CSCI361

Introduction to Blockchain and Cryptocurrency

Features of Cryptocurrency

- Peer-to-peer transfer of electronic money
- No centralised entity to control transactions
- Based on the cryptographic primitives
  - ✓Digital signature
  - ✓Hash function
- There are numerous cryptocurrencies nowdays → Bitcoin, Ethereum, Ripple, …etc

Ledger – Where Everything Begins

- Financial transaction is all about managing a ledger
- The ledger records deposits

Alice deposits $100

Bob deposits $70

Charlie deposits $130

Diana deposits $90

Ledger

- And debits

…Deposits…

Alice pays Bob $10

Bob pays Charlie $40

Charlie pays Diana $30

Diana pays Alice $35

Ledger

- Assume that the ledger is public i.e., accessible from anyone

…Deposits…

Alice pays Bob $10

Bob pays Charlie $40

Charlie pays Diana $30

Diana pays Alice $35

❖ Anyone can add lines to the ledger.

Ledger

- Problem

…Deposits…

Alice pays Bob $10

Bob pays Charlie $40

Charlie pays Diana $30

Diana pays Alice $35

❖ Bob may want to put "Alice pays Bob $100" to the ledger. (Why? So obvious!)

Ledger

- How to prevent this? – Through Digital Signature!

…Deposits…

Alice pays Bob $10 S_{Alice}

Bob pays Charlie $40 S_{Bob}

Charlie pays Diana $30 $S_{Charlie}$

Diana pays Alice $35 S_{Diana}

- Alice can generate a digital signature on “Alice pays Bob”. Other people also can do the same.
- As signature is unforgeable, it’s hard for an adversary to add a line without knowing the private key.

Ledger

- Hang on...What if Bob does the following?

…Deposits…

Alice pays Bob $10 S_{Alice}

Alice pays Bob $10 S_{Alice}

Alice pays Bob $10 S_{Alice}

Alice pays Bob $10 S_{Alice}

❖ All the lines are valid!

Ledger

- We need a unique seqeunce number for each transaction.

…Deposits…

1 Alice pays Bob $10 S^{1}_{Alice}

2 Alice pays Bob $10 S^{2}_{Alice}

3 Alice pays Bob $10 S^{3}_{Alice}

4 Alice pays Bob $10 S^{4}_{Alice}

- Each signature must be different and again it’s hard to create one (or forge) without knowing the private key.
- Digital signature solved the problem of adding a valid transaction entry to the ledger!

Ledger

- Overspending : Oops! Bob has only $70!

…Deposits…

1 Bob pays Alice $30 S^1_{Bob}

2 Bob pays Charlie $20 S^2_{Bob}

3 Bob pays Alice $40 S^3_{Bob}

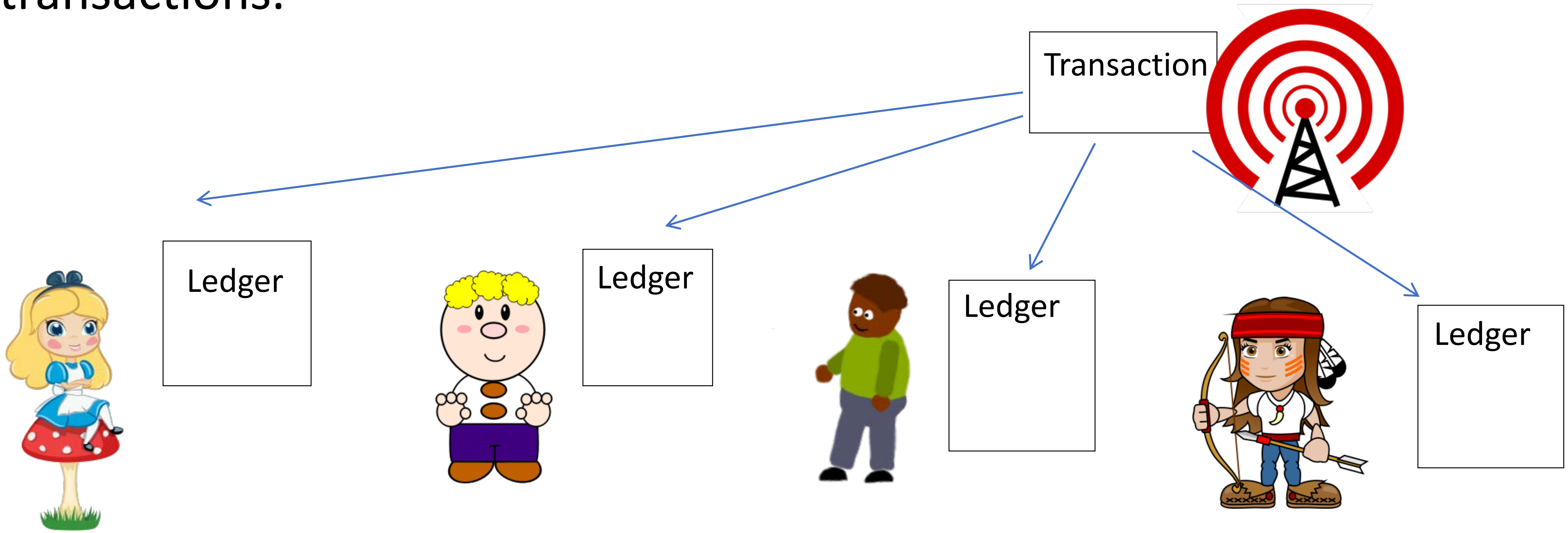
- Therefore we need to track Bob's all past transactions! (We need to refer to Bob's deposit.)
- In general, we need to keep the history of the ledger.

Ledger

- The ledger just described is nothing new. – It can be one of the ledgers held by banks today
- We trust the ledger as we trust the bank.
- But cryptocurrencies want to remove the role of the central authority in managing transactions.
- How?

Private Ledger?

- The idea is to broadcast transactions so that every participant should record them on their private ledger to track and validate the transactions.

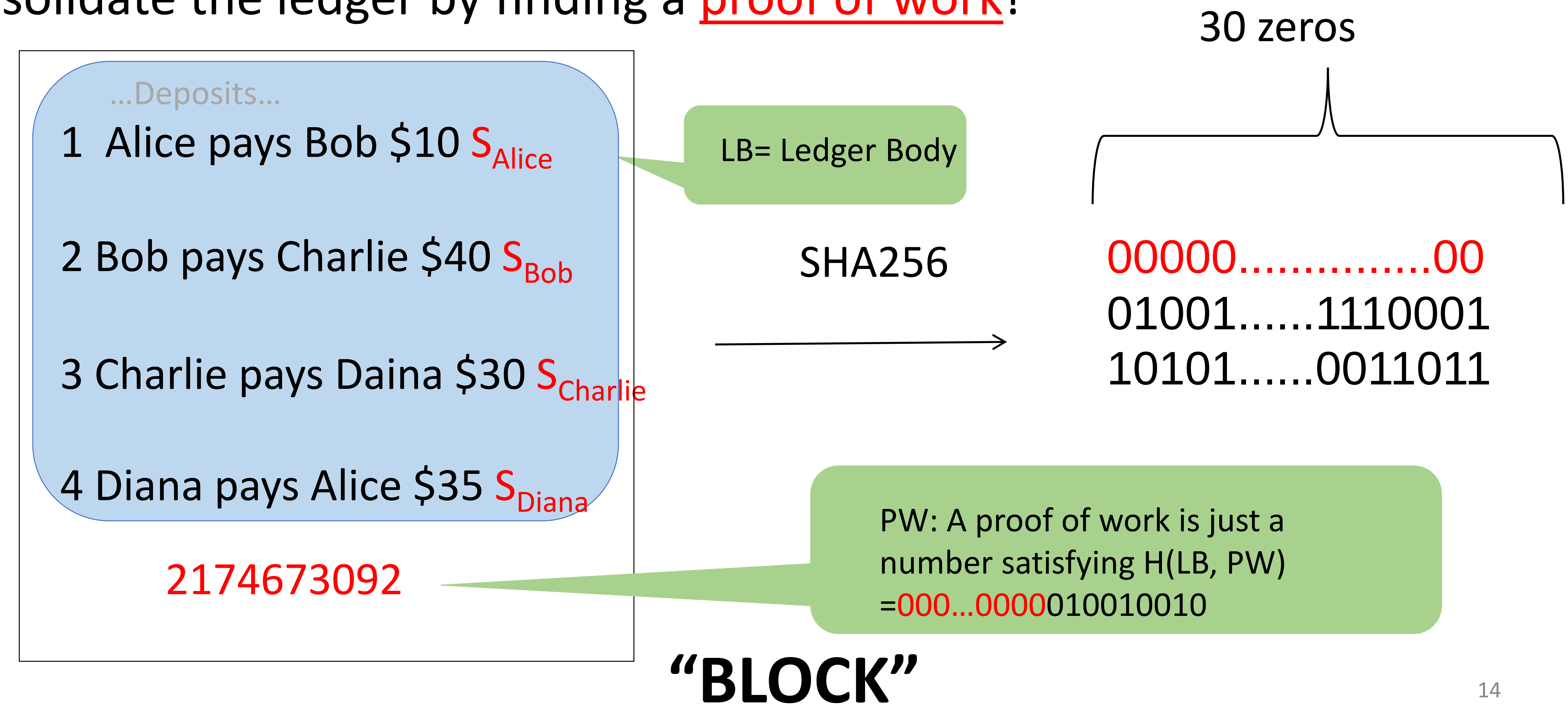


Further Problems to Solve

- But we can’t just let participants record transactions on their ledger
  - ✓The ledger should be the same for everyone.
  - ✓Someone should consolidate the transactions in the ledger but we don’t want a centralised entity to do it.
  - ✓We ask someone who is interested to put time/efforts to consolidate the transactions.
  - ✓That person is called a “Miner”.
  - ✓He/She will perform the task by finding a “proof of work”.

Proof of Work

- Cosolidate the ledger by finding a proof of work!



30 zeros

…Deposits…

1 Alice pays Bob \$10 S_{Alice}

2 Bob pays Charlie \$40 S_{Bob}

3 Charlie pays Daina \$30 $S_{Charlie}$

4 Diana pays Alice \$35 S_{Diana}

2174673092

LB= Ledger Body

SHA256

00000…………….00
01001……1110001
10101……0011011

PW: A proof of work is just a number satisfying H(LB, PW) =000…0000010010010

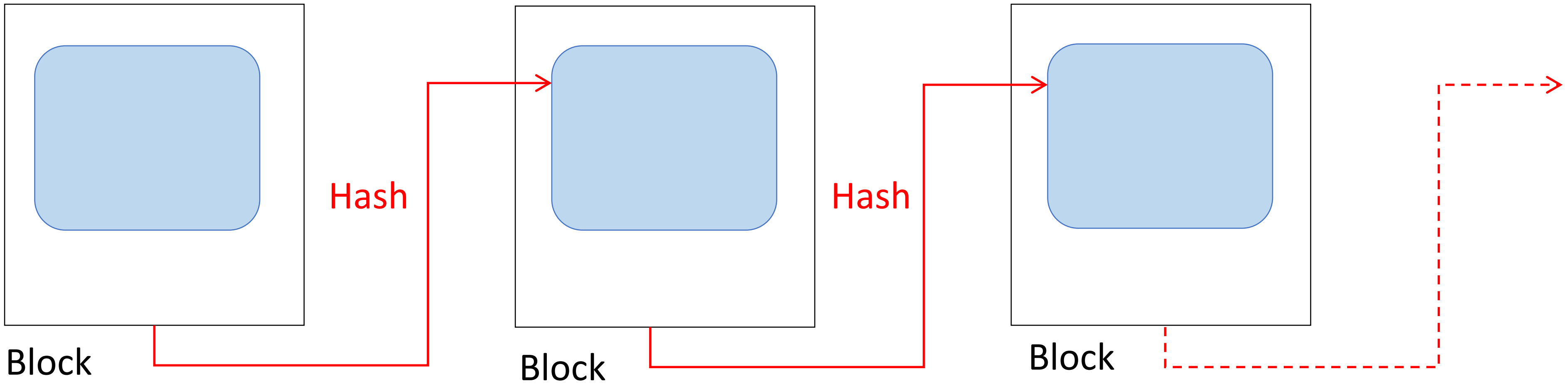
“BLOCK”

Proof of Work

- Is it hard to find such number?
  - ✓Yes but not impossible.
  - ✓If a Miner needs 30 leading zeros, he/she will have to try 2^{30} numbers on average assuming that hash output is random.
  - ✓ Have you seen a person running the bunch of computers for “mining”?
- Why does the Miner do it?
  - ✓To get financial reward: Miners have to compete against each other to find a proof of work for a block of up to 2400 transactions <u>every 10 minutes.</u>
  - ✓In Bitcoin, a proof of work is called a “<u>Nonce</u>”

Blockchain

- Chaining: We need to record the history of transactions consistently (No missing transactions/modifications..etc.): To achieve this, we have *not only* the ledger body *but also* the previous block



Blockchain

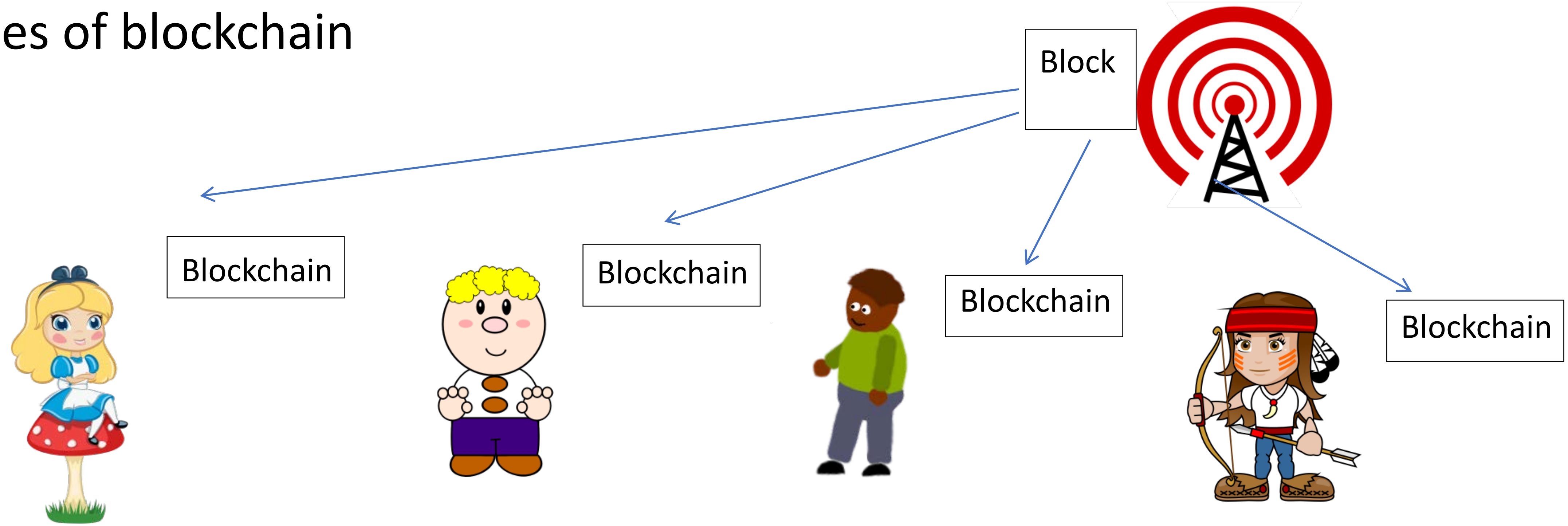
- A constantly growing ledger that keeps a permanent record of all the transactions that have taken place, in a secure chronological and immutable way.

Miners’ Job (Summary)

- Listening for transactions and creating blocks
- Broadcasting those blocks
- Getting rewarded with money (cryptocurrency)

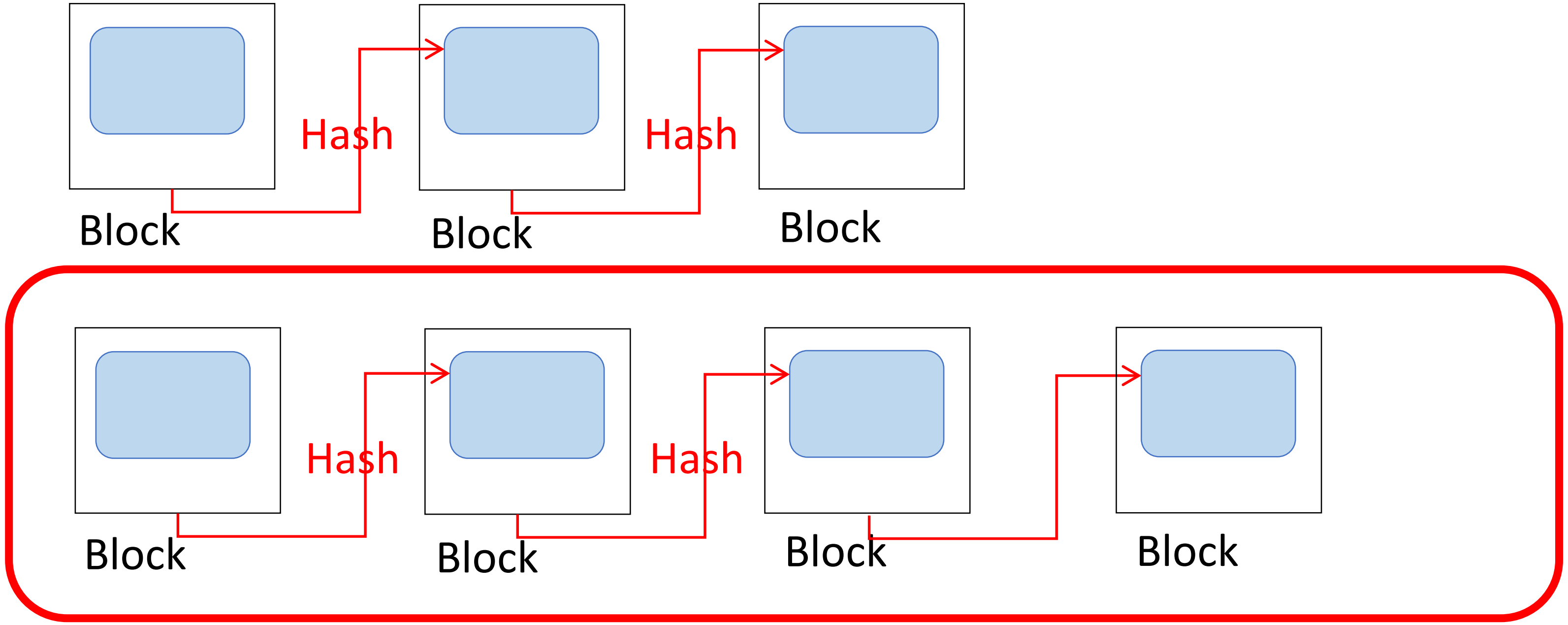
Users’ Job (Summary)

- Just listening for broadcast blocks from miners and update their own copies of blockchain



An Important Blockchain Rule

- If there are two distinct blockchains with possibly conflicting transaction histories, always accept the longest one.



Fooling Blockchain (?)

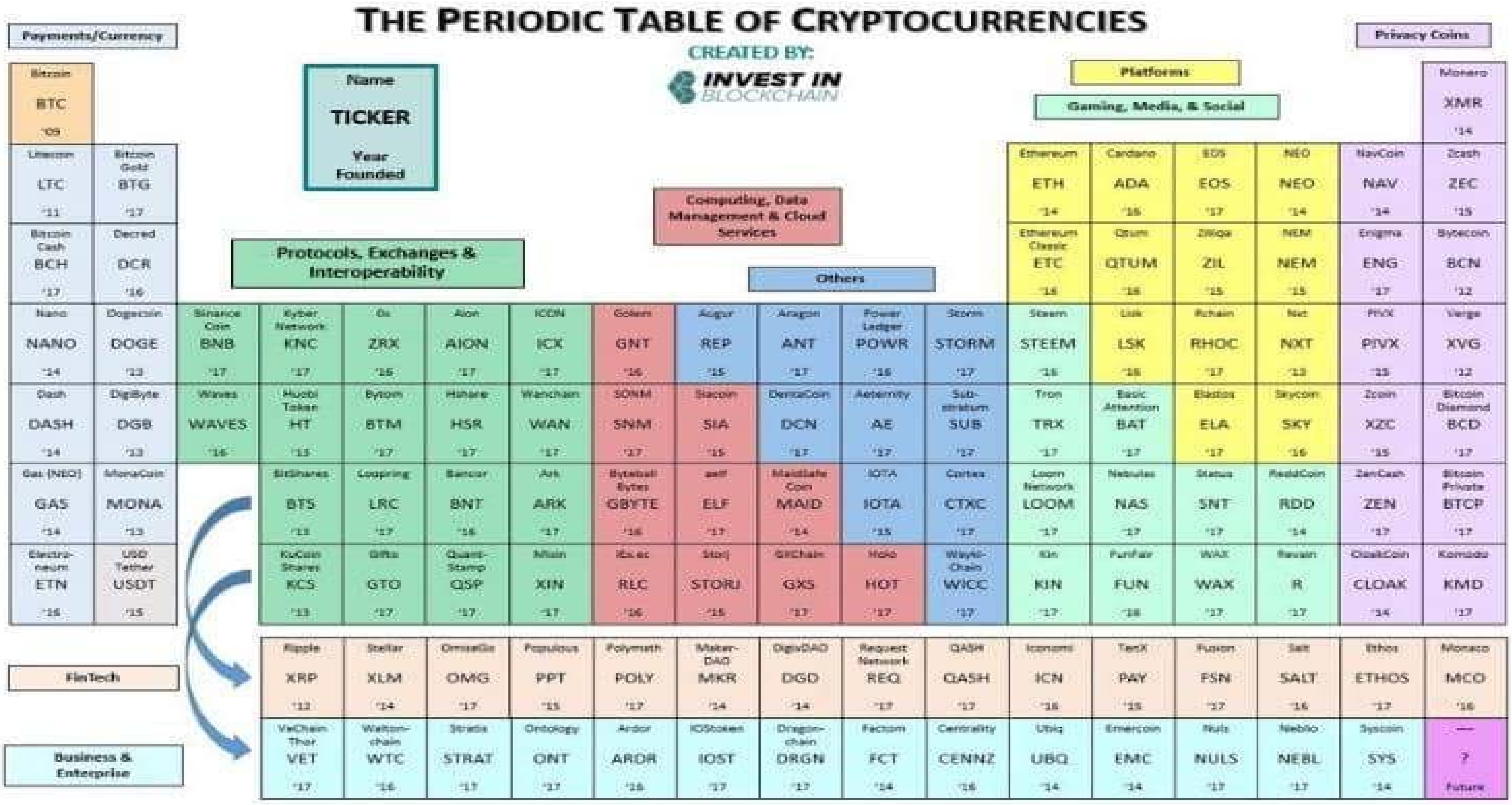
- Scenario: Alice tries to fool Bob with a fraudulent block, which does not have a proof of work from the Miner.
  - ➢Alice could get a proof of work herself.
  - ➢But the problem is Alice needs to work out all the proofs of work after this (fraudulent) block.
  - ➢Bob still receives another blocks from other Miners. If the resulting blockchain is longer, he should accept it by the rule.
  - ➢Can Alice keep adding fraudulent blocks in the chain?

  The answer is no. Unless she has close to 50% of the computing resources among all the Miners, the probability becomes overwhelming that the block chain that all of the other Miners are working on grows faster than the single fraudulent blockchain that Alice is feeding to Bob.

Cryptocurrency

- Now drop $ sign from the ledger.
- We can replace it with any cryptocurrency.
- Cryptocurrency is being created as a reward for mining, but the reward amount will reduce half every four years. → The value of currency is maintained.
- Future of cryptocurrency? <u>I don’t know.</u>

The Periodic Table of Cryptocurrencies



THE PERIODIC TABLE OF CRYPTOCURRENCIES

CREATED BY:

INVEST IN BLOCKCHAIN

Payments/Currency

Name
TICKER
Year Founded

Protocols, Exchanges & Interoperability

Computing, Data Management & Cloud Services

Others

Platforms

Gaming, Media, & Social

Privacy Coins

FinTech

Business & Enterprise

Bitcoin BTC '09																	Monero XMR '14
Litecoin LTC '11	Bitcoin Gold BTG '17											Ethereum ETH '14	Cardano ADA '15	EOS EOS '17	NEO NEO '14	NavCoin NAV '14	Zcash ZEC '15
Bitcoin Cash BCH '17	Decred DCR '16											Ethereum Classic ETC '16	Qtum QTUM '16	Zilliqa ZIL '15	NEM NEM '15	Enigma ENG '17	Bytecoin BCN '12
Nano NANO '14	Dogecoin DOGE '13	Binance Coin BNB '17	Kyber Network KNC '17	0x ZRX '16	Aion AION '17	ICON ICX '17	Golem GNT '16	Augur REP '15	Aragon ANT '17	Power Ledger POWR '16	Storm STORM '17	Steem STEEM '16	Lisk LSK '16	Rchain RHOC '17	Nxt NXT '13	PIVX PIVX '15	Verge XVG '12
Dash DASH '14	DigiByte DGB '13	Waves WAVES '16	Huobi Token HT '13	Bytom BTM '17	Hshare HSR '17	Wanchain WAN '17	SONM SNM '17	Siacoin SIA '15	DentaCoin DCN '17	Aeternity AE '17	Sub-stratum SUB '17	Tron TRX '17	Basic Attention BAT '17	Elastos ELA '17	Skycoin SKY '16	Zcoin XZC '15	Bitcoin Diamond BCD '17
Gas (NEO) GAS '14	MonaCoin MONA '13		BitShares BTS '13	Loopring LRC '17	Bancor BNT '16	Ark ARK '17	Byteball Bytes GBYTE '16	aelf ELF '17	MaidSafe Coin MAID '14	IOTA IOTA '15	Cortex CTXC '17	Loom Network LOOM '17	Nebulas NAS '17	Status SNT '17	ReddCoin RDD '14	ZenCash ZEN '17	Bitcoin Private BTCP '17
Electro-neum ETN '16	USD Tether USDT '15		KuCoin Shares KCS '13	Gifto GTO '17	Quant-Stamp QSP '17	Mixin XIN '17	iExec RLC '16	Storj STORJ '15	GXChain GXS '17	Holo HOT '17	Wayki-Chain WICC '17	Kin KIN '17	FunFair FUN '16	WAX WAX '17	Revain R '17	CloakCoin CLOAK '14	Komodo KMD '17
			Ripple XRP '12	Stellar XLM '14	OmiseGo OMG '17	Populous PPT '15	Polymath POLY '17	Maker-DAO MKR '14	DigixDAO DGD '14	Request Network REQ '17	QASH QASH '17	Iconomi ICN '16	TenX PAY '15	Fusion FSN '17	Salt SALT '16	Ethos ETHOS '17	Monaco MCO '16
			VeChain Thor VET '17	Walton-chain WTC '16	Stratis STRAT '17	Ontology ONT '17	Ardor ARDR '16	IOStoken IOST '17	Dragon-chain DRGN '17	Factom FCT '14	Centrality CENNZ '16	Ubiq UBQ '14	Emercoin EMC '14	Nuls NULS '17	Neblio NEBL '17	Syscoin SYS '14	— ? Future