NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

CC0007 Science and Technology for Humanity

Blockchain Revolution

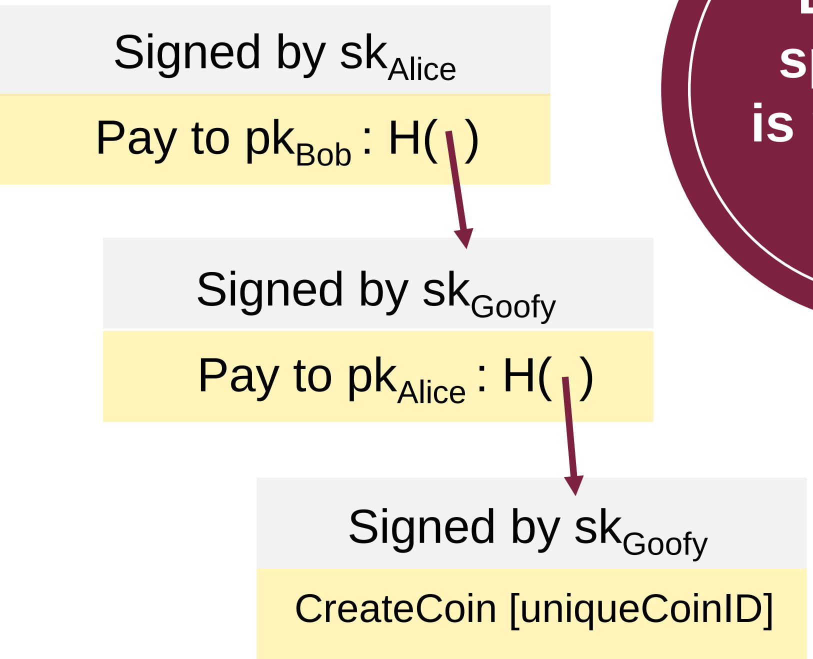
Asst Prof Li Yi, NTU

How Does Blockchain Work?

A Simple Cryptocurrency: GoofyCoin

GoofyCoin rules:

1. Goofy can create new coins: “**CreateCoin[uniqueCoinID]**”
2. Whoever owns a coin can pass it on to someone else by signing a statement that saying, “**Pass on this coin to X**” (where X is specified as a public key).
3. Anyone can **verify the validity of a coin by following the chain of hash pointers** back to its creation by Goofy, verifying all signatures along the way.



Signed by sk_{Alice}

Pay to pk_{Bob} : H( )

Signed by sk_{Goofy}

Pay to pk_{Alice} : H( )

Signed by sk_{Goofy}

CreateCoin [uniqueCoinID]

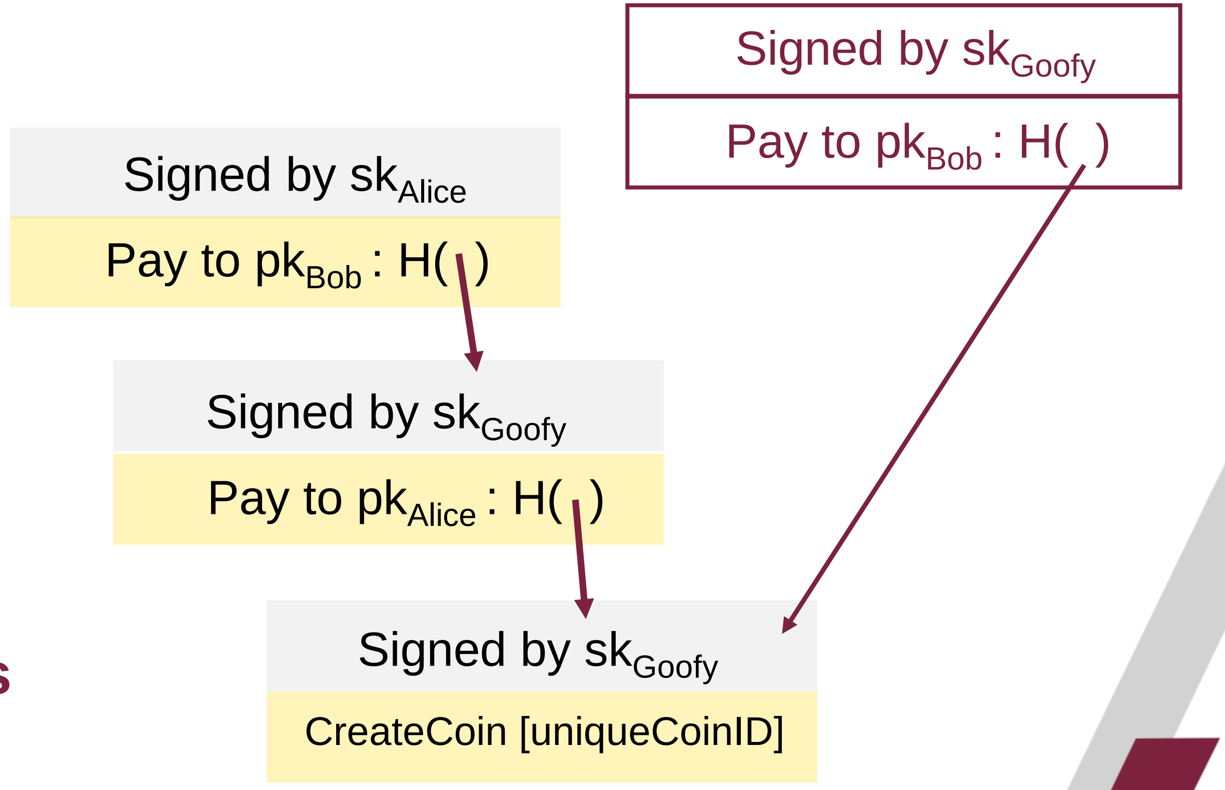
Double-spending is possible! Why?

Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

A Simple Cryptocurrency: GoofyCoin

GoofyCoin Rules:

1. Goofy can create new coins: "**CreateCoin[uniqueCoinID]**"
2. Whoever owns a coin can pass it on to someone else by signing a statement that saying, "**Pass on this coin to X**" (where X is specified as a public key)
3. Anyone can **verify the validity of a coin by following the chain of hash pointers** back to its creation by Goofy, verifying all of the signatures along the way



Signed by sk_{Goofy}

Pay to pk_{Bob} : H( )

Signed by sk_{Alice}

Pay to pk_{Bob} : H( )

Signed by sk_{Goofy}

Pay to pk_{Alice} : H( )

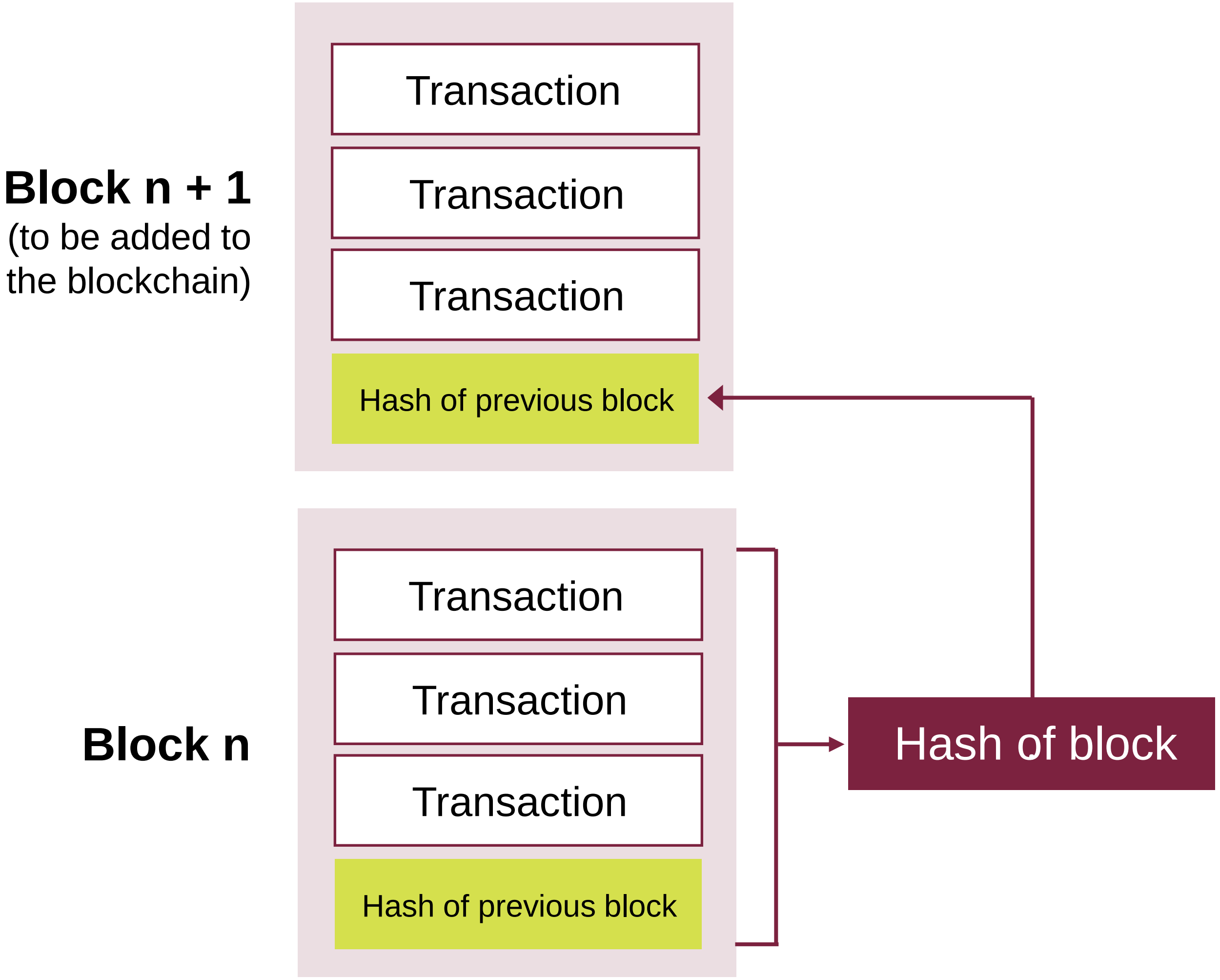
Signed by sk_{Goofy}

CreateCoin [uniqueCoinID]

Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

Solving the “Double-Spending” Problem

- **Who gets to add the next block?**
- Some nodes are known as **miners**. Miners add blocks to the blockchain.
- In order to add a block to the blockchain, a miner needs to do the following:
  - Take the transactions in the previous block and combine it with the hash of the previous block to derive its hash.
  - Store the derived hash into the current block.



Lee, W-M. (2018). *Understanding how blockchain works*. NDC Conferences. Retrieved July 20, 2022 from https://blog.ndcconferences.com/understanding-blockchain/

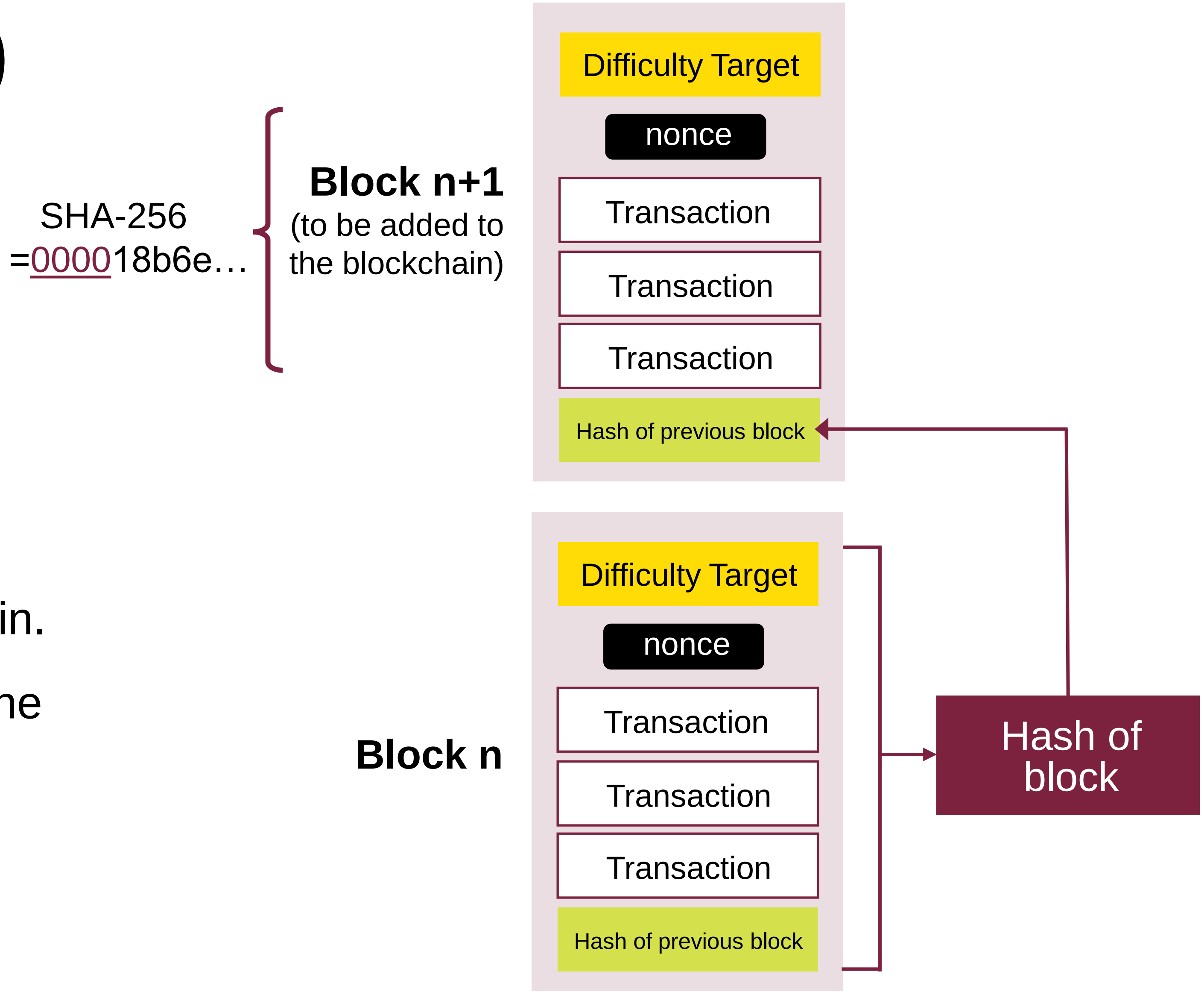
Proof of Work (PoW)

- A mechanism to help reach consensus on the state of the blockchain.
- PoW requires the nodes to demonstrate they have burned CPU in order to win the right to create the next block.
    - A piece of data which was difficult (costly, time-consuming) to produce so as to satisfy certain requirements.
    - It must be trivial to check whether data satisfies said requirements.
    - Hashcash (SHA-256) is the PoW function used to solve difficult mathematics problems.
    - **Mining** is usually the process in which this proof occurs.

WeUseCoins. (n.d.). *What is bitcoin mining?* Retrieved July 20, 2022 from https://www.weusecoins.com/en/mining-guide/

Proof of Work (PoW)

- Miners work hard to find the value of **nonce**.
  - Once the nonce is found, the entire block and the nonce is broadcasted to other nodes.
  - The block has been mined and ready to be added to the blockchain.
  - Other miners can now verify that the nonce does indeed satisfy the difficult target.
  - The miner earns the mining fees and transaction fees.



Lee, W-M. (2018). *Understanding how blockchain works*. NDC Conferences. Retrieved July 20, 2022 from https://blog.ndcconferences.com/understanding-blockchain/

Building a Blockchain for Students’ Grades

Students

- Student identities are concealed.
- Each student has a public key that matches a private key that only the student knows.

	Public Key	Private Key
Student 1	ad59da	c8fc47b6fe
Student 2	bd9ebc	4382af3398
Student 3	c67445	56164d905c

Faculties

- Miners
- Other participating nodes
- Miners mine blocks, all nodes verify and vote

Christianson, J. S. (2022, February 10). *How to teach blockchain with “The Blockchain Game!”*. Medium. https://medium.com/predict/how-to-teach-blockchain-with-the-blockchain-game-44360c542c81. CC BY-NC-SA 4.0.

Pool of Grade Records

Block 1

Course:	Parks 320
Student:	ad59da
Grade:	F

Block 2

Course:	Engineering 300
Student:	bd9ebc
Grade:	B

Block 3

Course:	Business 200
Student:	c67445
Grade:	C

Christianson, J. S. (2022, February 10). *How to teach blockchain with "The Blockchain Game!".* Medium. https://medium.com/predict/how-to-teach-blockchain-with-the-blockchain-game-44360c542c81. CC BY-NC-SA 4.0.

Go Miners, Go

Hash = Nonce + a + b + c – Value of last two digits of previous hash

a = Value of the first letter of the course

b = Value of the first letter of the student’s public key

c = Value of the grade

Nonce = Value between 1 and 3 that you will adjust to calculate a hash that can be evenly divisible by 3

Table

A	65	N	78
B	66	O	79
C	67	P	80
D	68	Q	81
E	69	R	82
F	70	S	83
G	71	T	84
H	72	U	85
I	73	V	86
J	74	W	87
K	75	X	88
L	76	Y	89
M	77	Z	90

Christianson, J. S. (2022, February 10). *How to teach blockchain with “The Blockchain Game!”.* Medium. https://medium.com/predict/how-to-teach-blockchain-with-the-blockchain-game-44360c542c81. CC BY-NC-SA 4.0.

Our First Block

Hash: 212

Genesis Block
Course: -
Student: -
Grade: -

Block 1
Course: Parks 320
Student: ad59da
Grade: F

Block	Course	Student	Grade	Nonce (1-3)	Prev Hash	a	b	c	Hash
									212
1	Parks 320	ad59da	F		12	80	65	70	

Hash = Nonce + a + b + c – Value of last two digits of previous hash

Christianson, J. S. (2022, February 10). *How to teach blockchain with "The Blockchain Game!".* Medium. https://medium.com/predict/how-to-teach-blockchain-with-the-blockchain-game-44360c542c81. CC BY-NC-SA 4.0.

Finishing the Block: Hashing

Hash: 212

Genesis Block
Course: -
Student: -
Grade: -

Hash: 204

Block 1
Course: Parks 320
Student: ad59da
Grade: F

Block	Course	Student	Grade	Nonce (1-3)	Prev Hash	a	b	c	Hash
									212
1	Parks 320	ad59da	F	I	12	80	65	70	204

Hash = Nonce + a + b + c – Value of last two digits of previous hash

Christianson, J. S. (2022, February 10). *How to teach blockchain with "The Blockchain Game!"*. Medium. https://medium.com/predict/how-to-teach-blockchain-with-the-blockchain-game-44360c542c81. CC BY-NC-SA 4.0.

Finishing the Block: Verifying and Voting

Hash: 212

Genesis Block
Course: -
Student: -
Grade: -

Hash: 204

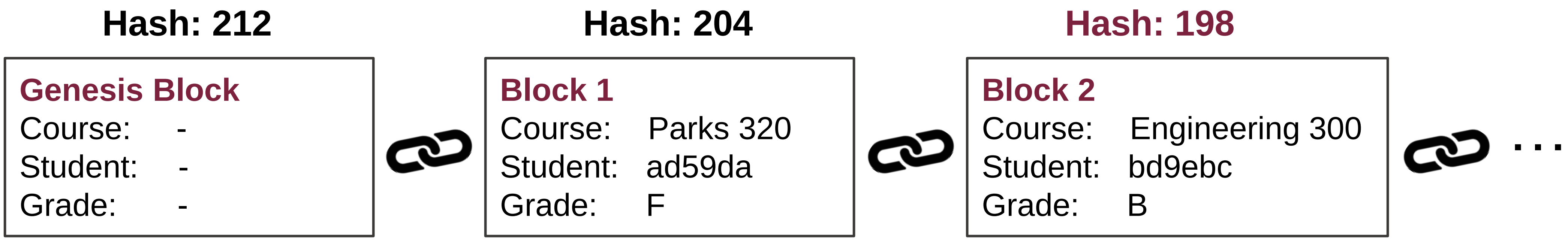
Block 1
Course: Parks 320
Student: ad59da
Grade: F

Block	Course	Student	Grade	Nonce (1-3)	Prev Hash	a	b	c	Hash
									212
1	Parks 320	ad59da	F	I	12	80	65	70	204

Hash = Nonce + a + b + c – Value of last two digits of previous hash

Christianson, J. S. (2022, February 10). *How to teach blockchain with "The Blockchain Game!"*. Medium. https://medium.com/predict/how-to-teach-blockchain-with-the-blockchain-game-44360c542c81. CC BY-NC-SA 4.0.

Second Block



Hash: 212

Genesis Block
Course: -
Student: -
Grade: -

Hash: 204

Block 1
Course: Parks 320
Student: ad59da
Grade: F

Hash: 198

Block 2
Course: Engineering 300
Student: bd9ebc
Grade: B

. . .

Block	Course	Student	Grade	Nonce (1-3)	Prev Hash	a	b	c	Hash
									212
1	Parks 320	ad59da	F	I	12	80	65	70	204
2	Engineering 300	bd9ebc	B	I	4	69	66	66	198

Hash = Nonce + a + b + c – Value of last two digits of previous hash

Christianson, J. S. (2022, February 10). *How to teach blockchain with "The Blockchain Game!".* Medium. https://medium.com/predict/how-to-teach-blockchain-with-the-blockchain-game-44360c542c81. CC BY-NC-SA 4.0.

Discussion

- What if "Student 1" loses his/her private key? we cannot retrieve
- What if a student pays off a node to change the score stored in "Block 1"? result inconsistency

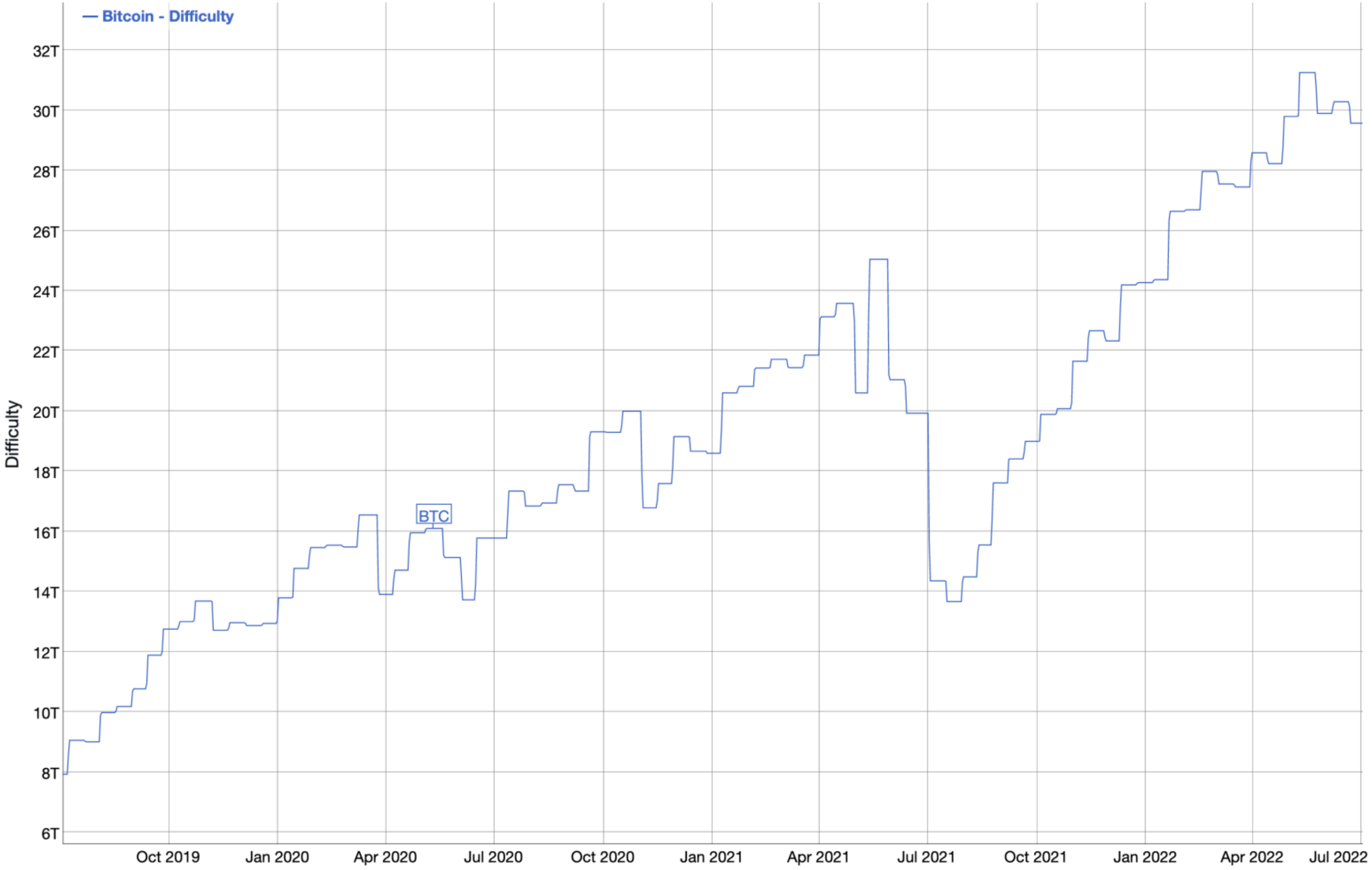
Block	Course	Student	Grade	Nonce (1-3)	Prev Hash	a	b	c	Hash
									212
1	Parks 320	ad59da	F ⚡	I	12	80	65	70	204
2	Engineering 300	bd9ebc	B	I	4 ⚡	69	66	66	198 ⚡

Christianson, J. S. (2022, February 10). *How to teach blockchain with "The Blockchain Game!".* Medium. https://medium.com/predict/how-to-teach-blockchain-with-the-blockchain-game-44360c542c81. CC BY-NC-SA 4.0.

Mining Difficulty

- Satoshi Nakamoto: “The more mining power the network has, the harder it is to guess the answer to the mining math problem”
- **Self-adjusting** to the accumulated mining power the network possesses.
- Why did Satoshi do this?
  - **On average**, a new block will be added every **10 minutes** (i.e., the nonce will be guessed every 10 minutes on average).
  - A sort of “arms race” to get the most efficient and powerful miners.

Mining Difficulty



Mining Revolution

CPU mining

GPU mining

FPGA mining

Can be design for ← other coin

ASIC mining → Specific coin

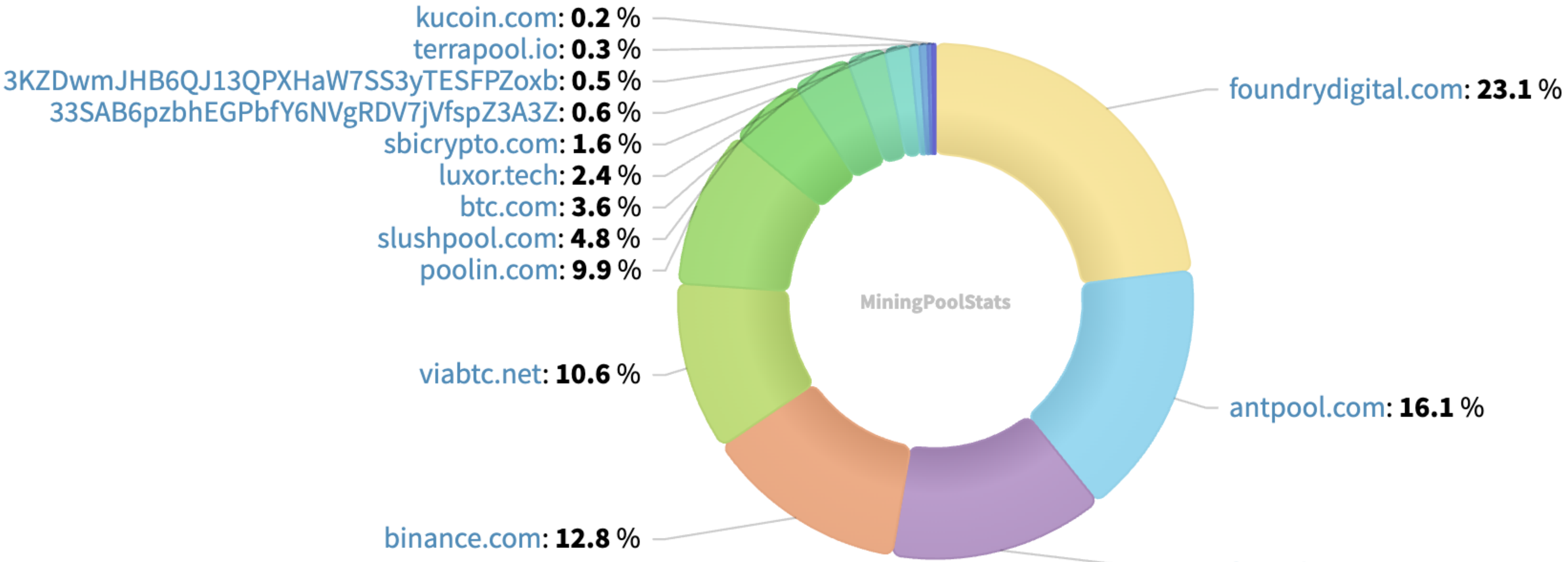
after design algo cannot be change

more power efficiency

Mining Pools

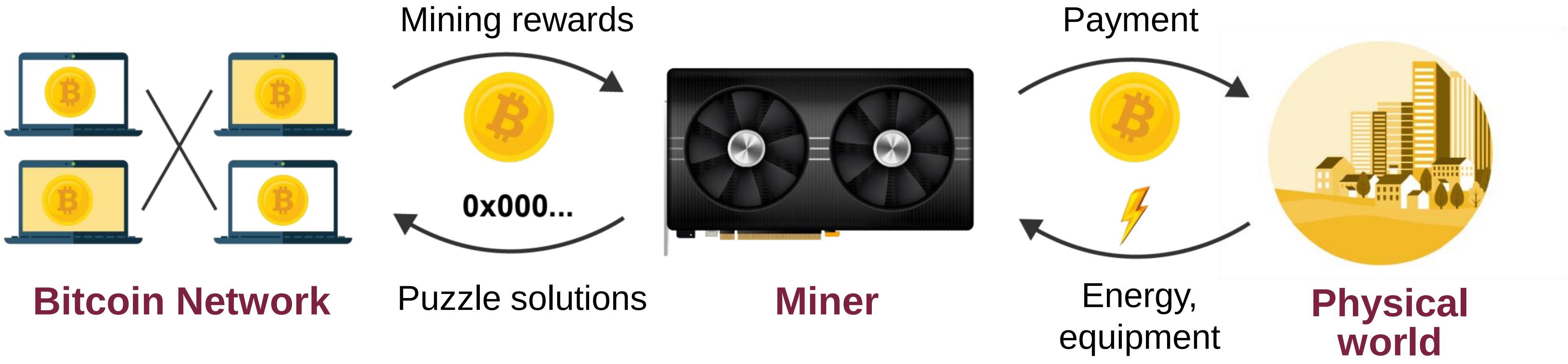
- **Idea:** Miners group together to form a “pool” (i.e., combine their mining power to compete more effectively).
- Once the pool wins, the reward is divided among the pool members based on their contributed mining power.
  - **Pros:** Reduce the variance of mining rewards; easy to upgrade the network
  - **Cons:** Pool manager must be trusted; centralised

Mining Pool Distribution



Proof-of-Stake and Virtual Mining

- Goal of mining is to enable a form of voting on the state of the blockchain
  - Miners invest in computer cycles
  - Computing power is translated to votes
- Mining in PoW is costly
  - Hardware equipment
  - Energy



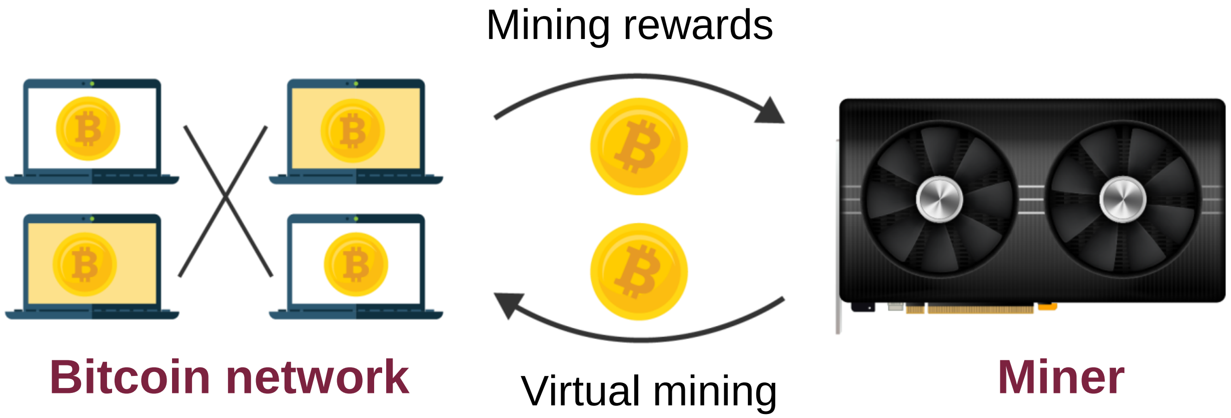
Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

→ big player can hv better successful mining

Proof-of-Stake and Virtual Mining

- Can we remove the step of spending money on energy and equipment?
  - After all, this is only to prove who has invested more in mining.
  - Votes come directly from the proportion of the currency they hold.

- Advantages of virtual mining
  - It reduces the environmental footprint of PoW.
  - Large shareholders have an incentive to do things that would benefit the system as a whole.
  - This is essentially **Proof-of-Stake (PoS)**.
  - Ethereum and Algorand are adopting PoS as an alternative to PoW.



Mining rewards

Bitcoin network

Virtual mining

Miner

Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

Types of Blockchain

Public blockchain

Private blockchain

Consortium blockchain

Public Blockchain

- Anyone can run the public code, start mining, make a transaction, explore and validate the blockchain.
- Each transaction is verified by every node before it is written to the system.
- **Examples: Bitcoin, Ethereum, Algorand**

Private Blockchain

- R/W permissions are kept centralised by one organisation.
- **Examples: Ripple, Multichain, Corda**

Consortium Blockchain

Also known as federated blockchain

- Controlled by a set of pre-selected nodes, members of the consortium can run code, start mining and make transactions.
- **Examples: R3, HyperLedger Fabric**

Blockchain 2.0: Decentralised Applications

Decentralised Applications (DApps)

→ On top of blockChain plattform

- The Do-It-Yourself platform for decentralised programs is also known as **Decentralised Applications**
- The infrastructure for running DApps worldwide
- First proposed in 2013 and then brought to life in 2014 by Vitalik Buterin, the co-founder of Bitcoin Magazine
- Goal: Ro truly decentralise the internet

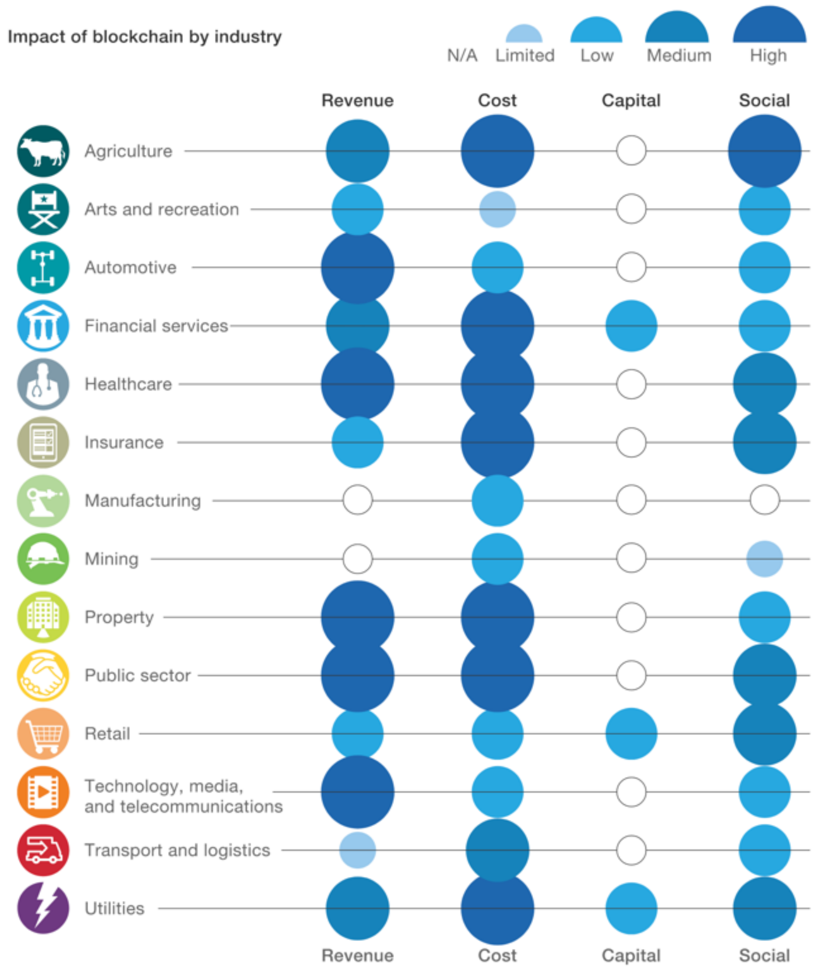
ethereum

- **Ethereum** in 2022:
  - **48 million** smart contracts
  - **2,970** DApps deployed
  - **49.38K** active users/day
  - **102.18K** transactions/day

State of the DApps. (n.d.). *DApp statistics*. Retrieved July 20, 2022 from https://www.stateofthedapps.com/stats

Smart Contracts

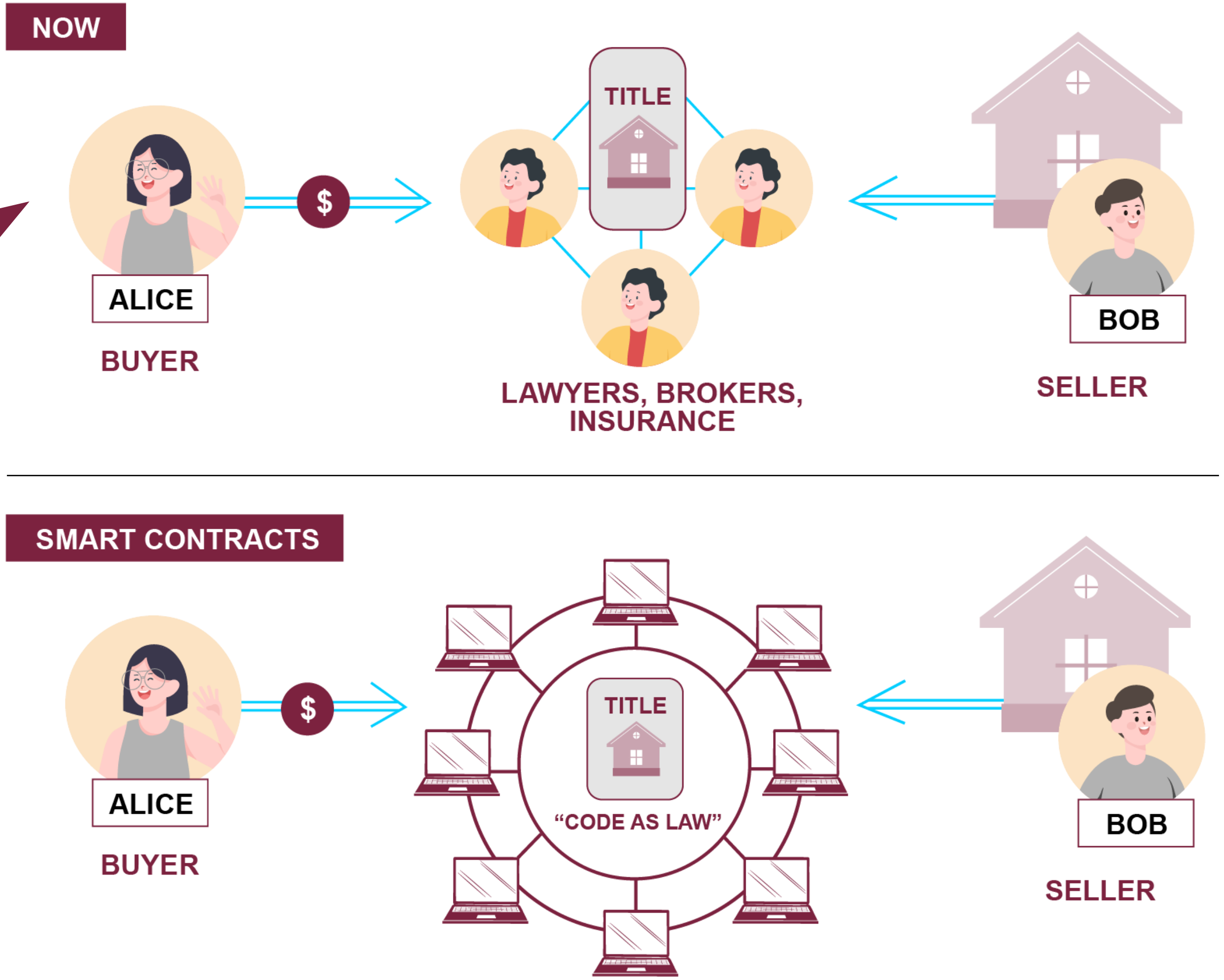
- User-defined self-executing computer programs running on top of blockchain
- Managing exchange of digital assets
- Applications across many different sectors



McKinsey&Company

Buying a House on Ethereum

How do I validate the ownership of the house and trust the seller in transferring it?



NOW

ALICE

BUYER

$

TITLE

LAWYERS, BROKERS, INSURANCE

BOB

SELLER

SMART CONTRACTS

ALICE

BUYER

$

TITLE

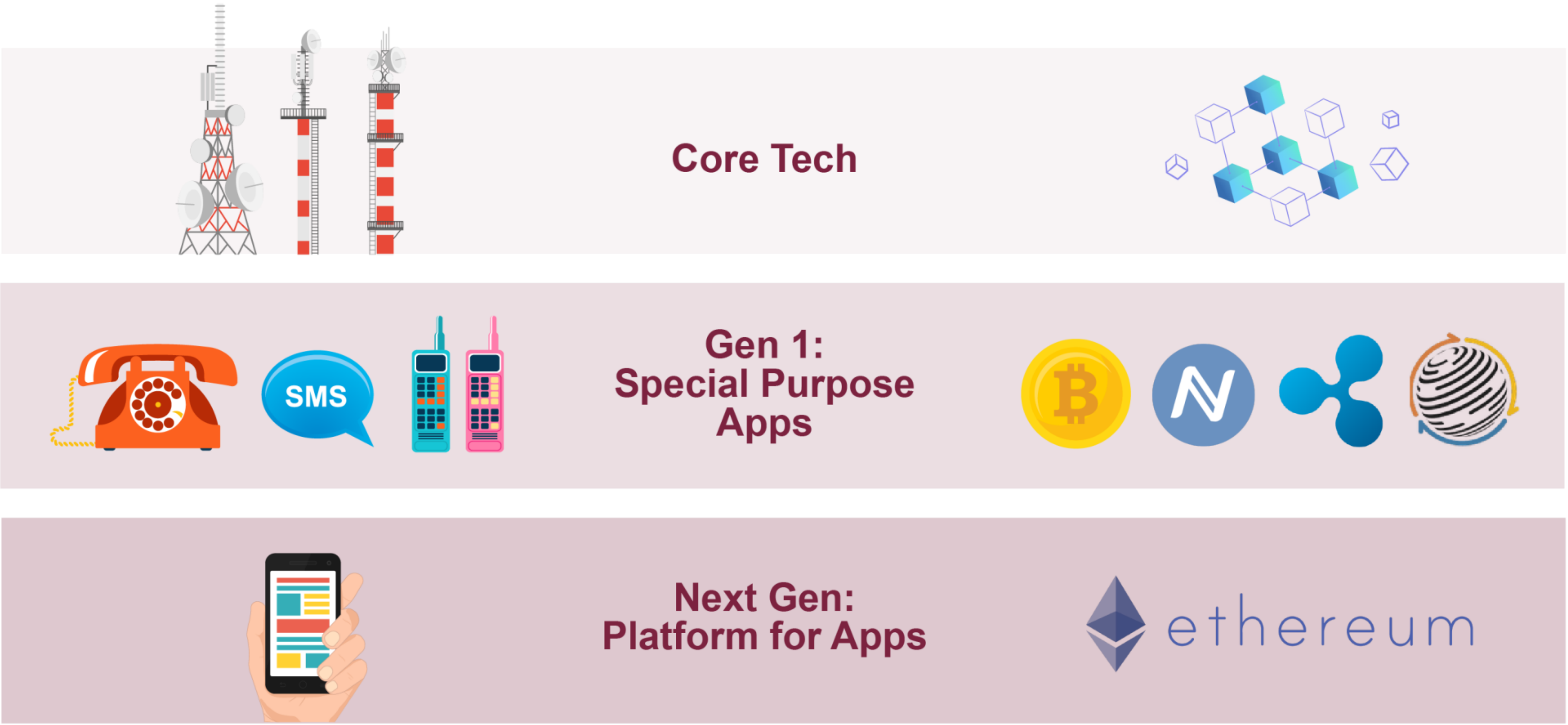
“CODE AS LAW”

BOB

SELLER

How do I trust the buyer on making the agreed payment in time?

Blockchain/Bitcoin/Ethereum



Core Tech

Gen 1:
Special Purpose
Apps

Next Gen:
Platform for Apps