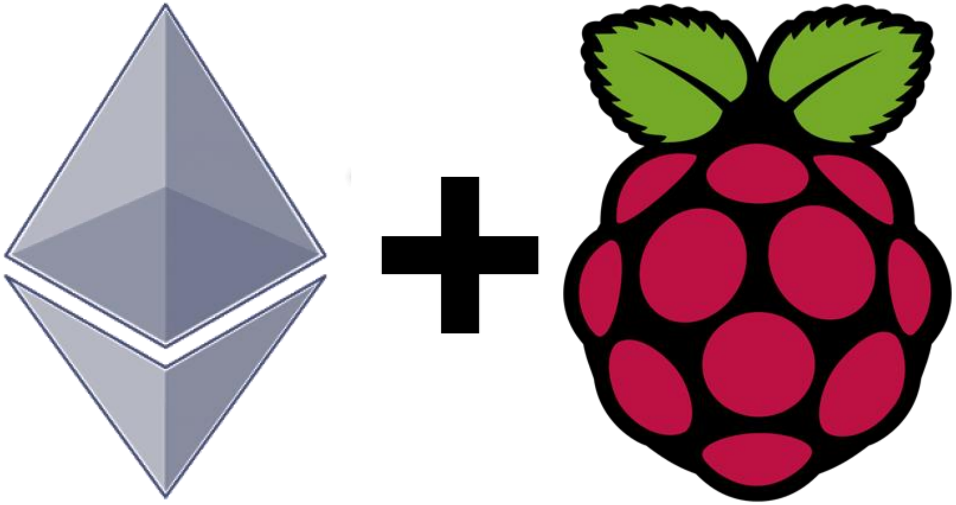
Your message will be wrapped in an asset and sent with the transaction.

Beep, boop, waiting for your input...

ILLINOIS INSTITUTE OF TECHNOLOGY

Practical Exercise 04

- Build a Working Prototype Ethereum Blockchain using Raspberry Pi



Practical Exercise 04
Part 01 - Getting Started

- Setting up Ethereum on Raspberry Pi – Part 01
- Visit this link and follow the instructions:
  - https://www.rs-online.com/designspark/exploring-ethereum-with-raspberry-pi-part-1-getting-started

Practical Exercise 04
Part 02 - Setting up a Private Blockchain

- Setting up Ethereum on Raspberry Pi – Part 02
- Visit this link and follow the instructions:
  - https://www.rs-online.com/designspark/exploring-ethereum-with-raspberry-pi-part-2-creating-a-private-blockchain

REFERENCES

References

- Antonopoulos, A. M. (2018). Mastering Bitcoin: Programming the Open Blockchain, second edition. Sebastopol, CA: O’Reilly Media, Inc.
- Associated Press. (2014). Mt. Gox finds 200,000 missing bitcoins. Retrieved from http://money.msn.com/business-news/article.aspx?feed=AP&date=20140321&id=17454291 on March 21, 2014.
- Bahga, A. and Madisetti, V. (2017). Blockchain Applications: A Hands-On Approach. Published by Arshdeep Bahga and Vijay Madisetti. www.blockchain-book.com .
- Bambara, J. J. and Allen P. R. (2018). Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions. New York, NY: McGraw-Hill Education.
- Bashir, I. (2018). Mastering Blockchain, second edition. Birmingham, UK: Packt Publishing Ltd.
- BBC. (2014). Troubled MtGox Bitcoin boss emerges after shut down Retrieved from http://www.bbc.com/news/technology-26352442 on February 26, 2014.
- Bitcoin. (2014). Bitcoin. Retrieved from https://bitcoin.com/ on April 10, 2014.
- Bitcoin Charts. (2014). Bitcoin Charts. Retrieved from http://bitcoincharts.com/ on March 1, 2014.
- Bitcoin Foundation. (2014). Bitcoin Foundation. Retrieved from https://bitcoinfoundation.org/ on April 10, 2014.
- Bitcoin Links: http://bit.ly/1eixu78 (over 272 million)
- Bitcoin.org. (2014). Bitcoin.org FAQs.. Retrieved from https://bitcoin.org/en/faq on April 10, 2014.

ILLINOIS INSTITUTE
OF TECHNOLOGY

References

- Bitcoin Scammers. (2014). Bit Coin Scammers. Retrieved from http://bitcoinscammers.com/ on April 9, 2014.
- Brown, E. Bitcoin bubble could burst as investors rush to withdraw cash. Retrieved from http://www.zdnet.com/bitcoin-bubble-could-burst-as-investors-rush-to-withdraw-cash-7000026410/ on February 17, 2014.
- Casey, M. J. and Vigna, P. (2018). The Truth Machine: The Blockchain Reference and the Future of Everything. New York, NY: St. Martin's Press.
- Caughey, M. (2013). Bitcoin Step by Step, second edition. Amazon Digital Services.
- Caughey, M. (2013). Bitcoin Mining Step by Step. Amazon Digital Services.
- Champagne, P. (2014). The Book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto. Published by E53 Publishing, LLC.
- Chen, C. (2014). PBOC Orders All Chinese Banks And Third Party Payment Processors To Close Accounts Of Chinese Bitcoin Exchanges by 4/15. Retrieved from http://www.cryptocoinsnews.com/2014/03/27/pboc-orders-all-chinese-banks-third-party-payment-processors-shut-accounts-15-chinese-bitcoin-exchanges-april-15th/ on March 27, 2014.
- Dannen, C. (2017). Introducing Ethereum and Solidity: Foundations of Crytocurrency and Blockchain Programming for Beginners. New York, NY: Apress
- De Filippi, P. and Wright, A. (2018). Blockchain and the Law: the Rule of Code. Cambridge, MA: President and Fellows of Harvard College.

References

- Demeester, T. (2014). Whither the Price of Bitcoin? Retreived from http://www.coindesk.com/whither-price-bitcoin/ on April 12, 2014.
- Dhillon, V., Metcalf, D., and Hooper, M. (2017). Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Nake It Work for You. New York, NY: Apress.
- Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.
- Eddison, L. (2017). Ethereum: A Deep Dive into Ethereum. Published by Leonard Eddison.
- Etwaru, R. (2017). Blockchain Trust Companies. Indianapolis, IN: Dog Ear Publishing.
- Gerard, D. (2107), Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum, and Smart Contracts. Published by David Gerard. www.davidgerard.co.uk/blockchain .
- Hacking, J. (2014). Calif. man, Satoshi Nakamoto denies to be a Bitcoin founder. Retrieved from http://www.thewestsidestory.net/2014/03/07/calif-man-satoshi-nakmoto-denies-bitcoin-founder/ on March 7, 2014.
- Hornyak, T. (2014). 'Malleability' attacks not to blame for Mt. Gox's missing bitcoins, study says. Retrieved from http://www.pcworld.com/article/2114200/malleability-attacks-not-to-blame-for-mt-goxs-missing-bitcoins-study-says.html on March 27, 2014.
- Incencio, R. (2014). Ransomware and Bitcoin Theft Combine in BitCrypt. Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-and-bitcoin-theft-combine-in-bitcrypt/ on March 27, 2014.
- Kadhim Shubber, K. 2014. Gavin Andresen Steps Down as Bitcoin's Lead Developer. Retrieved from http://www.coindesk.com/gavin-andresen-steps-bitcoins-lead-developer/ on April 8, 2014.

ILLINOIS INSTITUTE OF TECHNOLOGY

References

- Laurence, T. (2017). Blockchain for Dummies. Hoboken, NJ: John Wiley & Sons, Inc.
- Lee, T. B. (2013). 12 questions about Bitcoin you were too embarrassed to ask. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/19/12-questions-you-were-too-embarrassed-to-ask-about-bitcoin/ on November 19, 2013.
- Markowitz, E. (2014). Cryptocurrencies Are the New Spam Frontier. Retrieved from http://www.vocativ.com/tech/bitcoin/cryptocurrencies-new-spam-frontier/ on March 28, 2014.
- Kadhim Shubber, K. 2014. Gavin Andresen Steps Down as Bitcoin's Lead Developer. Retrieved from http://www.coindesk.com/gavin-andresen-steps-bitcoins-lead-developer/ on April 8, 2014.

- Laurence, T. (2017). Blockchain for Dummies. Hoboken, NJ: John Wiley & Sons, Inc.
- Lee, T. B. (2013). 12 questions about Bitcoin you were too embarrassed to ask. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/19/12-questions-you-were-too-embarrassed-to-ask-about-bitcoin/ on November 19, 2013.
- Markowitz, E. (2014). Cryptocurrencies Are the New Spam Frontier. Retrieved from http://www.vocativ.com/tech/bitcoin/cryptocurrencies-new-spam-frontier/ on March 28, 2014.

- Ma, M. (2017). Blockchain Design Sprint: An Agile Innovation Workbook to Implement an Agile Design Sprint for your Blockchain Business. Published by Future Lab www.futurelabconsulting.com
- NameCheap. (2014. NameCheap accepts Bitcoin for Domain Name Registration. Retrieved from https://www.namecheap.com/domains/registration.aspx?utm_source=facebook&utm_medium=ppc&utm_content=Namecheap%2Baccepts%2Bbitcoin%2Bpayments&utm_campaign=Bitcoin%2Bcampaign on March 25, 2014.
- Nakamoto. S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf on November 1, 2013.

ILLINOIS INSTITUTE OF TECHNOLOGY

References

- Noyola, E. (2018). Ethereum: Ethereum, Tokens and Smart Contracts. Published by Eugenio Noyola.
- Peterson, O. (2018). An Introduction of Programmable Smart Contracts in Ethereum (Pt 1). Retrieved from https://www.linkedin.com/pulse/introduction-programmable-smart-contracts-ethereum-p1-%CE%BE%CE%BE%CE%BE-oliver/ on February 1, 2018.
- Petrovan, B. (2014) Researchers find Android apps that covertly mine Dogecoin, one of them with more than a million downloads. Retrieved from http://www.androidauthority.com/dogecoin-mining-android-apps-362142/ on March 27, 2014.
- Popper, N. (2013). Into the Bitcoin Mines, Retrieved from http://dealbook.nytimes.com/2013/12/21/into-the-bitcoin-mines/?hp&_r=0 on December 21, 2013.
- Preev. (2014). Current Value of Bitcoin. Retrieved from http://preev.com/ on March 20, 2014.
- Prusty, N. (2017). Building Blockchain Projects: Building Decentralized Blockchain Applications with Ethereum and Solidity. Birmingham, UK: Pact Publishing.
- SCGNEWS. (2014). Bitcoin Flash Crash - 80% Drop in Seconds - Down 20% After Stabilizing. Retrieved from http://scgnews.com/bitcoin-flash-crash-80-drop-in-seconds-down-20-after-stabilizing on February 10, 2014.
- SCGNEWS. (2014). The IRS Just Declared War on Bitcoin - Retroactively. Retrieved from http://scgnews.com/the-irs-just-declared-war-on-bitcoin-retroactively on March 27, 2014.
- Sharkey, T. (2014. Inside Bitcoins NYC Day 1: Bitcoin 2.0 Takes Center Stage. Retrieved from http://www.coindesk.com/inside-bitcoins-nyc-day-1-bitcoin-2-0-takes-center-stage/ on April 8, 2014.

ILLINOIS INSTITUTE OF TECHNOLOGY

References

- Solomon, D. (1998). Inside Windows NT, 2nd Edition. Redmond, WA: Microsoft Press.
- Wall Street Daily. (2014). Beware Bitcoin: An Insideous Ne Currency Scam - Free Investor's Report. Retrieved from http://signups.wallstreetdaily.com/X303Q1A8 on March 7, 2014.
- Wattenhofer, R. (2017). Distributed Ledger Technology: The Science of the Blockchain, second edition. Inverted Forest Technology.
- White, A. (2018). Blockchain: Discover the Technology Behind Smart Contracts, Wallets, Mining, and Cryptocurrency. Published by Andrew K. White.
- Wood, R. W. (2013). Sorry Bitcoin, IRS Gets Reports. Retrieved from http://www.forbes.com/sites/robertwood/2013/05/05/sorry-bitcoin-irs-gets-reports/ on March 15, 2014.
- Zetter, K. (2014). Digital Currency Founder: U.S. Indicted Me For Not Giving FBI My Source Code. Retrieved from http://www.wired.com/threatlevel/2014/01/liberty-reserve-source-code/ on January 30, 2014.

ILLINOIS INSTITUTE OF TECHNOLOGY

References:
Best Blockchain Texts

- **Mastering Blockchain - Second Edition**
  - by Imran Bashir
- **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You**
  - by Vikram Dhillon, David Metcalf, Max Hooper
- **Ethereum, tokens & smart contracts: Notes on getting started**
  - by Eugenio Noyola
- **Distributed Ledger Technology: The Science of the Blockchain**
  - by Roger Wattenhofer
- **The Book of Satoshi: The Collected Writings od Bitcoin Creator Satoshi Nakamoto**
  - By Phil Champagne

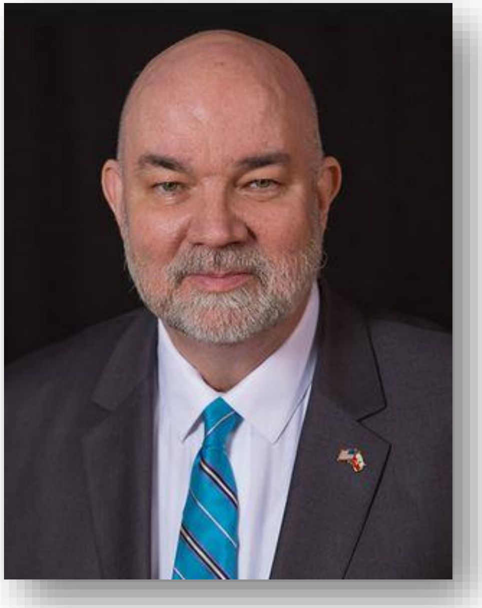
ILLINOIS INSTITUTE
OF TECHNOLOGY

Dedication

- Dedicated with never-ending love, respect, and gratitude to my dear Father-in-law and Mother-in-Law, Wiesiek Roguski (http://billslater.com/wiesiek) and Wiesia Roguska (http://billslater.com/wiesia).

Presenter Bio: William Favre Slater, III

- **Lives in Chicago; Cybersecurity professional by day, Professor at night**
- **Married to my Best Friend and Soul Mate, Ms. Joanna Roguska**
- **Current Position – Project Manager / Sr. IT Consultant at Slater Technologies, Inc.** Working on projects related to
  - Security reviews and auditing
  - Blockchain consulting
  - ISO 27001 Project Implementations
  - Subject Matter Expert for preparing Risk Management and Security Exams at Western Governor's State University in UT
  - Providing subject matter expert services to Data Center product vendors and other local businesses.
  - Designing and creating a database application that streamlines program management, security management, risk management and reporting activities, for management of teams of IT workers and developers in teleworking environments. It will first be a Windows application and then be ported to the web.
  - Developing and presenting technical training materials for undergraduate and graduate students at the Illinois Institute of Technology in the areas of Blockchain and Blockchain development, Data Center Operations, Data Center Architecture, Cybersecurity Management, and Information Technology hardware and software.
  - Created an eBook with articles about Security, Risk Management, Cyberwarfare, Project Management and Data Center Operations
  - Professor at Illinois Tech for 10 years



Slater Technologies

William Favre Slater, II

- 312-758-0307
- slater@billslater.com
- williamslater@gmail.com
- http://billslater.com/interview
- 1515 W. Haddon Ave., Unit 309
  Chicago, IL 60642
  United States of America

William Favre Slater, III