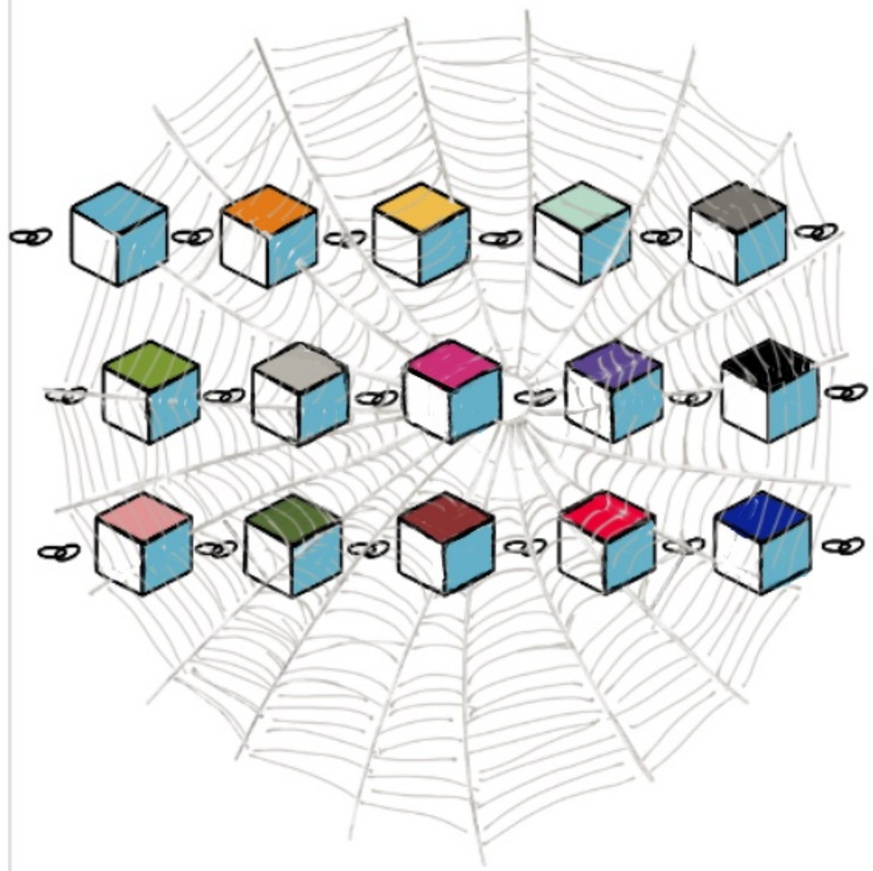


WEB 3

By

Aidanjali Venkatramanan

SCOPE

BACKGROUND & INTRODUCTION

- WEB 1 & WEB 2
- WEB 3 CONCEPTS
- DECENTRALISATION
- CENSORSHIP

MECHANICS OF WEB 3

- BLOCKCHAIN
- GAME THEORY
- ENCRYPTION
- VALUE EXCHANGE

CURRENCY

- MONEY
- CRYPTOCURRENCY
- EXCHANGES

BITCOIN

- TRANSACTIONS
- MINING
- CONSENSUS
- REWARDS & FEES
- ATTACKS, COSTS, COMPLEXITY

QUICK COMPARISON

- BITCOIN AND ETHEREUM

BUILDING THE WEB 3 ECOSYSTEM

- SMART CONTRACTS
- BLOCKCHAIN TRILEMMA
- LAYERS & DAPPS
- TOKENS

BLOCKCHAIN & ECONOMICS

- PROBLEMS FOR THE TOOL
- ECONOMICS OF BLOCKCHAIN
- IMPACT ON INCUMBENTS
- PERMISSIONED / PERMISSIONLESS
- WHY IS IT COMPELLING ?
- WHERE DOES IT FAIL ?
- CHALLENGES OF OWNING CRYPTO
- ADOPTION CHALLENGES
- FOCUS OF WEB 3
- THE COST OF TRUST

+ UNANSWERED QUESTIONS

REFERENCES

BACKGROUND

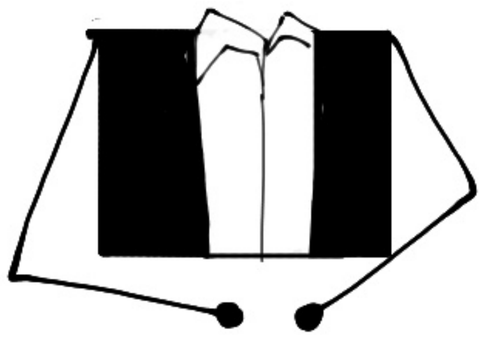
THE WEB

WEB : NOT THE SAME AS INTERNET

HYPERTEXT + TCP + DNS = WWW



THIS IS FOR EVERYONE



TIM BERNERS-LEE

KNOWN AS THE INVENTOR OF THE WEB

CONTRACT FOR THE WEB

TIM BERNERS-LEE CALLS FOR COMMITMENT

TO SAFEGUARDING THE FUTURE OF THE WEB

https://contractfortheweb.org

GOVERNMENTS

INTERNET

FOR EVERYONE

INTERNET

ALWAYS AVAILABLE

RESPECT

PRIVACY & RIGHTS

COMPANIES

ACCESSIBLE &

AFFORDABLE INTERNET

PROTECT

PRIVACY & DATA

BUILD

TRUST

TECHNOLOGY PROMOTES

BEST OF HUMANITY

CITIZENS

CREATE &

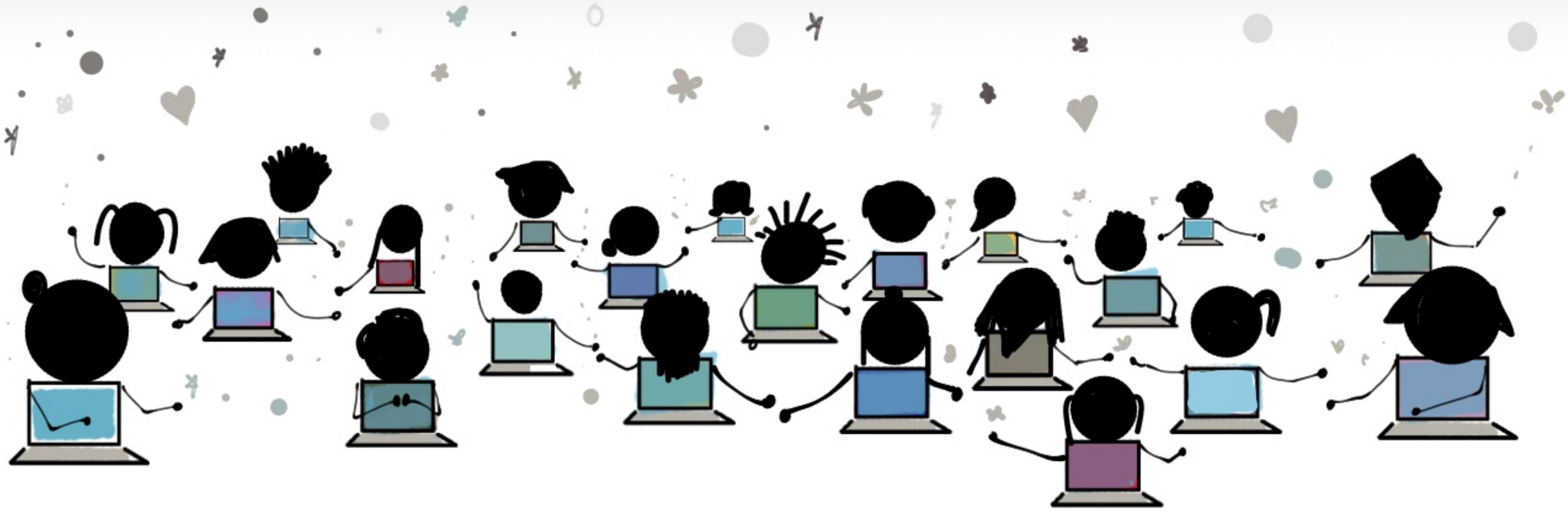
COLLABORATE

RESPECT CIVIL

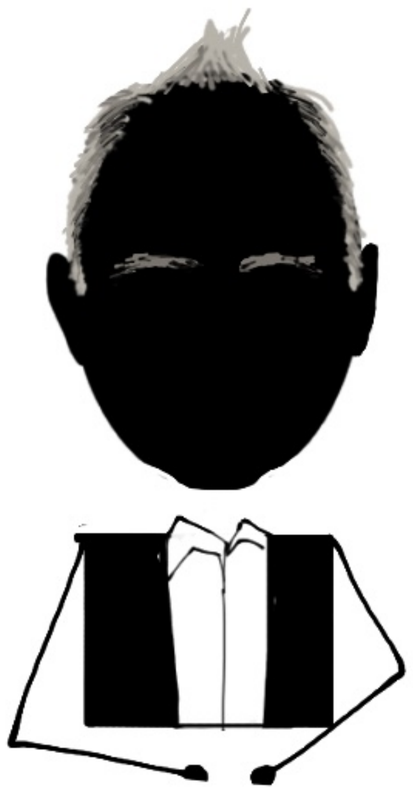
DISCOURSE

FIGHT FOR

THE WEB



WHAT HELPED THE INTERNET GROW



w3.org/DesignIssues/Principles.html

DECENTRALISATION & TOLERANCE

ARE THE LIFE-BREATH OF THE INTERNET

NON-PROPRIETARY

COMMUNICATION

PROTOCOLS



APPLICATION LAYER (HTTP)

TRANSPORT LAYER (TCP)

NETWORK LAYER (IP)

DATA LINK LAYER

HARDWARE

CABLE



APPLICATION LAYER (HTTP)

TRANSPORT LAYER (TCP)

NETWORK LAYER (IP)

DATA LINK LAYER

HARDWARE

TO JOIN THE INTERNET,

READ THE STANDARDS

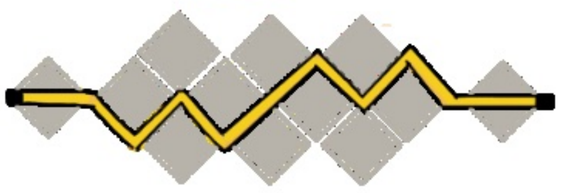
FOR THESE PROTOCOLS

AND MAKE SURE

YOUR DEVICE FOLLOWS THEM.

NOW MAINTAINED BY

IETF



INTERNET ENGINEERING TASK FORCE

IT WAS THIS OPENNESS AND ABSENCE OF CENTRAL CONTROL THAT ALLOWED THE INTERNET TO GROW ORGANICALLY.

WEB 1.0

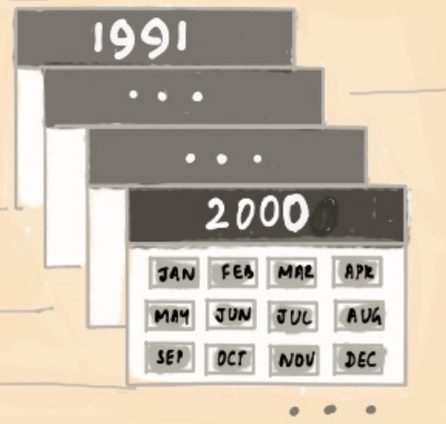
REFERS TO THE EARLY YEARS OF THE WEB : 1990s - early 2000s



RETROSPECTIVELY

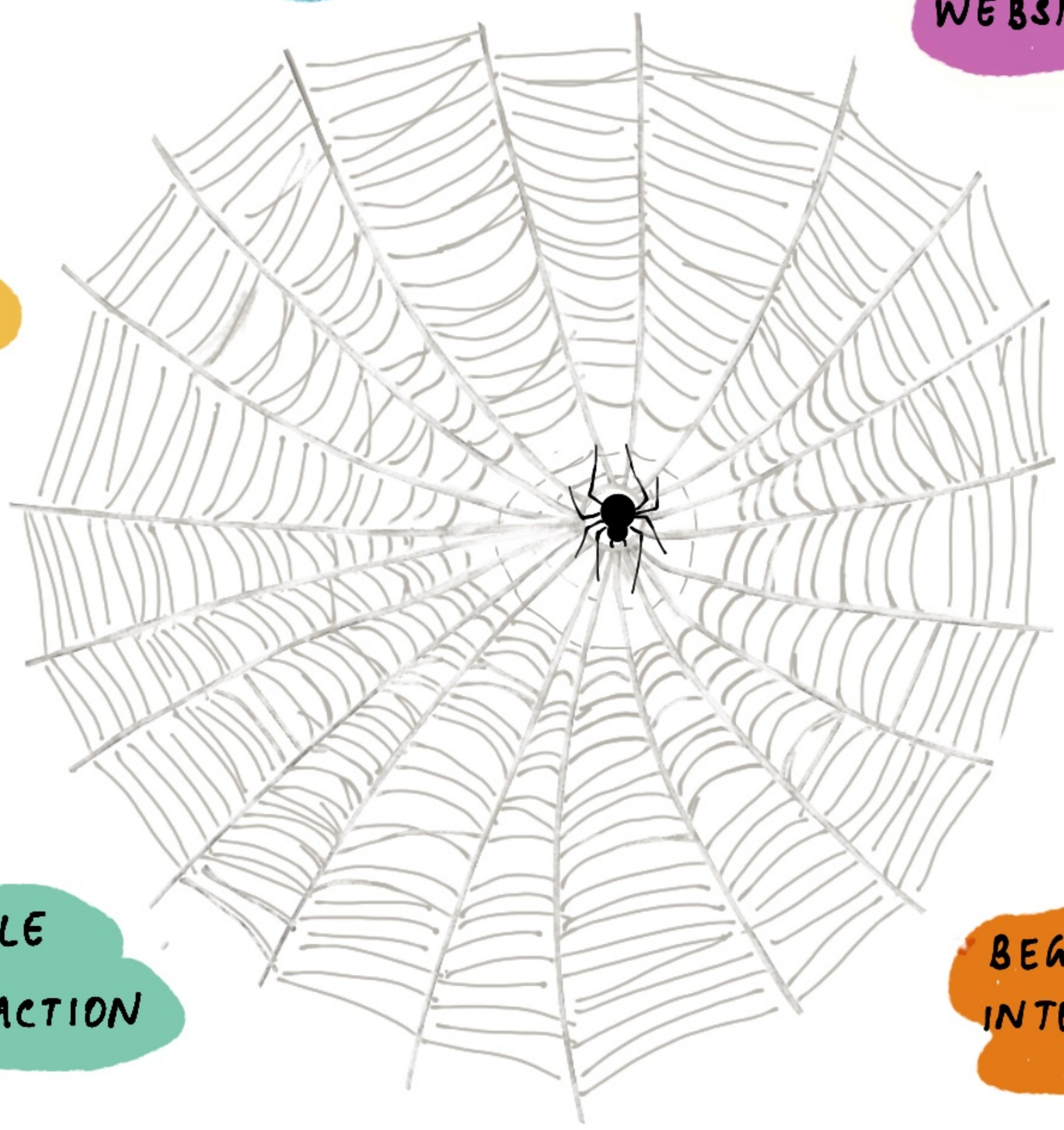
NAMED

TIME-PERIOD



DOT COM BOOM

PERSONAL WEBSITES



READ ONLY WEB

MOSTLY STATIC HTML

VERY LITTLE USER-INTERACTION

BEGINNINGS OF INTERACTIVE PAGES

AGE OF INFORMATION

WEB 2.0

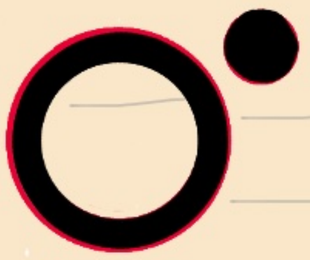
WEB 2.0 WAS A MORE INTENTIONAL NAME

USED BY



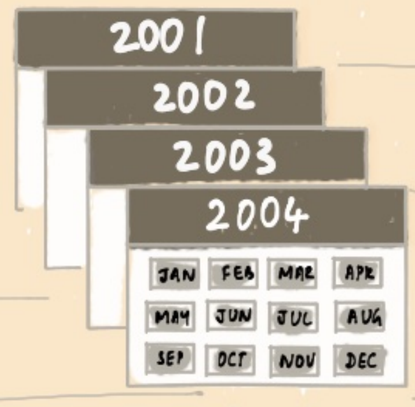
DARCY DINUCCI

MADE POPULAR BY

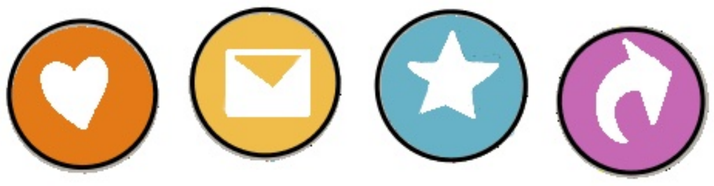


O'REILLY

TIME PERIOD



UNTIL ABOUT NOW



SOCIAL NETWORKS



DYNAMIC TAILORED CONTENT

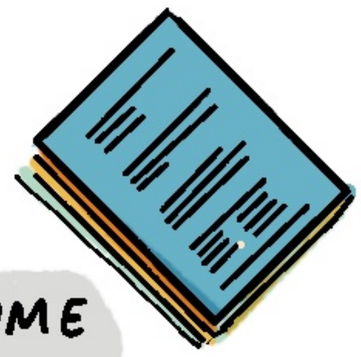


USER GENERATED CONTENT

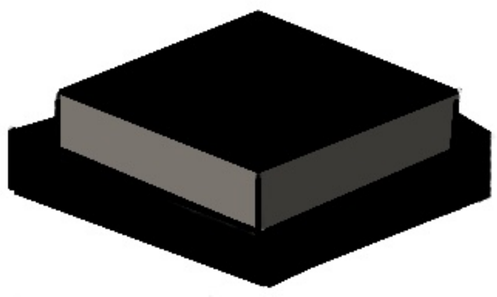




GROWTH OF E-COMMERCE



SOME GOVERNMENT REGULATION



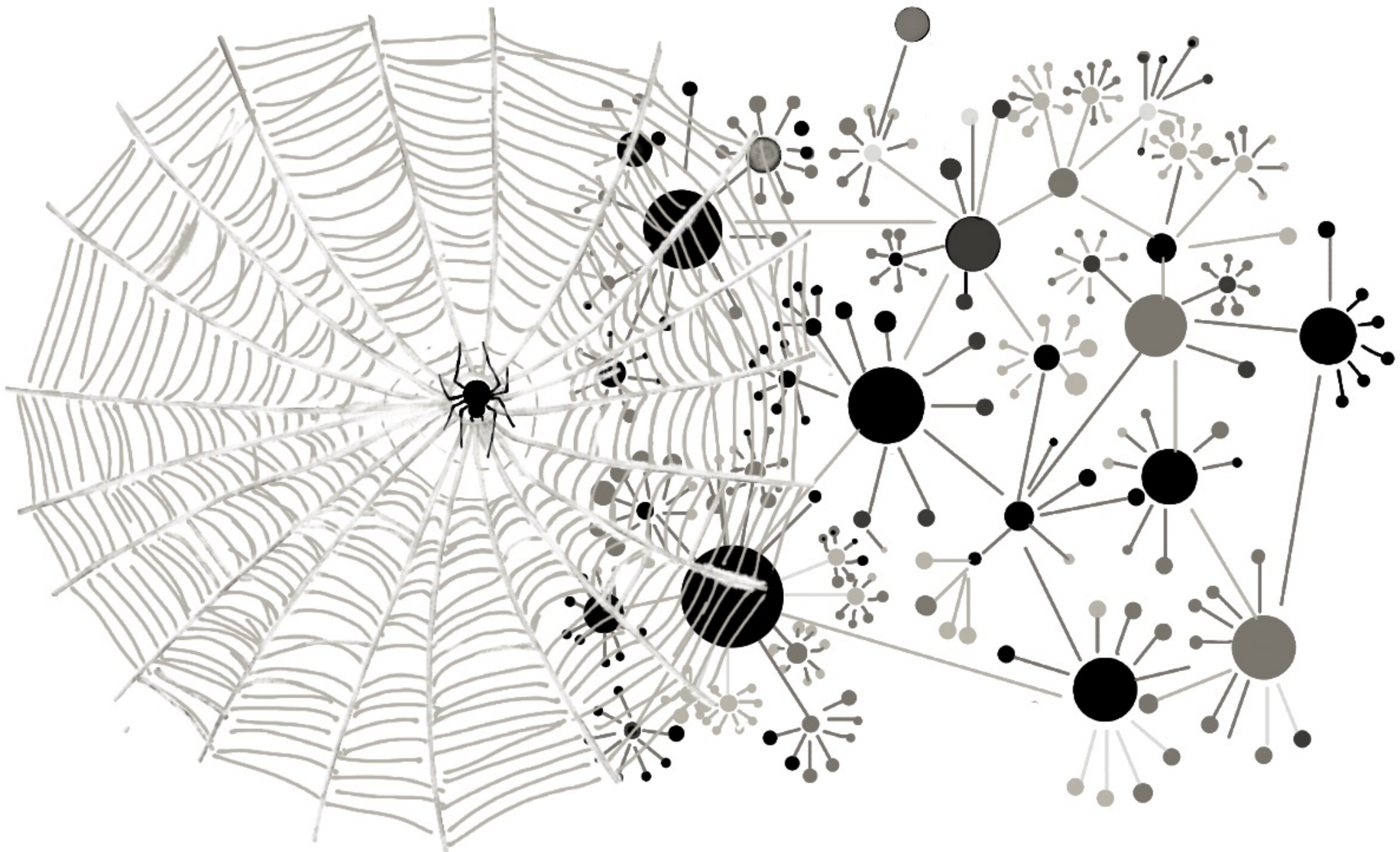
AGE OF PLATFORMS



MONETISATION OF CONTENT

A WORD OF CAUTION

THERE ARE NO CLEAR, UNANIMOUS DEFINITIONS OF WEB 1 OR WEB 2



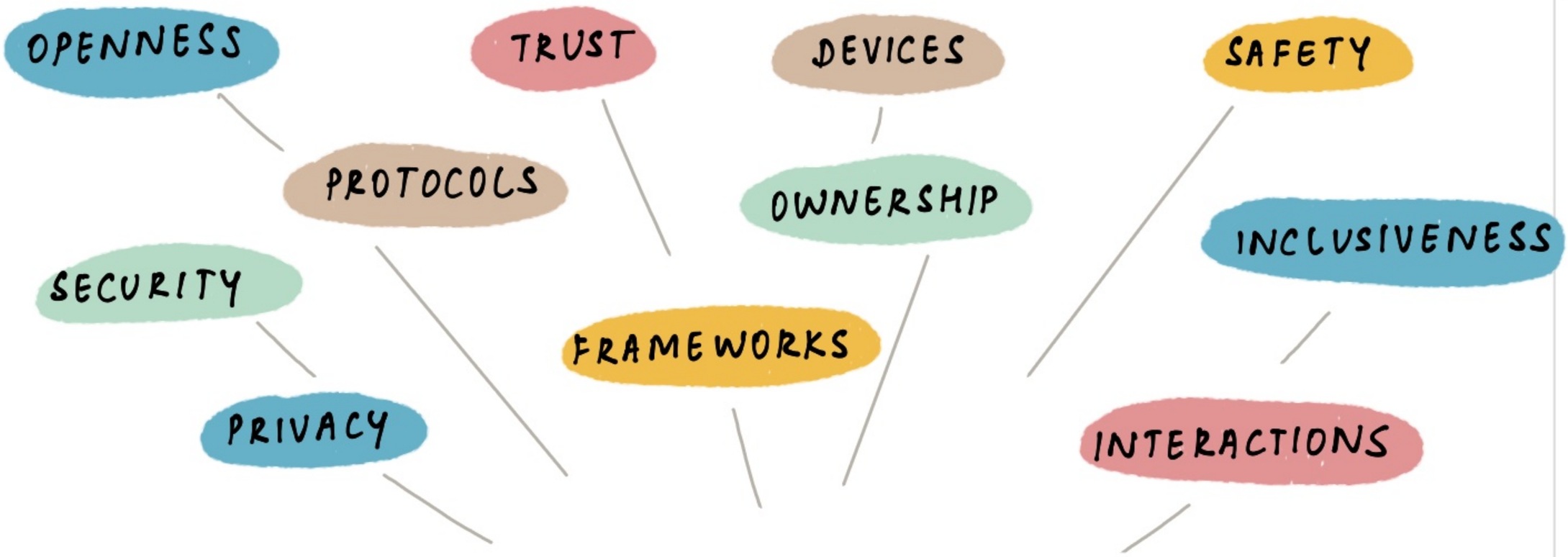
THE BOUNDARIES BETWEEN THEM ARE ALSO FAIRLY BLURRY

FOR EXAMPLE, NATIVE APPS MOVING TO BEING WEB BASED POSSIBLY ENCOURAGED ONLINE SHOPPING.

THE DEFINITIONS ARE LOOSE AND NEED TO BE TREATED AS SUCH

THE NEXT VERSION ?

RETHINK AND QUESTION EVERYTHING



TWO IDEAS HAVE EMERGED IN THE QUEST FOR WHAT COMES NEXT AS THE FUTURE VERSION OF THE WEB.

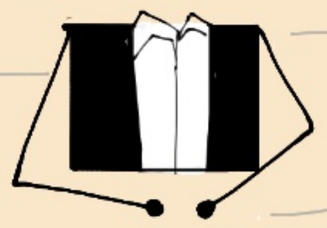
ONE IDEA IS:

WEB 3.0

ACTIONABLE INFORMATION



Semantic web

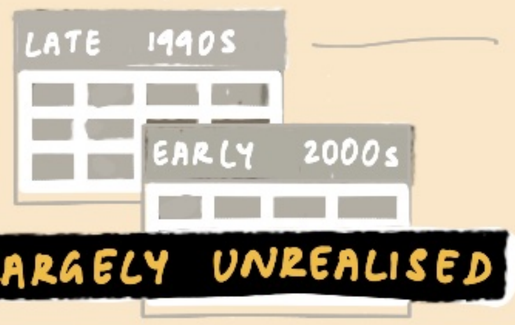


TIM BERNERS-LEE

WEB 3.0

- ALL INTERNET DATA IS STRUCTURED AND MACHINE READABLE
- MAY AUTOMATE PHYSICAL WORLD

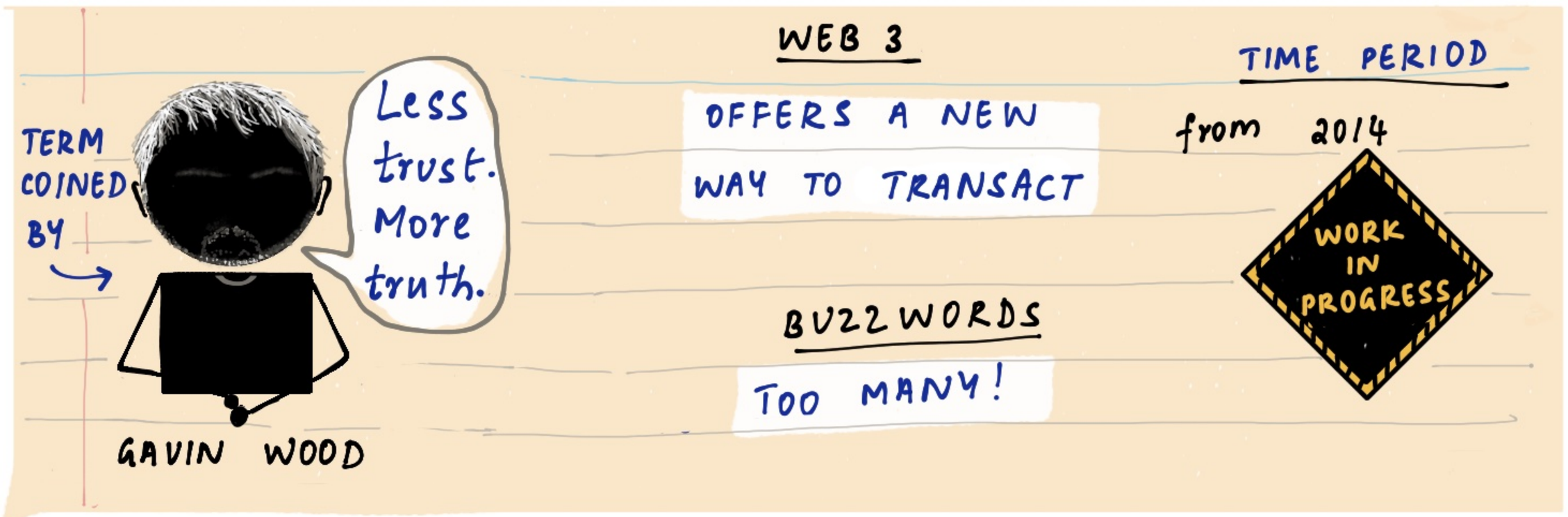
TIME PERIOD



THE OTHER IDEA IS:

WEB 3

TOKEN-BASED ECONOMICS AND MORE



INTRODUCTION

IT IS THIS SECOND VIEW OF THE FUTURE WEB WHICH IS THE SUBJECT OF THIS BOOK

WEB3 IS A POLARISING TOPIC.

THERE ARE DISAGREEMENTS ON DEFINITION AND SCOPE. THERE ARE FINANCIAL FRAUDS AND SCAMS. THERE ARE ENERGY COSTS. THERE IS A LOT OF RESEARCH AND BILLIONS IN INVESTMENT.

NO WONDER THEN THAT WEB3 EVOKES STRONG REACTIONS FROM SUPPORTERS AND CRITICS.

WEB3's CORE VALUE IS DECENTRALISATION. ITS UNDERLYING TECHNOLOGY IS CONSTRUCTED WITH MATHEMATICS AND ECONOMICS.

AS WITH ANY OTHER TECHNOLOGY, WEB3 COMES WITH ITS OWN SET OF JARGON AND BREATHLESS PROMISES.

THIS BOOK WILL TAKE YOU THROUGH SOME OF THE COMPLEX HISTORY AND BEGINNINGS. IT WILL TAKE A FAIRLY DETAILED TECHNICAL TOUR OF THE MECHANICS. IT WILL ALSO HELP TO SEE PAST THE HYPE AND DISCOVER THE LIMITATIONS.

MOST IMPORTANTLY, I HOPE THAT IT WILL HELP YOU BE PART OF CONVERSATIONS AND FIND THE RIGHT QUESTIONS TO ASK

WEB 3 CONCEPTS

LET US START WITH THE IDEA OF WEB3 AS DESCRIBED BY GAVIN WOOD AND THE INVESTORS, TECH COMPANIES & CRYPTOCURRENCY ENTHUSIASTS TO WHO IT APPEALED



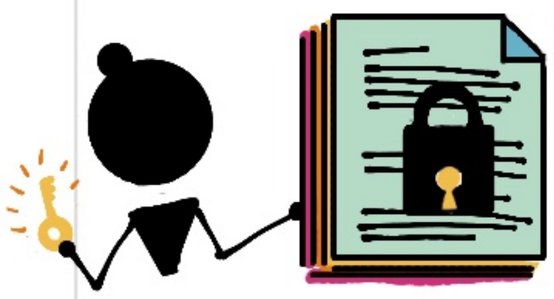
DECENTRALISED SERVERS & DATABASES



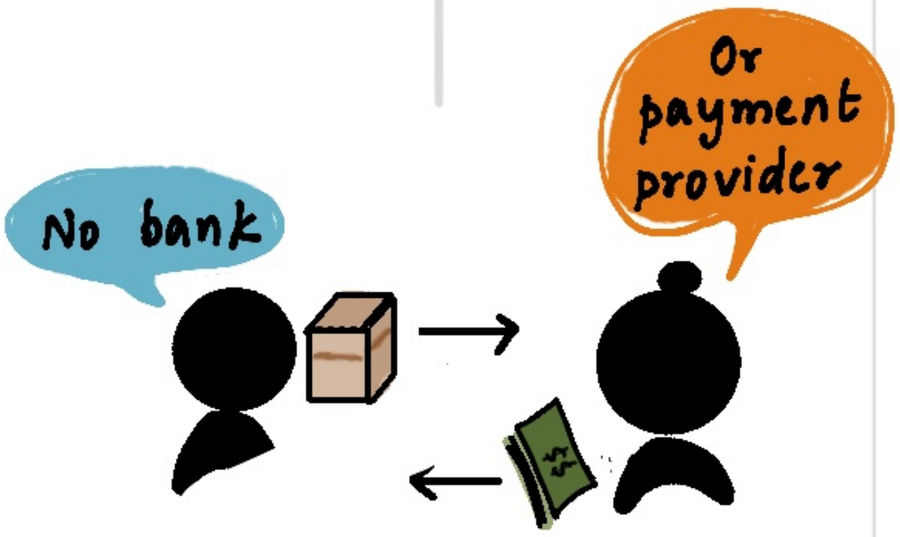
PERMISSIONLESS NETWORKS



TAMPER RESISTANT DATA



PSEUDONYMOUS IDENTITY



TRUSTLESS INTERACTIONS



OPEN SOURCE CODE

THERE IS ALSO A VIEW THAT CONCEPTS OF ARTIFICIAL INTELLIGENCE AND VIRTUAL REALITY NETWORKS LIKE METAVERSE ARE PART OF WEB3

WHAT WEB3 CLAIMS TO SOLVE

WEB 2.0 ...



WEB 2.0 RESULTS IN A HUGE AMOUNT OF DATA AND CONTENT BEING GENERATED

CONTROLLED BY A FEW



A HANDFUL OF COMPANIES OWN MOST OF THE INFRASTRUCTURE, SERVICES AND THE DATA GENERATED.

LOSS OF PRIVACY



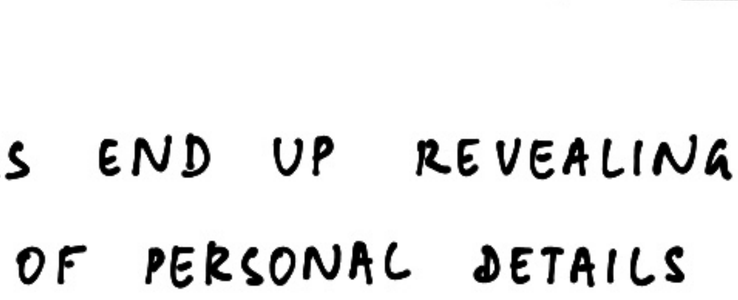
USERS END UP REVEALING A LOT OF PERSONAL DETAILS TO THESE COMPANIES

LOSS OF CONTROL



USERS HAVE LITTLE OR NO SAY IN HOW THEIR DATA IS USED OR THE TERMS OF SERVICE

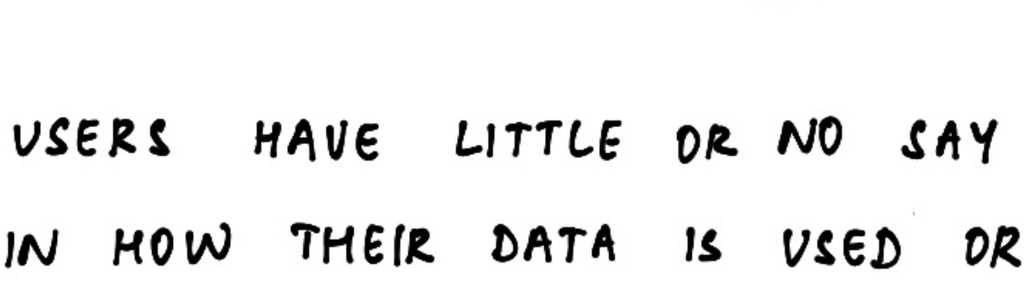
MONETISATION OF DATA



MEAWHILE, COMPANIES SELL THIS DATA TO ADVERTISERS OR CREATE FILTER BUBBLES TO ~~ENGAGE~~ USERS.

EMOTIONALLY
RETAIN

RELIANCE ON THIRD PARTY



THIRD PARTIES SUCH AS BANKS ARE REQUIRED TO TRANSACT. WHEN BANKS FAIL, THE ECONOMY SINKS.

WEB3 IDEALS

INDIVIDUAL CONTROL OF



PERSONAL DETAILS



ASSETS



CONTENT

COLLECTIVE OWNERSHIP THROUGH



HOSTING DATA/CODE

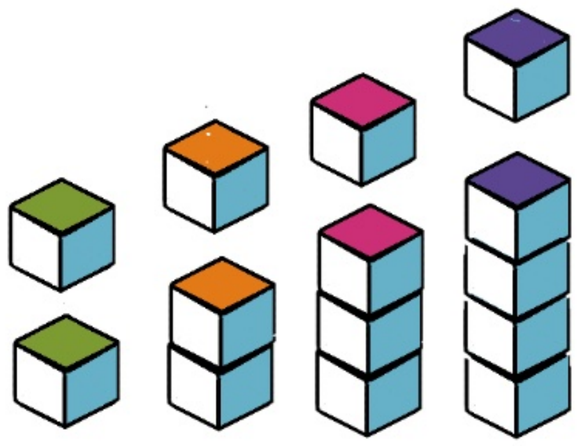


PARTICIPATION



GOVERNANCE

NEW UNDERLYING TECHNOLOGY



BLOCKCHAIN

NEW WEB3 BASED MARKETS

DECENTRALISED **FI**NANCE

NON **F**UNGIBLE **T**OKENS

DECENTRALISED **APP**LICATIONS

INITIAL **C**OIN **O**FFERINGS

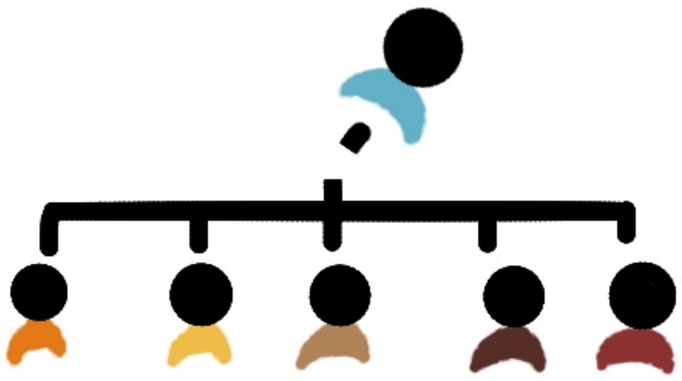
WILL A CENTRAL BODY CENSOR ME?

	INDIVIDUALS	FOR EXAMPLE: GETTING A LOAN GETTING REVIEW RATINGS
	BUSINESSES	WHEN PUBLIC POLICY/REGULATION MIGHT BE A BARRIER TO ENTRY
	CRIMINAL ENTITIES	WHEN LAW PREVENTS PEOPLE FROM DRUGS, TERRORISM, SLAVERY, PORN, MONEY LAUNDERING ETC
	VULNERABLE GROUPS	WHEN THE RIGHTS OF CERTAIN GROUPS ARE THREATENED
	CITIZENS / NATIONS	IN OPPRESSIVE REGIMES OR WHEN THE ECONOMY IS DEPRESSED

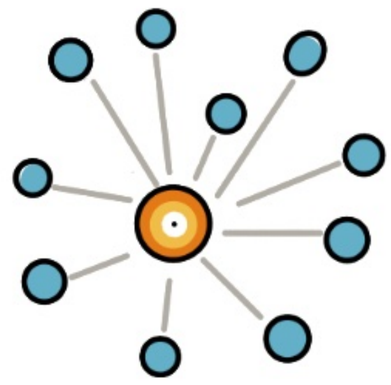
DECENTRALISATION

ADAPTED FROM INTERNET POLICY REVIEW ON DECENTRALISATION

HERE ARE SOME FACTORS THAT DRIVE DECENTRALISATION



TRANSFER OF CONTROL



NO SINGLE POINT OF FAILURE



TRANSPARENCY



RESILIENCE



RESOURCE SHARING



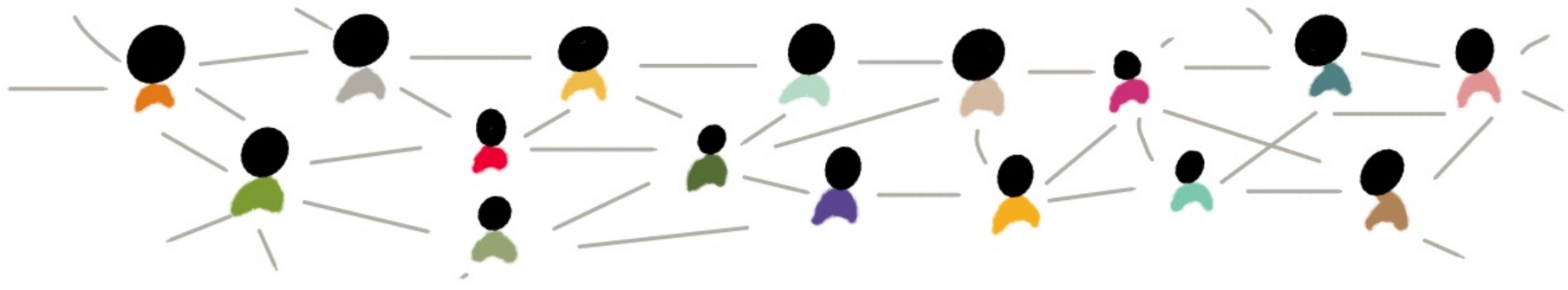
INFORMATION SECURITY

A TECHNICAL DECENTRALISATION SHARES CONCERNS WITH- BUT DOES NOT ALWAYS LEAD TO SOCIAL, POLITICAL OR ECONOMIC DECENTRALISATION. LET US LOOK AT SOME REASONS WHY.

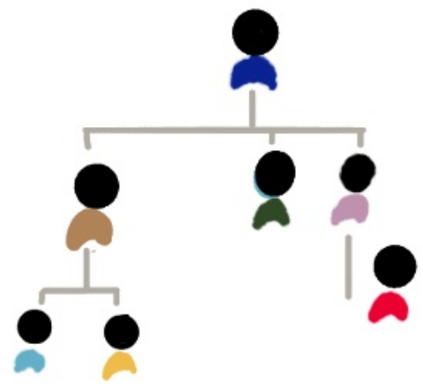
policyreview.info/concepts/decentralisation

DECENTRALISATION CHALLENGES

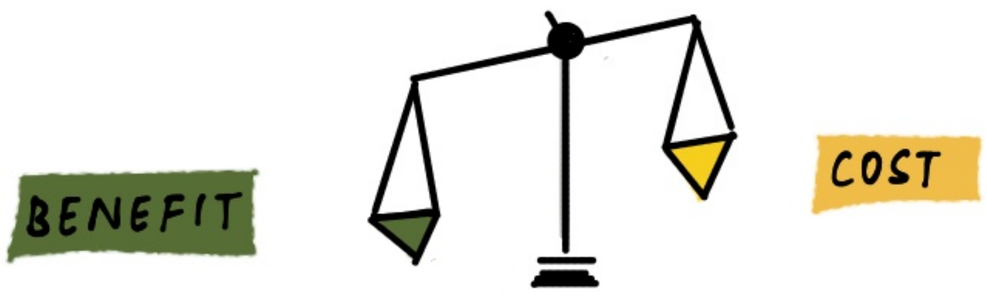
A DECENTRALISED NETWORK REQUIRES COORDINATION (GOVERNANCE) AS NO SINGLE MEMBER HAS A VIEW OF THE WHOLE SYSTEM.



A NETWORK DECENTRALISED BY DESIGN MIGHT HAVE OTHER CENTRALISING SIDE-EFFECTS SUCH AS HIDDEN HIERARCHIES



THE AIM OF A DECENTRALISED NETWORK MIGHT ONLY BE MET IF THE BENEFITS OF USING IT EXCEED ITS COSTS FOR ITS MEMBERS



A DECENTRALISED NETWORK IS MORE OPEN/ACCEPTING. THIS LEAVES IT A VICTIM TO BAD BEHAVIOURS

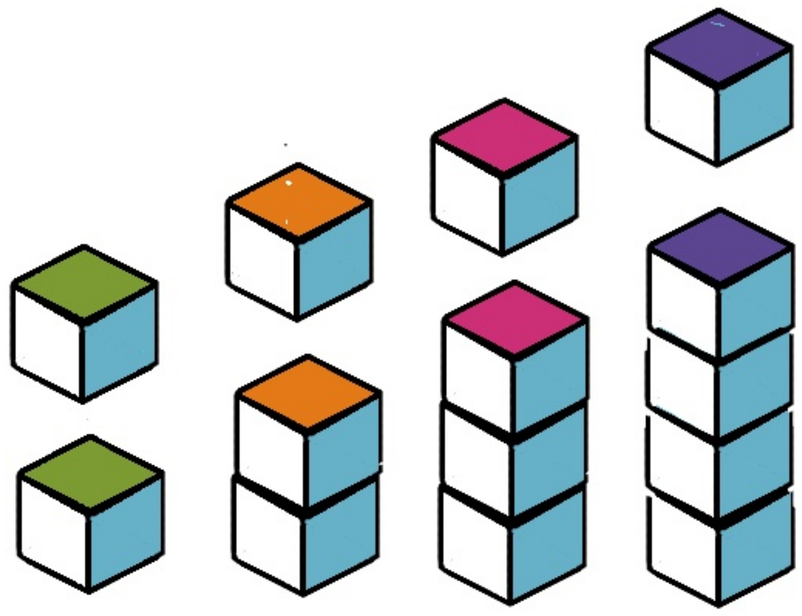


DECENTRALISATION IS

- A DESIGN PRINCIPLE
- AN AIM TOWARDS A GOAL
- A CLAIM SOMETIMES NOT FUCFICLED

MECHANICS OF WEB 3

MECHANICS OF WEB3

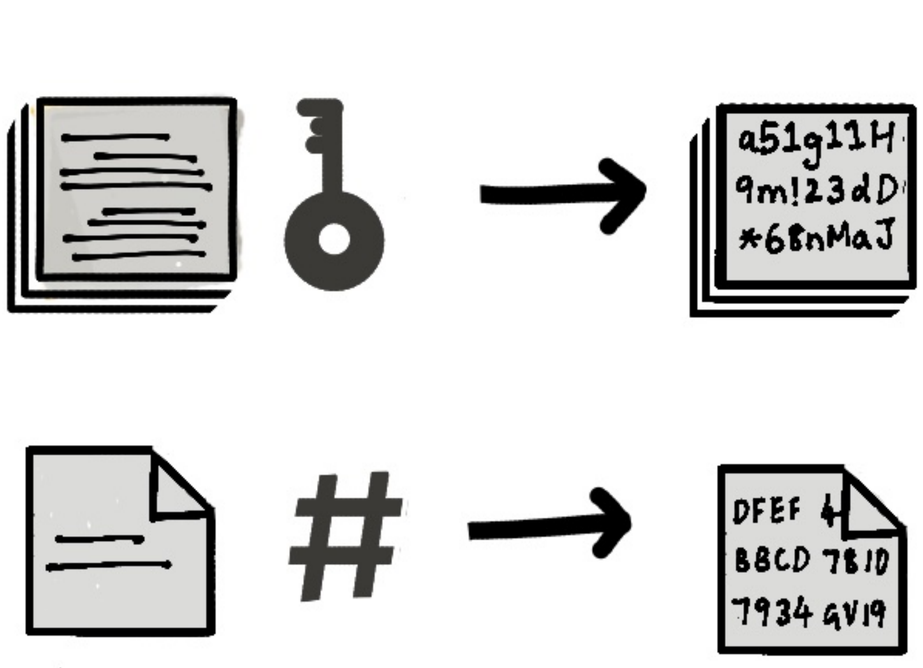


A DECENTRALISED INTERNET BASED ON BLOCKCHAIN TECHNOLOGY

SOME GAME THEORY FOR DECISION MAKING

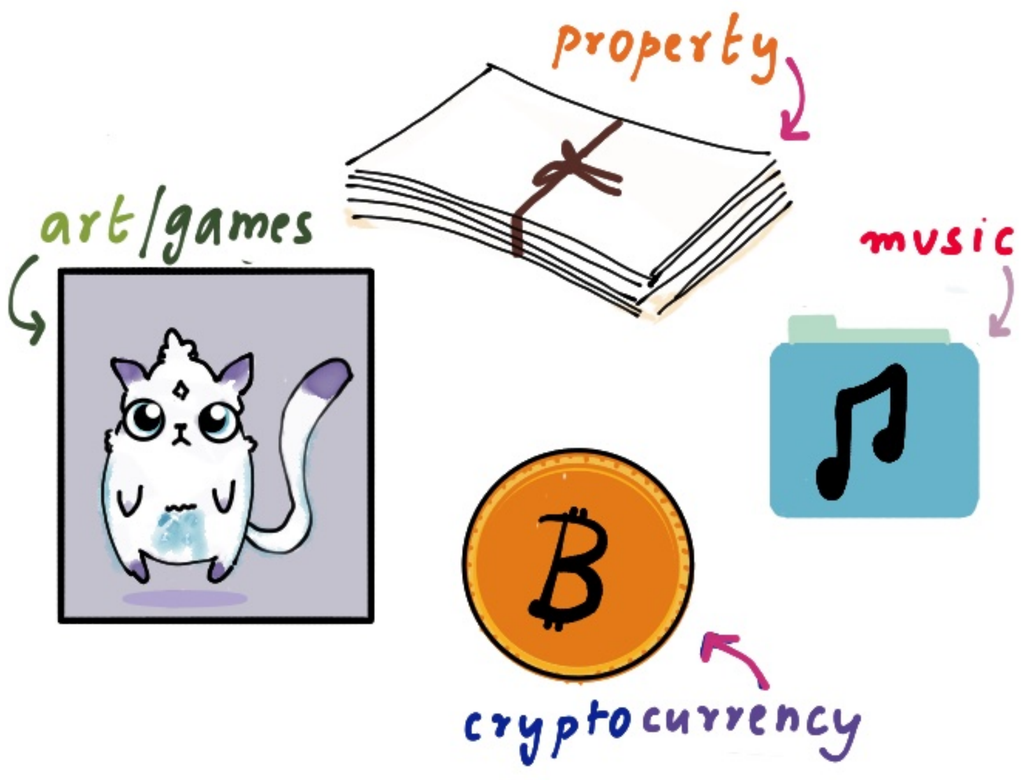
- PRISONER'S DILEMMA -

A / B	HARMS B	HELPS B
HARMS A	A LOSES B LOSES	A LOSES B WINS
HELPS A	A WINS B LOSES	A WINS B WINS



SECURITY OPERATIONS LIKE ENCRYPTION & HASHING

ENABLING PEER-TO-PEER EXCHANGE OF VALUE WITH NO INTERMEDIARY.



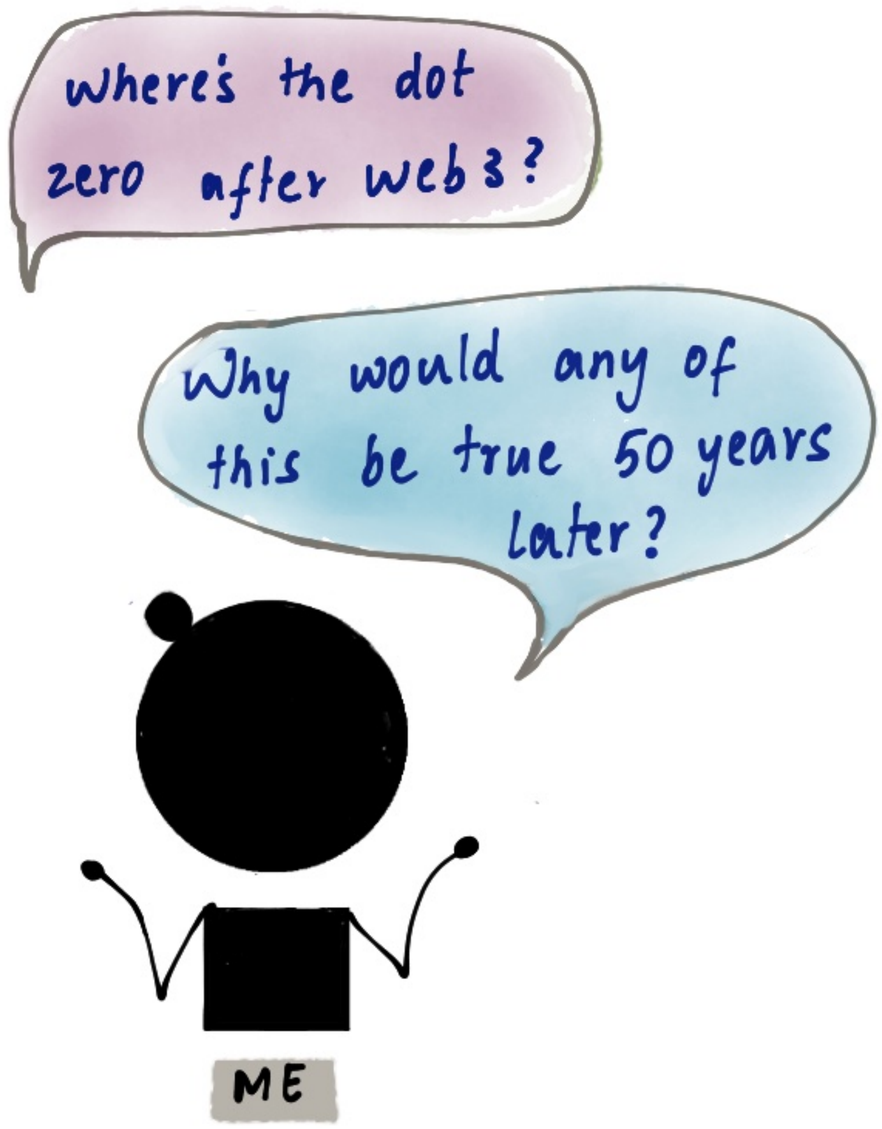
OPINIONS

ALMOST EVERYONE HAS AN OPINION ABOUT WHAT WEB3 IS AND ISN'T. IT ISN'T WELL-DEFINED OR WIDELY AGREED. HOWEVER, SOME PEOPLE DISLIKE THE VERY IDEA.

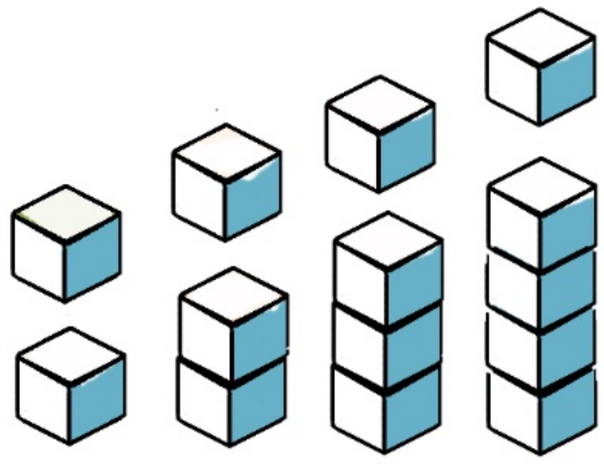
HERE ARE TWO FAMOUS EXAMPLES:







WHERE NEXT?

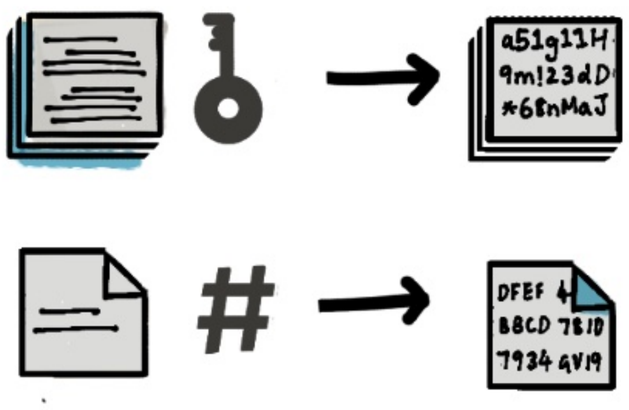


BLOCKCHAIN

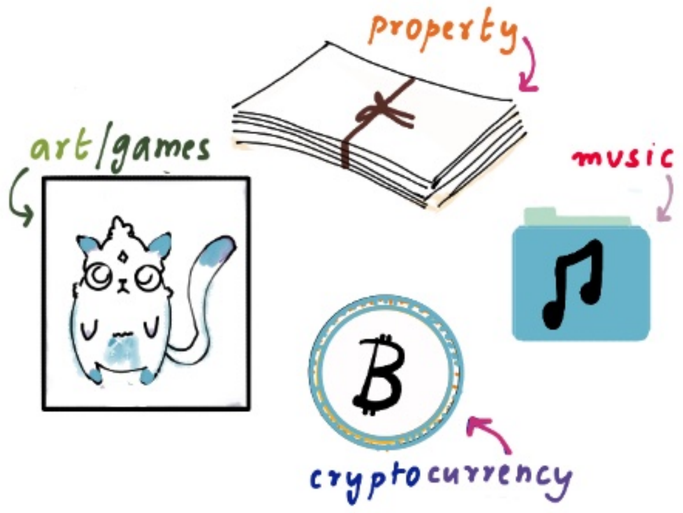
GAME THEORY

- PRISONER'S DILEMMA -

B \ A	HARMS B	HELPS B
HARMS A	A LOSES B LOSES	A LOSES B WINS
HELPS A	A WINS B LOSES	A WINS B WINS



ENCRYPTION



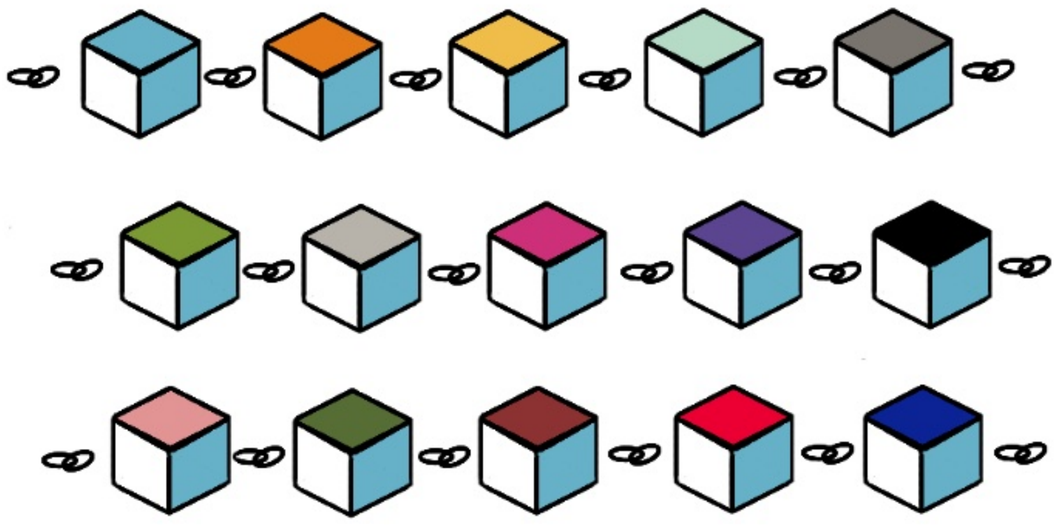
VALUE EXCHANGE

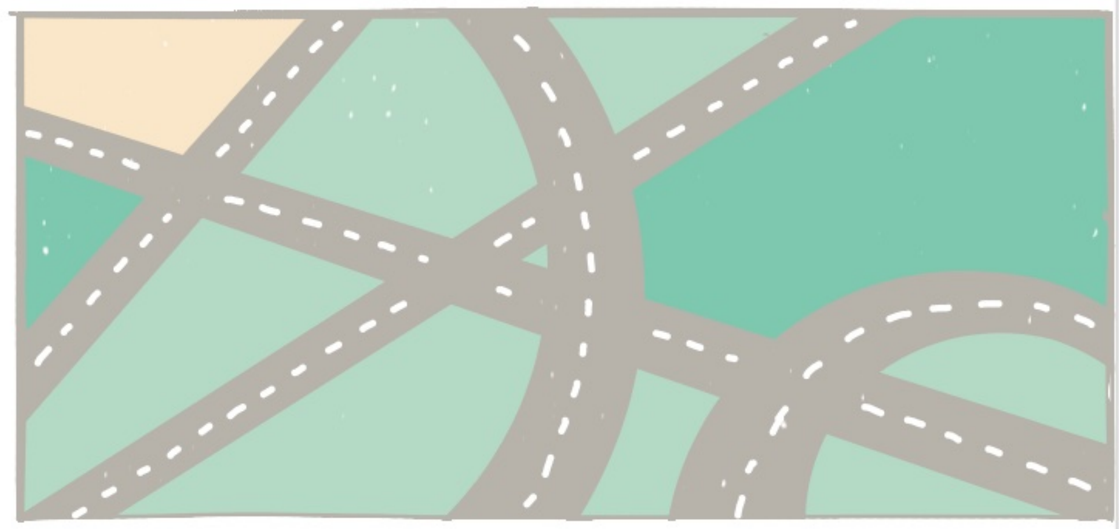
BLOCKCHAIN

DESCRIBING WHAT MANY BELIEVE TO BE THE MAIN STRUCTURAL ELEMENT OF WEB 3

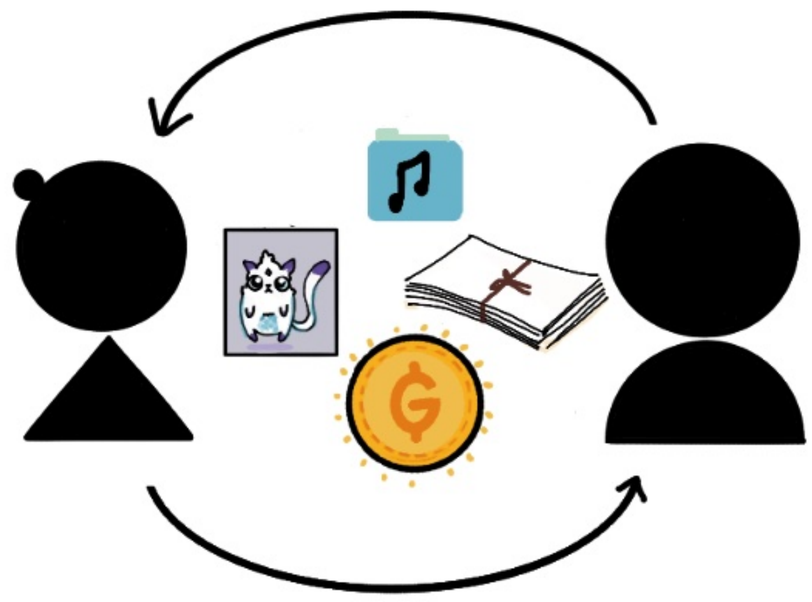
WHAT IS A BLOCKCHAIN?

A BLOCKCHAIN IS INFRASTRUCTURE





THAT ENABLES PEER-TO-PEER TRANSFER OF VALUE.





SOME EXAMPLES

ETHEREUM

HYPERLEDGER FABRIC

RIPPLE

QUORUM

R3 CORDA

BAB7 M25 G45

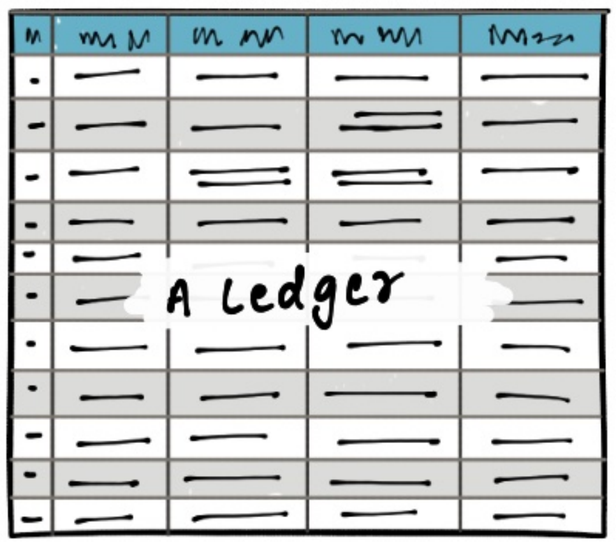
AP-1 ROUTE66 NH44

M876 G6 HWY 1

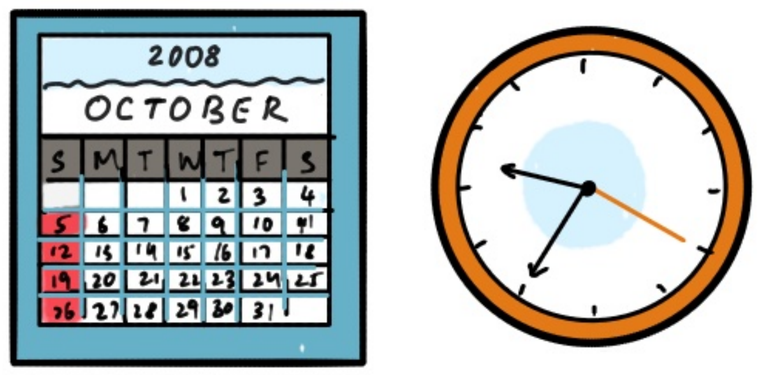
AH2 HIGHWAY7 ROUTE 1

WHAT IS A BLOCKCHAIN?

A TRANSACTION/OWNERSHIP LOG

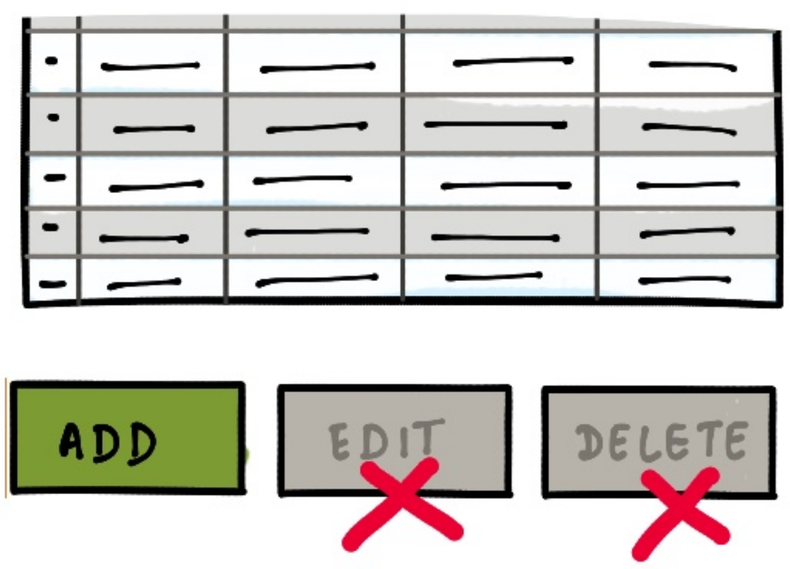


IT IS TIMESTAMPED

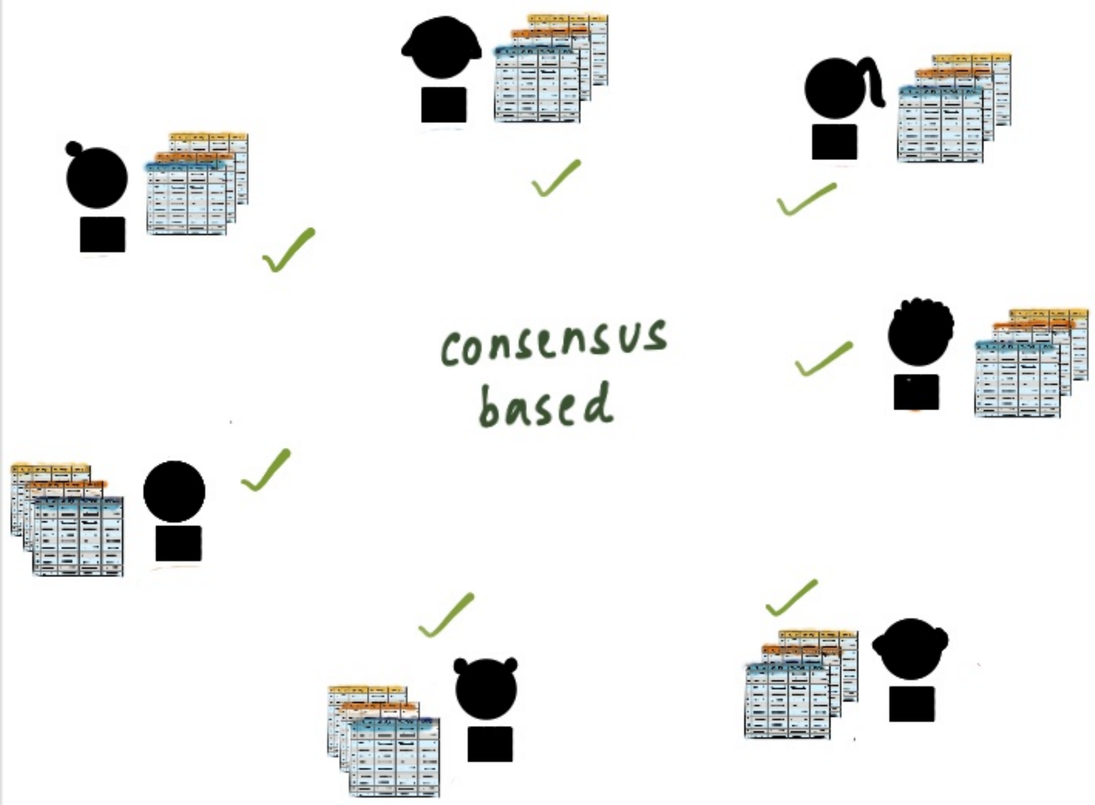


28 OCT 2008 09:35:20 AM

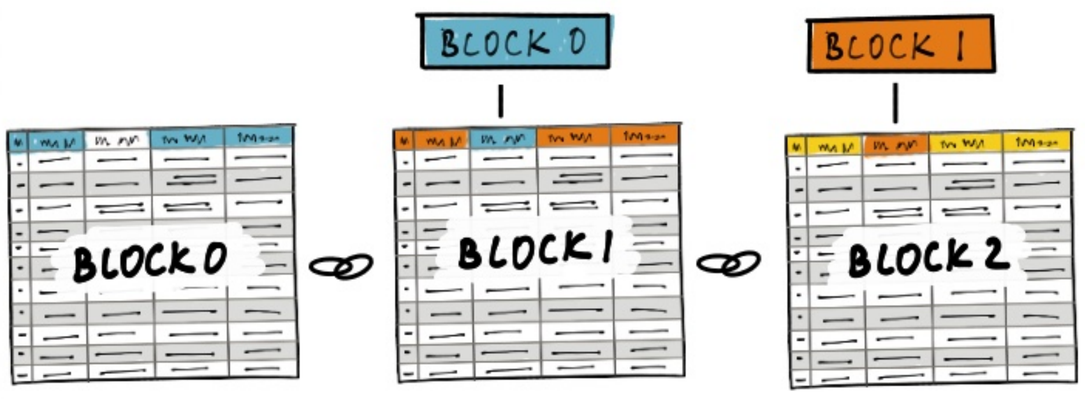
IT IS APPEND ONLY



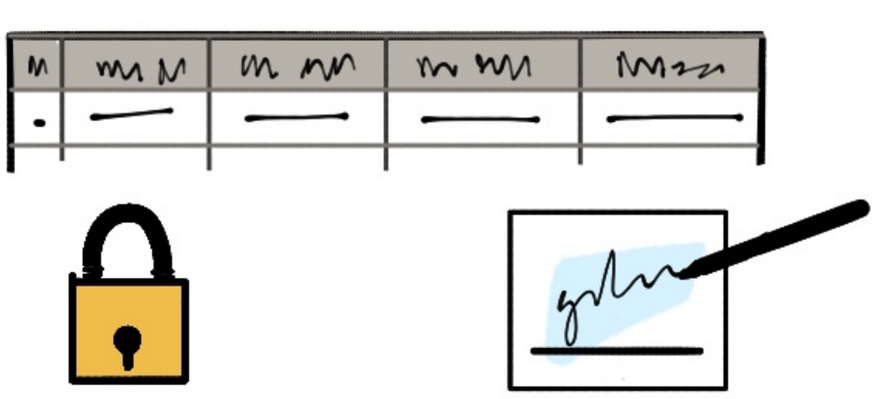
IT IS DISTRIBUTED



IT IS GROUPED AND LINKED

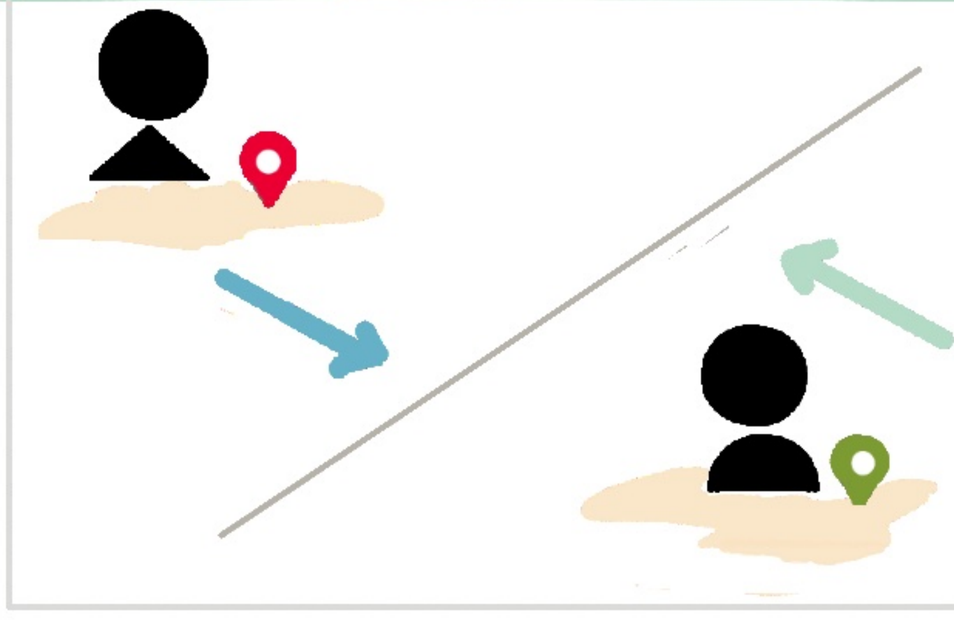


IT IS SECURE

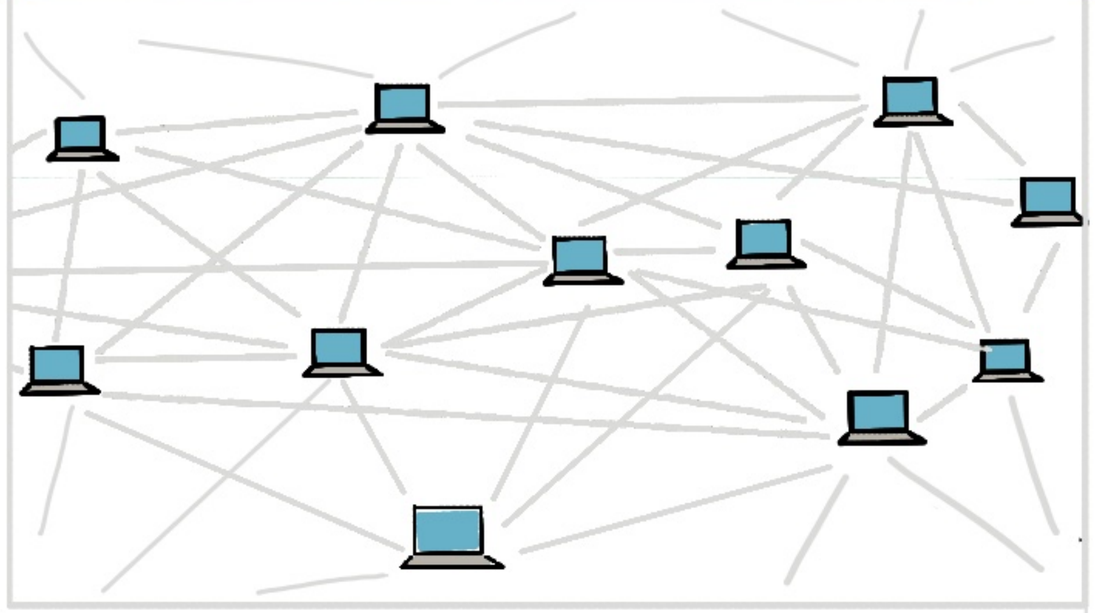


WHAT DOES A BLOCKCHAIN DO?

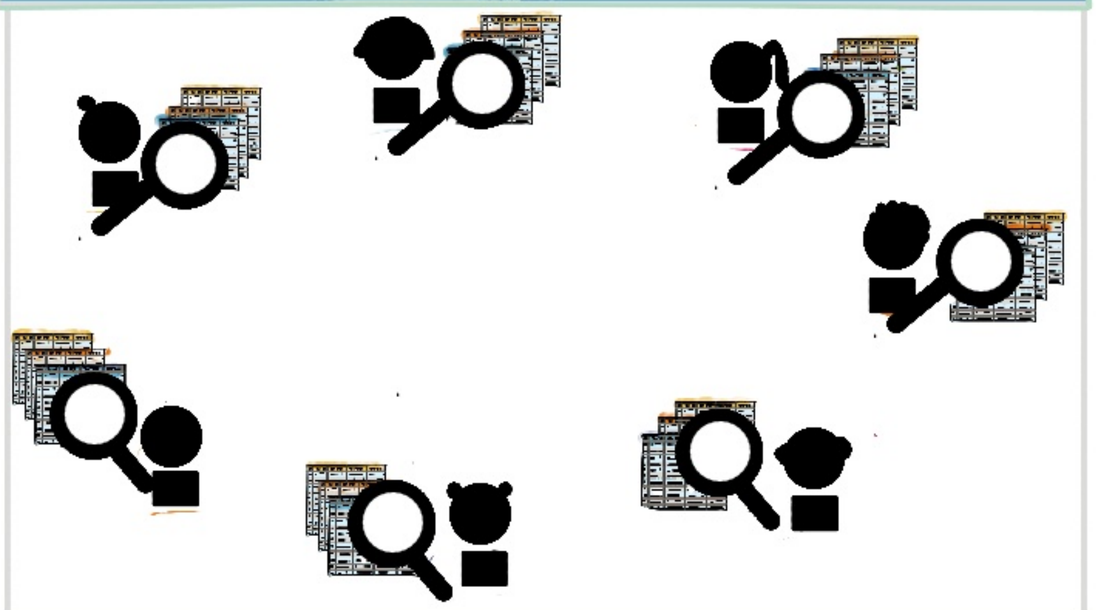
ENABLES STRANGERS TO TRANSACT



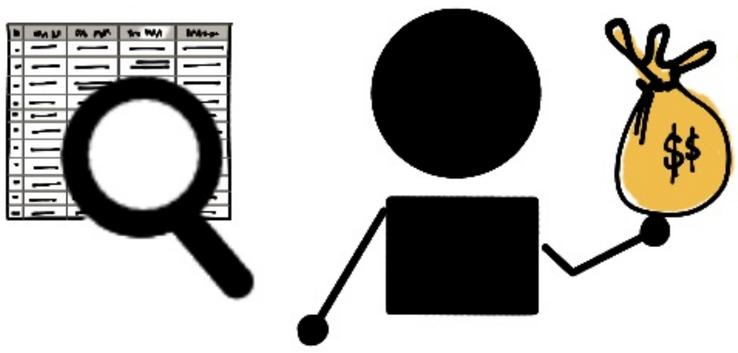
IN A DECENTRALISED NETWORK



WITH A CONSENSUS PROTOCOL AND



AN ECONOMIC INCENTIVE MODEL



WHILE KEEPING DATA CRYPTOGRAPHICALLY SECURE

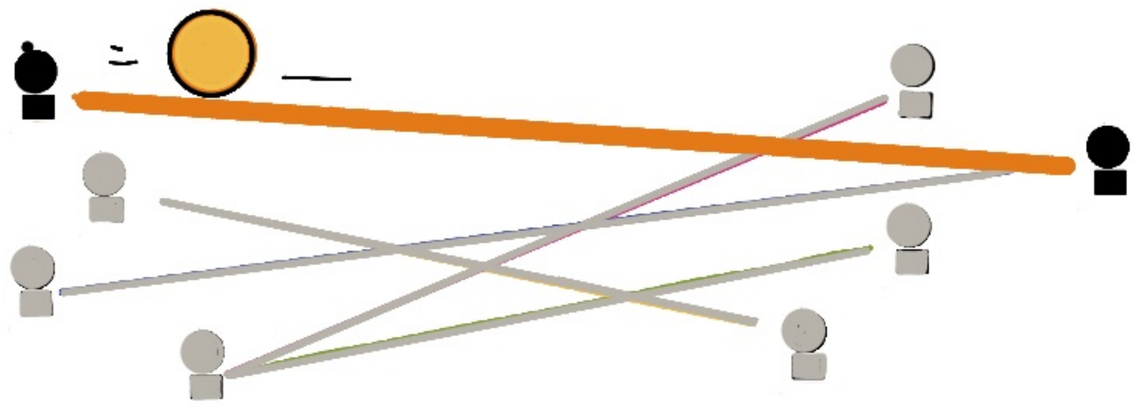


WHAT HAPPENS IN A BLOCKCHAIN?

ASSETS AND THEIR OWNERS ARE LISTED IN PUBLIC

ALL PRIOR TRANSACTIONS ARE PUBLIC

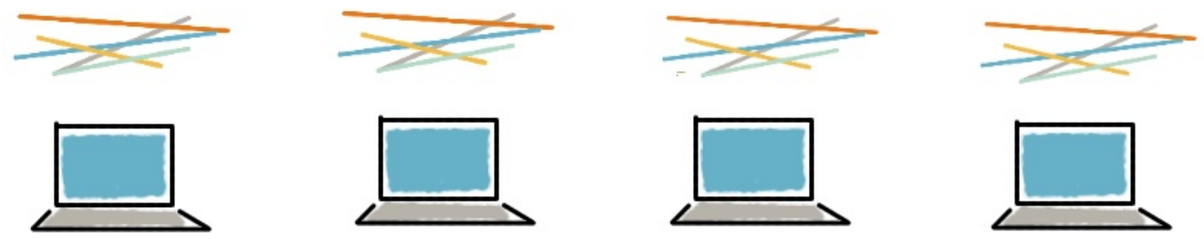
AN OWNER WANTS TO TRANSFER AN ASSET



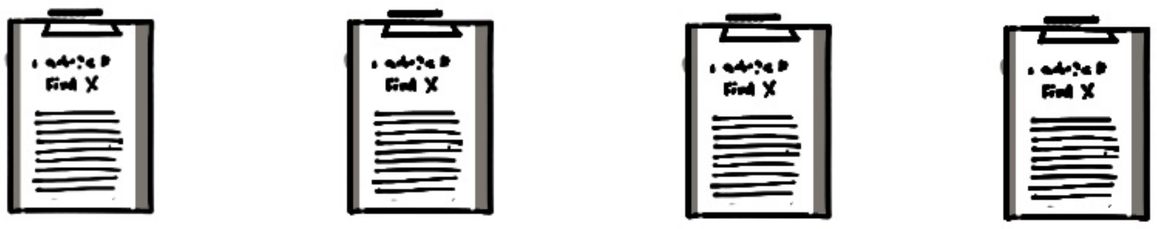
ALL TRANSACTIONS ARE BROADCAST TO THE NETWORK



ALL MEMBER NODES VALIDATE TRANSACTIONS ...



... SOLVE A MATHEMATICAL PUZZLE TO EARN REWARD



WINNER ADDS NEXT BLOCK OF TRANSACTIONS TO THE CHAIN



ASSET TRANSFER IS COMPLETE

AN EARLY BLOCKCHAIN IDEA



DIGITAL DATA IS EASILY MODIFIABLE





HABER

WE OUGHT TO TIME-STAMP DATA, NOT THE MEDIUM



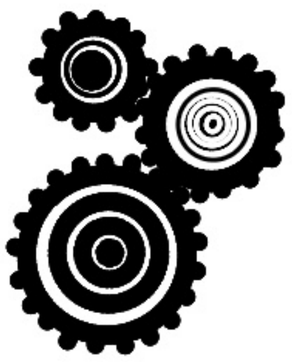
STORNETTA

Journal of CRYPTOLOGY (1990s) Vol 3 No 2

HOW TO TIME-STAMP A DIGITAL DOCUMENT

STUART HABER
stuart@bellcore.com

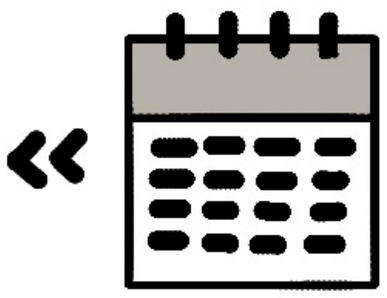
W SCOTT STORNETTA
stornetta@bellcore.com



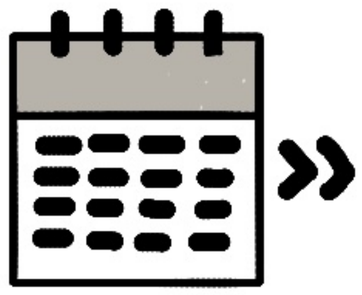
COMPUTATIONALLY PRACTICAL



MAINTAINS DOCUMENT PRIVACY



INFEASIBLE TO BACK DATE



INFEASIBLE TO FORWARD DATE

Search for 'Longest running blockchain is on New York Times'

GAME THEORY

STUDYING INTERACTIONS AND THE DECISION MAKING PROCESS

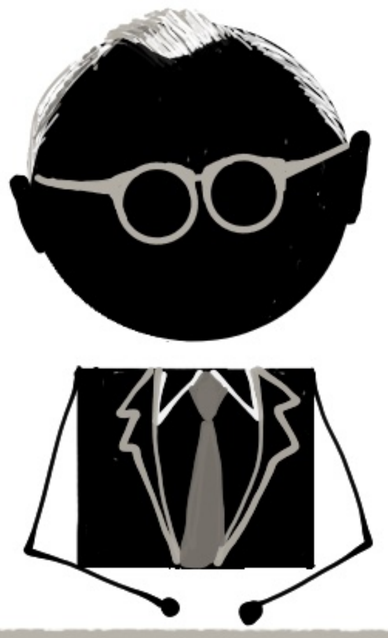
GAME THEORY

GAME THEORY IS A MATHEMATICAL TOOL
USED TO ANALYSE INTERDEPENDENT DECISIONS AND OUTCOMES



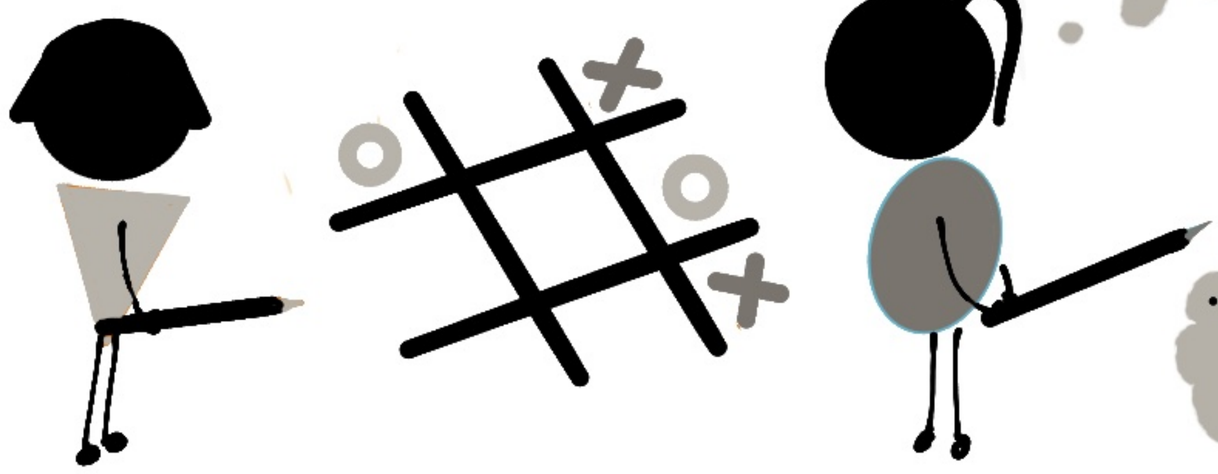
JOHN VON NEUMANN

MATHEMATICALLY FORMALISED IN THE 1940s BY



OSKAR MORGENSTERN

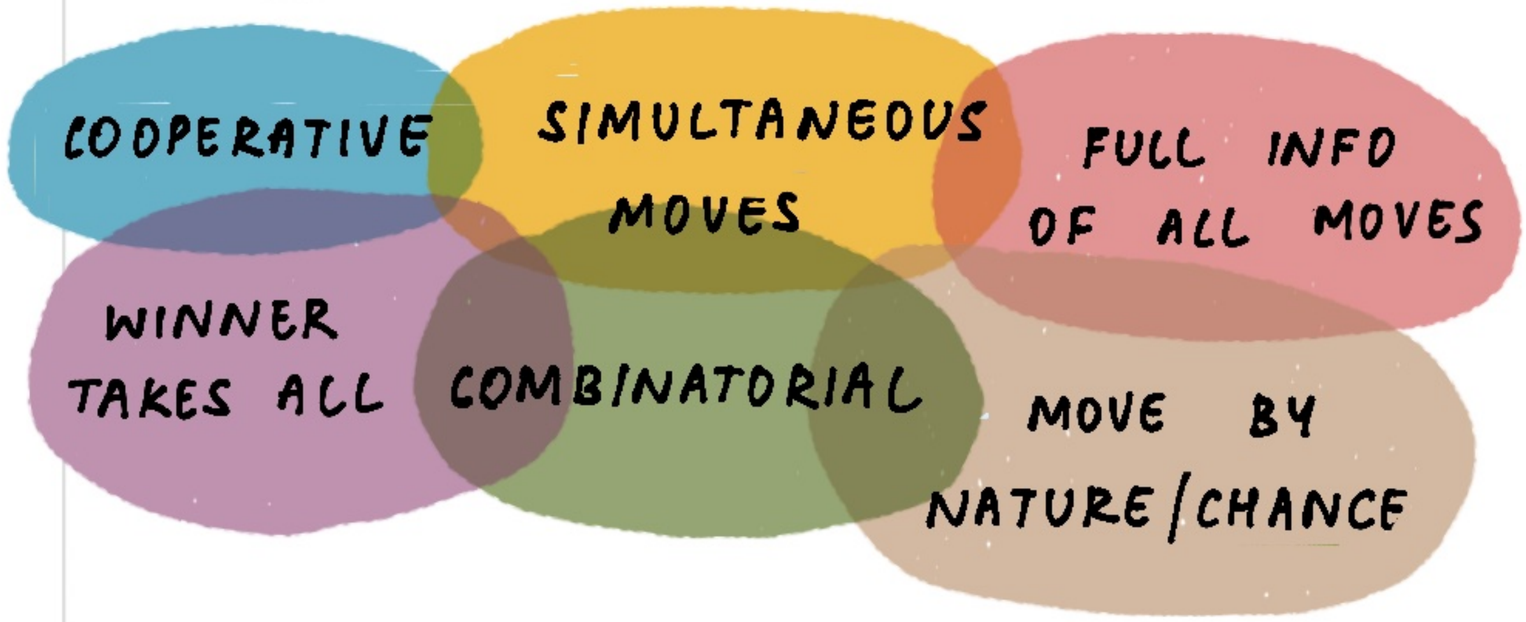
- PLAYERS
- STRATEGIES
- PAYOFFS



what move shall i make..?

...knowing my opponent's options

SOME TYPES OF 'GAMES'



APPLICATIONS



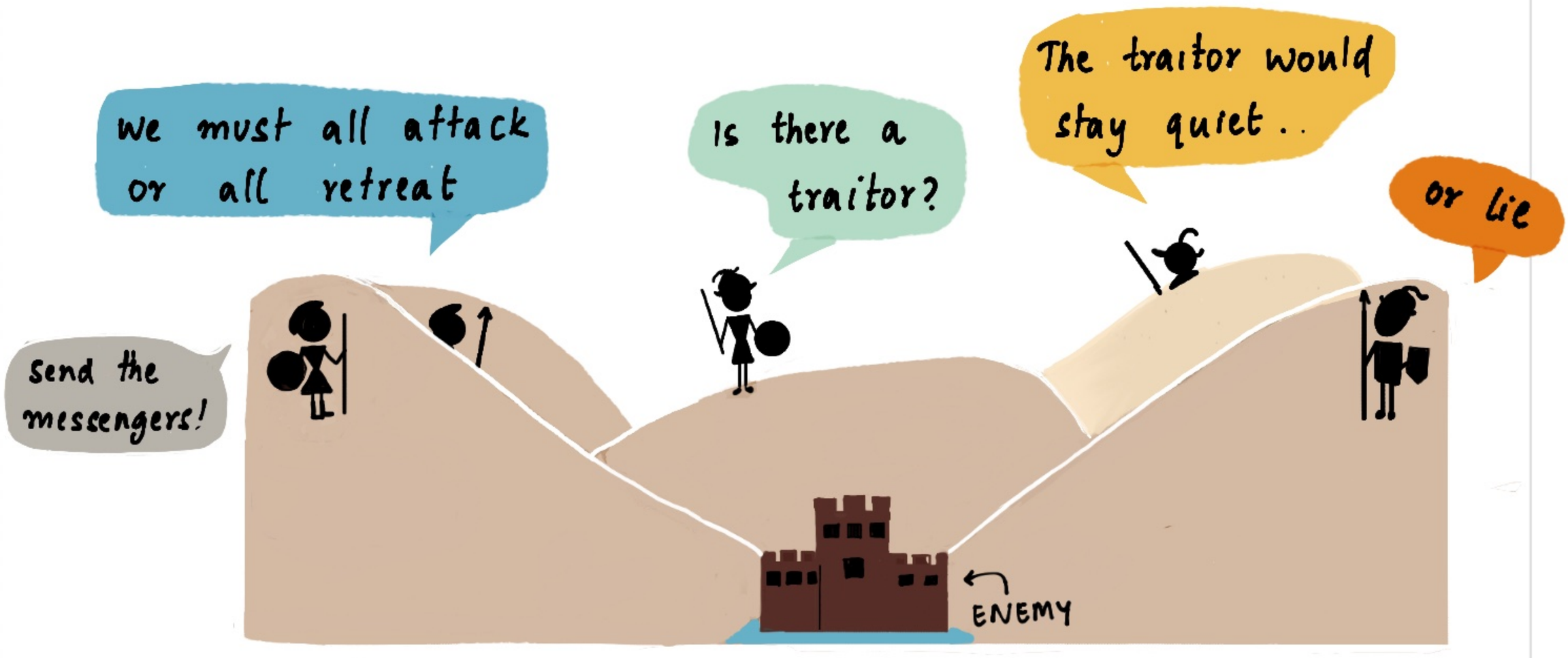
THE BYZANTINE GENERAL'S PROBLEM STUDIED BY GAME THEORY EXPLAINS HOW STRANGERS ON A BLOCKCHAIN COME TO A CONSENSUS.

BYZANTINE GENERALS PROBLEM

THIS PROBLEM IS A THOUGHT EXPERIMENT TO DESCRIBE SCENARIOS UNDER WHICH GENERALS COULD CARRY OUT A COORDINATED MOVE

UNDERSTANDING THIS WILL LAY THE FOUNDATION TO THE PROTOCOL PROOF-OF-WORK USED IN BITCOIN FOR CONSENSUS.

GOAL
- THE GENERALS MUST ACT ON A COMMON PLAN.
- TRAITORS CANNOT BE ALLOWED TO SPOIL THE PLAN





LESLIE LAMPORT

The Byzantine Generals Problem (1982)

LESLIE LAMPORT, ROBERT SHOSTAK and MARSHALL PEACE

SRI International

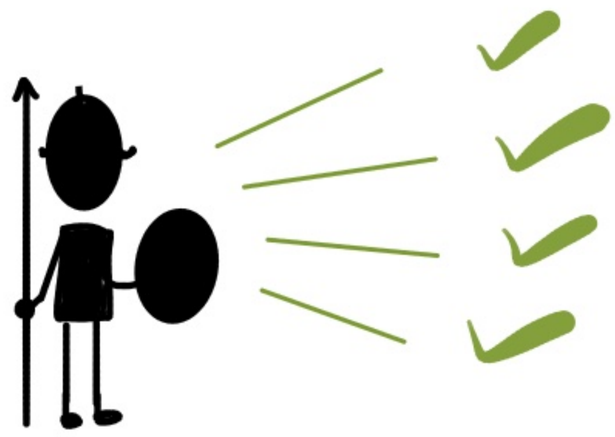
<solves with 2 algorithms>

1) WITH ORAL MESSAGES

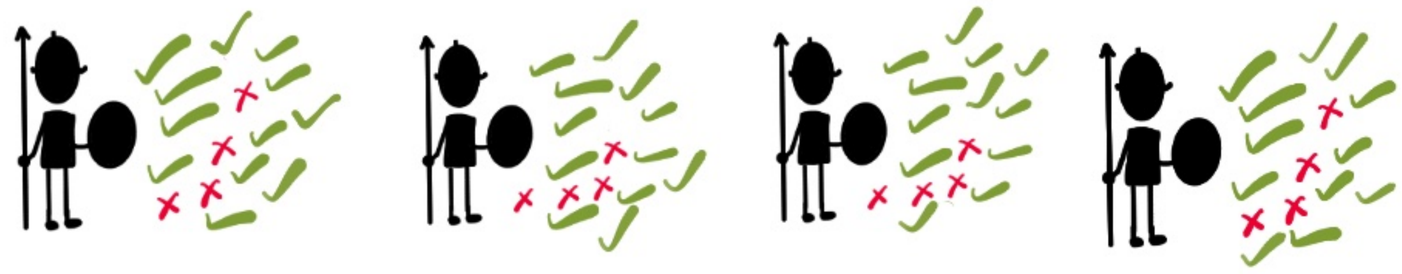
2) WITH UNFORGEABLE WRITTEN MESSAGES

FINDING A SOLUTION

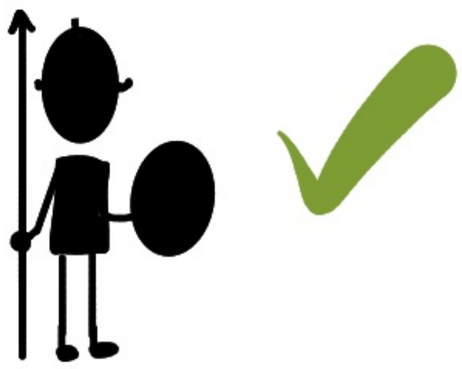
EACH GENERAL SENDS THE OTHERS HIS DECISION



THE GENERALS CAN EACH COMBINE THE INFORMATION

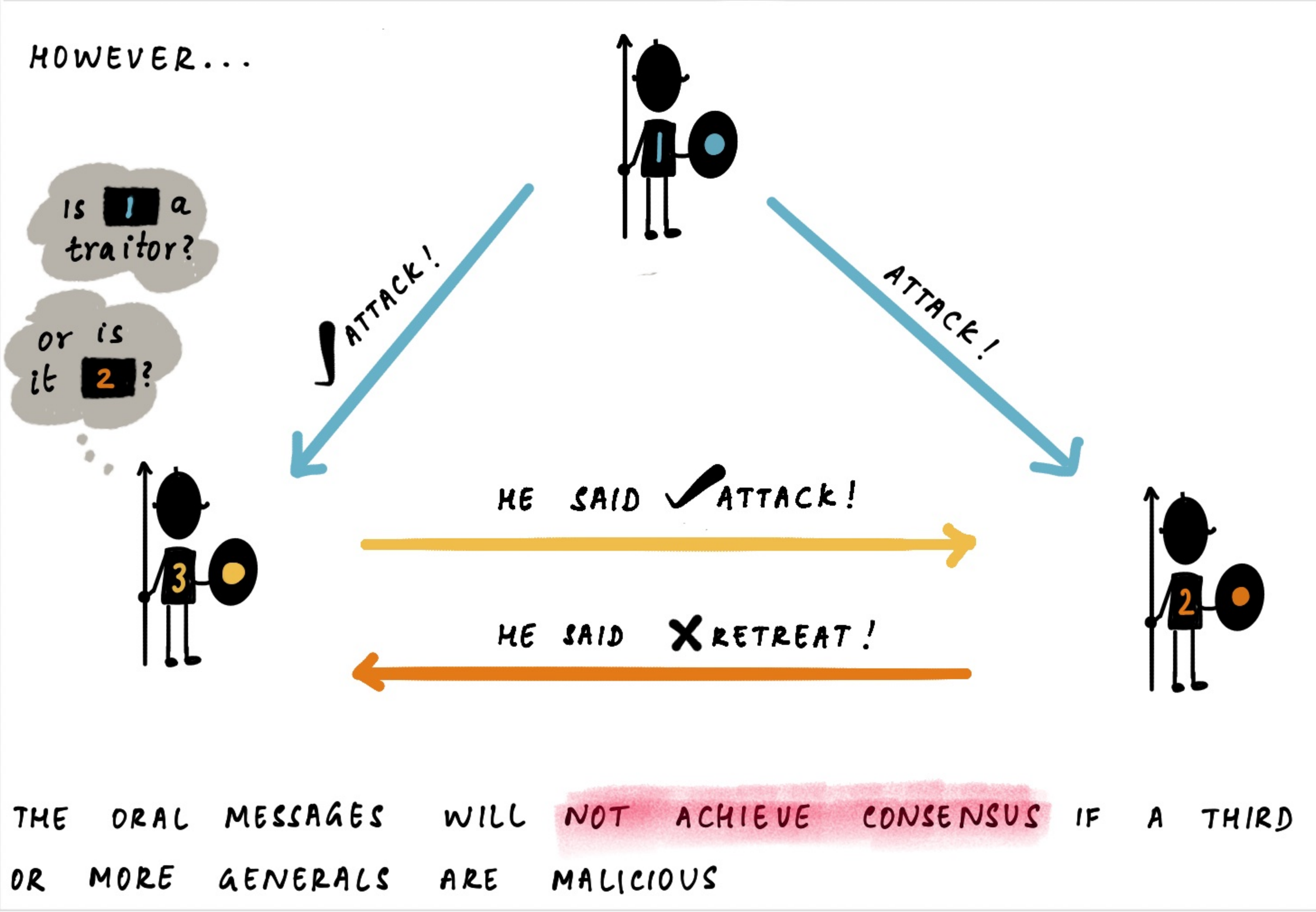


THE FINAL DECISION IS BY A MAJORITY VOTE



we all agree that we know what each is thinking!

HOWEVER...



THE ORAL MESSAGES WILL NOT ACHIEVE CONSENSUS IF A THIRD OR MORE GENERALS ARE MALICIOUS

SOLUTION 1: ORAL MESSAGES

ASSUME

ABSENCE OF MESSAGE CAN BE DETECTED

EVERY MESSAGE SENT IS DELIVERED CORRECTLY

RECEIVER KNOWS WHO THE SENDER IS

DECISION MAKING

EACH RECORDS WHAT THEY HEAR AND

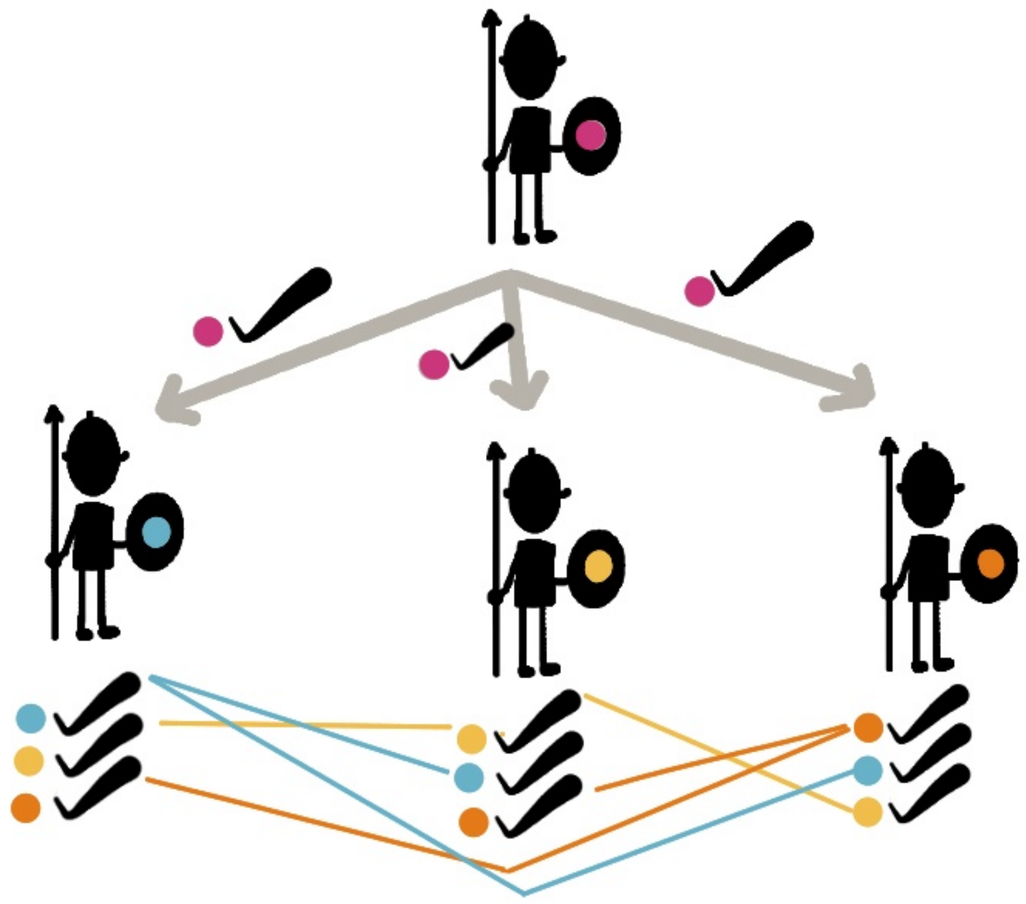
EACH SEND OTHERS WHAT THEY HEARD FROM THE GENERAL

THE DECISION WITH THE MAJORITY WINS

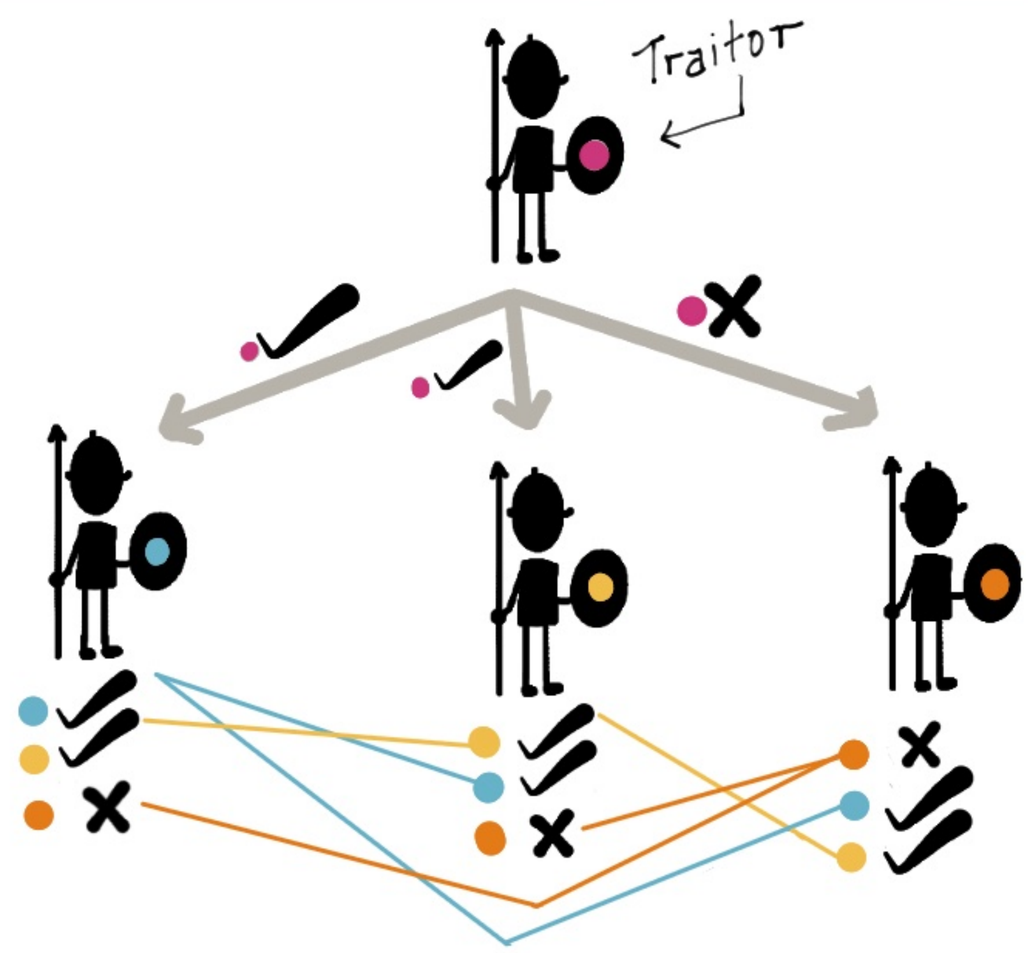
EACH CASE ENDS IN AGREEMENT

OVER 2/3 LOYAL GENERALS PREVAIL OVER TRAITORS

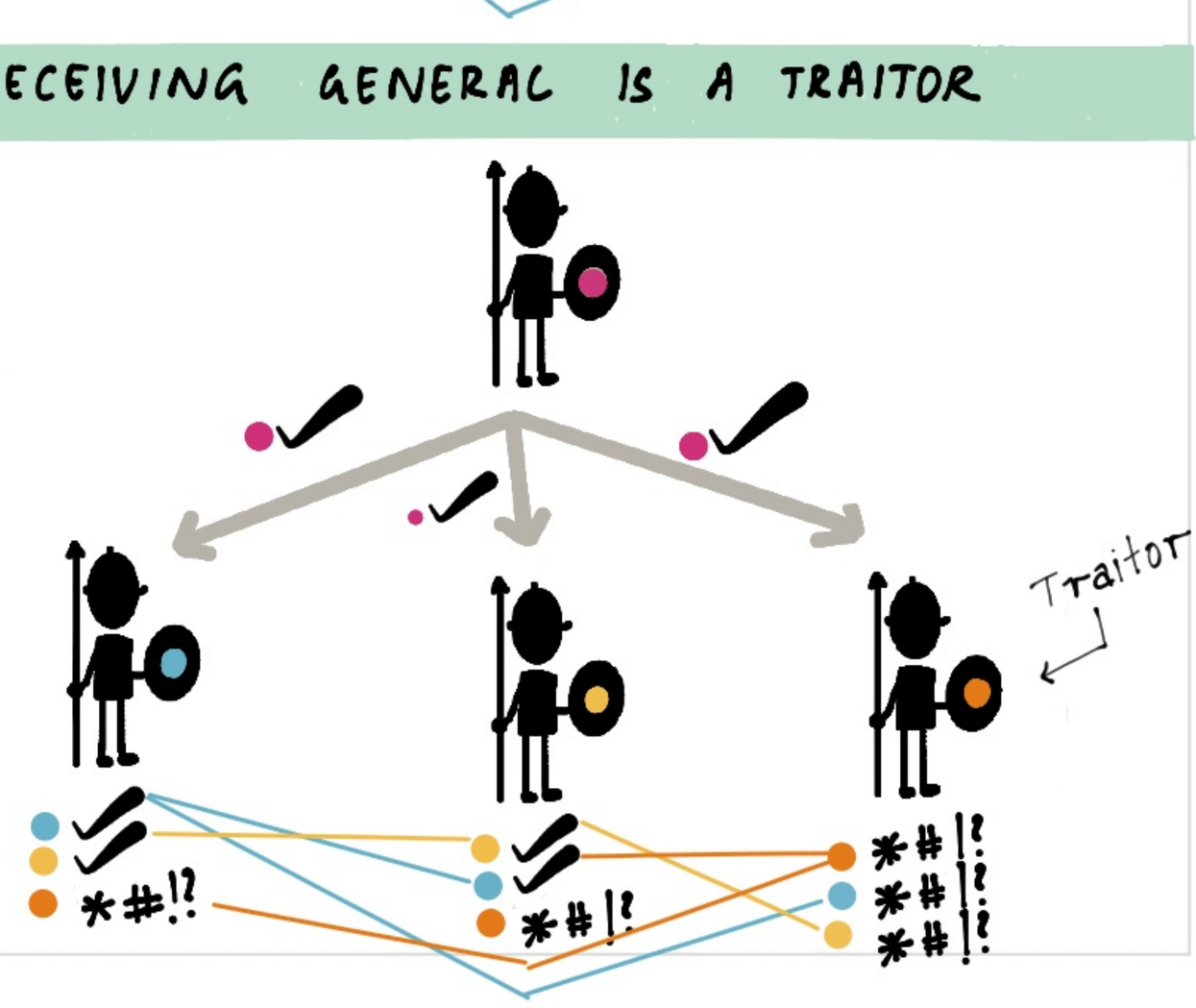
EVERYONE IS LOYAL



THE SENDING GENERAL IS A TRAITOR



A RECEIVING GENERAL IS A TRAITOR

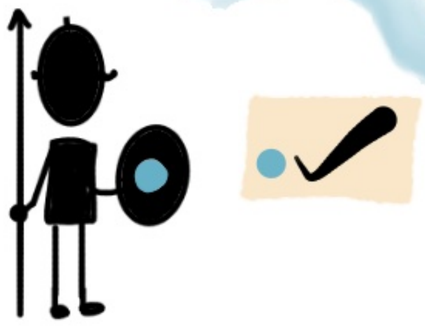


SOLUTION 2: WRITTEN MESSAGES

THE TRAITOR'S ABILITY TO LIE IS THE FLAW WITH ORAL MESSAGES

THE WRITTEN MESSAGES SOLUTION INVOLVES A SIGNED MESSAGE

THE  SIGNATURE IS UNFORGEABLE AND VERIFIABLE

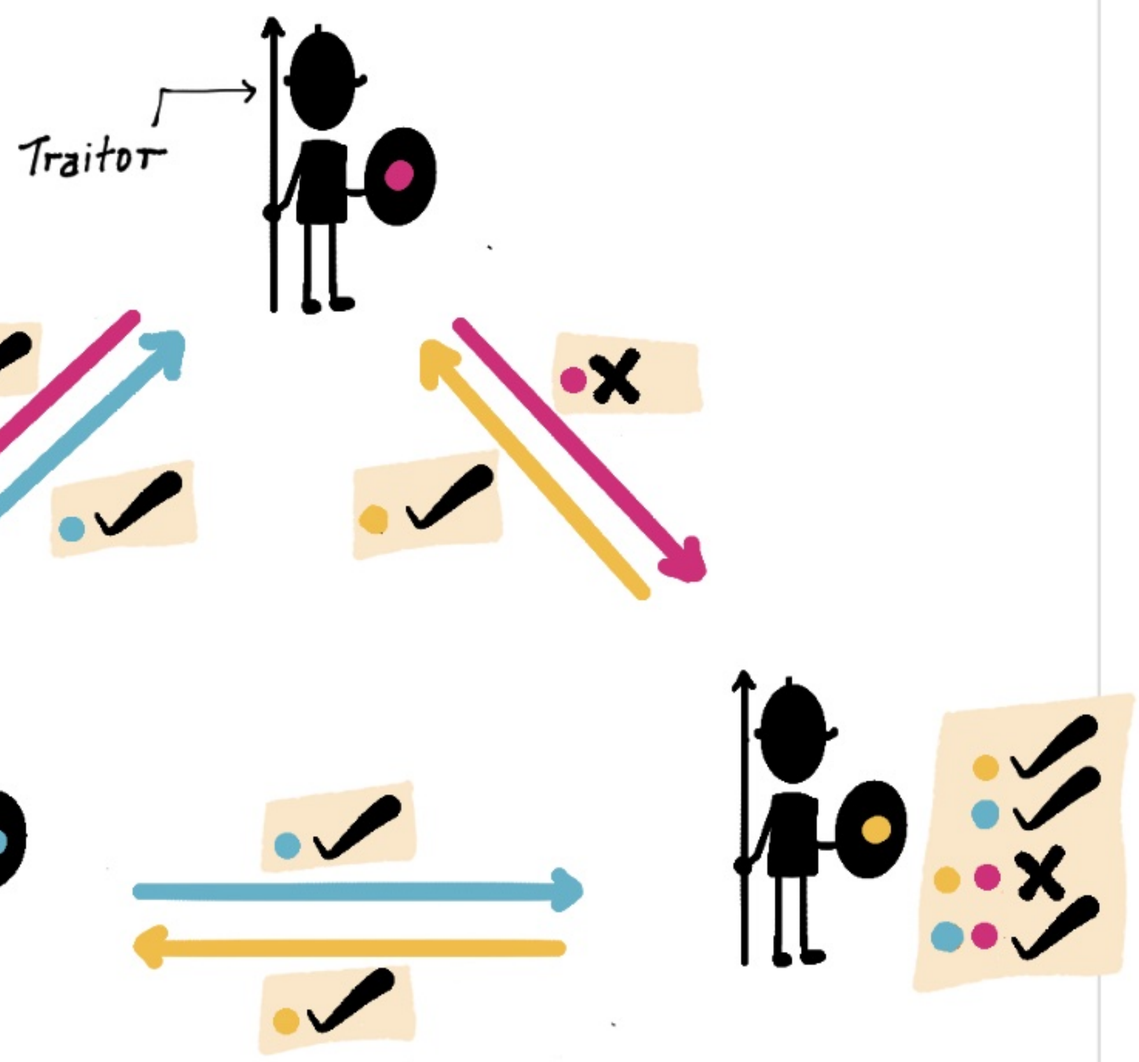


THE SENDER ADDS THEIR SIGNATURE TO THE WRITTEN MESSAGE



WHEN THE RECEIVER PASSES IT ON, THEY APPEND THEIR OWN SIGNATURE TO THE ORIGINAL MESSAGE

EVEN WITH 1 TRAITOR OUT OF 3 GENERALS, IT IS VERY CLEAR TO ARRIVE AT A MAJORITY AGREEMENT



ENCRYPTION

IN THIS SECTION WE LOOK AT CRYPTOGRAPHIC HASH FUNCTIONS AND PUBLIC KEY CRYPTOGRAPHY AND HOW THEY KEEP A BLOCKCHAIN SECURE

THE ONE-WAY FUNCTION

MODERN ENCRYPTION WORKS ON THE BASIS OF ONE-WAY FUNCTIONS.

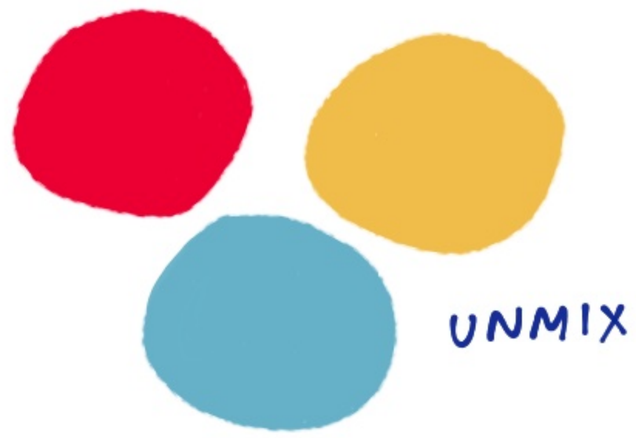
OPERATIONS WHICH ARE :

✓ EASY TO DO



13 x 16 = ____

⧗ HARD TO UNDO



208 = ____ x ____

●●● SEE 'HOW TO TELL SECRETS' IN THIS SERIES FOR MORE DETAIL ●●●

IN CRYPTOGRAPHY, A ONE WAY FUNCTION IS A MATHEMATICAL OPERATION WITH THE DATA

ONE WAY FUNCTIONS SHOW UP IN A BLOCKCHAIN AS

HASH FUNCTIONS

AN ALGORITHM

applied to

ANY TYPE / SIZE DATA

results in

FIXED LENGTH UNIQUE STRING

PUBLIC KEY CRYPTOGRAPHY

TWO LONG NUMBERS

CONNECTED BY A FORMULA

securely

SCRAMBLE / UNSCRAMBLE A MESSAGE

HASH FUNCTIONS

CRYPTOGRAPHIC HASH FUNCTIONS

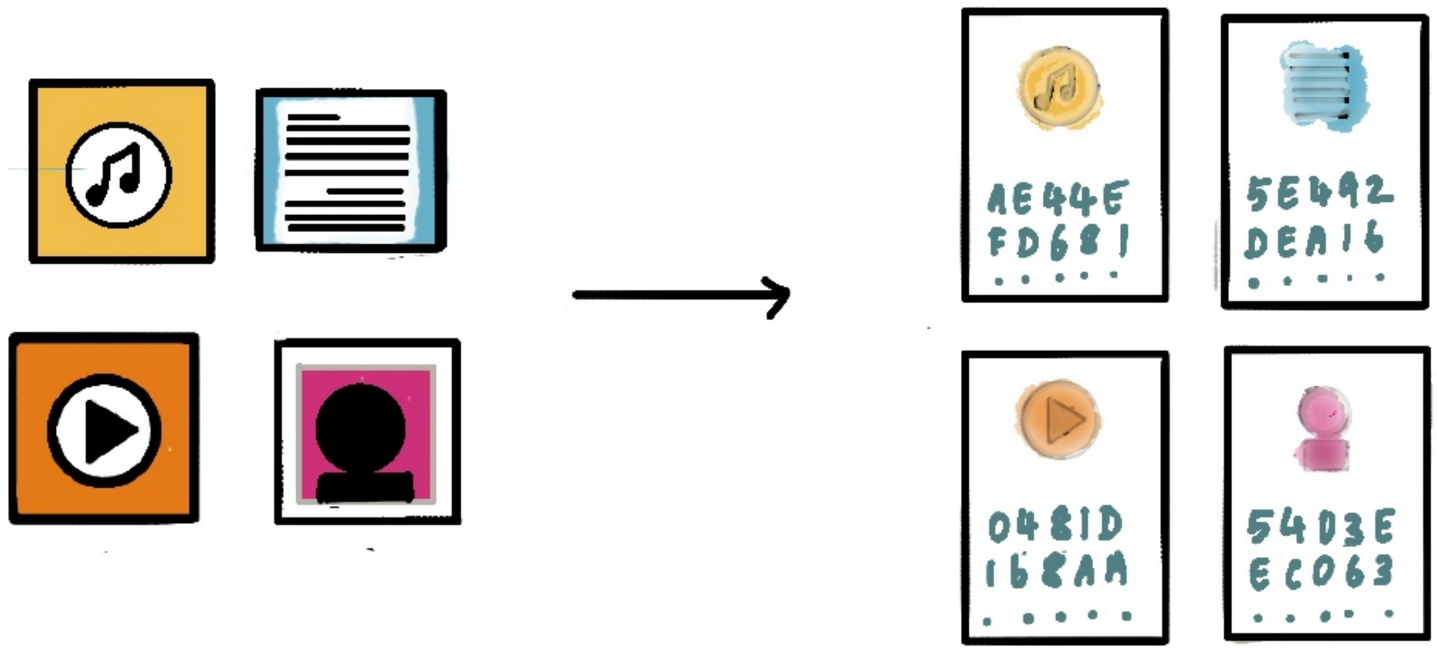
USED TO



TO SECURELY STORE TRANSACTIONS

WHAT THEY DO

TAKE DIGITAL DATA AND...



THE HASH IS SPACE-EFFICIENT

...TURN IT TO A FIXED SIZE HEXADECIMAL NUMBER

EXAMPLES

- SHA-256 - BY THE NSA
- KECCAK-256 - BY BERTONI, DAEMEN, PEETERS, VAN ASSCHE
- MD5 - BY RON RIVEST

A NOTE ON HEXADECIMAL

WHAT IS HEXADECIMAL?

HEXADECIMAL IS A NUMBER SYSTEM WITH BASE 16

FROM $\emptyset$ – F

EXAMPLES

10 → A

11 → B

12 → C

13 → D

14 → E

15 → F

A – F ARE VALID NUMERALS

SPECIAL NOTATION

A `0x` PREFIX IDENTIFIES A NUMBER AS HEXADECIMAL

0 → 0x0

1 → 0x1

2 → 0x2

9 → 0x9

10 → 0xA

11 → 0xB

USES

THIS FORMAT IS USED IN MICROCONTROLLERS, AS THEY MANIPULATE DATA & BITS AT A TIME. YES, BYTE-SIZE.

DECIMAL TO HEXADECIMAL

$(78)_{10}$ ⟶ TO HEX

16 | 78		
16 | 4	→	14
0	→	4

0x4E

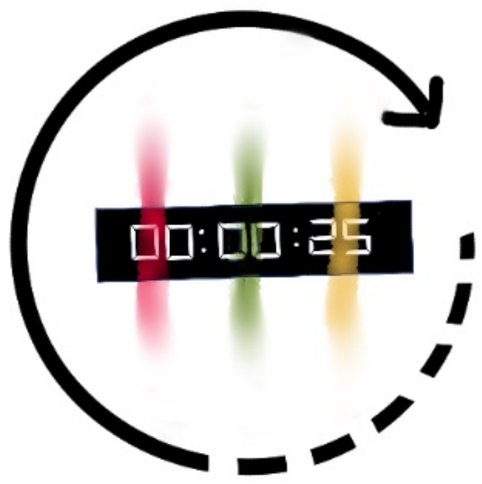
HEXADECIMAL TO DECIMAL

$(78)_{16} = 7 \times 16^{1} + 8 \times 16^{0}$

$= 120$

A HASH FUNCTION

IS FAST



DOES NOT TAKE UP
SIGNIFICANT
COMPUTATIONAL OVERHEAD

IS DETERMINISTIC

SAME FILE
SAME OUTPUT





→ 846538edba6f6959.....

→ 846538edba6f6959.....

IS NON REVERSIBLE



HELPS TO IDENTIFY THE ORIGINAL

AS DOES A...



...PHOTOGRAPH



...FINGERPRINT



...DIALLING CODE

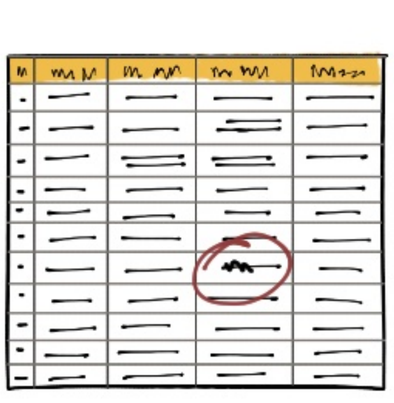
THE AVALANCHE EFFECT

A SMALL CHANGE IN INPUT

INPUT DATA	blockchain
OUTPUT HASH	ef1797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1

CAUSES A DRAMATIC CHANGE IN OUTPUT

INPUT DATA	Blockchain
OUTPUT HASH	625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1



THUS, HASH FUNCTIONS HELP TO DETERMINE WHETHER SOMEONE HAS MEDDLED WITH THE DATA



PUBLIC KEY CRYPTOGRAPHY



ALSO KNOWN AS

ASYMMETRIC KEY CRYPTOGRAPHY

USED TO

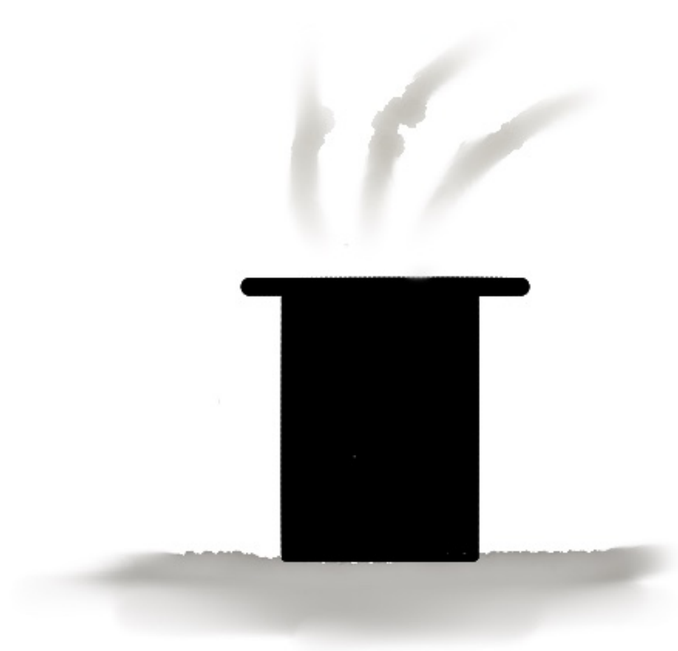


TO IDENTIFY

WHO YOU ARE

WHAT DOES IT DO?

USE TWO MATHEMATICALLY RELATED KEYS







ONE TO

ENCRYPT/SIGN



ONE TO

DECRYPT/VERIFY

EXAMPLES

- RSA (RIVEST SHAMIR ADLEMAN)
- ECC (ELLIPTIC CURVE CRYPTOGRAPHY)

INTENDED RECEIVER

THE WHOLE POINT OF CRYPTOGRAPHY

MESSAGE : UNTAMPERED

RECEIVER : INTENDED

SENDER : VERIFIABLE

KEY(S) : BASED ON MATHS/COMPUTER SCIENCE

A PUBLIC KEY KNOWN TO ALL





A PRIVATE KEY KNOWN ONLY TO THE INDIVIDUAL

- POSTAL ADDRESS — LETTER BOX KEY
- EMAIL ID — PASSWORD







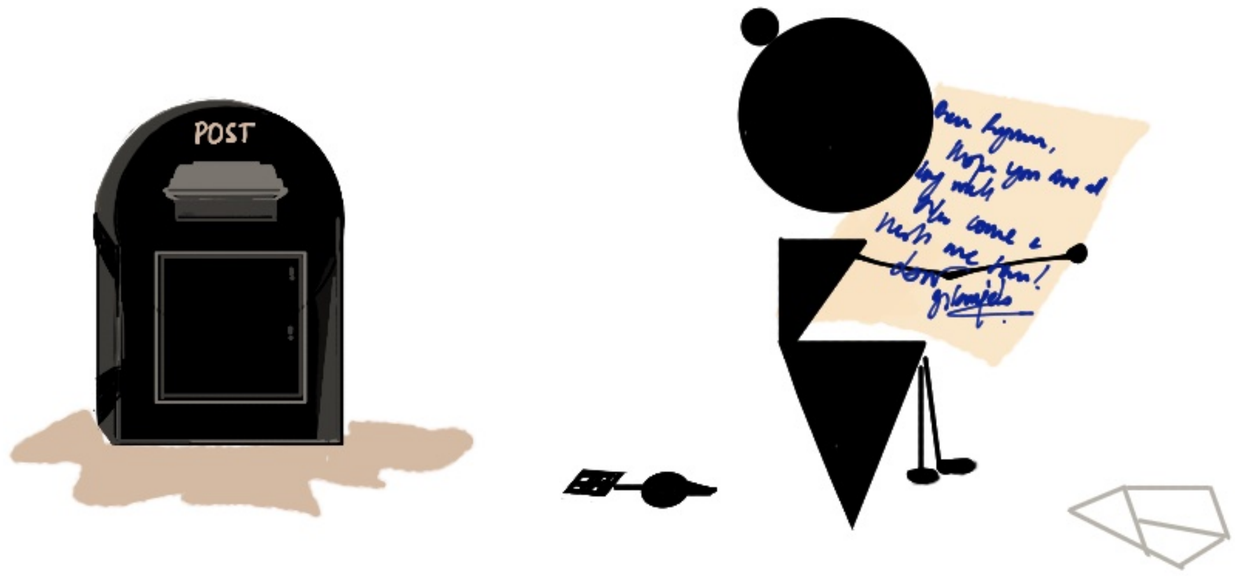
SECURING A MESSAGE WITH A PUBLIC KEY IS EASY

GETTING TO THE MESSAGE IS HARD

UNLESS THE PRIVATE KEY IS KNOWN

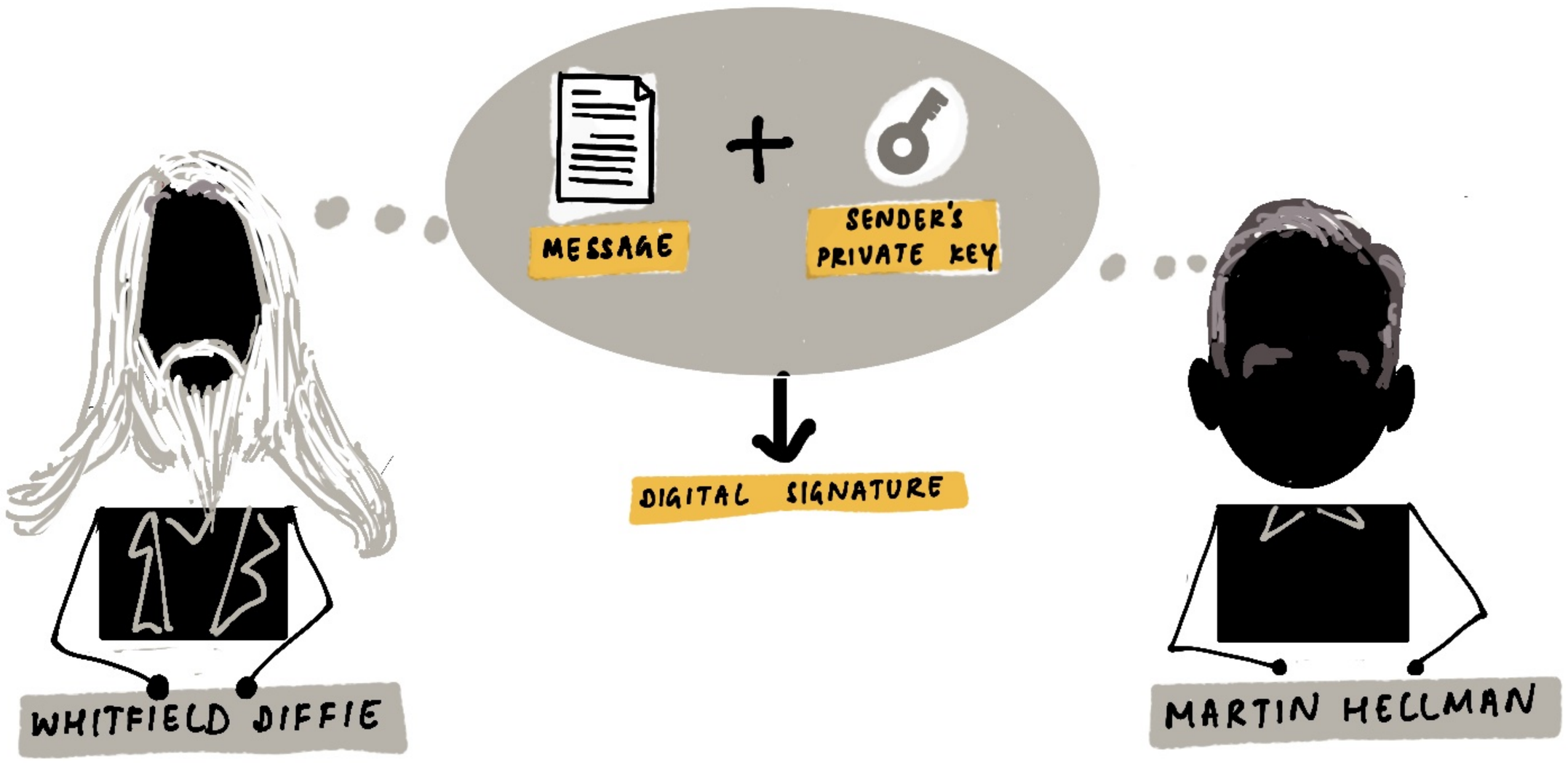
THIS ENSURES THAT ONLY THE INTENDED RECEIVER CAN ACCESS THE MESSAGE/ASSET BEING SENT

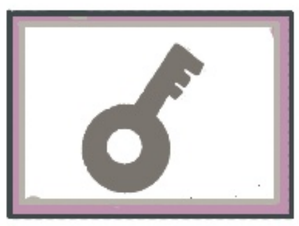
VERIFIED SENDER



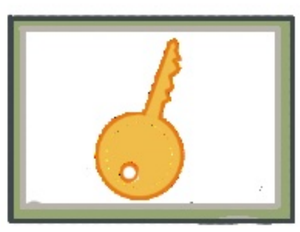
A SIGNATURE BINDS THE SENDER TO THE MESSAGE

DIGITAL SIGNATURES TO VERIFY THE SENDER OF A MESSAGE WAS FIRST PROPOSED BY DIFFIE AND HELLMAN





DOES THAT MEAN WE ENCRYPT WITH A PRIVATE KEY?



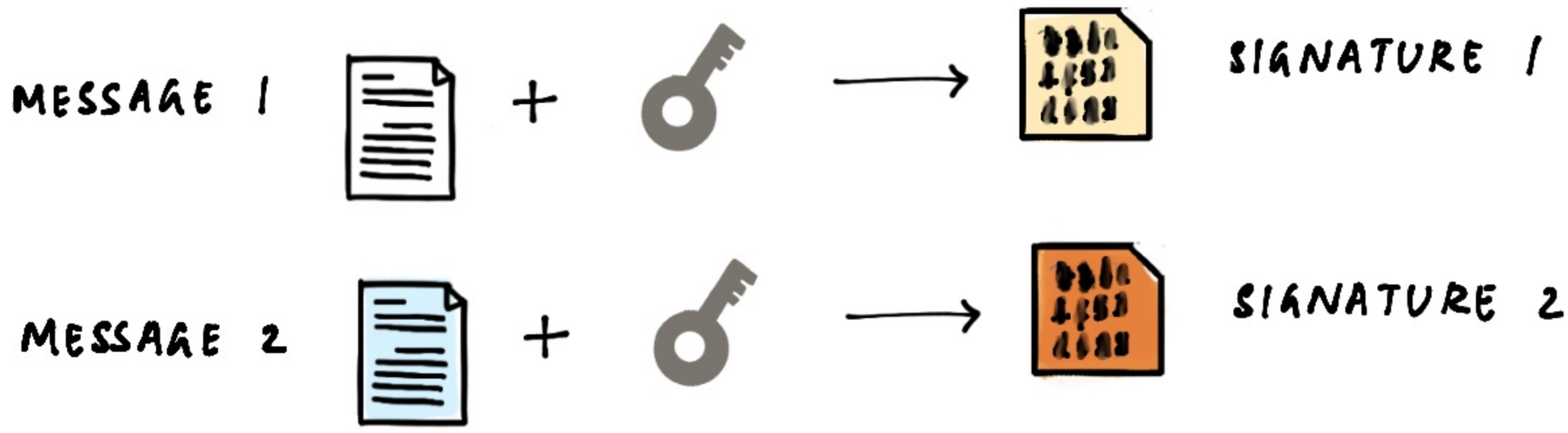
YES! THE PUBLIC KEY CAN DECRYPT IT



ONLY THE OWNER HAS THE PRIVATE KEY TO ENCRYPT IT!

DIGITAL SIGNATURES

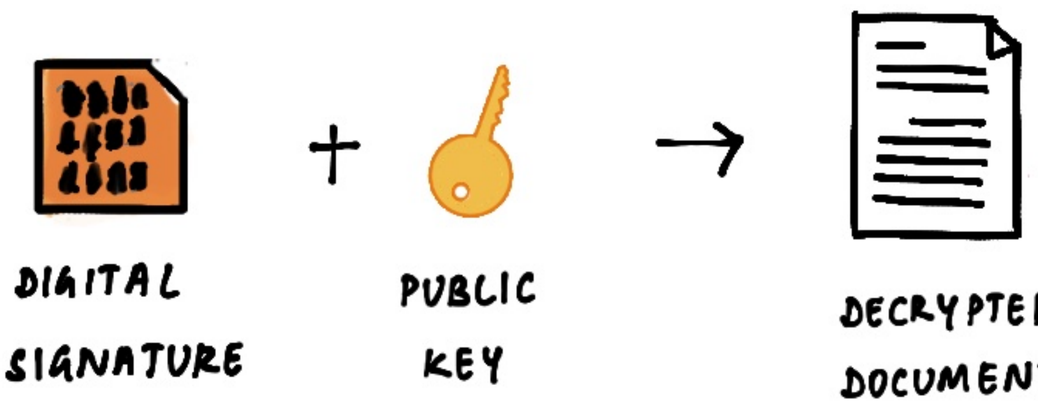
ARE UNIQUE TO A MESSAGE



ARE NOT FORGEABLE



PROVE OWNERSHIP OF THE PUBLIC KEY



PROVING THAT THE PUBLIC KEY IS OWNED BY THE ONE WHO SIGNED WITH THE PRIVATE KEY!

ARE SECURE. REALLY!! WHEN A PUBLIC KEY CAN DECRYPT IT ?!



LET US SEE HOW

UNTAMPERED MESSAGES

A DIGITAL SIGNATURE IS USED TO PROVE THAT A DOCUMENT HAS NOT BEEN TAMPERED — TYPICALLY IN 3 STAGES

HASH → SIGN → VERIFY



NEEDS TO SEND A



TO





APPLIES A HASH FUNCTION



TO



CREATING





SIGNS THE



WITH THEIR



CREATING





SENDS BOTH





TO

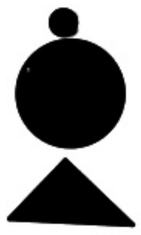




VERIFIES THAT



BELONGS TO





HASHES



CREATING



WHICH SHOULD MATCH

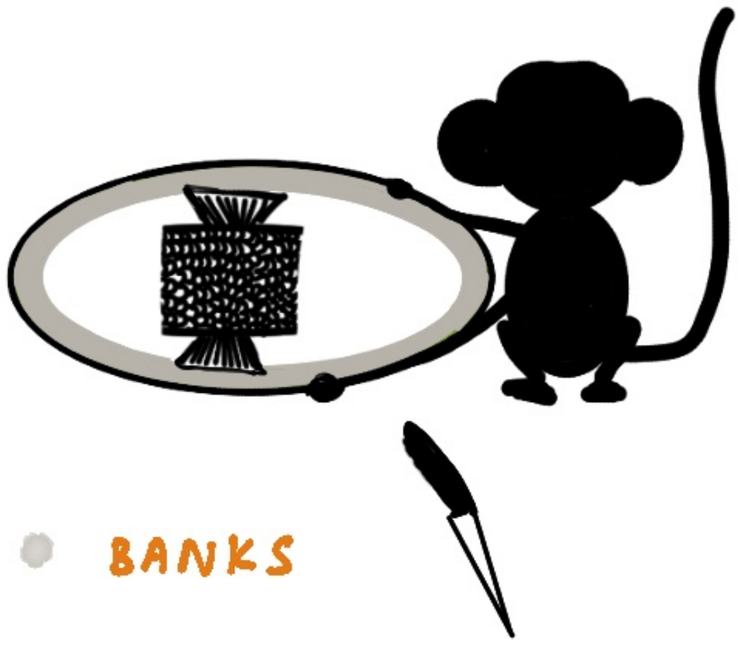


✓ VERIFYING THAT IT WAS UNTAMPERED

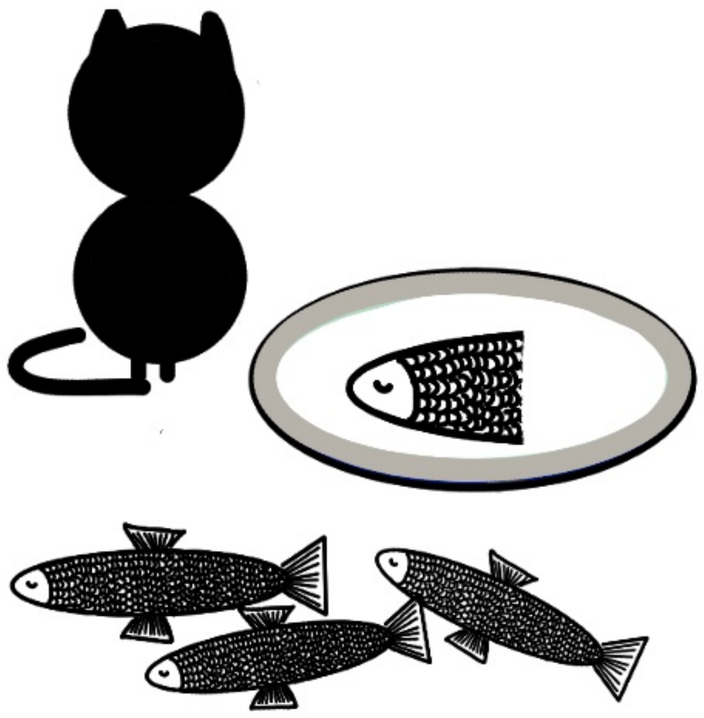
VALUE EXCHANGE

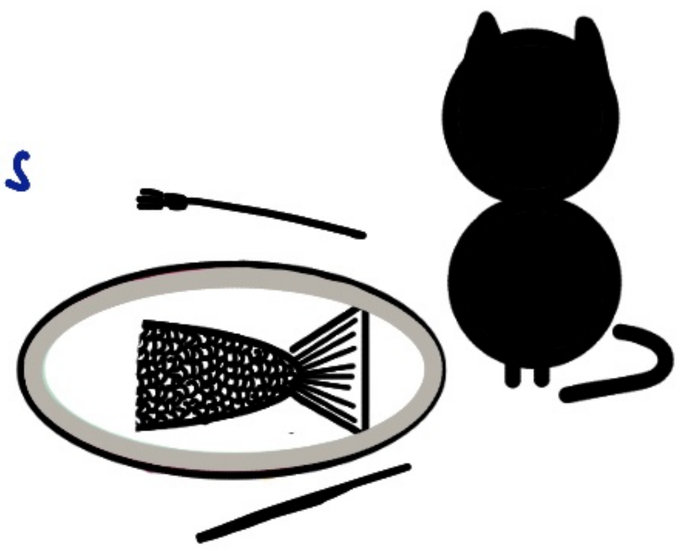
WHO IS AN INTERMEDIARY?

AN INTERMEDIARY IS A TRUSTED THIRD PARTY THAT FACILITATES FINANCIAL TRANSACTIONS BETWEEN TWO OR MORE PARTIES



- BANKS
- STOCK EXCHANGES
- MUTUAL FUNDS
- INSURANCE COMPANIES





INTERMEDIARIES

- CONNECT SPENDERS TO LENDERS
- MAY STORE FINANCIAL ASSETS
- PROCESS TRANSACTIONS AT SCALE
- CHARGE FEES/ ECONOMIC RENTS
- AUTHENTICATE THE OTHER PARTY
- MAY PROVIDE GUARANTEES
- ARE SUBJECT TO REGULATION
- ALSO SUBJECT TO FRAUD/FORGERY

EXCHANGE OF VALUE WITH INTERMEDIARY



MY BANK

NOTIFY

YOUR BANK

-$12

+$12

MY BANK

YOUR BANK

+$12

-$12

CENTRAL BANK

ADJUST BALANCES WITH CENTRAL BANK

MY BALANCE

UPDATE BALANCES

YOUR BALANCE

THERE IS A COST TO EACH TRANSFER

THIS COST INCREASES WITH EVERY ADDITIONAL FINANCIAL INSTITUTION THAT COMES BETWEEN THE SENDER AND RECEIVER

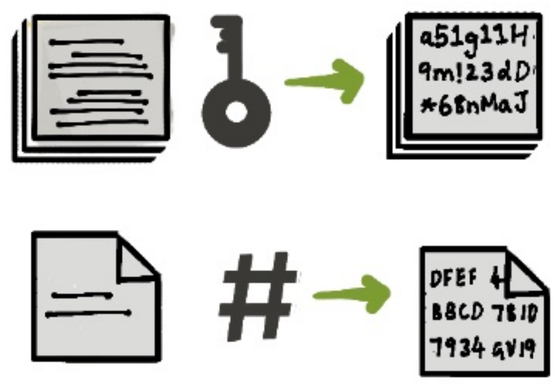
...AND WITH NO INTERMEDIARY

TRUST IS PLACED IN THE TECHNOLOGY / BLOCKCHAIN PROTOCOL









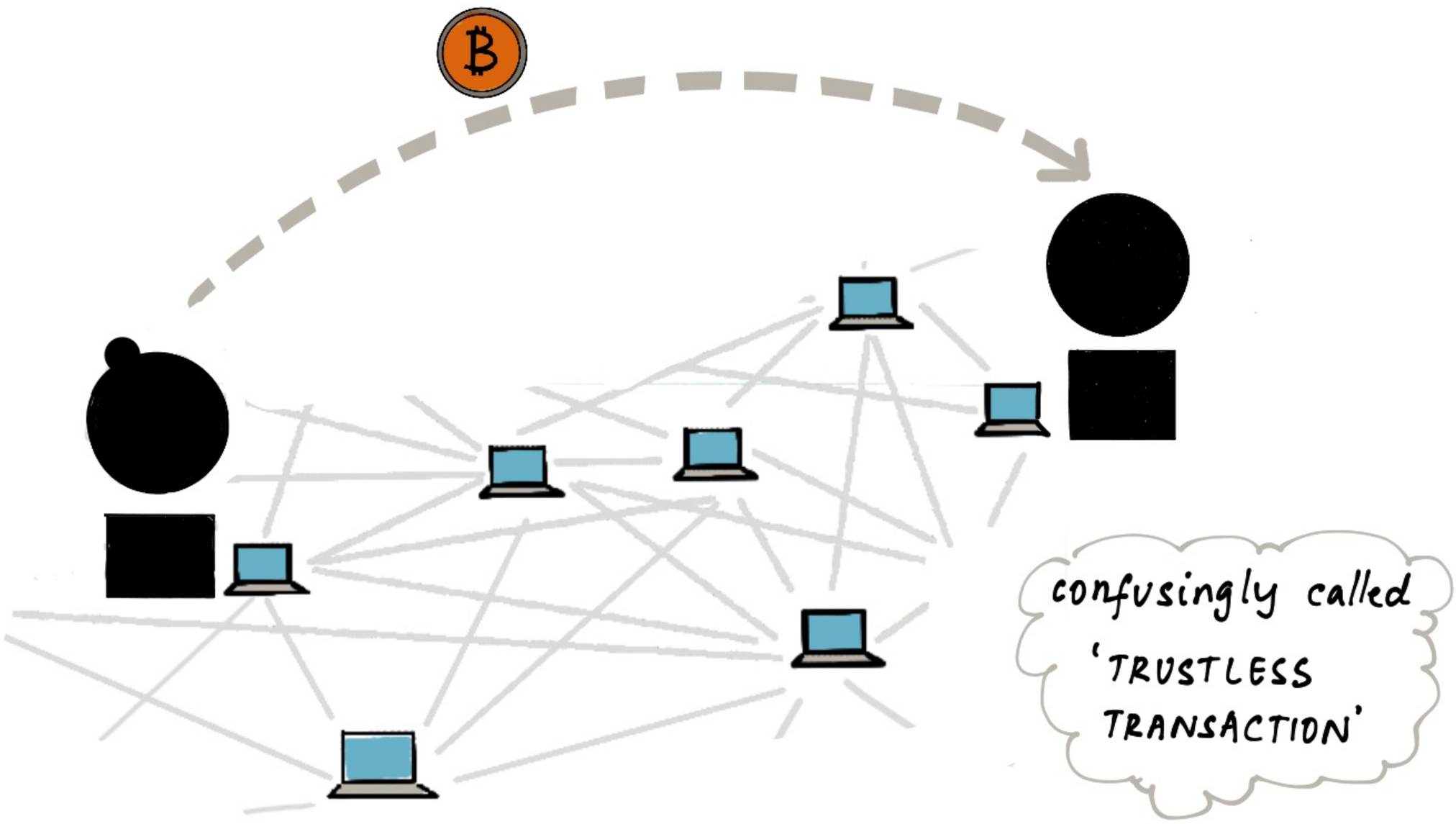
PUBLIC LEDGERS

CONSENSUS PROTOCOLS

ECONOMIC INCENTIVES

CRYPTOGRAPHIC OPERATIONS

ENABLING SPEEDIER TRANSACTIONS AT LOWER COSTS



NO INTERMEDIARY ≠ NO COSTS

WE SHALL COME BACK TO THIS IN A LATER SECTION OF THE BOOK CALLED 'WHAT IS THE COST OF TRUST?'

CURRENCY & CRYPTOCURRENCY

FIRST, A QUICK QUIZ

PICK A PIC THAT COMES TO MIND WHEN YOU HEAR THE WORD CRYPTO!

a) SECRET WRITING

UHDG WKH
ERRN 'KR2
WR WHOO
VHFUHWV'
EB JLWDQMDDL
-caesar shift 3

b) CRYPTO CURRENCY



c) A CRYPT



d) I LIVE UNDER A ROCK

IF YOU CHOSE

a) ★★★★★ YOU'D BE RIGHT, THAT'S CRYPTOGRAPHY

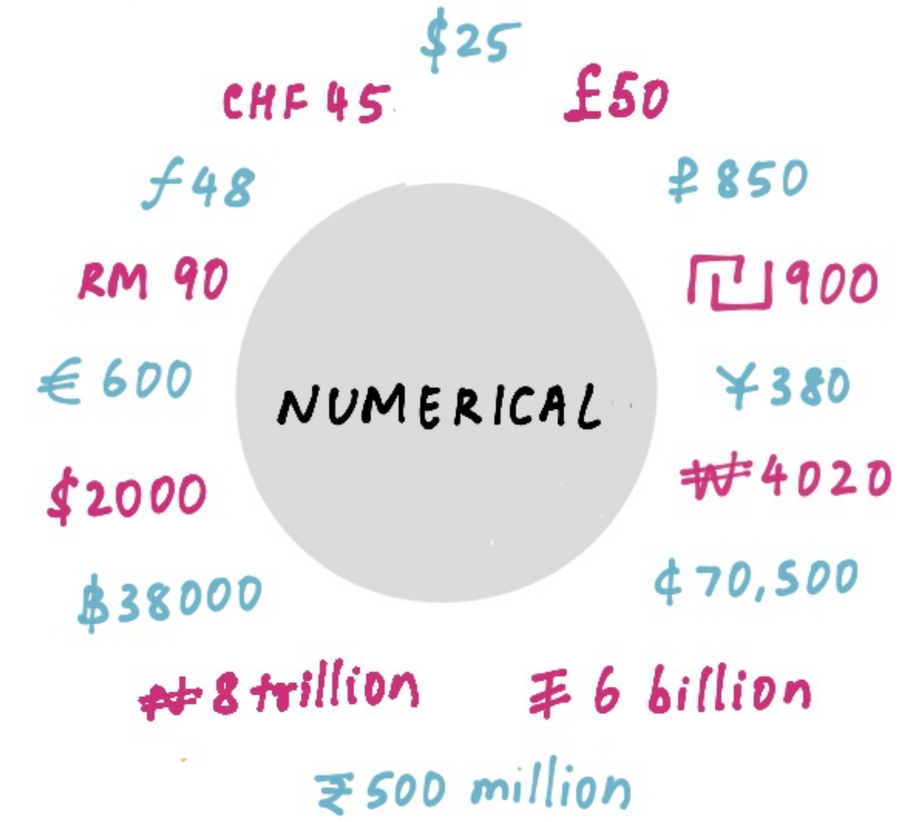
b) $$$$ YOU'D BE RIGHT AGAIN - 'CRYPTO' HAS BEEN CO-OPTED TO MEAN CRYPTOCURRENCY/CRYPTOASSET/DIGITAL CURRENCY

c) Whoops! YOU MISSED THE 'O'

d)  PLEASE CHECK BACK IN 30 YEARS!

MONEY VS CURRENCY

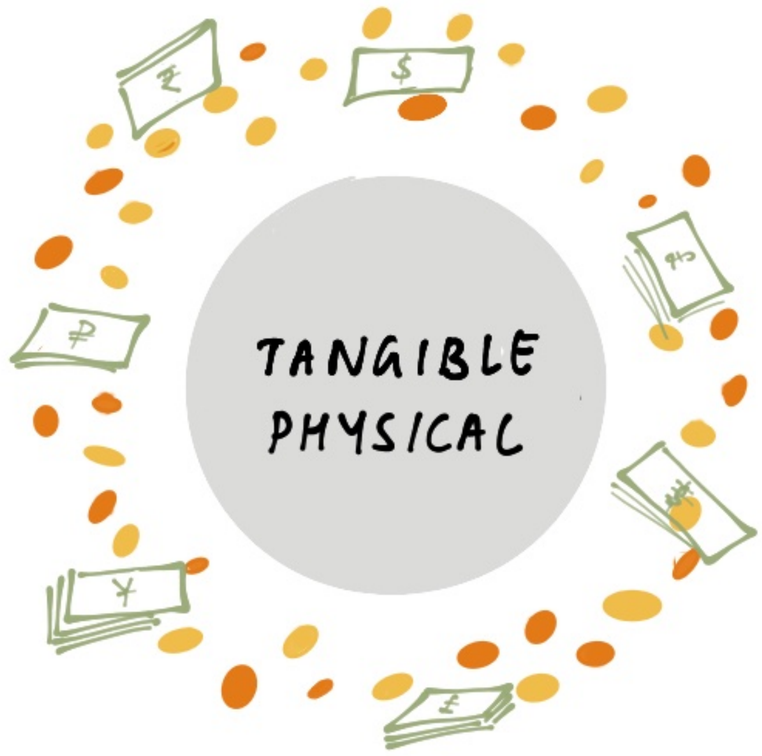
MONEY



ELECTRONIC DEPOSITS

CHEQUES

CURRENCY



NOTES

COINS

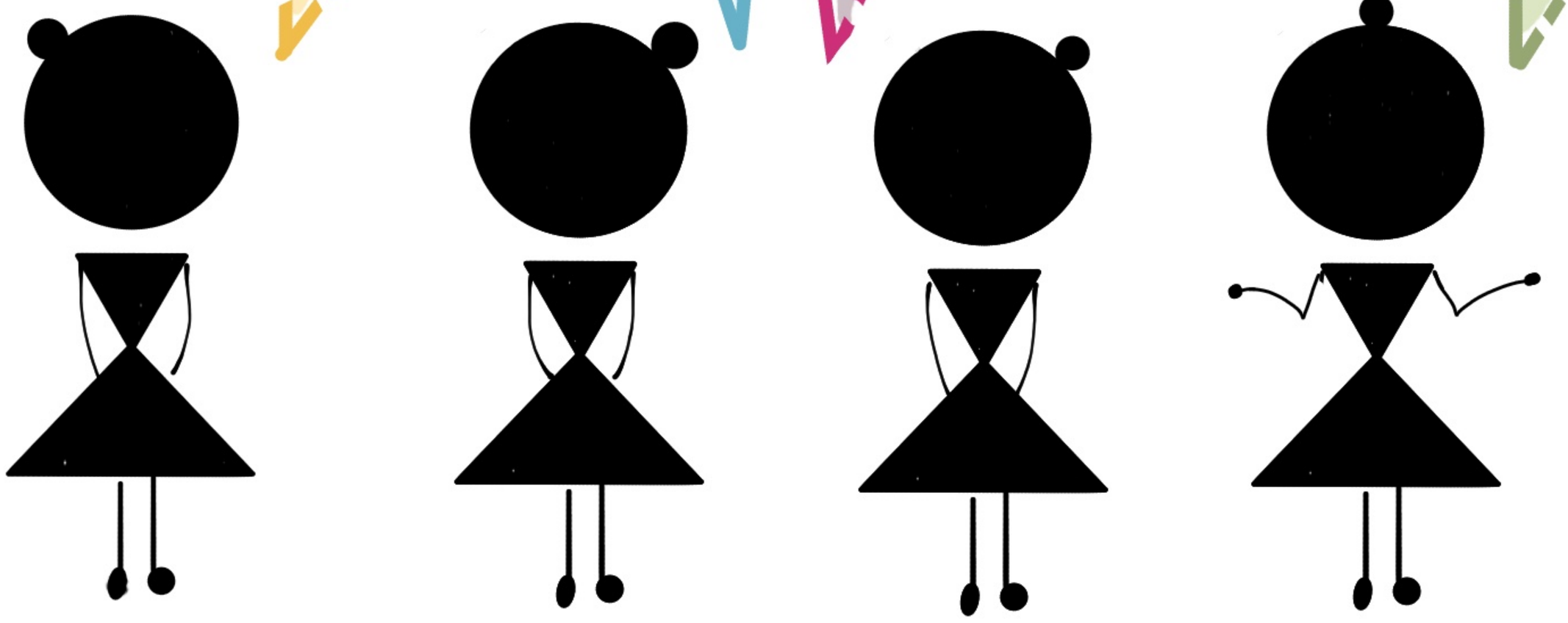
HARD TO COUNTERFEIT

GOVERNMENT-BACKED MONEY IS CALLED FIAT MONEY

GOLD OR SILVER IS COMMODITY MONEY

CURRENCY IS LESS THAN 5% OF ALL MONEY

THAT MAKES BITCOIN CRYPTO**MONEY**?!



MONEY IS

VALUABLE AND SCARCE



YET NOT FINITE IN SUPPLY

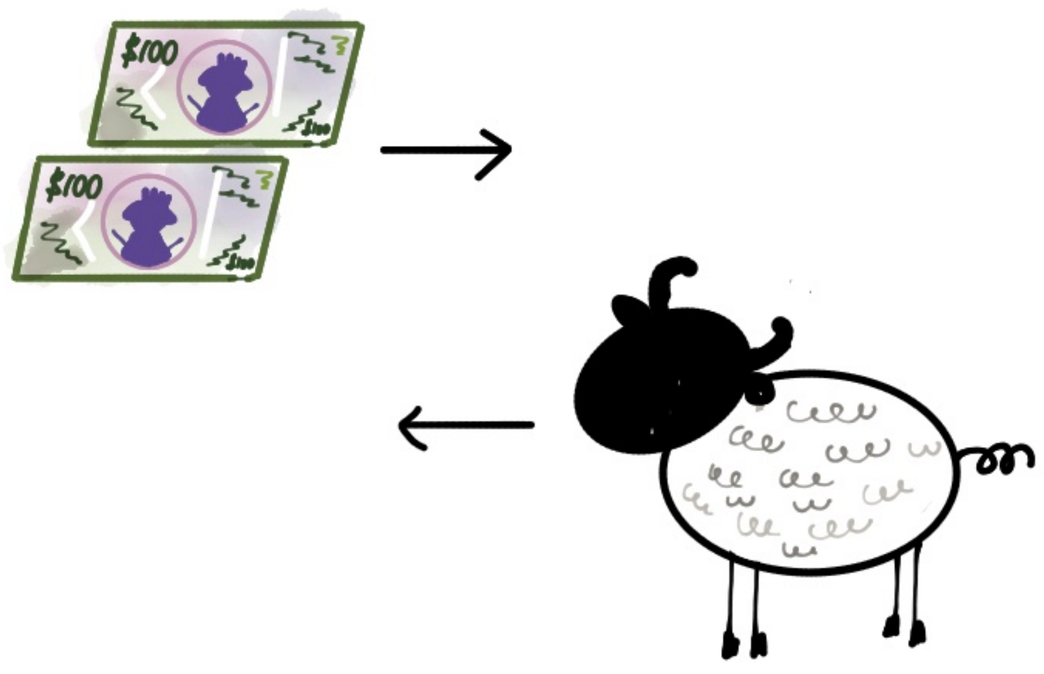
PORTABLE AND DIVISIBLE



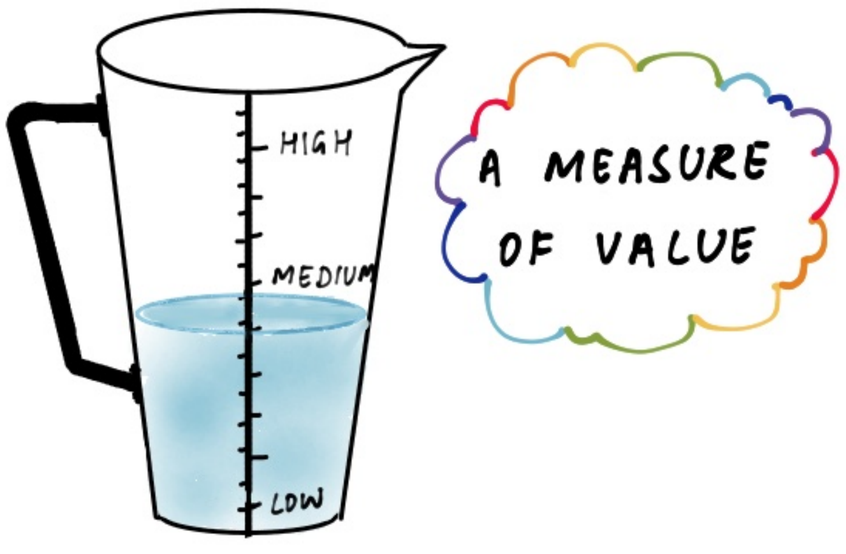
A STORE OF VALUE



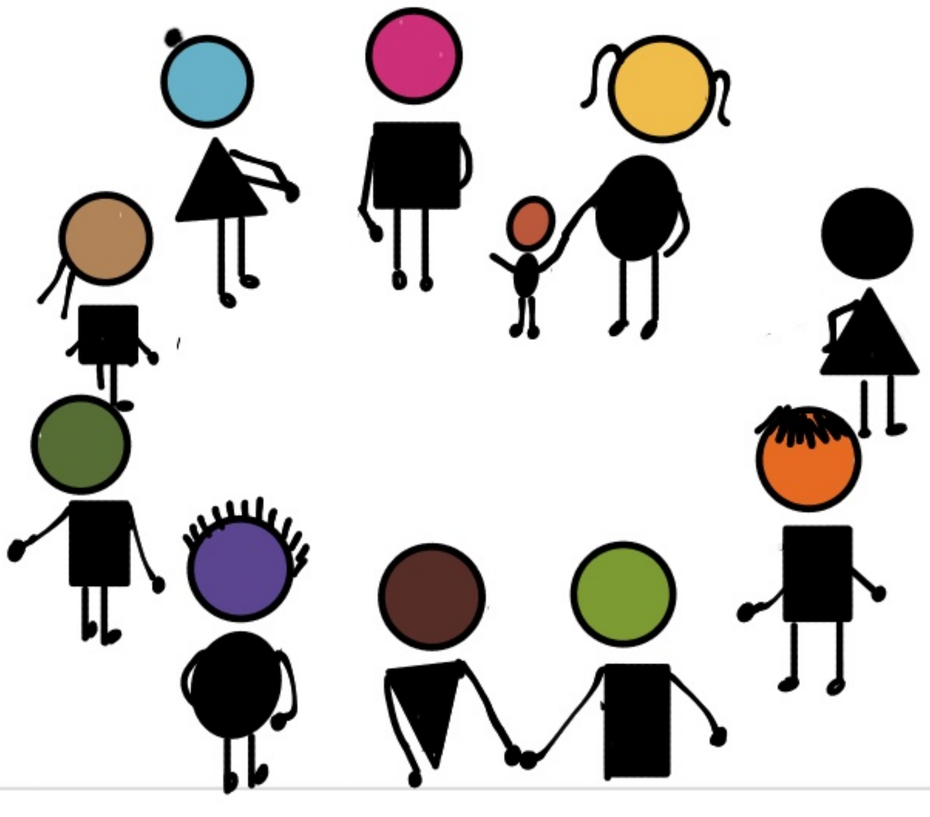
A MEDIUM OF EXCHANGE



A UNIT OF ACCOUNT



A SOCIAL CONSTRUCT



DIGITAL CURRENCY

DIGITAL CURRENCY (NOT A PERFECT TERM) IS USED TO REFER TO DIGITAL MONEY/ASSETS THAT EXIST ONLY IN ELECTRONIC FORM.

THERE ARE BROADLY 3 KINDS OF DIGITAL CURRENCIES



VIRTUAL CURRENCY

USES 'MONEY'/TOKENS CONTROLLED BY DEVELOPERS, ALGORITHMS e.g. GAMING



CRYPTOCURRENCY

USES CRYPTOGRAPHY TO SECURE/VERIFY TRANSACTIONS - MOSTLY UNREGULATED

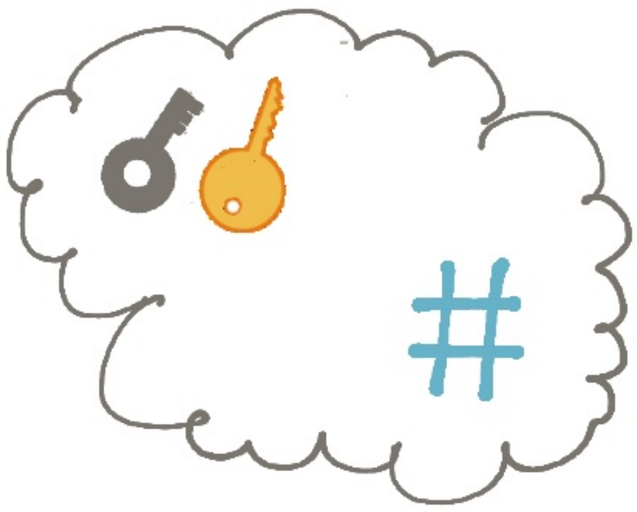


CENTRAL BANK DIGITAL CURRENCY

USED AND REGULATED LIKE FIAT MONEY AND ENABLES DIRECT INTERACTION BETWEEN GOVERNMENT & CITIZEN

CRYPTOCURRENCY

A DIGITAL TOKEN/ASSET/MONEY

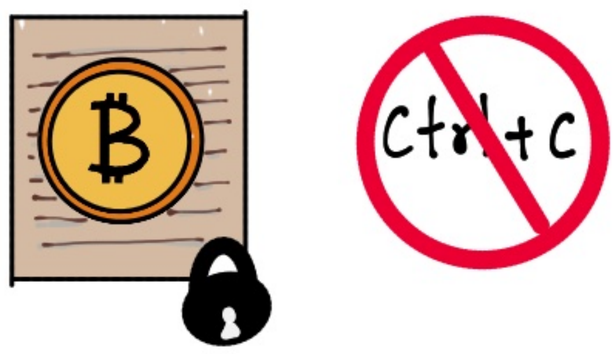




SECURED BY CRYPTOGRAPHY

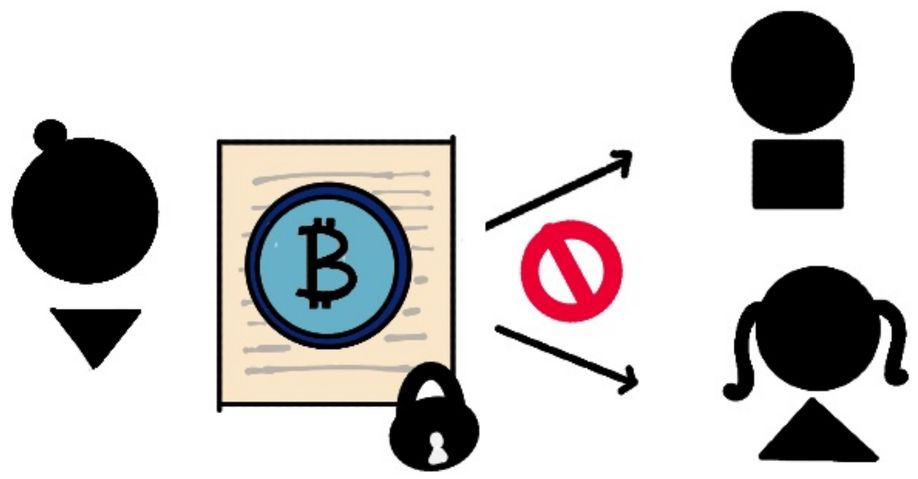
VERIFIED VIA A DIGITAL LEDGER

HARD TO COUNTERFEIT



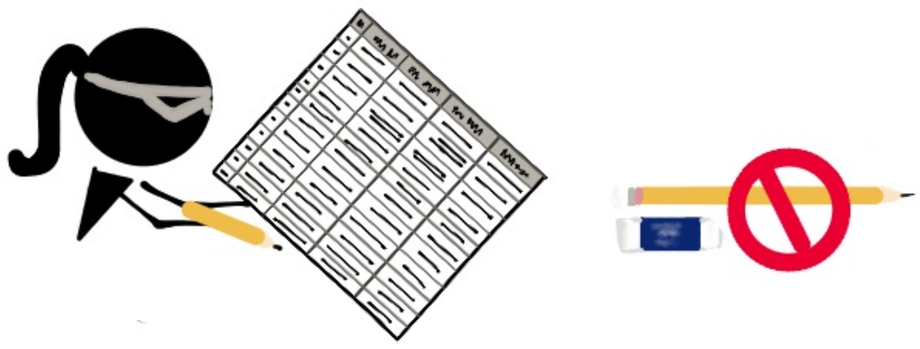
ie. MAKE A COPY

HARD TO DOUBLE-SPEND



ie. ISSUING THE SAME CRYPTOCURRENCY TO 2 PARTIES

HARD TO TAMPER



ie. EDIT/ALTER PREVIOUS ENTRIES. AKA IMMUTABLE

AS WITH DIGITAL CURRENCY

- INSTANT TRANSFER

  OVER THE INTERNET

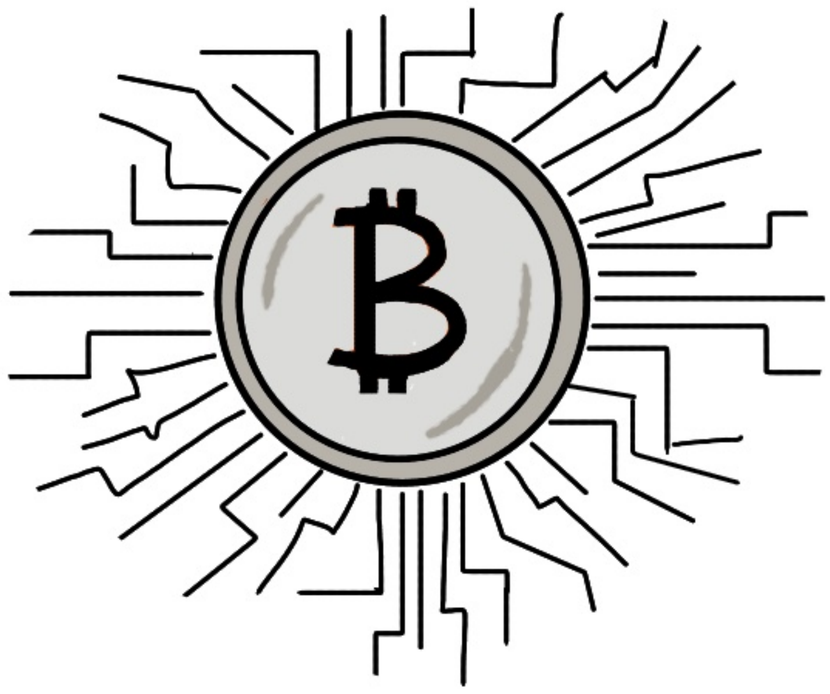
  ACROSS BORDERS

- NO DISTRIBUTION COST

A BLOCKCHAIN-BASED CURRENCY

BITCOIN IS THE FIRST CURRENCY
BUILT ON BLOCKCHAIN TECHNOLOGY

BITCOIN IS
A BLOCKCHAIN

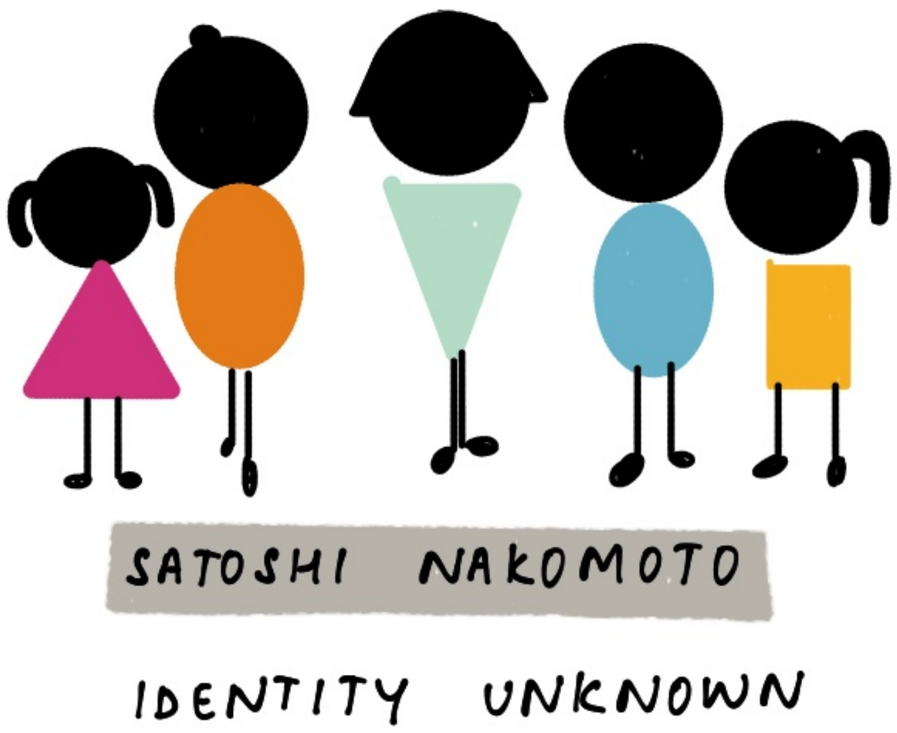


bitcoin IS ALSO
THE CURRENCY

-CRYPTO-CURRENCY

BLOCKCHAIN IS NOT = BITCOIN

THE IDEA WAS PUBLISHED
IN A PAPER IN 2008
UNDER THE NAME OF
SATOSHI NAKOMOTO



SATOSHI NAKOMOTO

IDENTITY UNKNOWN

2008

Satoshi Nakomoto
www.bitcoin.org

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.

p.s. It is open source.

BITCOIN WASN'T THE FIRST IDEA

BITCOIN STANDS FIRMLY ON THE SHOULDERS OF THESE GIANTS WHO HAD THOUGHT ABOUT HOW MONEY COULD BE KEPT OR MOVED OVER THE INTERNET (but didn't quite succeed)

DAVID CHAUM - 1989

DIGICASH

IDEA FOR ANONYMOUS TRANSACTIONS USING 'BLIND SIGNATURES'

ADAM BACK - 1997

HASH CASH

IS A PROOF-OF-WORK ALGORITHM TO LIMIT ATTACKS THAT AIM TO CRASH A SYSTEM BY OVERLOAD

NICK SZABO - 1998

BIT GOLD

A CONCEPT FOR DECENTRALISED VIRTUAL CURRENCY. PROTOCOLS SIMILAR TO BITCOIN!

WEI DAI - 1998

B MONEY

A PAPER ON ELECTRONIC CURRENCY: ANONYMOUS AND DISTRIBUTED, WITH CONTRACTS

OTHERS

MONDEX

CYBERCASH

E GOLD

LUCRE

M PESA

LIBERTY RESERVE

BITCOIN ISN'T THE LAST IDEA EITHER

THERE ARE ~10,000 CRYPTOCURRENCIES & GROWING AS OF 2023

- ALGORAND
- CARDANO
- DOGECOIN
- ETHEREUM
- GOLEM
- ICON
- LITECOIN
- MONERO
- NANO
- POLKADOT
- RIPPLE
- STRATIS
- TETHER
- XRP
- ZCASH

THEY CAN BE ACQUIRED THROUGH EXCHANGES/APPS LIKE...

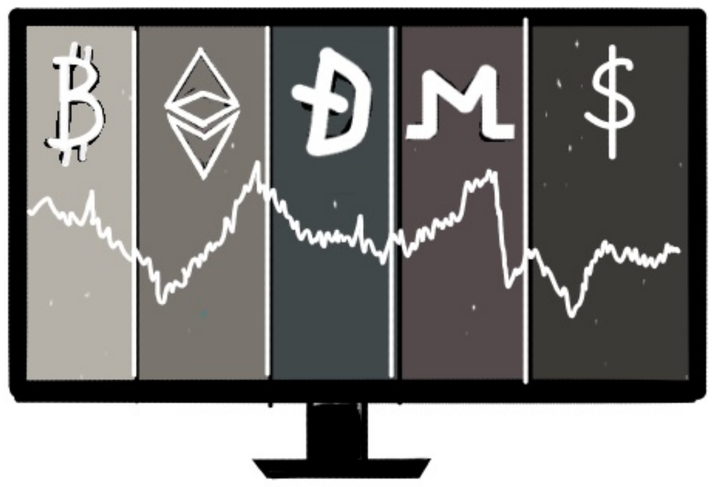
- COINBASE
- BINANCE
- UPHOLD
- KRAKEN
- GEMINI
- BITSTAMP
- CRYPTO.COM
- OKX
- HUOBI
- KUCOIN
- BINGX
- BYBIT
- BITFINEX
- PHEMEX
- LBANK
- UPBIT
- BITGET
- MEXC GLOBAL
- GATE.IO
- COINSTORE
- TIDEX
- BITSTAMP
- LATOKEN
- EXMO
- MAX MAICOIN
- OKCOIN
- INDODAX
- BKEX
- XT.COM
- P2B

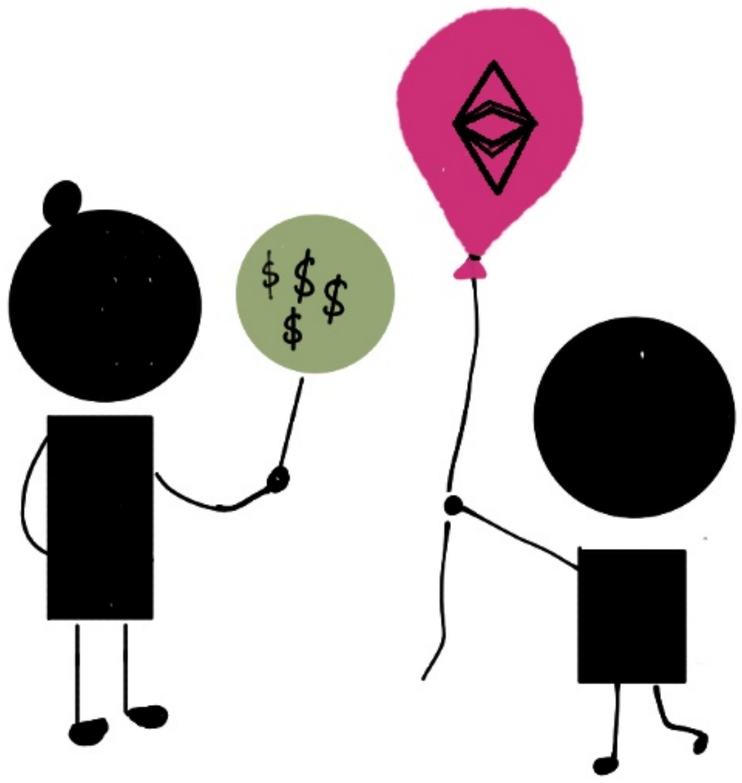
THE LIST GOES ON

... WHICH MAKE MONEY FROM TRADING FEES, LOYALTY TOKENS, LISTING FEES, INITIAL PUBLIC OFFERING FEES, MARKET MAKING, ADVERTISING ETC.

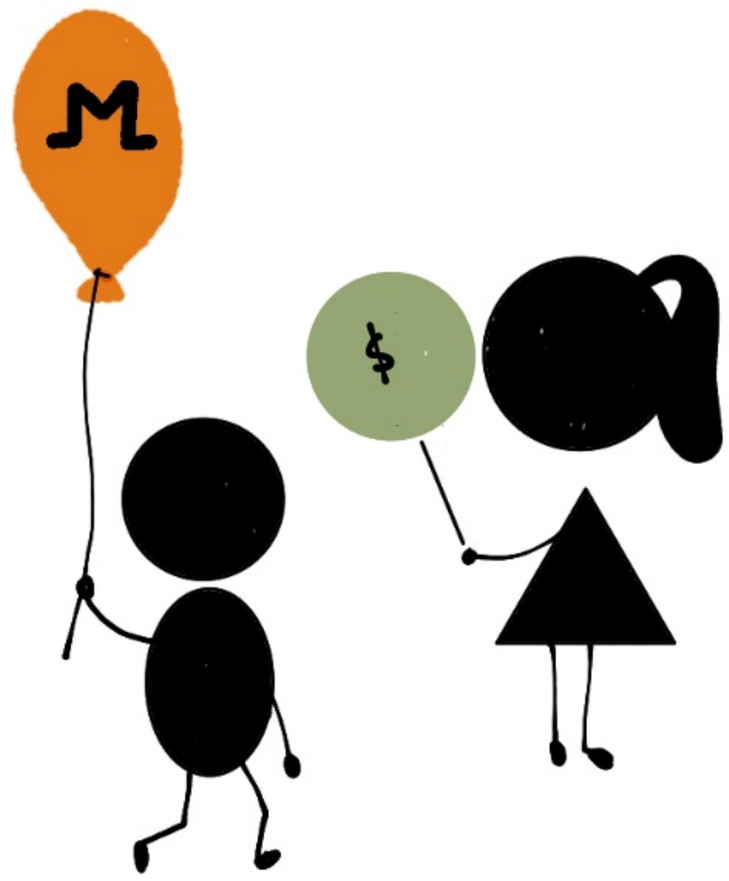
ON EXCHANGES - 1

CRYPTOCURRENCIES ARE TRADED ON PLATFORMS CALLED EXCHANGES WHERE PEOPLE COME TO ...



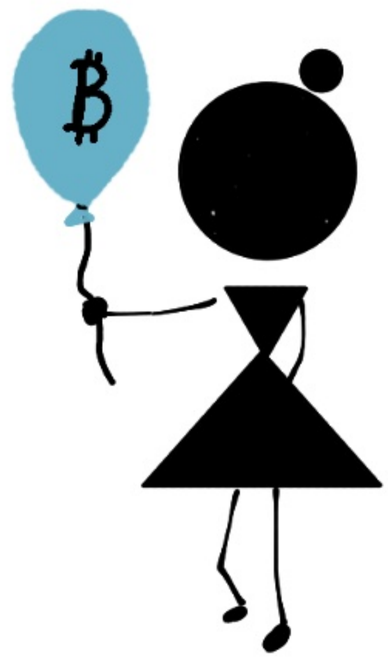


BUY CRYPTO



SELL CRYPTO





EXCHANGE ONE CRYPTO FOR ANOTHER

ON EXCHANGES - 2

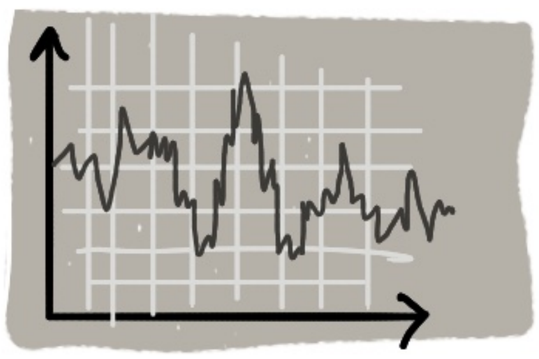
SOME ARE CENTRALISED

- OVERSEEN BY AN OPERATOR
- MAINTAIN KEYS TO ASSETS
- NEED IDENTITY PROOFS
- MAY GIVE COMPENSATION
- NEED $ DEPOSITS

SOME ARE NOT CENTRALISED

- RUN ON USER OWNED NODES
- USERS MANAGE OWN KEYS
- CAN USE PSEUDO IDENTITY
- PEER TO PEER EXCHANGE

EXCHANGES ARE NOT REGULATED OR LEGAL IN EVERY COUNTRY



SPECULATION/VOLATILITY

HAVE ~~COULD~~ CAUSED

BANKRUPTCIES



EXCHANGES MAY SIMPLY

LOCK FUNDS

WITHOUT RETURNING



EXCHANGE COULD BE

SHUT DOWN

BY GOVERNMENTS

BITCOIN

IN THIS NEW SECTION, WE LOOK AT BITCOIN TO UNDERSTAND HOW A BLOCKCHAIN FUNCTIONS IN PRACTICAL TERMS.

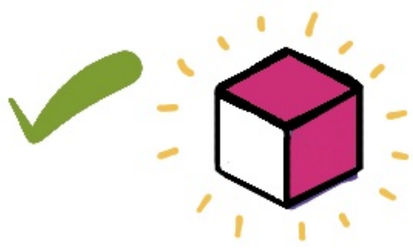
THE BITCOIN LANDSCAPE

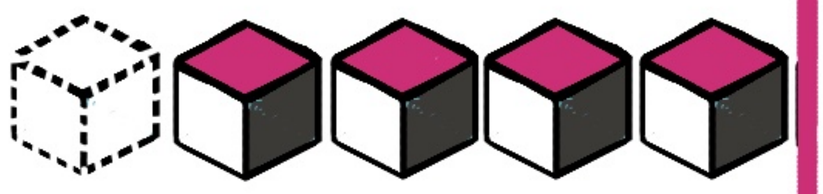


BITCOIN, REWARDS & WALLETS







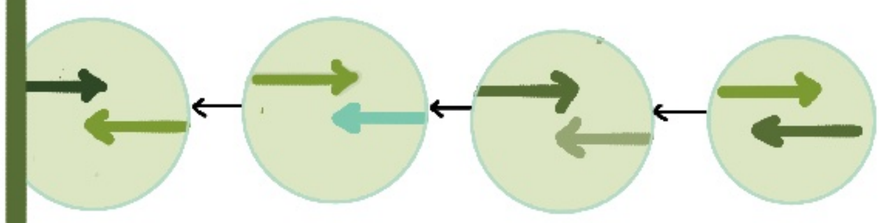


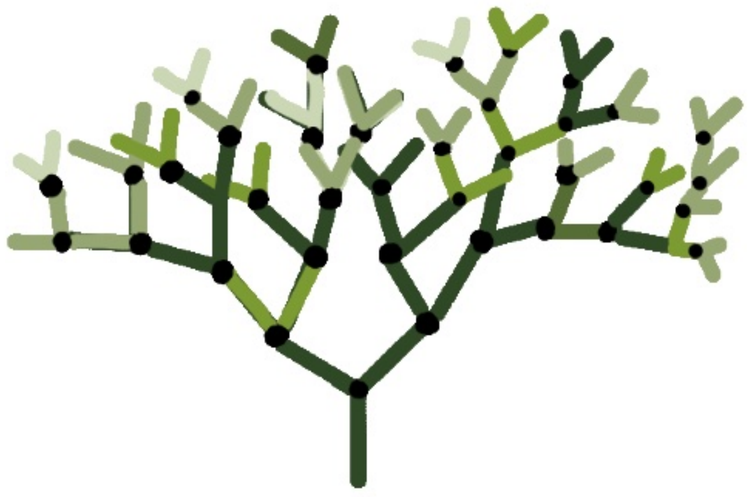
PROOF OF WORK





MINERS, NODES AND MINING



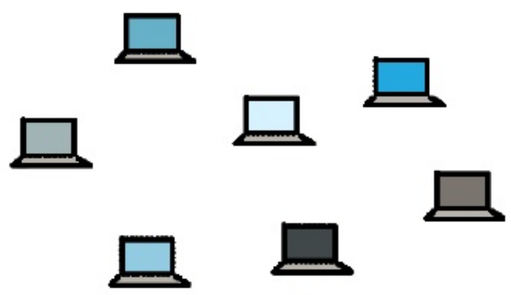


TRANSACTIONS, MERKLE TREES AND BLOCKS

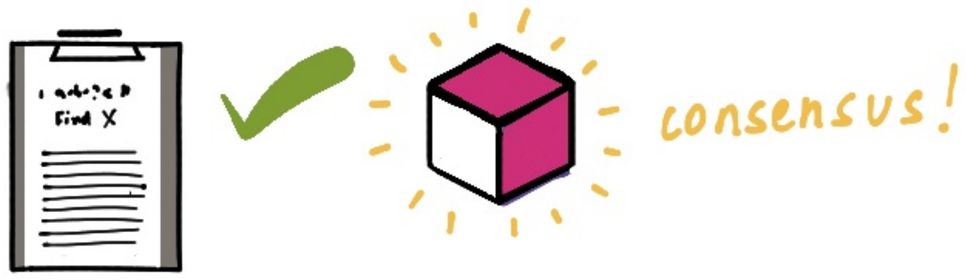
PATH WE TAKE



TRANSACTIONS



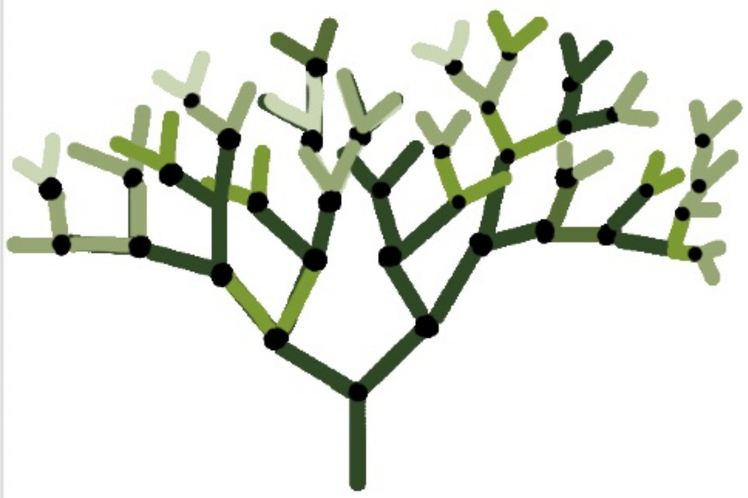
MININA



CONSENSUS



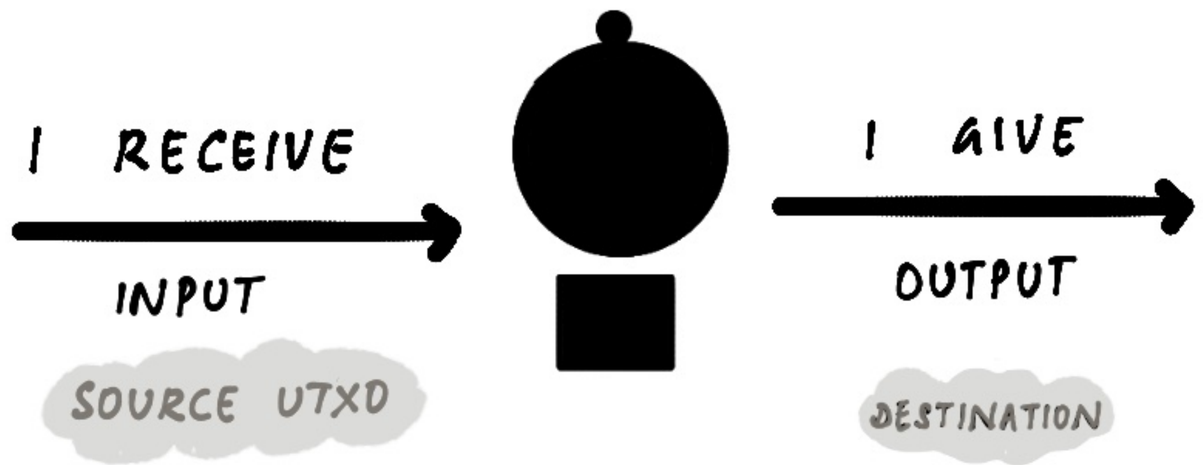
THAT EARNS REWARDS



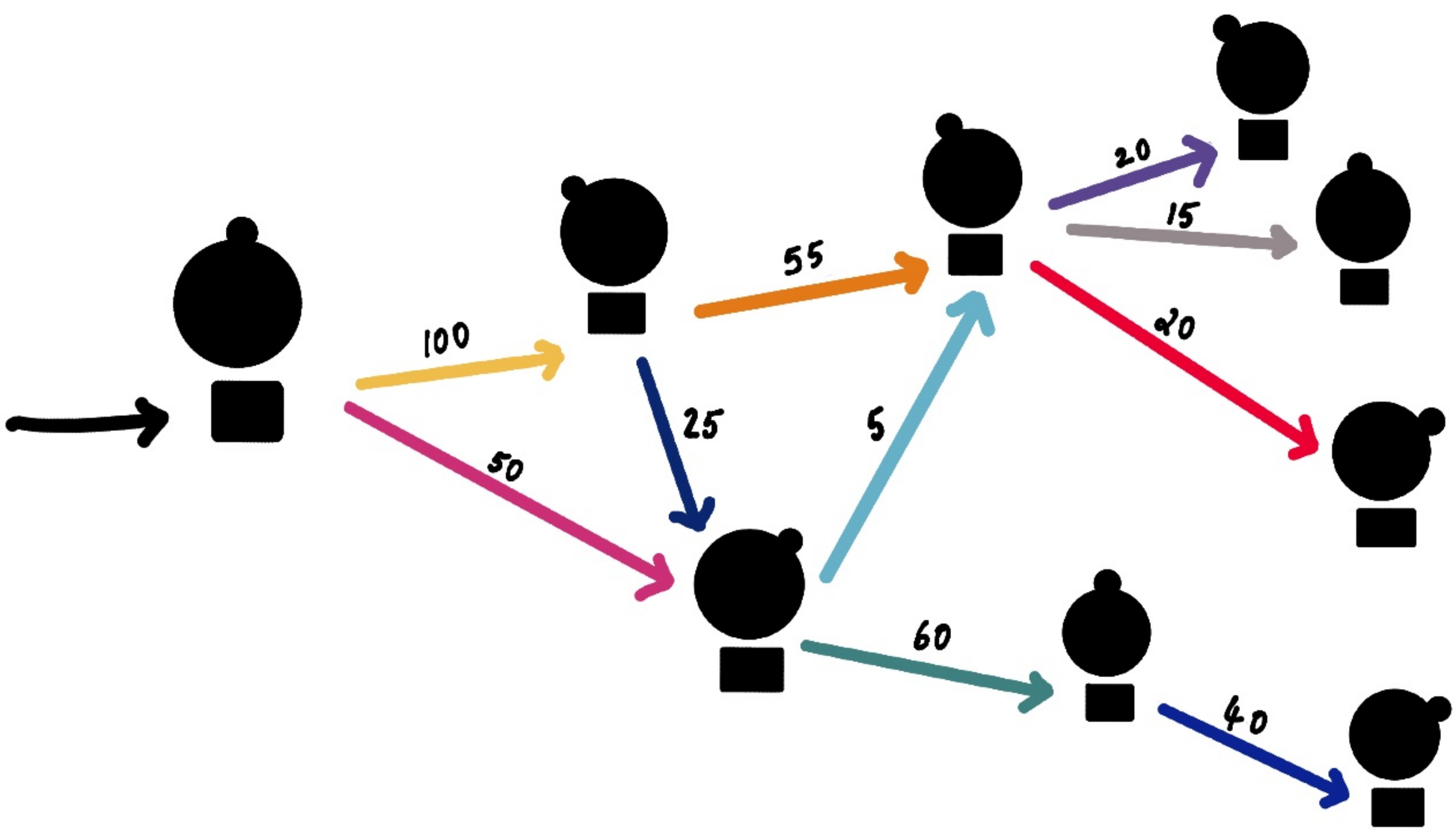
TRANSACTIONS, MERKLE TREES AND BLOCKS

WHAT IS A TRANSACTION?

A TRANSACTION, VERY SIMPLY:



A TRANSACTION IS A VALUE TRANSFER FROM SENDER TO RECEIVER



MORE SPECIFICALLY,

TRANSACTIONS TRANSFER RIGHTS FROM SENDER TO RECEIVER

EXPLORE A TRANSACTION

	TRANSACTION ID	
INPUT →	PREVIOUS TRANSACTIONS OF ASSET RECEIVED	SHE GAVE 60
OUTPUT →	AMOUNT OF ASSET TO TRANSFER	40
→	ACCOUNT OWNER(S) WHO WILL RECEIVE ASSETS	YOU
→	ANY CHANGE TO BE RETURNED TO SELF	19
	FEES (IMPLICIT)	INPUTS - OUTPUTS

THESE ARE THE MAIN ATTRIBUTES OF A TRANSACTION

WHEN I RECEIVE BITCOIN

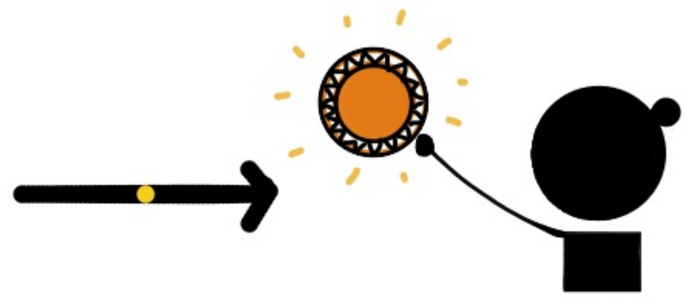
WHEN I RECEIVE BITCOIN



I CAN THEN 'S(P)END' IT

BY UNLOCKING ITS VALUE

THIS SPENDABLE OUTPUT ...

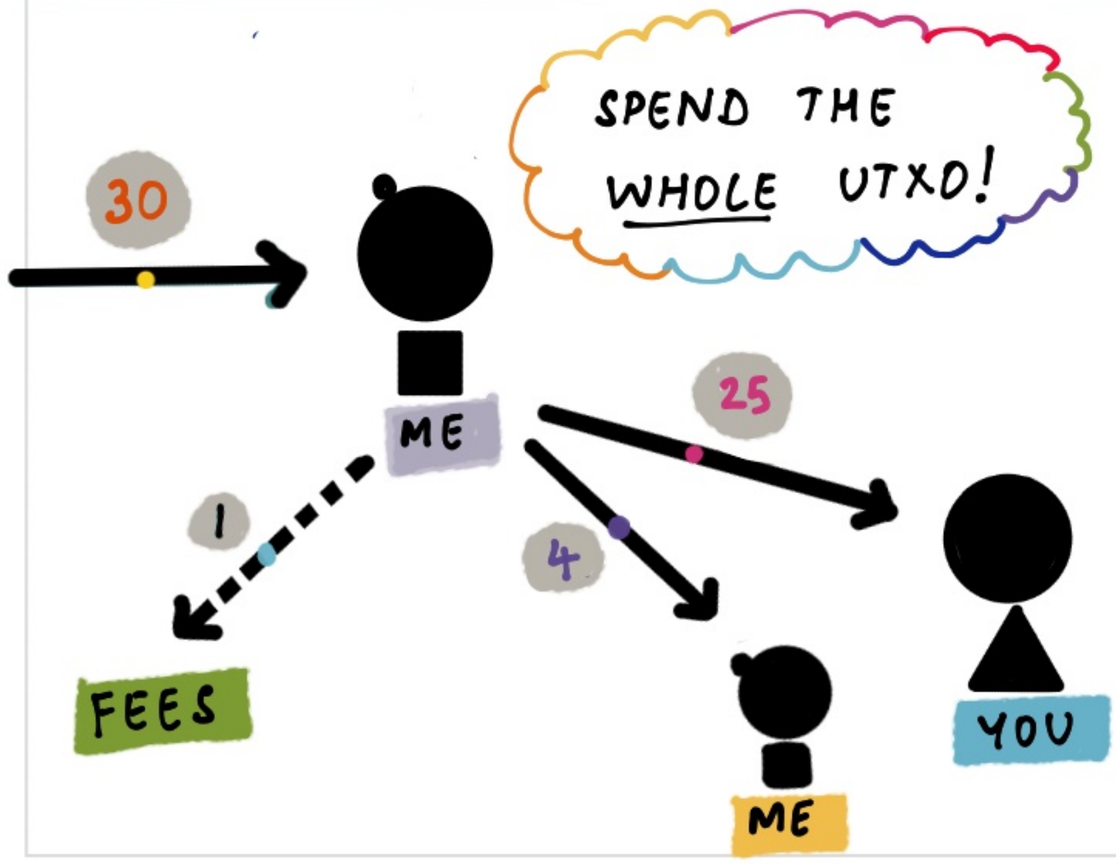


OF A TRANSACTION IS CALLED

UTXO OR

UNSPENT TRANSACTION OUTPUT

TO SEND 25 BITCOINS

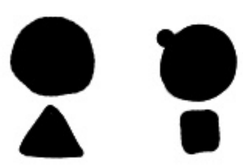


TO SPEND BITCOIN, SPECIFY ...



THE AMOUNT OF BITCOIN

TO TRANSFER



TO WHO



WHEN THE AMOUNT

WILL BE AVAILABLE

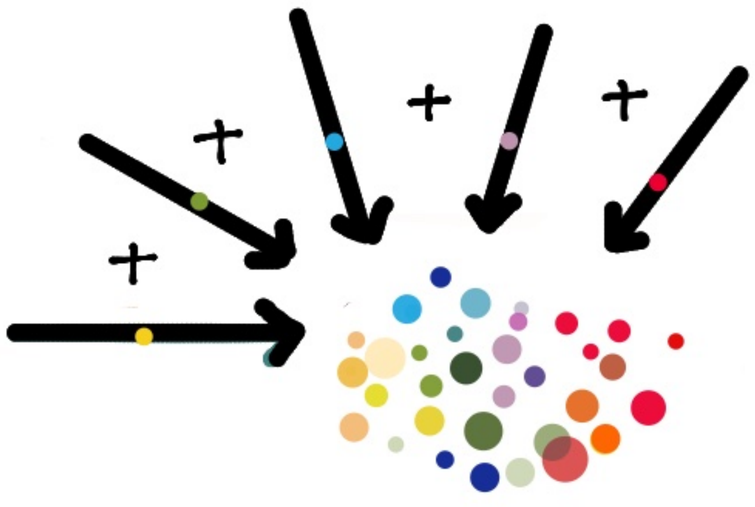
I CANNOT UN-SEND BITCOIN



TRANSACTIONS

ARE IRREVERSIBLE

MY ACCOUNT BALANCE IS...

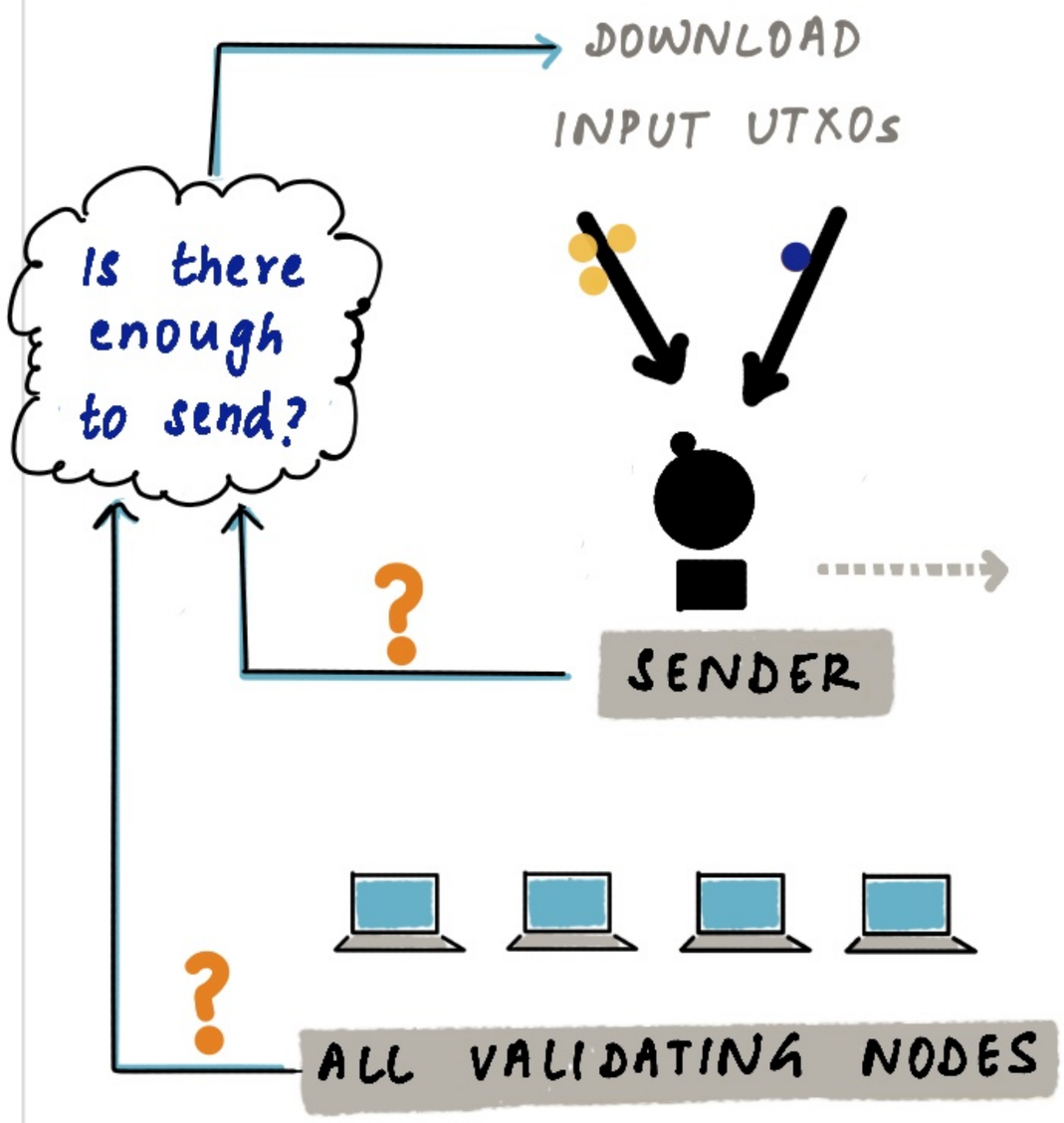


...THE SUM OF ALL UTXOs

ACROSS ALL TRANSACTIONS

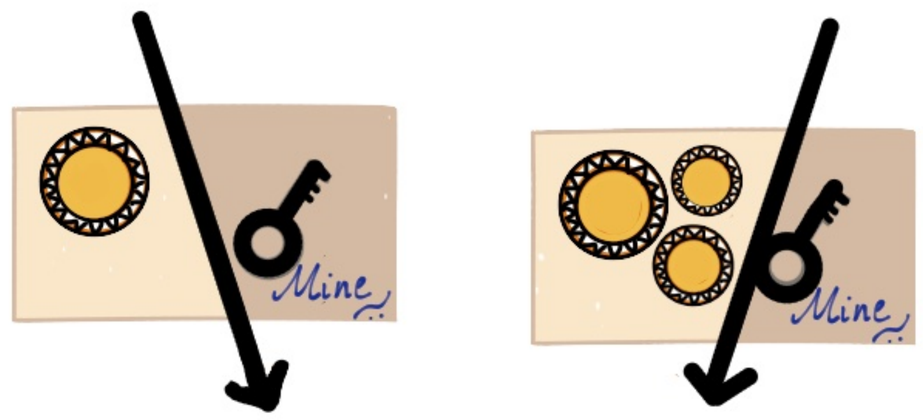
WHEN I SEND BITCOIN, I...

RETRIEVE INPUT UTXOs



SIGN EVERY INPUT...

... BEFORE SENDING IT



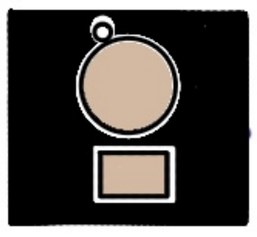
- ✓ PROVING MY OWNERSHIP
- ✓ AUTHORISING SPENDING
- ✓ AND I CANNOT DENY IT!

LOCK/UNLOCK VALUE

THROUGH SCRIPTS THAT



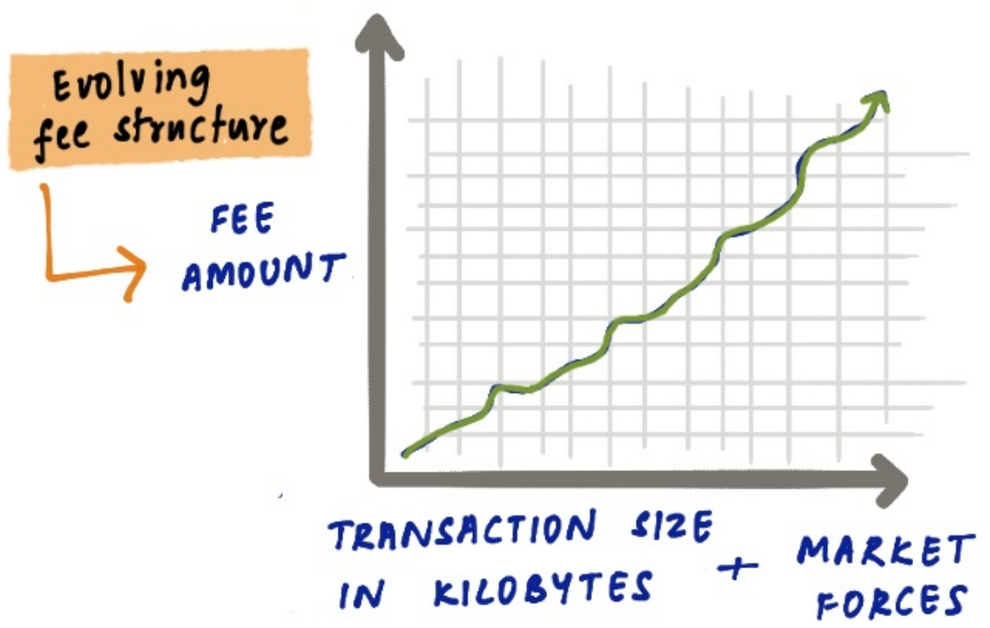
SET AN EARLIEST VALIDITY TIME FOR IT



VERIFY IDENTITY/OWNERSHIP

OF A TRANSACTION

PAY REQUIRED FEES (IMPLICIT)



FEES = SUM(INPUTS) − SUM(OUTPUTS)

several steps to calculate

High-fee transactions are prioritised for adding to next block

ADDRESS, WALLET & KEYS

BITCOIN ADDRESS

BITCOIN ADDRESS

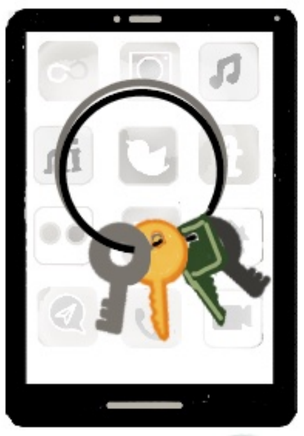
IS AN IDENTIFIER

REPRESENTS THE RECEIVER OF BITCOIN

MAKES PUBLIC TRANSACTIONS SEEM ANONYMOUS

IS THE ENCODED DOUBLE HASH OF A PUBLIC KEY

WALLET



WALLET IS A CONTAINER FOR PRIVATE KEYS

GIVES ACCESS TO BITCOIN

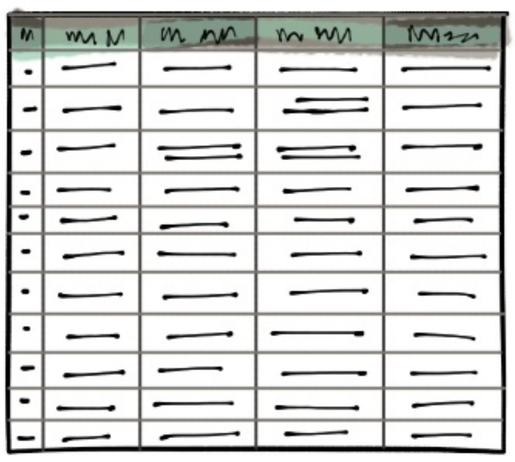
MANAGED WITH A PSEUDONYM

OFTEN HELD BY A THIRD PARTY (HIGH RISK)

THE ILLUSION OF ANONYMITY

TRANSACTIONS ON A BLOCKCHAIN APPEAR ANONYMOUS

IT IS POSSIBLE TO TRACE BITCOIN ADDRESSES TO INDIVIDUALS.



TRANSACTIONS ARE ALL PUBLICLY AVAILABLE



SOME EXCHANGES IMPLEMENT A KNOW-YOUR-CUSTOMER TO BUY CRYPTOCURRENCY

BLOCKCHAIN NETWORK ANALYSIS + KNOW YOUR CUSTOMER → TRACE PSEUDONYM TO REAL-WORLD IDENTITY

"FINANCIAL FORENSICS"

WHERE ARE TRANSACTIONS STORED?

EVERY

NODE

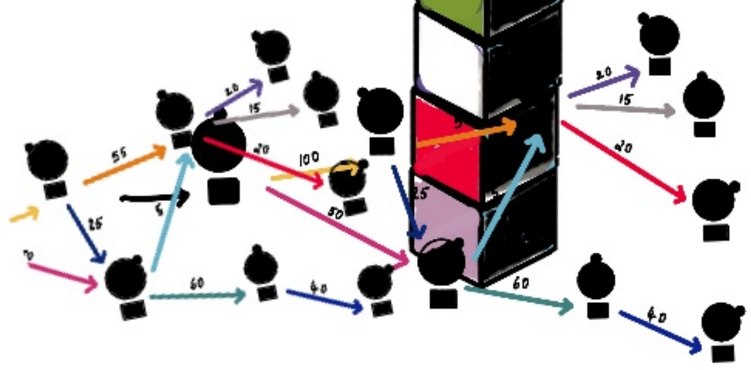
CAN

HOLD

THE TRANSACTIONS ARE

STRUCTURED DATA

HELD IN A FLAT FILE.



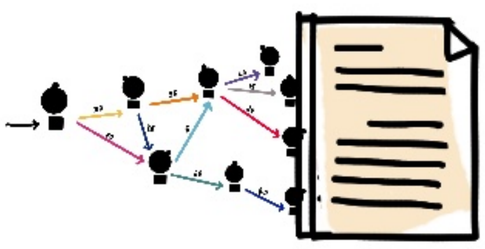
NO CENTRAL STORAGE

TRANSACTIONS

THE

OF

A COPY



THE BLOCKS HOLD

TRANSACTION HASHES —

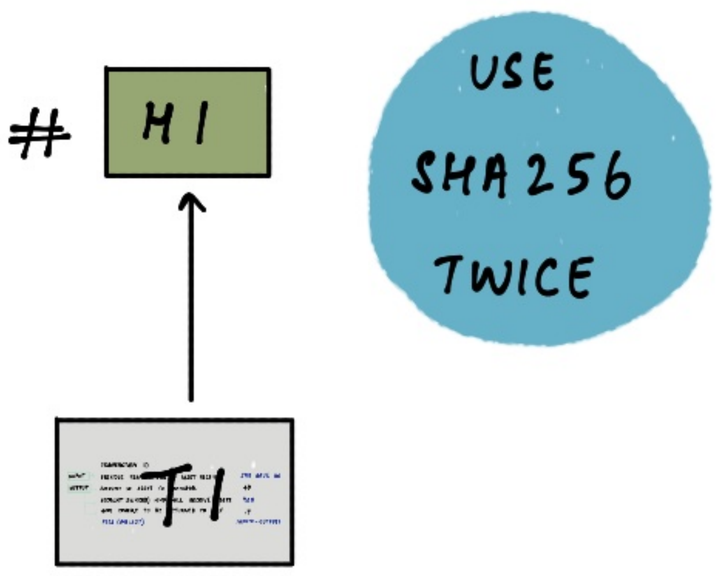
NODES CAN HOLD A COPY.

RAW TRANSACTIONS CAN BE VIEWED THROUGH INTERFACES LIKE

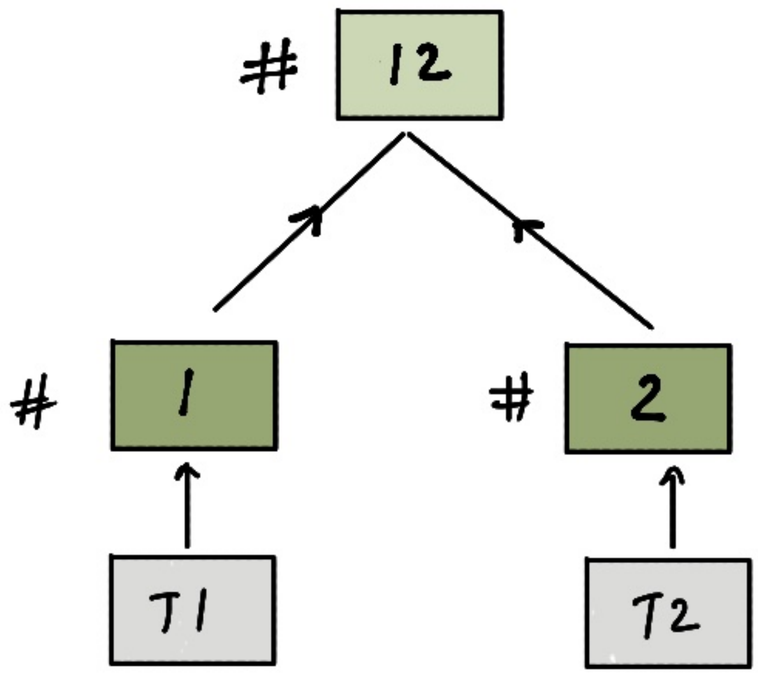
blockchain.com/explorer

TRANSACTION HASHES & MERKLE TREES

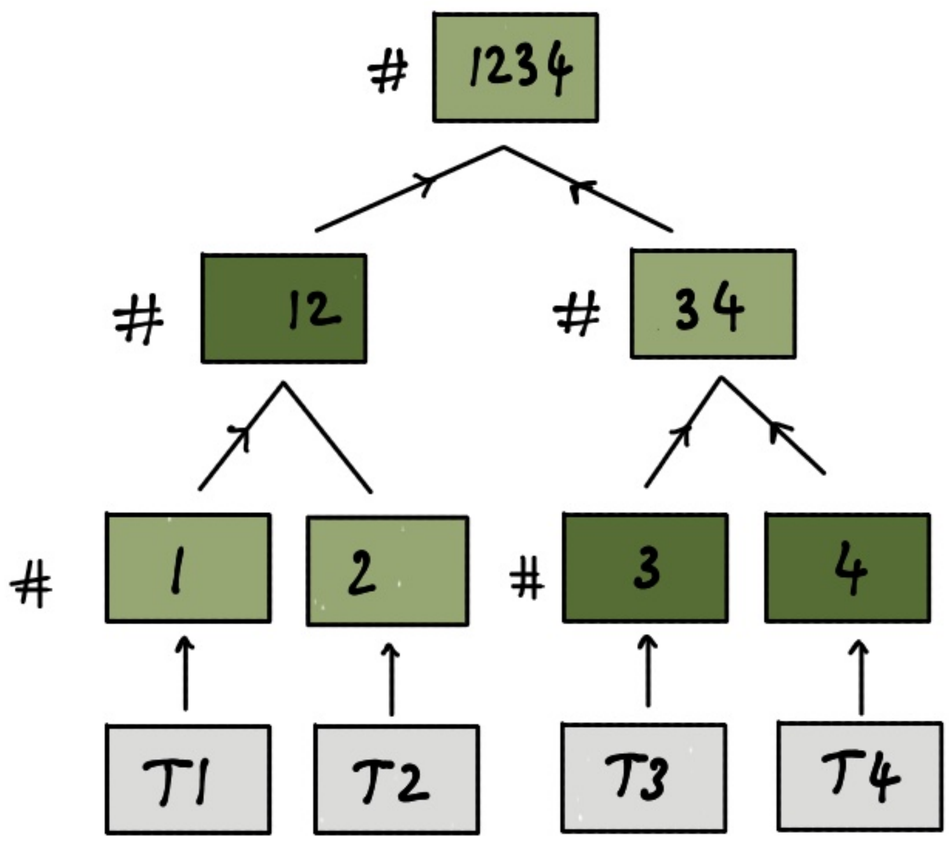
TRANSACTION AND ITS HASH



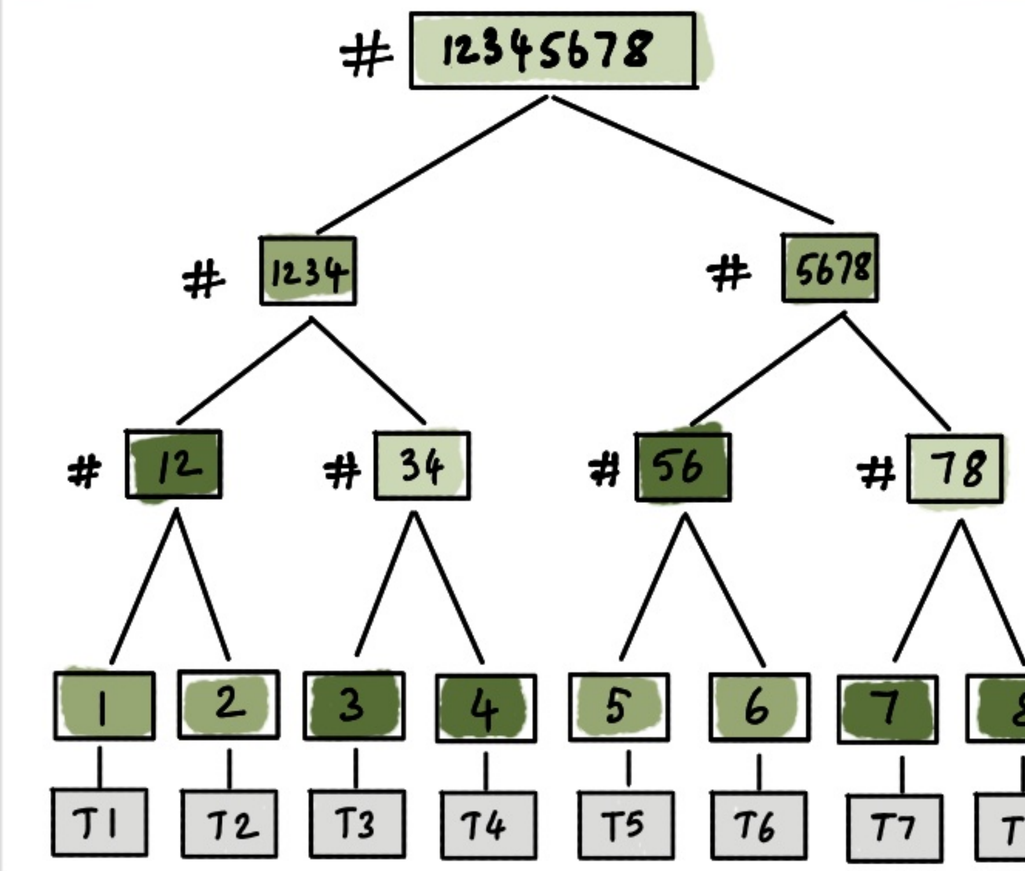
HASH OF TWO TRANSACTIONS



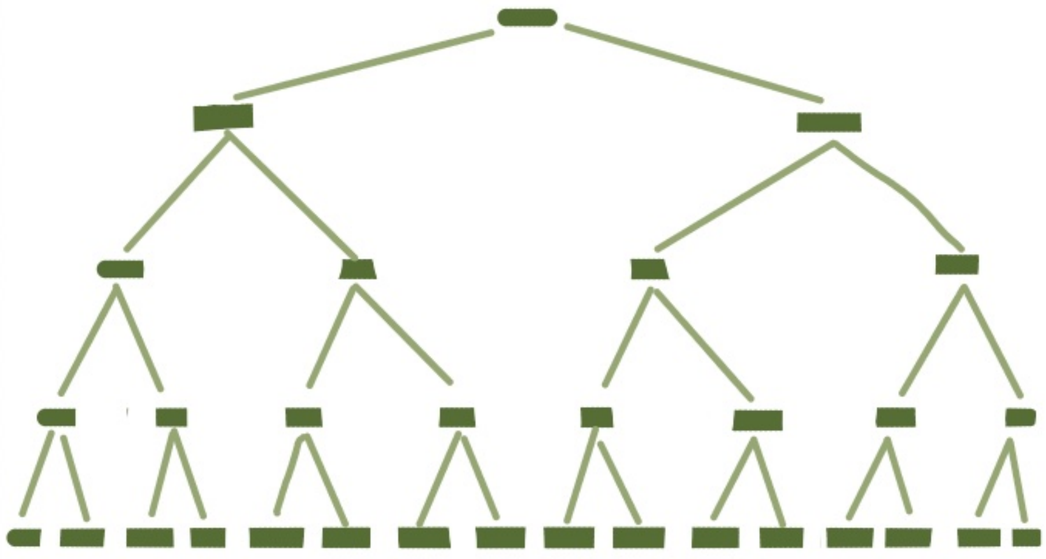
HASH OF 4 TRANSACTIONS



HASH OF 8 TRANSACTIONS



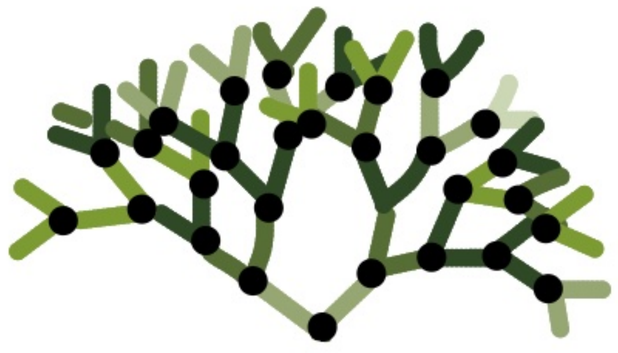
HASH OF N TRANSACTIONS



DOUBLE THE LAST, IF ODD

MERKLE TREE

THIS UPSIDE DOWN DATA TREE STRUCTURE IS THE MERKLE TREE



THE FINAL HASH = MERKLE ROOT

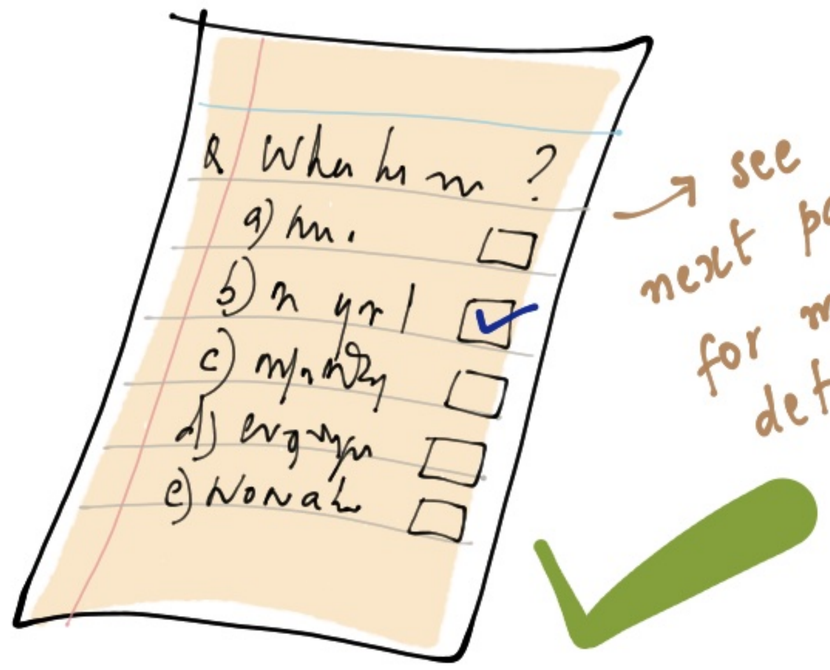
WHY MERKLE TREES?

THEY COMPRESS DATA



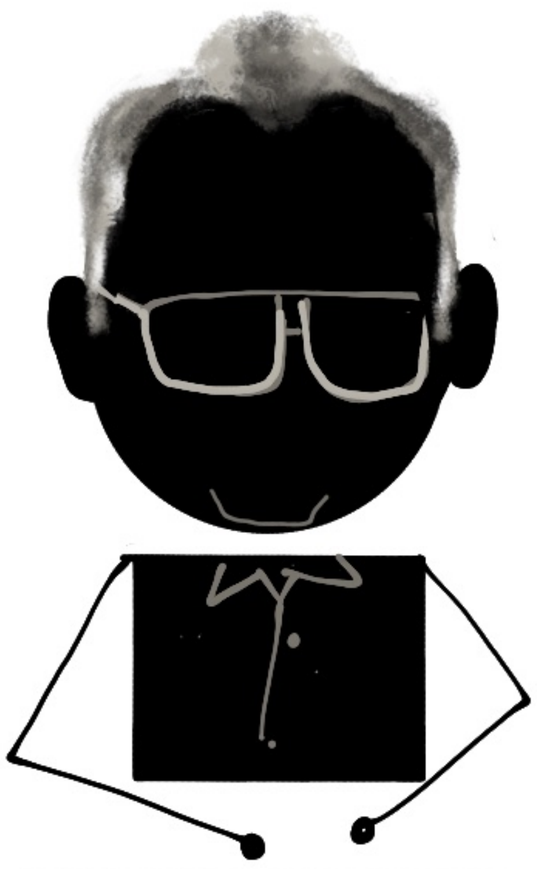
NO MATTER THE SIZE OF THE TRANSACTION DATA, THE FINAL HASH, THE MERKLE ROOT, IS 32 BYTES

THEY VERIFY TRANSACTIONS



THE HASHES LEND THEMSELVES TO VERIFICATION WITHOUT REVEALING THE TRANSACTION DETAILS

THEY ARE NAMED AFTER RALPH MERKLE...



RALPH MERKLE

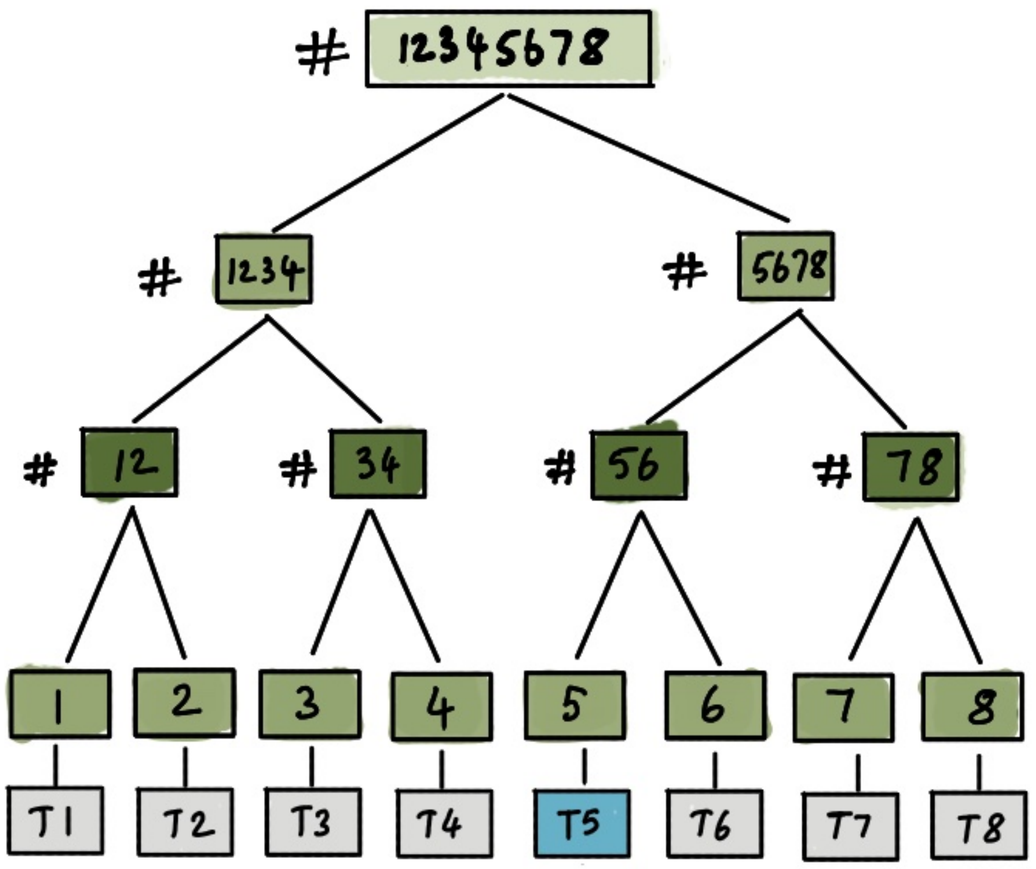
...WHO CAME UP WITH IT

CO-INVENTOR OF PUBLIC KEY CRYPTOGRAPHY

INVENTOR OF MERKLE SIGNATURES

MERKLE TREES & VERIFICATION - I

WE SAID EARLIER THAT MERKLE TREES VERIFY TRANSACTIONS.



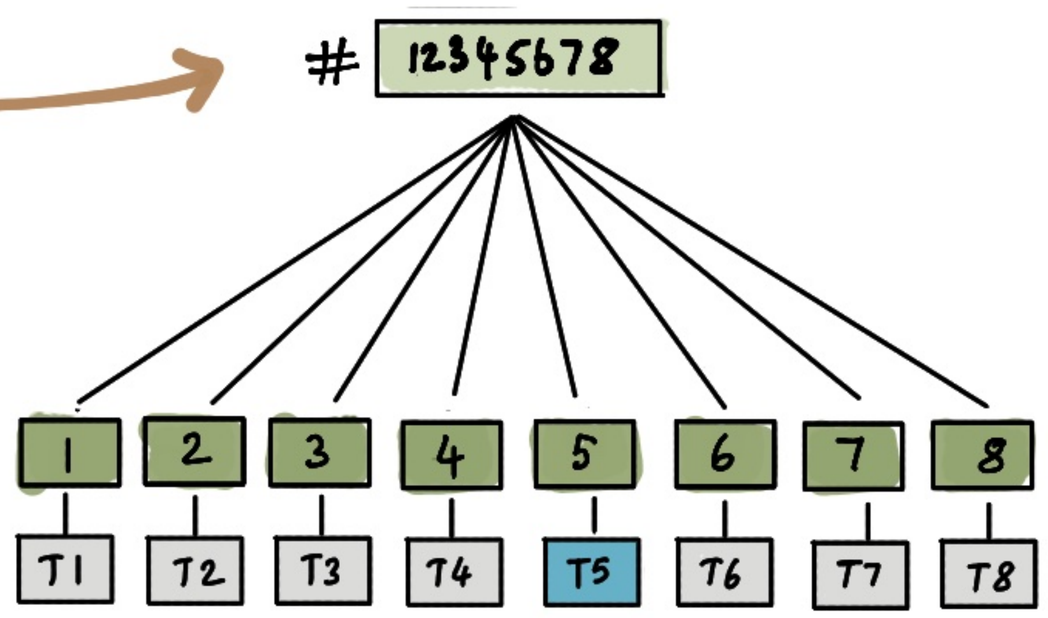
SUPPOSE

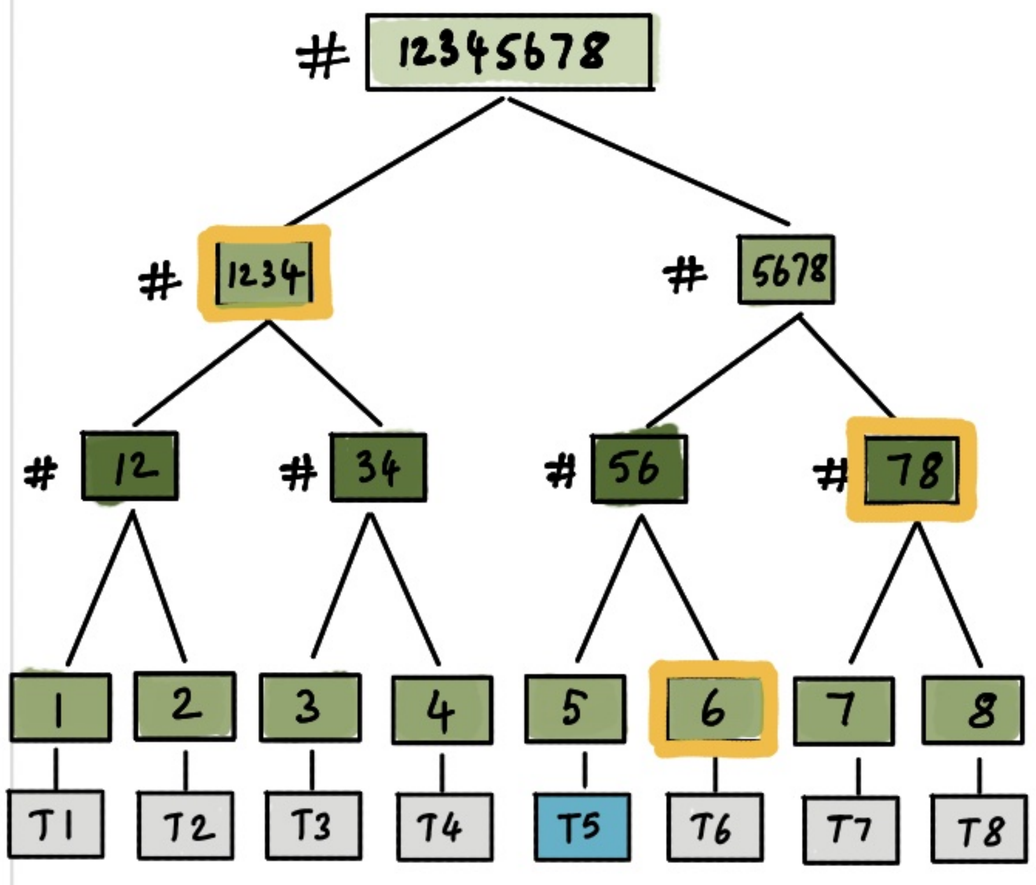
WE WANT TO CHECK IF T5 IS INCLUDED OR TAMPERED WITH IN THE ROOT.

IF THE MERKLE ROOT WAS CALCULATED THIS WAY,



WE'D HAVE TO RE-HASH ALL THE TRANSACTION HASHES AGAIN TO CHECK THE VALUE OF THE ROOT AGAINST ANOTHER COPY





THINGS ARE MORE EFFICIENT WITH THIS STRUCTURE GIVEN A MERKLE PATH OR MERKLE PROOF

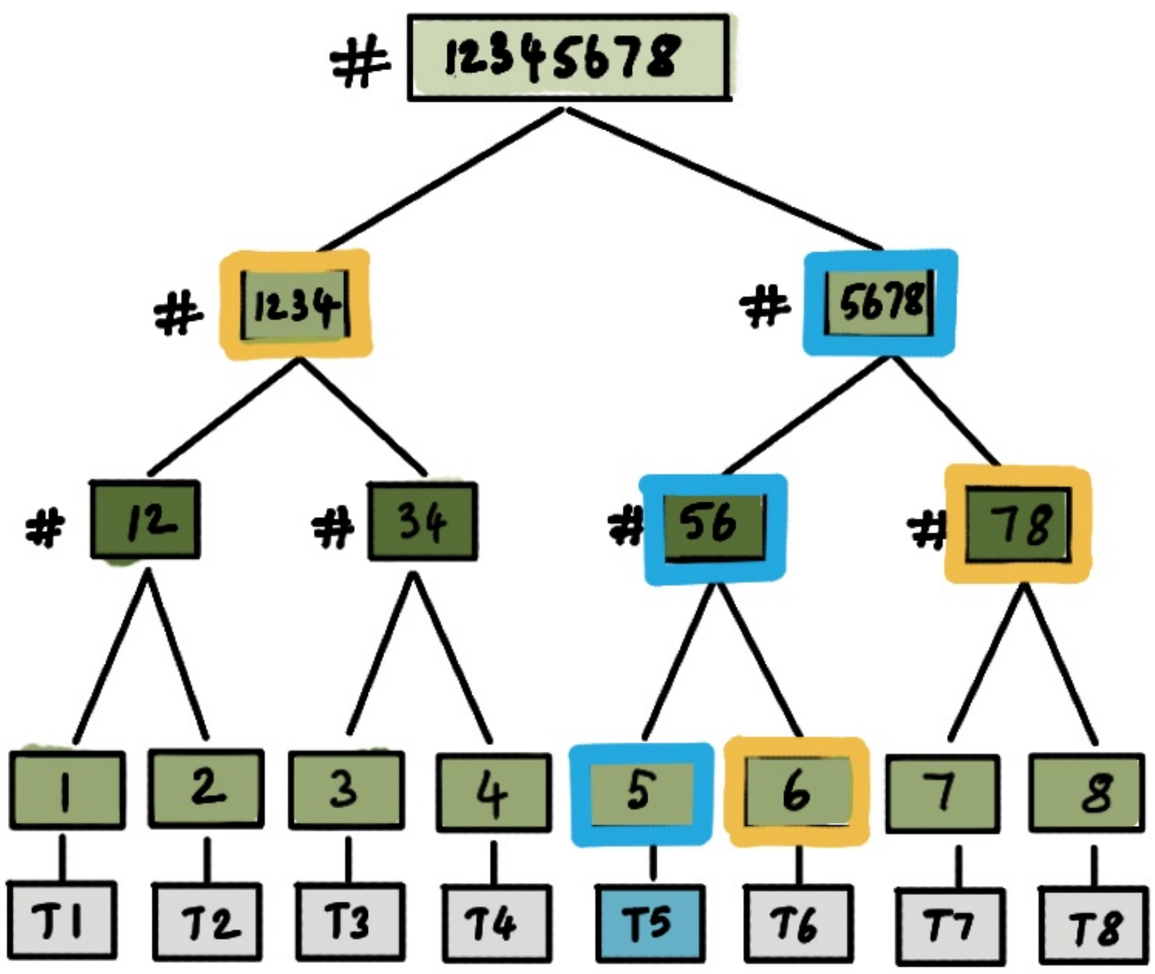
THE HASHES FORMING THE MERKLE PATH ARE IN YELLOW

MERKLE TREES & VERIFICATION - 2

MERKLE PATH OR MERKLE PROOF.

THE PATH OF HASHES THAT CONNECT A 'LEAF' NODE TO A MERKLE ROOT

IT IS THE MINIMUM NUMBER OF NODES NEEDED TO CALCULATE THE MERKLE ROOT AGAIN.



WITH THE HASHES GIVEN IN THE MERKLE PATH, WE NEED ONLY TO CALCULATE 3 ADDITIONAL HASHES TO ARRIVE AT THE ROOT

COUNT OF ADDITIONAL HASHES TO FIND, FOR N TRANSACTIONS $= \log_2(N)$

THE EFFICIENCY IS REALISED FOR A LARGE 'N', SAY 50,000, WHERE THE ADDITIONAL HASHES IS ONLY $\log_2 50{,}000 = 15.6096$ ← apply ceiling()

Note: The mathematical proof is beyond the scope of this book

BLOCK STRUCTURE

- SIZE
- HEADER (~80 bytes)
  - VERSION
  - PREVIOUS BLOCK (HEADER) HASH
  - MERKLE ROOT
  - TIMESTAMP
  - DIFFICULTY TARGET } related to Proof Of Work
  - NONCE } To be discussed later
- COUNT OF TRANSACTIONS (~2000 transactions)
- LIST OF TRANSACTIONS (~400 bytes each)

BLOCK HASH

A BLOCK HASH IS THE UNIQUE IDENTIFIER FOR A BLOCK.

IT IS :

- A CALCULATED VALUE
- THE HASH OF THE HEADER

BLOCK HEIGHT

A BLOCK'S HEIGHT IS THE DISTANCE OF A BLOCK FROM THE FIRST BLOCK.

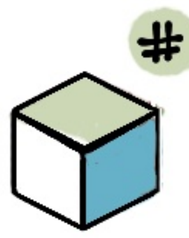
BLOCK HEIGHT IS NOT A UNIQUE IDENTIFIER.

CHAINING THE BLOCKS



TRANSACTIONS

VALID, VERIFIED



BLOCK

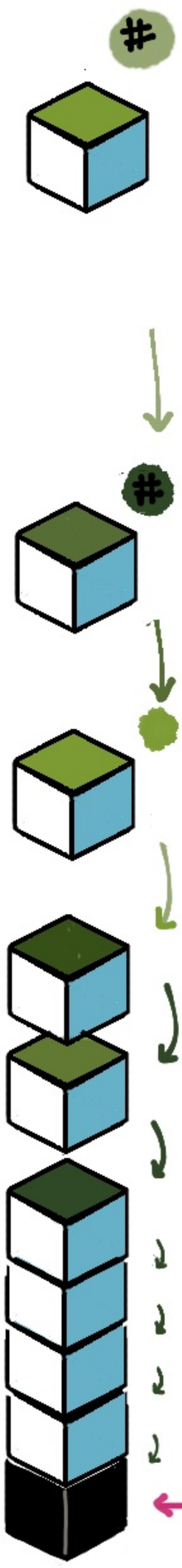
A BLOCK IS IDENTIFIED BY A HASH

we will look at how transactions are validated, in a separate section

A BLOCK REFERS PREVIOUS BLOCK'S HASH



THE GENESIS BLOCK IS THE FIRST BLOCK IN A BLOCKCHAIN AND IS USUALLY ENCODED IN THE SOFTWARE AND 'KNOWN' TO ALL NODES



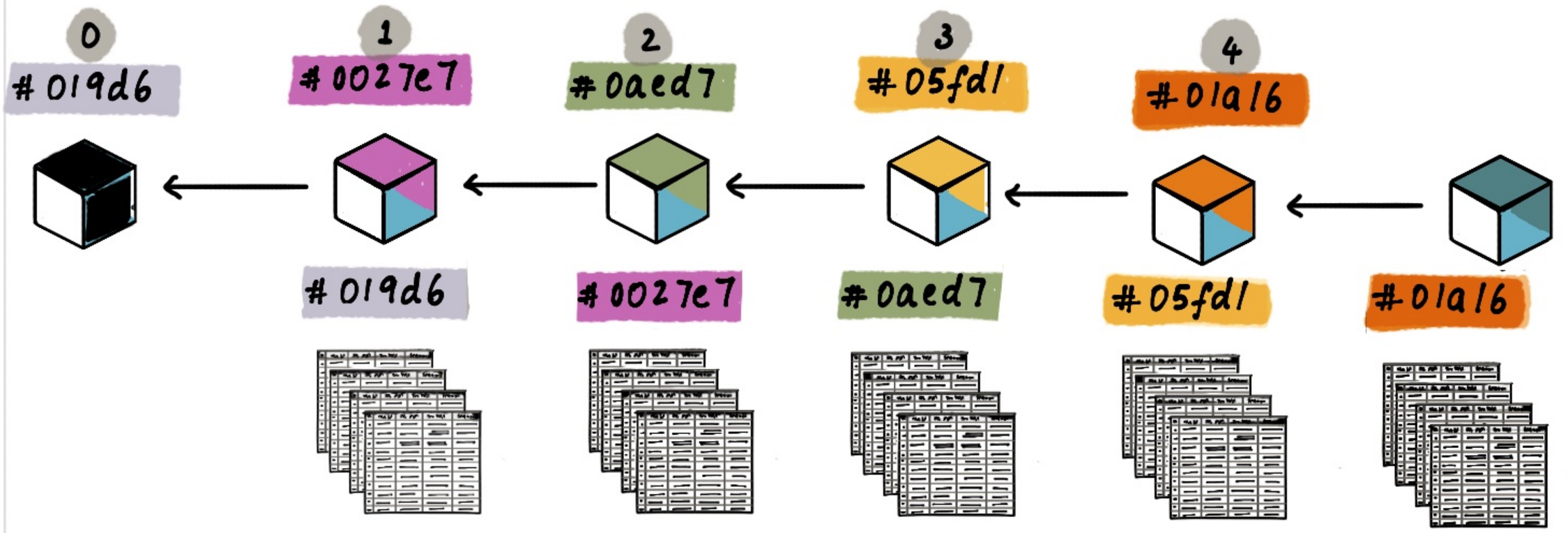
BLOCKCHAIN

ALL THE WAY BACK TO THE...

FIRST BLOCK OR GENESIS BLOCK

BLOCK IMMUTABILITY

THE BLOCK HEADER OF EVERY NEW BLOCK REFERS TO THE HASH OF THE PREVIOUS 'PARENT' BLOCK. THE HASH IS COMPUTED EACH TIME AND IS UNIQUE TO A BLOCK.



EITHER A TRANSACTION OR SOME META DATA.

CHANGE BLOCK 2

CHANGES HASH FOR BLOCK 2

CHANGES HASH FOR BLOCK 3

CHANGES HASH FOR BLOCK 4

CAUSES A SERIES OF EXPENSIVE RECALCULATIONS DOWN THE BLOCKCHAIN

NEEDS TO TRAVEL DOWN TO EVERY NODE THAT HOLDS A COPY OF IT

THIS MIGHT MAKE IT NEARLY IMPOSSIBLE TO TAMPER WITH DATA IN A BLOCKCHAIN

HENCE, THE CONFIDENT* USE OF THE WORD IMMUTABILITY IN BLOCKCHAINS

* nearly impossible



MINERS, NODES & MINING

WHO IS A MINER?

A MINER IS THE HUMAN ELEMENT ON A BLOCKCHAIN

A PERSON ON A BLOCKCHAIN

WHO OPERATES

ONE OR MORE

COMPUTING RESOURCES

WITH THE AIM OF

SOLVING A PUZZLE

CREATING A BLOCK

EARNING A REWARD

BY COMMITTING

HARDWARE

ELECTRICITY

THUS ALSO ENDS UP

MAINTAINING & } THE

SECURING } BLOCKCHAIN

UNLESS

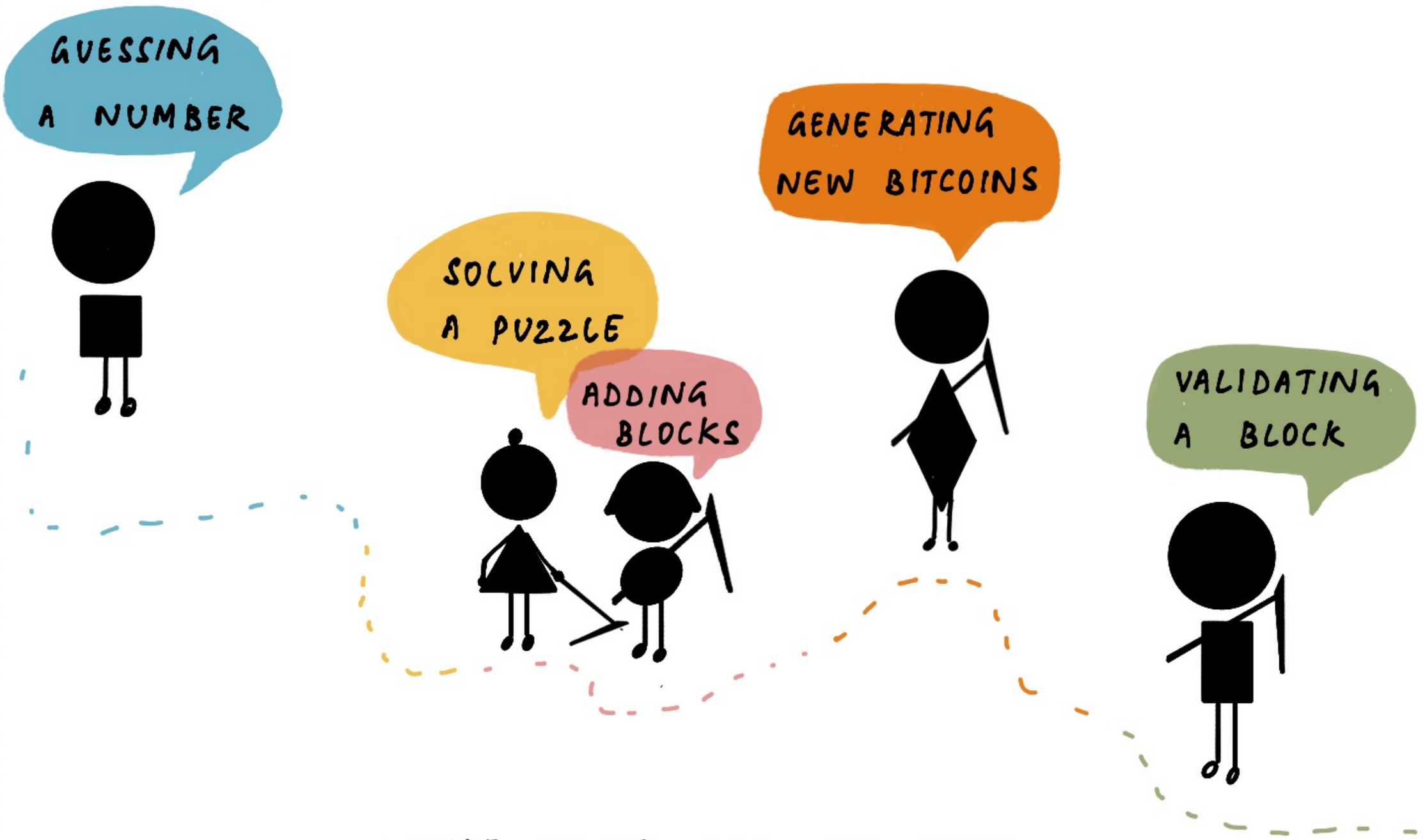
THEY HAVE CONTROL OF

51% OR MORE OF THE

NETWORK'S PROCESSING POWER.

WITHOUT honest MINERS, NO MATHEMATICS, PROTOCOLS OR ALGORITHMS CAN MAKE A BLOCKCHAIN TRUSTLESS, IMMUTABLE AND SO ON.

WHAT IS MINING?



WHILE THESE ARE ALL TRUE...

...MINING SERVES TWO PURPOSES

SUPPLIES NEW CURRENCY

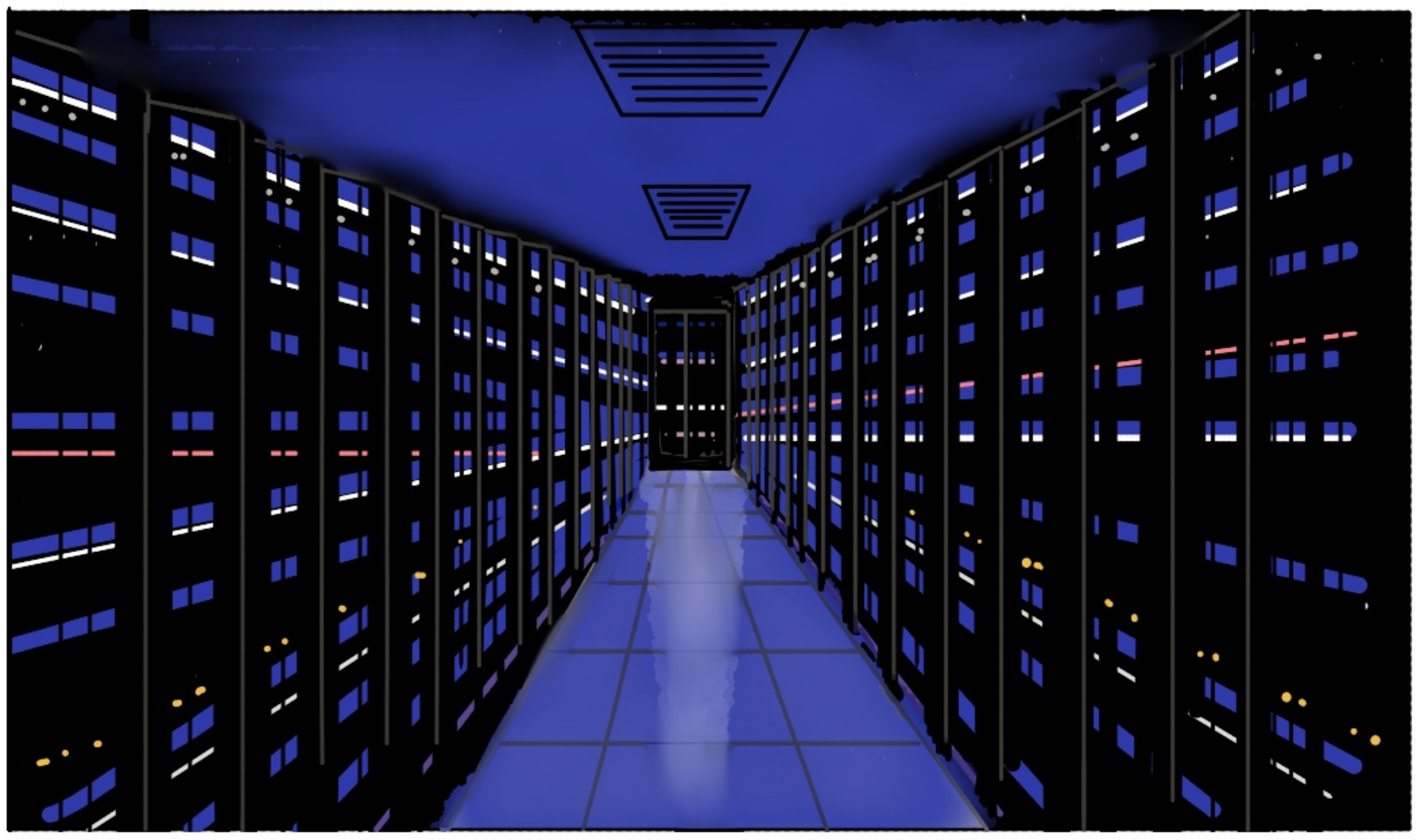
creating a new block generates new bitcoins

ENABLES DECENTRALISED CONSENSUS



Following the bitcoin protocol results in consensus

A MINING POOL



MINERS COMBINE THEIR RESOURCES INTO MINING POOLS TO INCREASE LIKELIHOOD OF FINDING A VALID BLOCK AND SHARE THE REWARDS

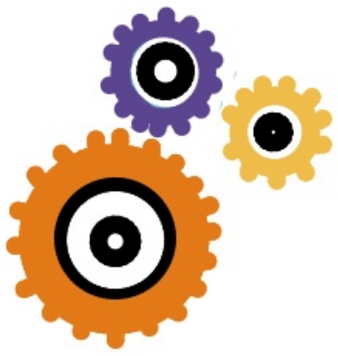
gets outdated quickly

THE STEADY EARNINGS HELP PAY FOR ELECTRICITY AND HARDWARE COSTS.

MINING POOLS ARE SOMETIMES MANAGED/CENTRALISED. THE POOLS COULD BE WELL-FUNDED IN ADDITION.

THIS INCREASES THE RISK OF MALICIOUS ATTACKS.

MINING: SOME FACTS



MINING IS

COMPUTATIONALLY

INTENSIVE



WHEN MORE MINERS

JOIN THE NETWORK,

THE DIFFICULTY LEVEL

OF THE PROBLEM INCREASES



IT ALWAYS TAKES

ABOUT 10 MINUTES

TO FIND A NEW BLOCK



HARDWARE IS SPECIALISED

AIMS TO BE MORE

ENERGY EFFICIENT

MOVING ON FROM CPUs, GPUs

TO FPGAs, ASICs



MINING IS

COMPETITIVE, CHALLENGING

AND COMES WITH

NO GUARANTEE OF SUCCESS



MINERS ARE REWARDED

FOR THEIR EFFORTS

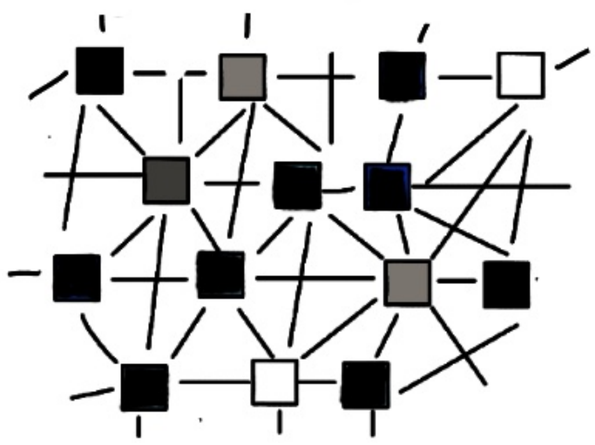
WHEN THEY SUCCEED

IN MAKING A BLOCK

WHAT IS A NODE ?

IN A NETWORK

A NODE IS





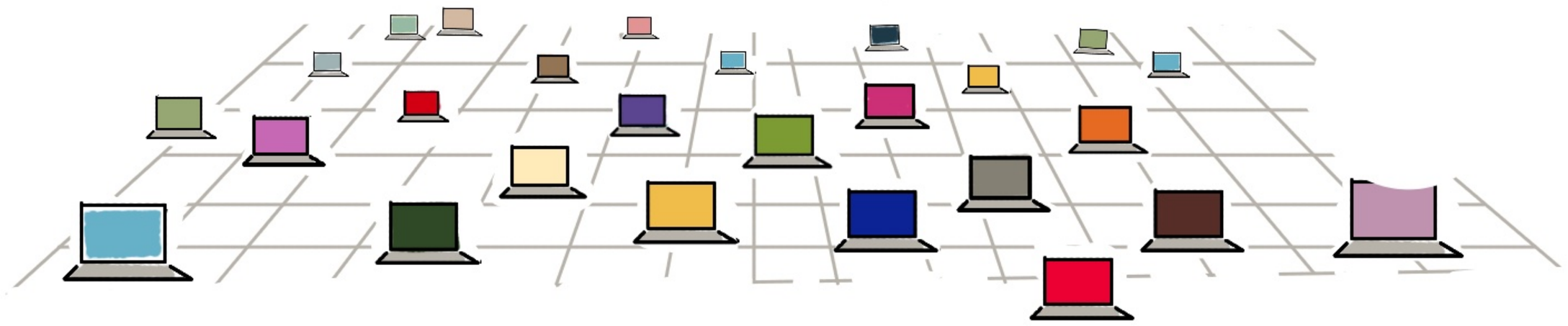
A DEVICE



A DEVICE

THAT PERFORMS

A FUNCTION



BITCOIN IS A PEER TO PEER NETWORK

THERE IS NO HIERARCHY

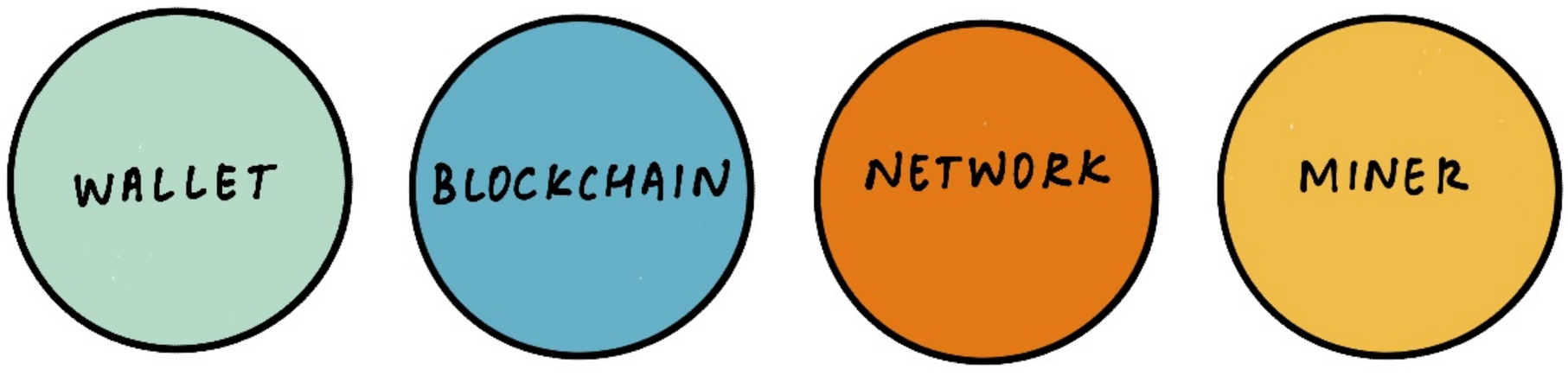
ALL NODES PROVIDE NETWORK SERVICES

NODES ALSO USE NETWORK SERVICES

ALL NODES VALIDATE TRANSACTIONS & BLOCKS

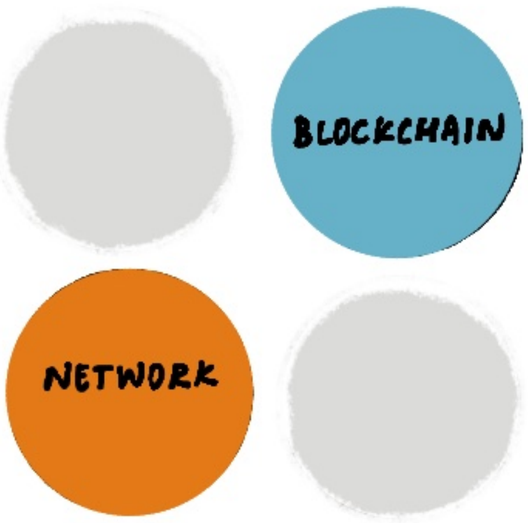
This helps achieve a decentralised flat network e.g. Napster → file sharing

NODES PERFORM ONE OR MORE OF THE FOLLOWING FUNCTIONS

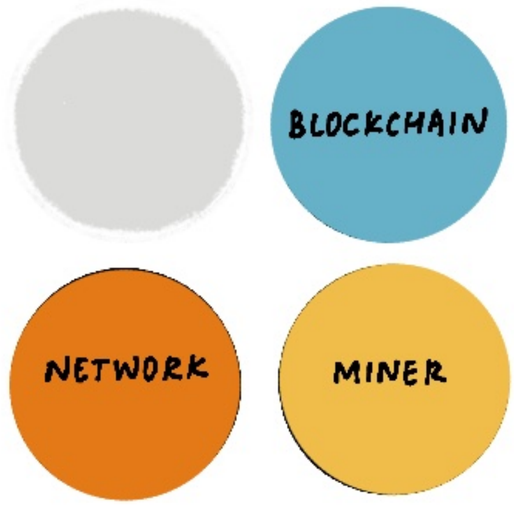


NODE 'CONFIGURATIONS'

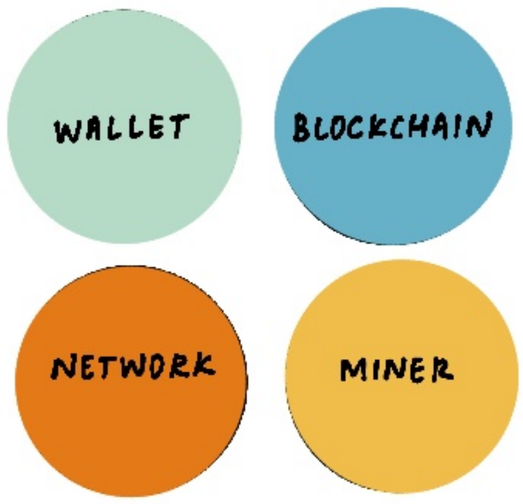
HERE ARE ONLY A FEW EXAMPLES OF COMMONLY OCCURING NODE 'CONFIGURATIONS' (TYPES)



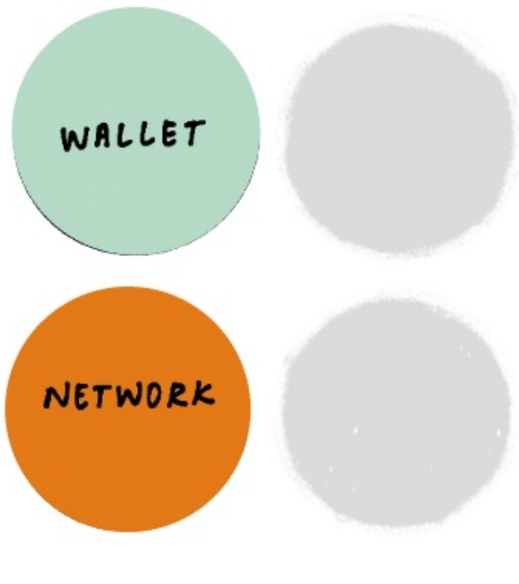
FULL BLOCKCHAIN NODE



SOLO MINER



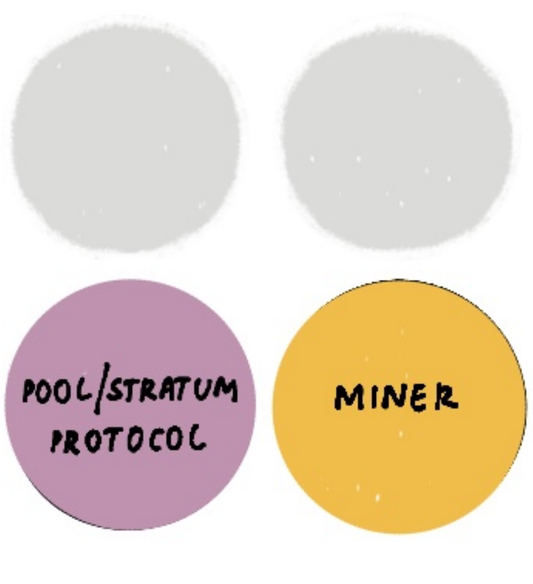
REFERENCE CLIENT OR BITCOIN CORE



LIGHTWEIGHT SPV WALLET

SPV = SIMPCLIFIED PAYMENT VERIFICATION, A METHOD TO VERIFY TRANSACTIONS

Use merkle paths to verify!



MINING NODE THAT CONNECTS TO POOL MINING NODES VIA A SUITABLE PROTOCOL

NODE FUNCTIONS

NETWORK

THIS IS ROUTING

- CONNECT — TO PEERS
- VALIDATE — TRANSACTIONS, BLOCKS
- PROPAGATE — TRANSACTIONS, BLOCKS

BLOCKCHAIN

THIS IS STORAGE

- STORE — ENTIRE BLOCKCHAIN LOCALLY
- VERIFY — TRANSACTIONS INDEPENDENTLY

USES UP (LOTS OF) STORAGE SPACE, SO NOT ALL NODES HAVE FULL COPY

WALLET

THIS IS KEYS & ACCESS TO BITCOIN

- CONTAINS — PRIVATE/PUBLIC KEY
- RELY ON — OTHER FULL NODES FOR INFO TO VALIDATE

HENCE, VULNERABLE / LESS SECURE

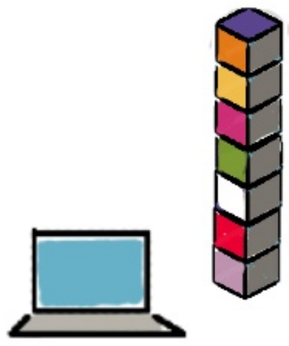
MINER

THIS IS CREATING NEW BLOCKS

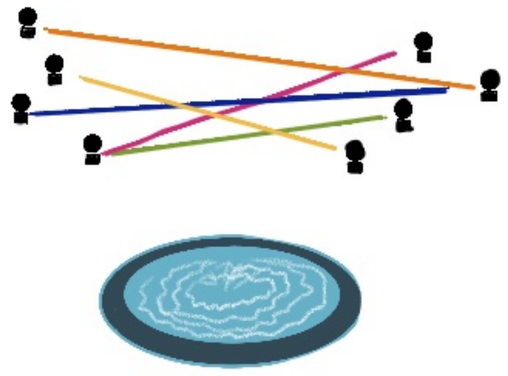
- RUN — SPECIAL MINING SOFTWARE
- CAN JOIN — MINING POOLS IF NO FULL COPY
- SOLVE — MATHEMATICAL PUZZLE

WINS MINING REWARDS OF NEW 'MINTED' BITCOIN

'MINING' A NEW BLOCK - 1



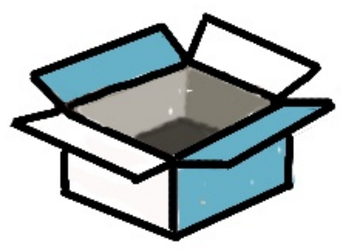
EVERY MINER HAS A FULL COPY OF THE BLOCKCHAIN AND LISTENS FOR NOTIFICATIONS



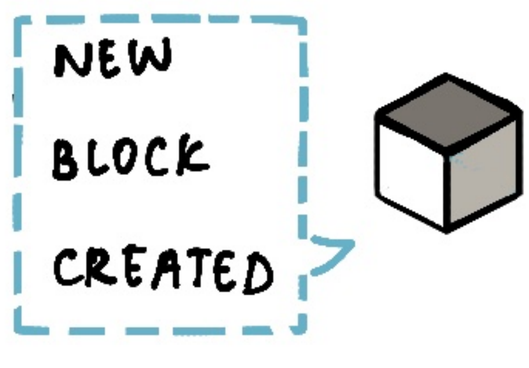
NODE LISTENS FOR NEW TRANSACTIONS AND ADDS THEM TO LOCAL MEMPOOL

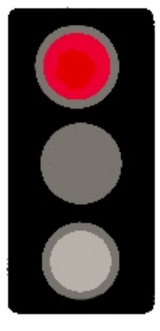


NODE VERIFIES EVERY TRANSACTION IN THE MEMPOOL

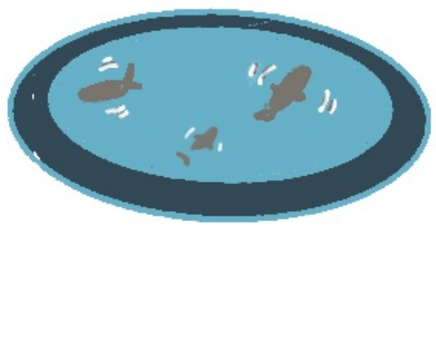


NODE COLLECTS TRANSACTIONS FROM MEMPOOL TO MAKE A CANDIDATE BLOCK



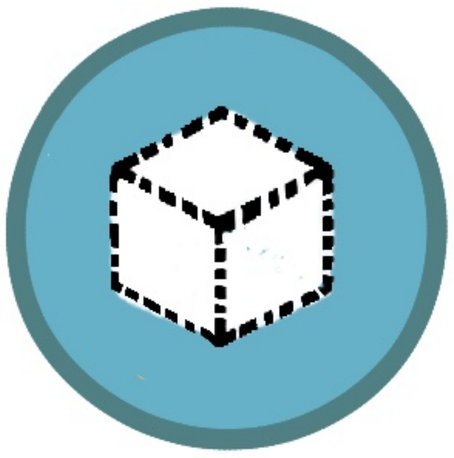


NOTIFICATION ENDS THE RACE TO MINE THE CURRENT BLOCK



NODE DISCARDS ANY TXNS FROM MEMPOOL ALREADY IN THE NEWEST BLOCK

'MINING' A NEW BLOCK - 2



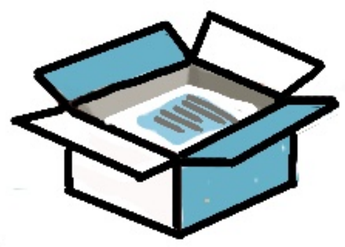
CREATE A NEW BLOCK WITH TRANSACTIONS

	Example of priority order
1.	OLDER + HIGH VALUE
2.	TRANSACTIONS WITH FEES
3.	NO-FEE TRANSACTIONS
	up to maximum block size

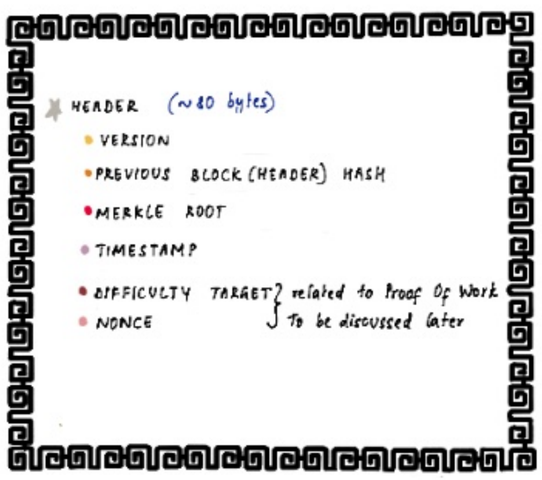
TRANSACTIONS HAVE A PRIORITY ORDER



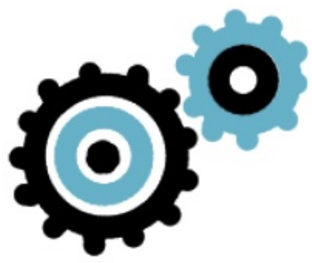
THE FIRST TRANSACTION IS THE COINBASE TRANSACTION ie. MINER'S REWARD



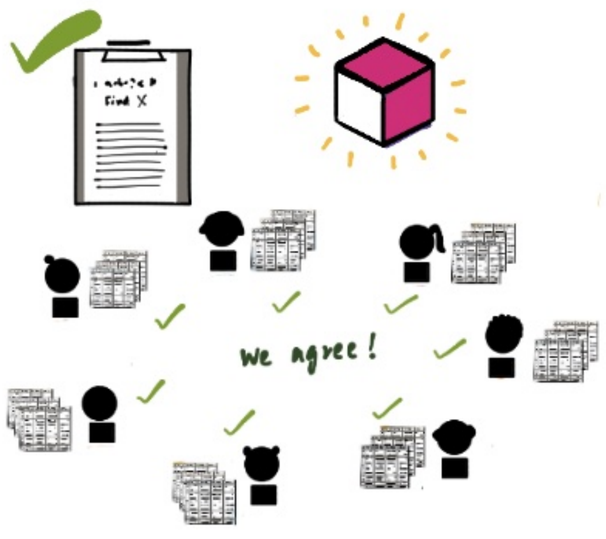
THE TRANSACTIONS REACH THE SIZE THRESHOLD FOR A BLOCK



THE NODE CONSTRUCTS THE BLOCK HEADER

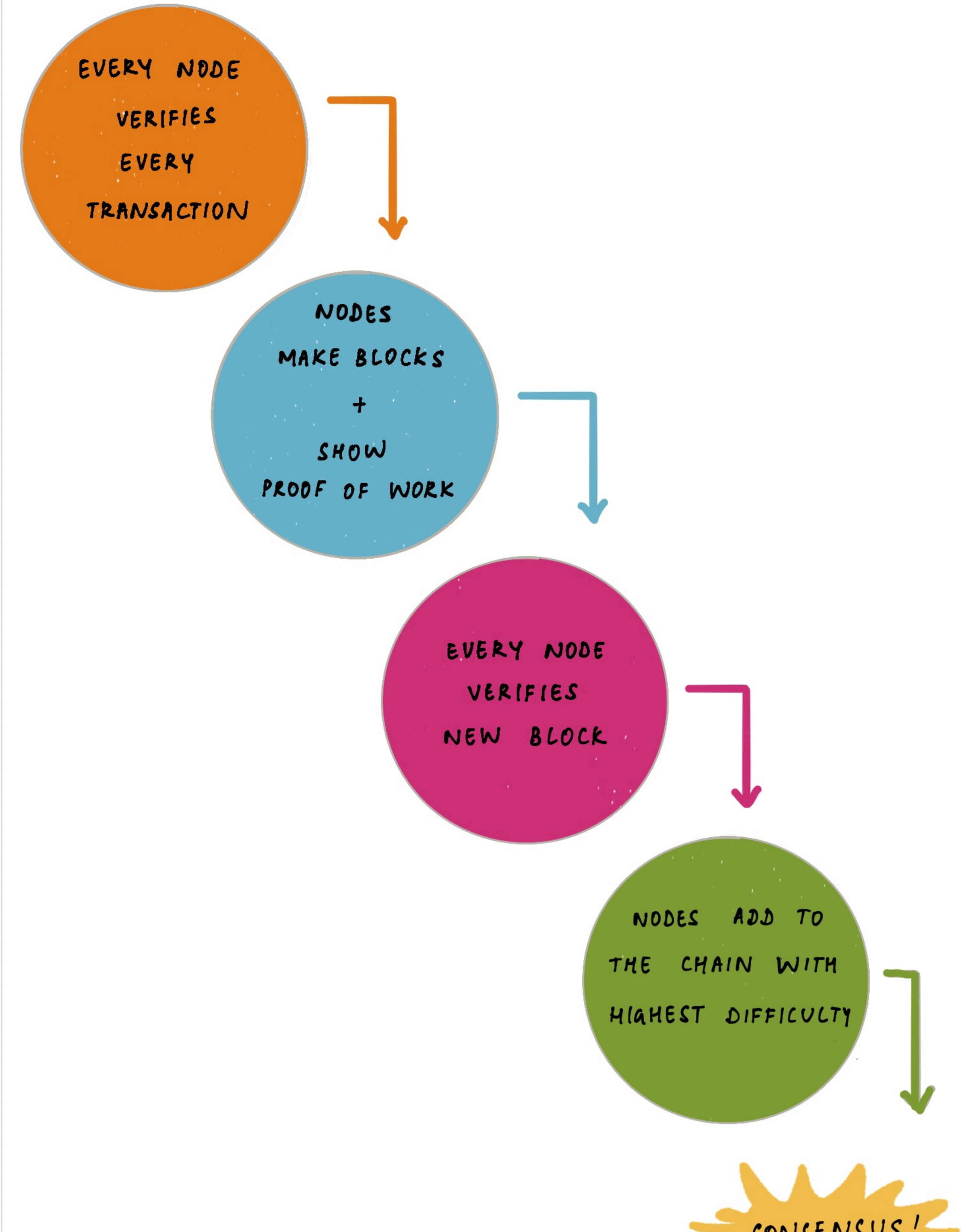


THE MINER ADDS PROOF OF WORK TO THE BLOCK



CONSENSUS AND PROOF OF WORK

HOW TO ACHIEVE CONSENSUS



EVERY NODE VERIFIES EVERY TRANSACTION

VERIFY TRANSACTIONS

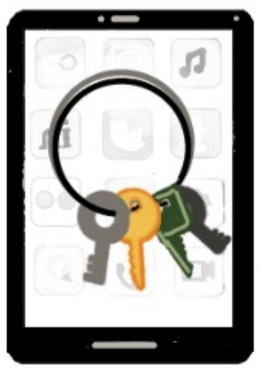
NODES MAKE BLOCKS + SHOW PROOF OF WORK

EVERY NODE VERIFIES NEW BLOCK

NODES ADD TO THE CHAIN WITH HIGHEST DIFFICULTY

CONSENSUS!

VERIFYING TRANSACTIONS



WALLET SOFTWARE

BROADCASTS SIGNED TRANSACTION



NODE



NODE

VALIDATES

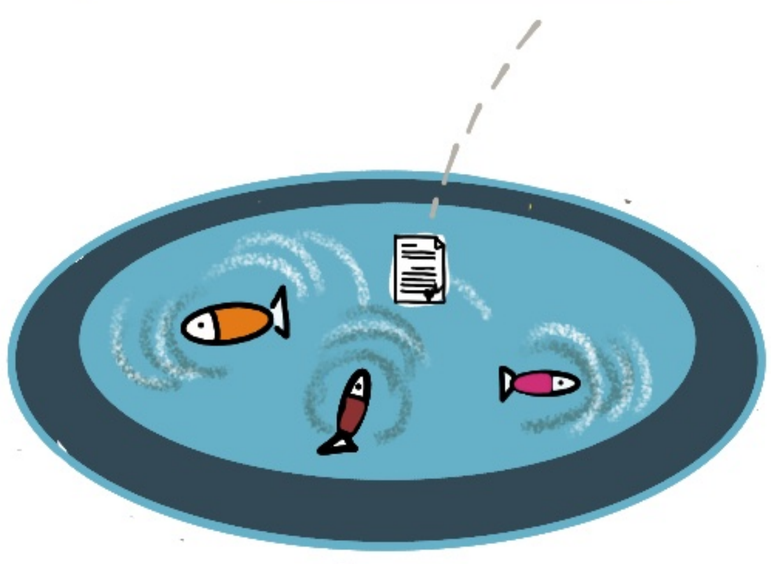


TRANSACTION

Most literature appears to use VALIDATE and VERIFY interchangeably.

ADDS TRANSACTION TO LOCAL POOL

SENDS IT TO OTHER CONNECTED NODES



THIS MEMORY POOL CONTAINS VALID UNCONFIRMED TXNS



TILL ALL NODES RECEIVE THE TRANSACTION

VERIFYING TRANSACTIONS

- NODES INDEPENDENTLY VALIDATE TRANSACTIONS BASED ON THESE CRITERIA

- A REJECTED TRANSACTION IS NOT PROPAGATED

** VALIDATION CRITERIA **

- [ ] CORRECTLY FORMED SYNTAX/STRUCTURE
- [ ] NON-EMPTY INPUTS/OUTPUTS
- [ ] TRANSACTION SIZE BETWEEN 100 BYTES - MAX SIZE
- [ ] OUTPUT AND TOTAL VALUE BETWEEN 0 - 21 MILLION COINS
- [ ] COUNT OF SIGNATURES WITHIN A LIMIT
- [ ] SOME REJECTION CRITERIA BASED ON
  - [ ] FEES
  - [ ] INADEQUATE FUNDS
  - [ ] LOCKING SCRIPT VALIDITY
  - [ ] REFERENCED OUTPUT FOUND IN ANOTHER TXN (for given input)
- [ ] PLUS A HANDFUL MORE

ONLY CERTAIN TRANSACTION ATTRIBUTES ARE VERIFIED

THE PRIVACY OF OTHER DATA IS PRESERVED

EVERY NODE VERIFIES EVERY TRANSACTION

PROOF OF WORK

NODES MAKE BLOCKS + SHOW PROOF OF WORK

EVERY NODE VERIFIES NEW BLOCK

NODES ADD TO THE CHAIN WITH HIGHEST DIFFICULTY

CONSENSUS!

PROOF OF WORK

PROOF OF WORK IS THE SOLUTION TO A PUZZLE

HASH (BLOCKHEADER + x) < TARGET

SO WHAT IS x ?

BLOCKHEADER IS

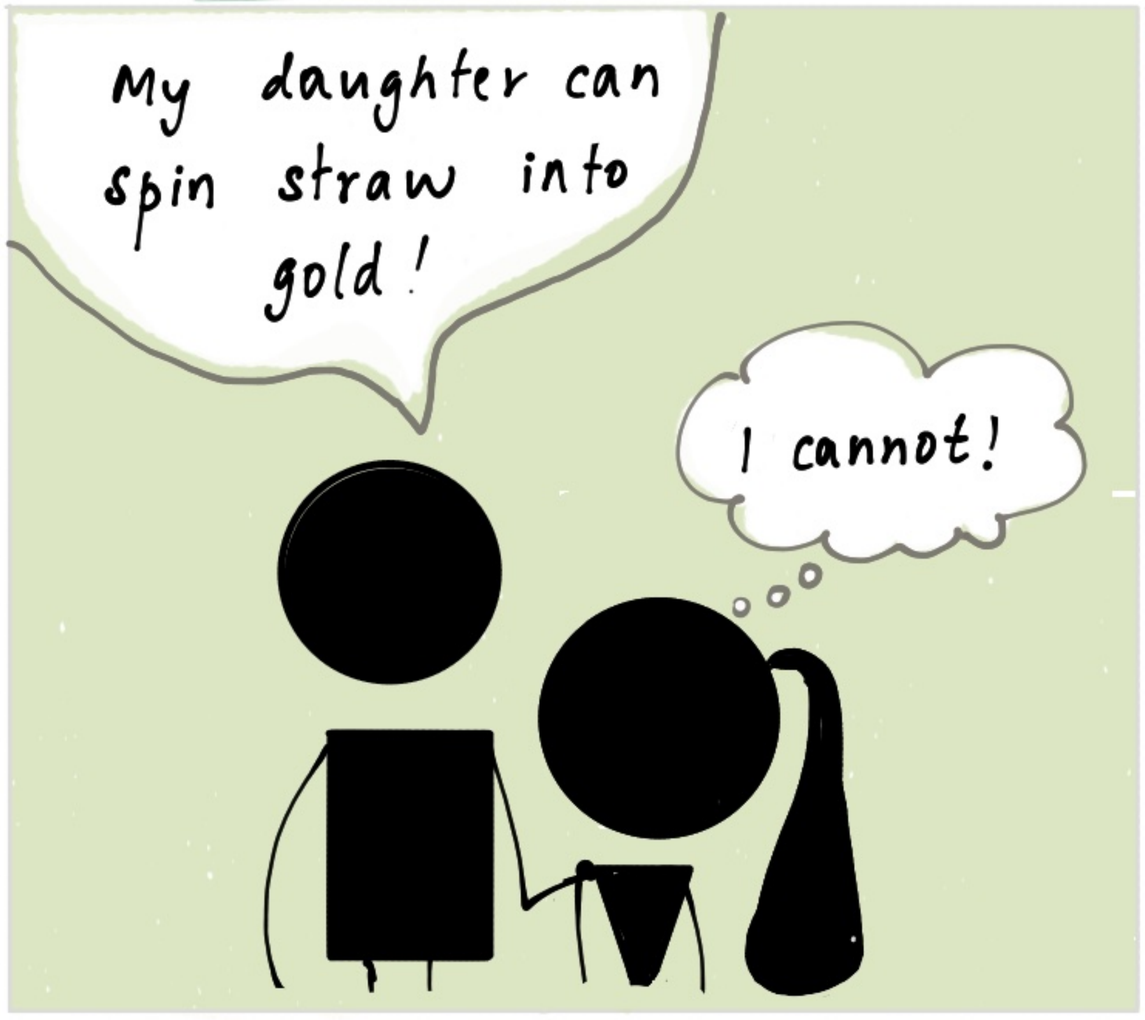
- HEADER (~80 bytes)
  - VERSION
  - PREVIOUS BLOCK (HEADER) HASH
  - MERKLE ROOT
  - TIMESTAMP
  - DIFFICULTY TARGET
  - NONCE

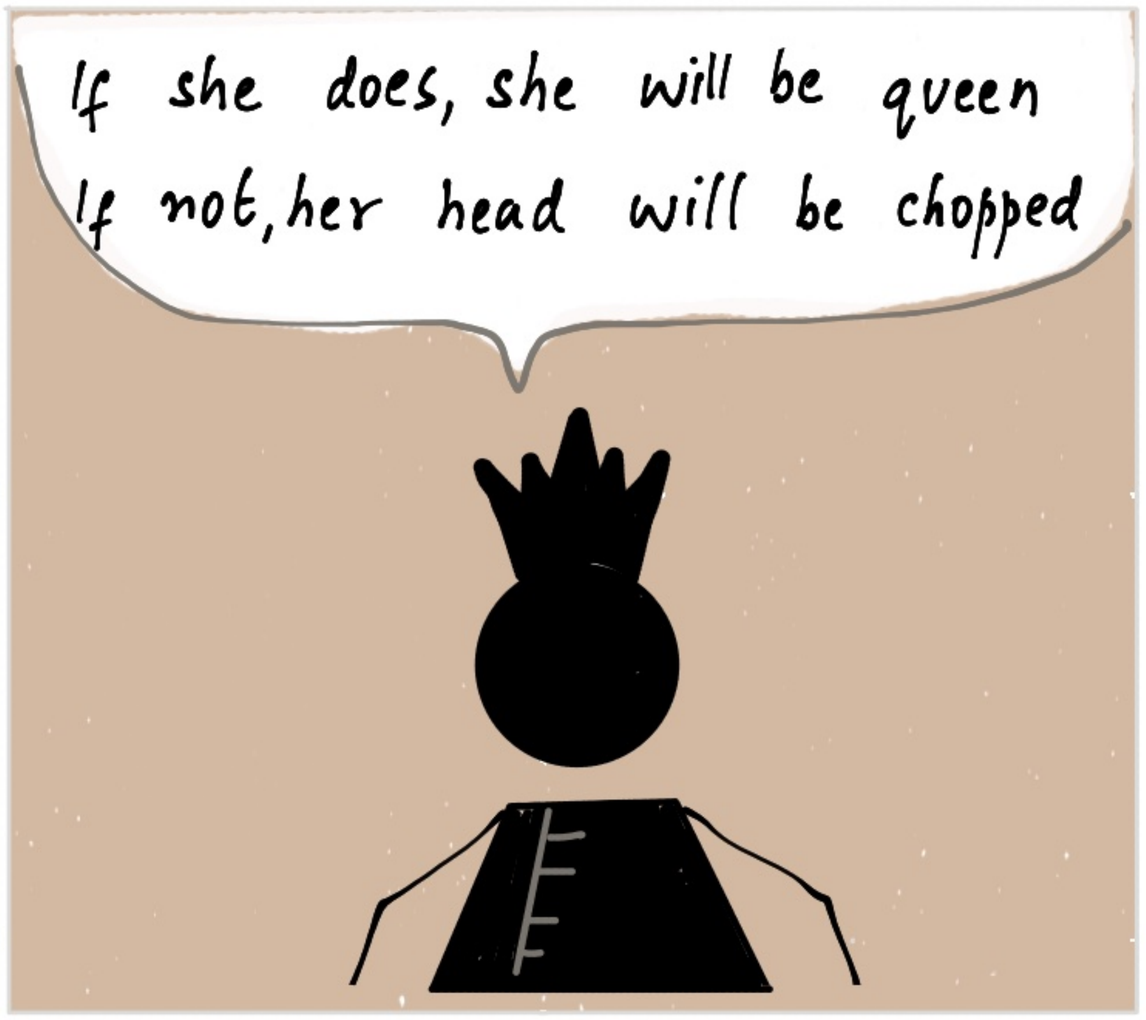
x → BETTER KNOWN AS NONCE

TARGET →
- A HASH, WITH MANY MANY LEADING ZEROES
- A VALUE THAT BITCOIN ADJUSTS AUTOMATICALLY

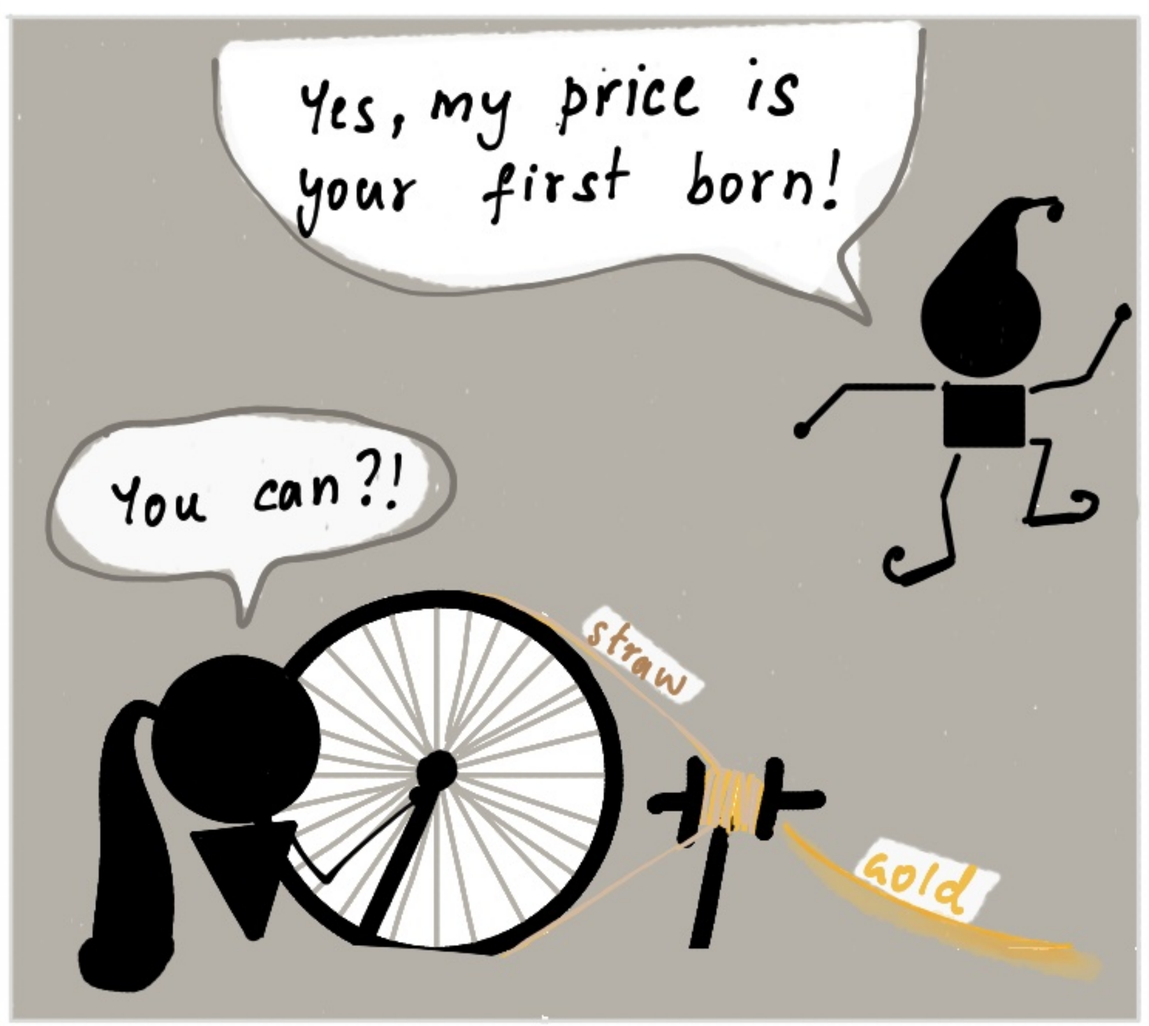
LET US SEE WHY THIS IS COMPUTATIONALLY INTENSIVE USING AN OLD FAIRY TALE WITH A GUESSING GAME

RUMPELSTILSKIN RETOLD -1





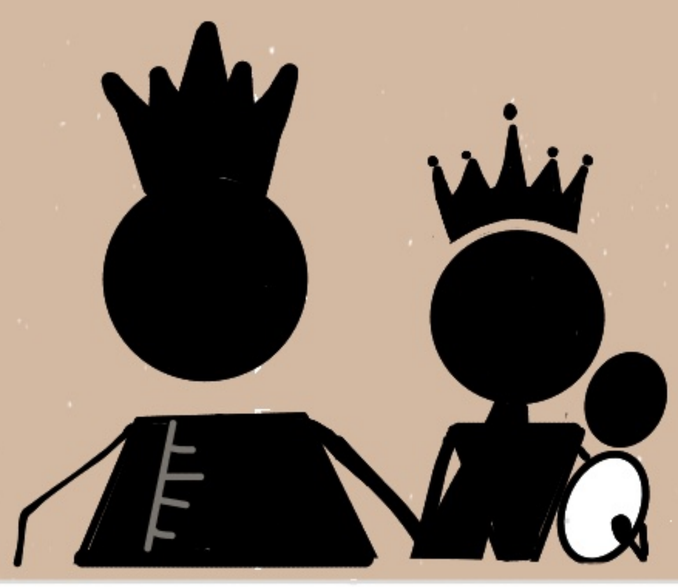


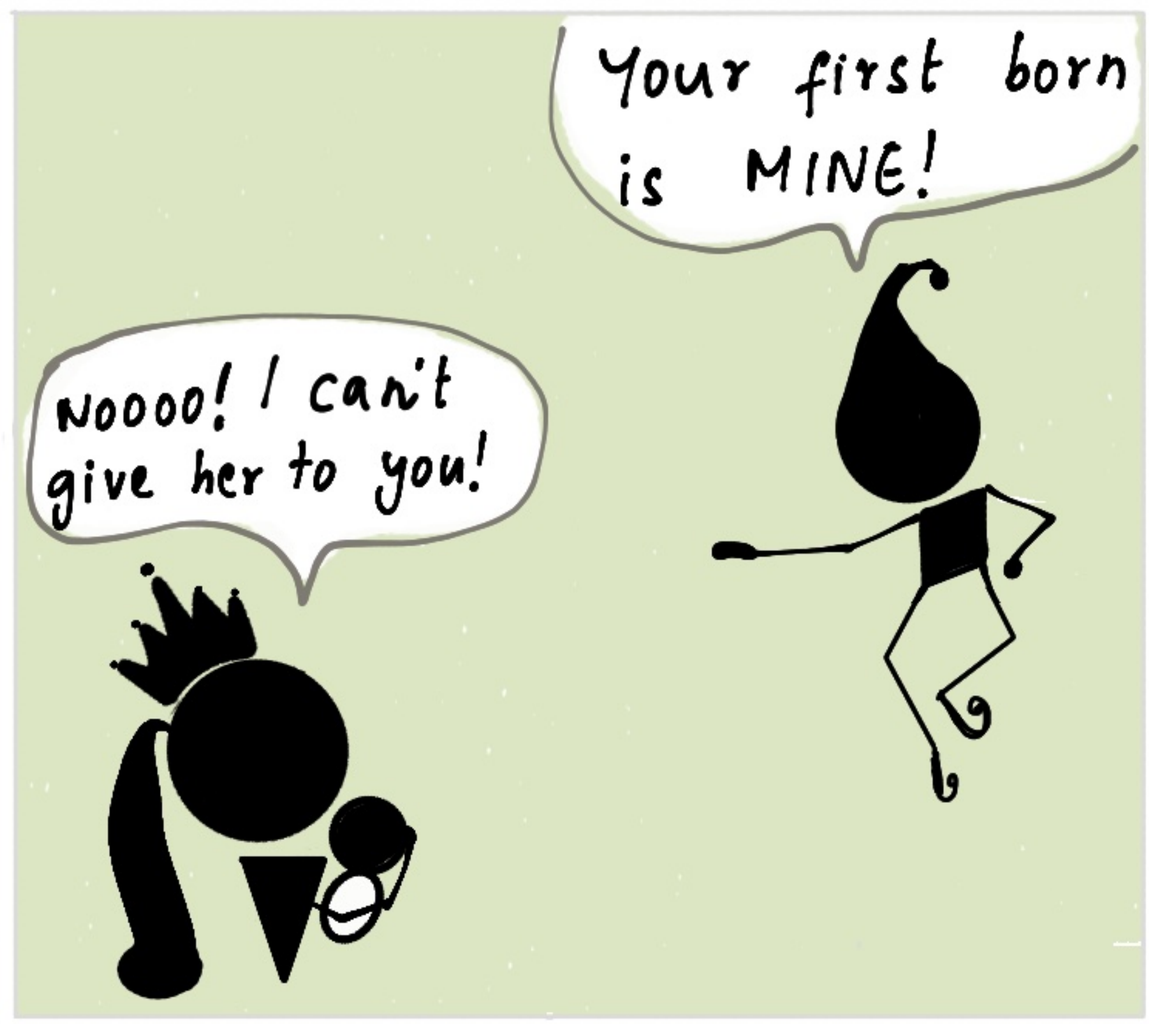


THE IMP DID HELP

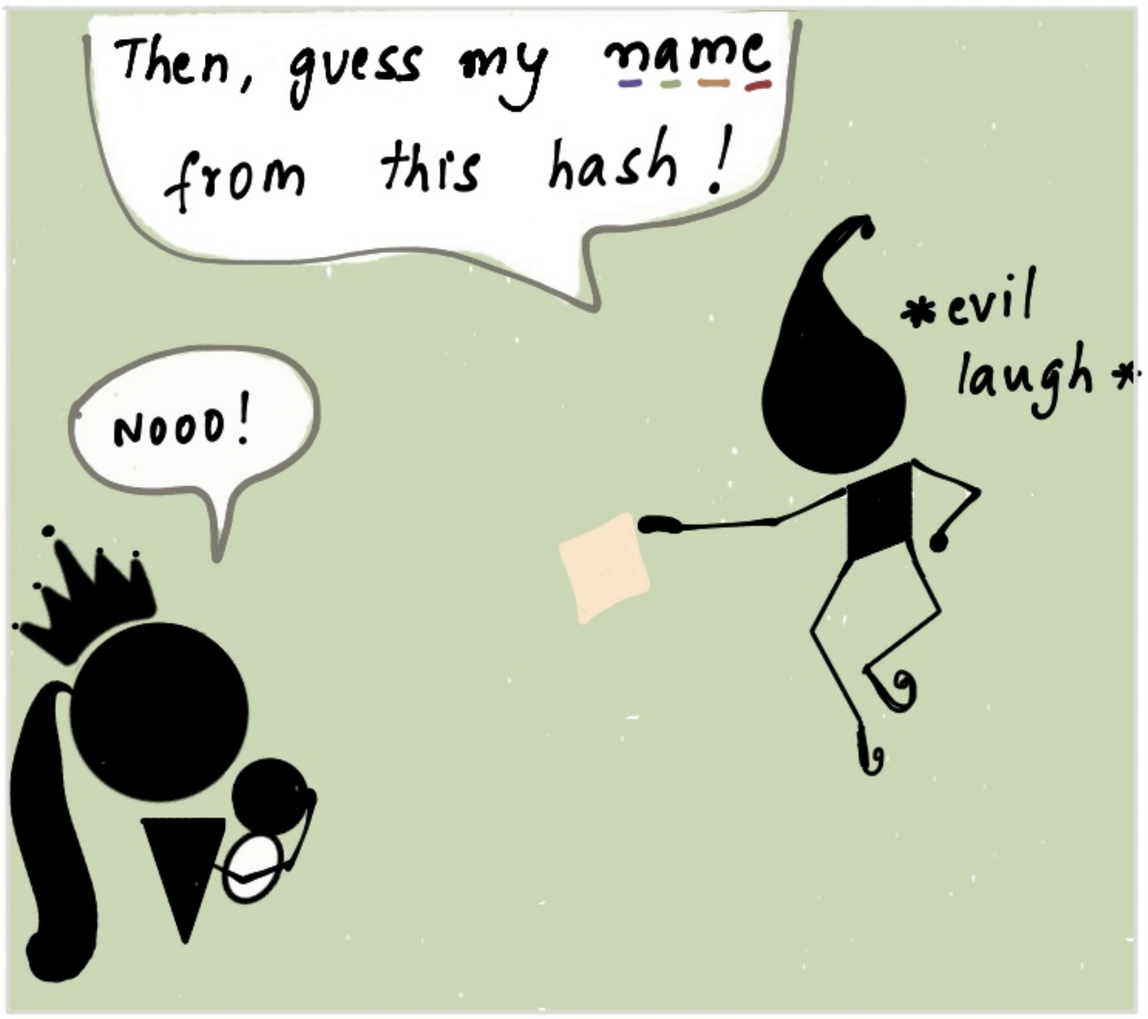
THE KING KEPT HIS WORD

AND SOON...





RUMPELSTILSKIN RETOLD - 2



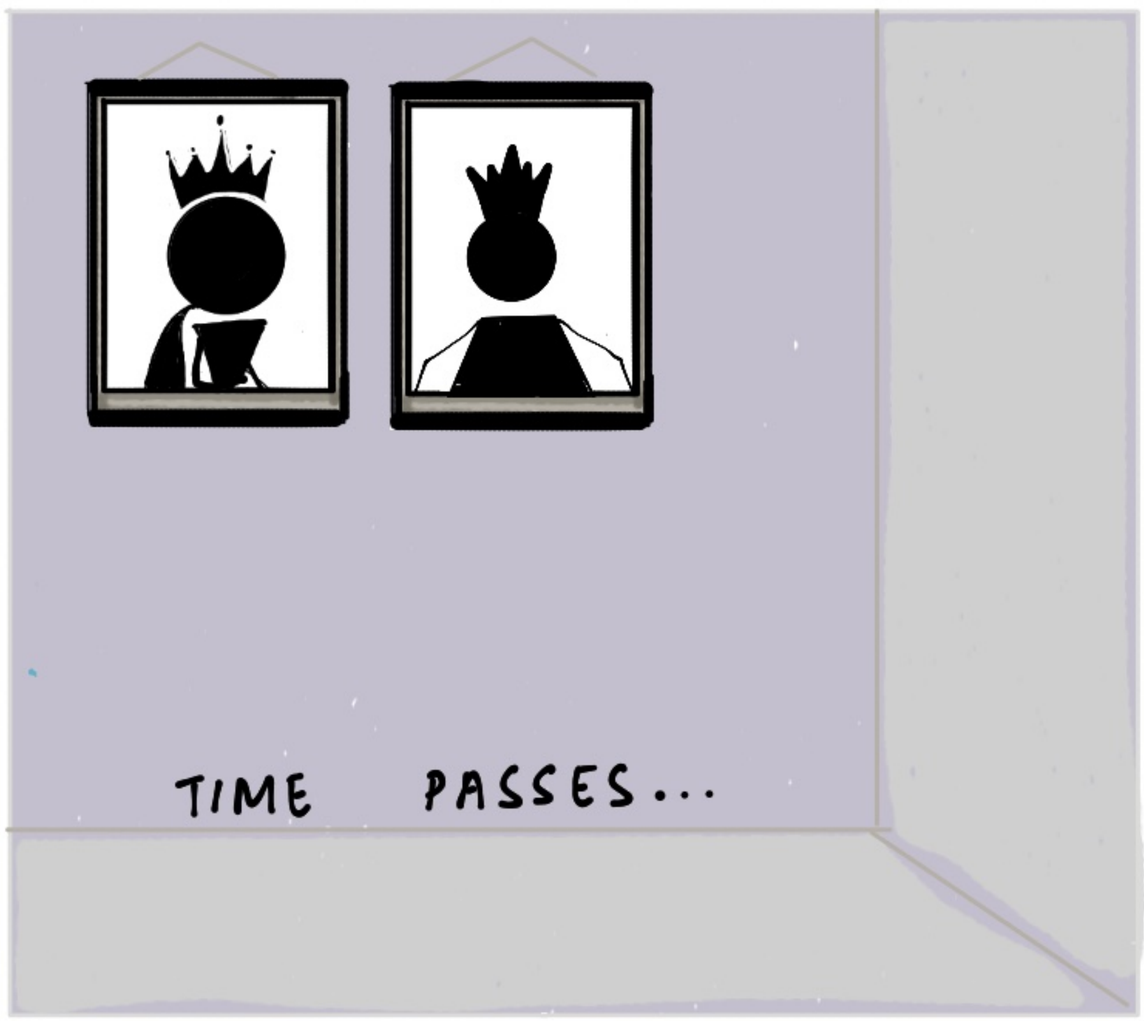
#HASH("my name is " + x) =

5b46a1d468cd87a
4da4f4721f7416eb
4ffe325de4a47ca89
b83c942b4dcb289

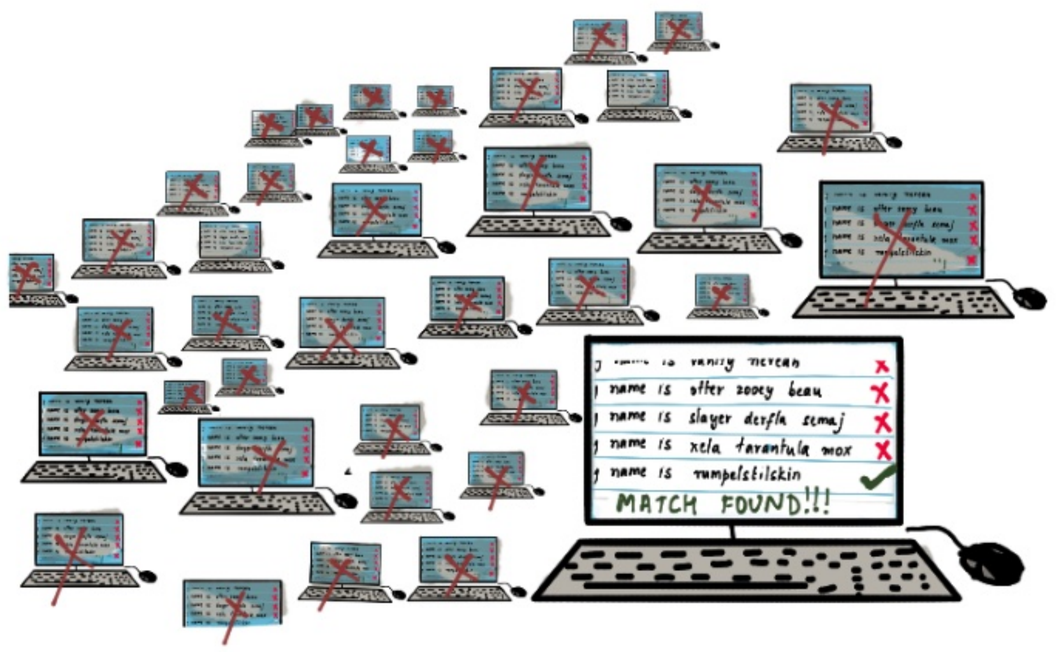
xorbin.com SHA256 calculator

iy name is dweezil shanda zumma	✗
y name is temperance goldscarch	✗
y name is candid lawrence	✗
y name is trixibel fif tincris	✗
y name is vanity neveah	✗
y name is otter zooey beau	✗
y name is slayer derfla semaj	✗
y name is xela tarantula mox	✗
y name is peridot quinn paityn	✗





A MILLION CENTURIES LATER...



RUMPELSTILSKIN RETOLD - 3

FOR A PARTICULAR INPUT, THE OUTPUT HASH WILL BE THE SAME

NO TWO NAMES CAN HAVE THE SAME HASH!

THE QUEEN **GUESSES**

A MAGIC-PERSON-NAME

HASHES IT WITH

THE PHRASE "my name is "

AND **COMPARES** IT TO

THE HASH THAT RUMPELSTILSKIN GAVE HER

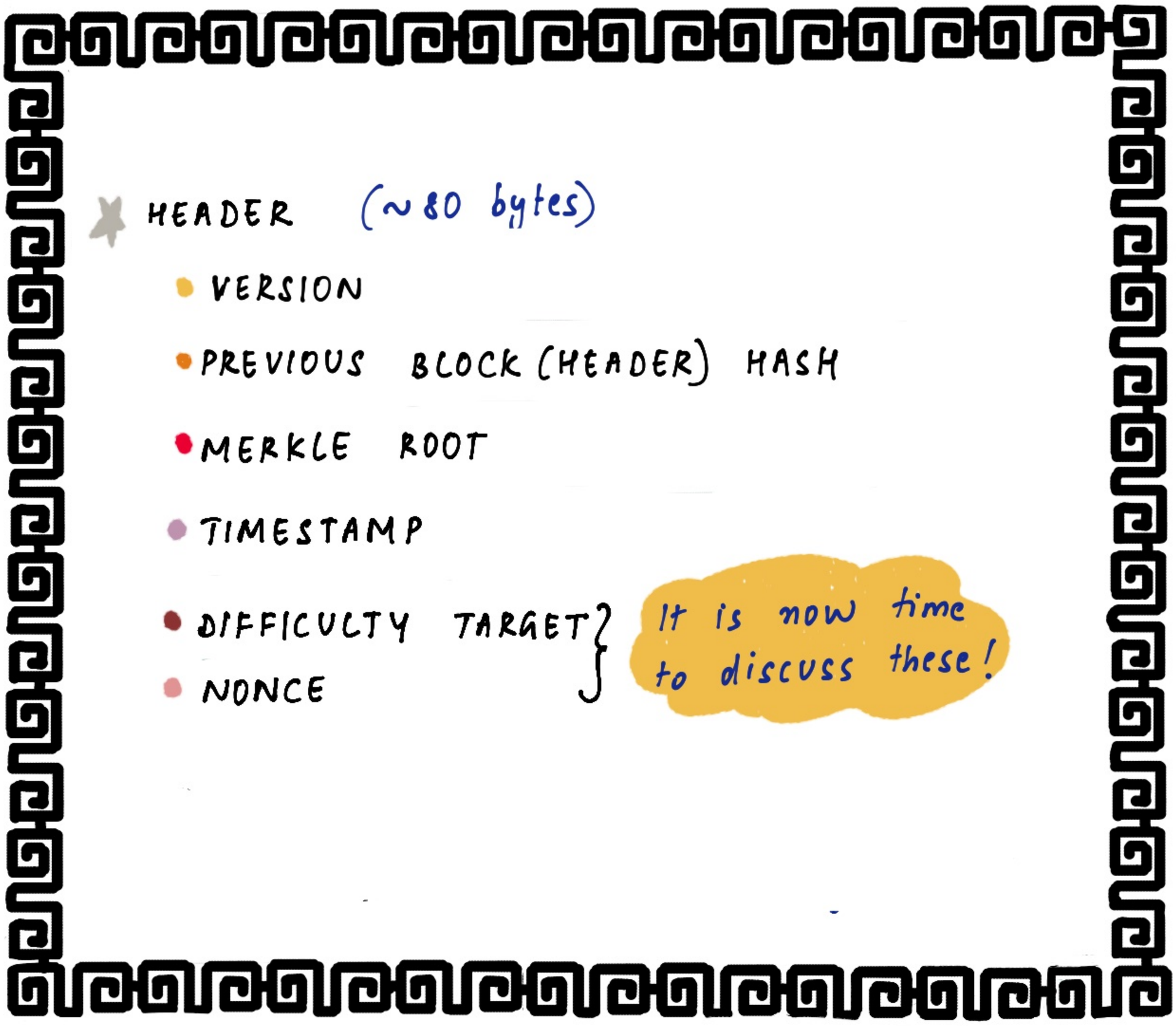
SOMETHING LIKE THIS:

"my name is " + x	→ HASH OF NAME
my name is dweezil shanda zumma	→ 4ec39ad97262....
my name is temperance goldscarch	→ 79bdb15df8fd9....
my name is candid lawrence	→ 18b98b9f2d6b....
my name is trixibel fif tincris	→ 76312da83239fb...
my name is vanity neveah	→ 7853a3538badc5..
my name is otter zooey beau	→ 0b5fda4595bc63...
my name is slayer derfla semaj	→ f947aa2b0b99a...
my name is xela tarantula mox	→ 6baaba75db77d...
my name is peridot quinn paityn	→ ac39e112d97566...

---

my name is rumpelstilskin → 5b46a1d468cd87a...

BLOCK HEADER : QUICK LOOK



OF THE FIELDS THAT GO INTO MAKING THE BLOCK HEADER, DIFFICUCTY AND NONCE ARE NOT EASICY APPARENT.

LET US LOOK INTO WHAT THEY ARE

DIFFICULTY - 1



TIME TO MINE A NEW BLOCK

DOES NOT DEPEND ON



NUMBER OF TRANSACTIONS

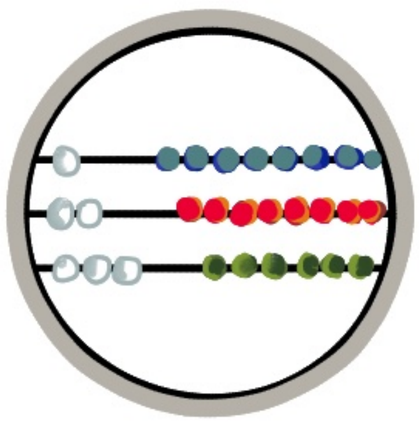


VALUE OF TRANSACTIONS



TIME TO MINE A NEW BLOCK

DEPENDS ✓ ON



NUMBER OF MINING NODES



PROCESSOR SPEEDS



IF THE DIFFICULTY OF MINING IS HIGH, MORE NODES MAY BE NEEDED TO COPE.

ANY ADDITIONAL CAPACITY COSTS MONEY

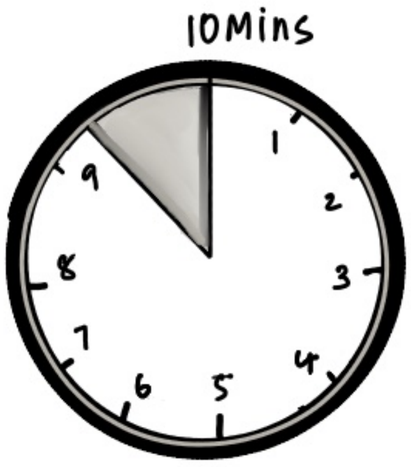
THE PRICE OF ELECTRICITY ALSO PLAYS A PART IN THE NUMBER OF MINERS

DIFFICULTY - 2

TO MAINTAIN A 10 MINUTE DURATION TO MINE A BLOCK, BITCOIN ADJUSTS THE DIFFICULTY LEVEL OF MINING EVERY TWO WEEKS (AUTOMATICALLY)



2 WEEKS = 2 X 7 X 24 X 60 MINUTES
= 20,160 MINUTES



IF THE MINING TIME IS 10 MINUTES

OVER → 2 WEEKS



THERE WOULD BE 2016 NEW BLOCKS

DIFFICULTY IS MEASURED IN (TERA)HASHES (TH)

NETWORK HASHRATE OR NET HASH = TH per second

BLOCK TIME = DIFFICULTY ÷ NETHASH

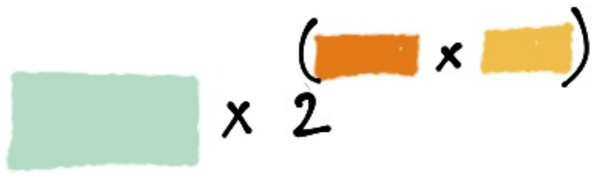
NEW DIFFICULTY = OLD DIFFICUCLTY × ACTUAL TIME FOR 2016 BLOCKS ÷ 20160 MINUTES

DIFFICULTY - 3

BLOCKS STORE THE DIFFICULTY AS A HASH VALUE

0x1b0404cb

THE DIFFICULTY TARGET IS DERIVED FROM THIS HASH → USING A FORMUCA



IN HEXADECIMAL THE DIFFICULTY TARGET HAS SEVERAL LEADING ZEROES

0000000000000040CB...

Look!

BITCOIN STORES THE TARGET AS A FLOATING POINT

256 BITS

FIRST FEW DOZEN BITS = Ø

A LOWER TARGET MEANS HIGHER DIFFICULTY

LIKE THROWING SEVERAL DICE AND EXPECTING ALL NUMBERS UNDER 3

FOR MORE DETAIL SEE en.bitcoin.it/wiki/Difficulty

NONCE - 1

A WINNING HASH WILL HAVE THE SAME NUMBER OF ZEROES OR ONE ADDITIONAL ZERO COMPARED TO THE TARGET HASH

PROBABILITY OF FINDING ...		
... A HASH STARTING WITH 1 ZERO	→	$\frac{1}{16}$ = 0.16.. %
... A HASH STARTING WITH 2 ZEROES	→	$\frac{1}{16} \times \frac{1}{16}$ = 0.02... %
... A HASH STARTING WITH 19 ZEROES (around year 2022)	→	ORDER OF 1×10^{-18}

THE BITCOIN NETWORK MEASURES

~224* EXA HASHES PER SECOND

AN EXA HASH IS 1×10^{18} HASHES

A HIGHER HASH RATE = HIGHER CHANCE OF OF A MINER NODE MINING A BLOCK

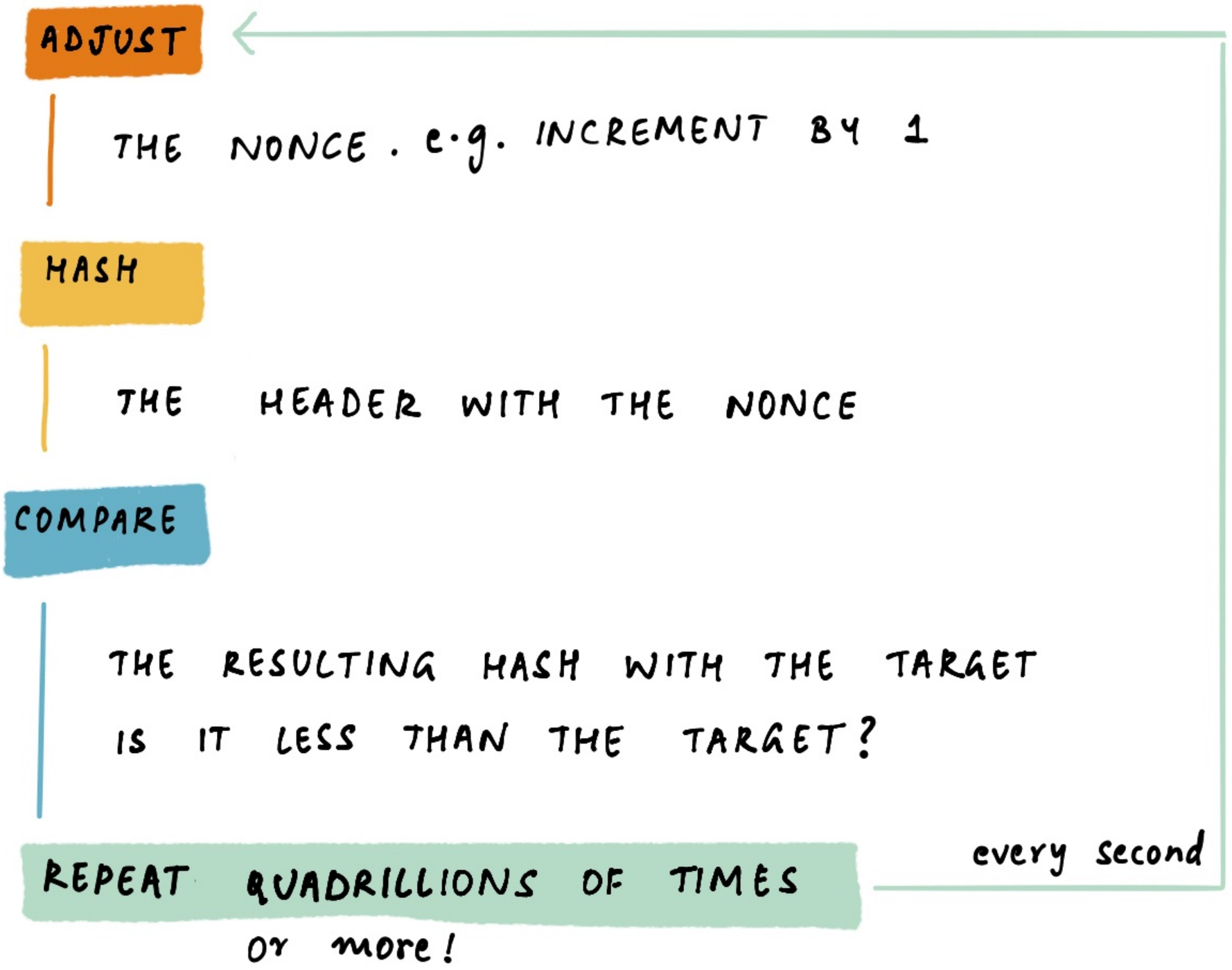
A HIGHER HASHRATE OF A BLOCKCHAIN = LOWER CHANCE OF A 51% TAKEOVER BY BAD ACTORS

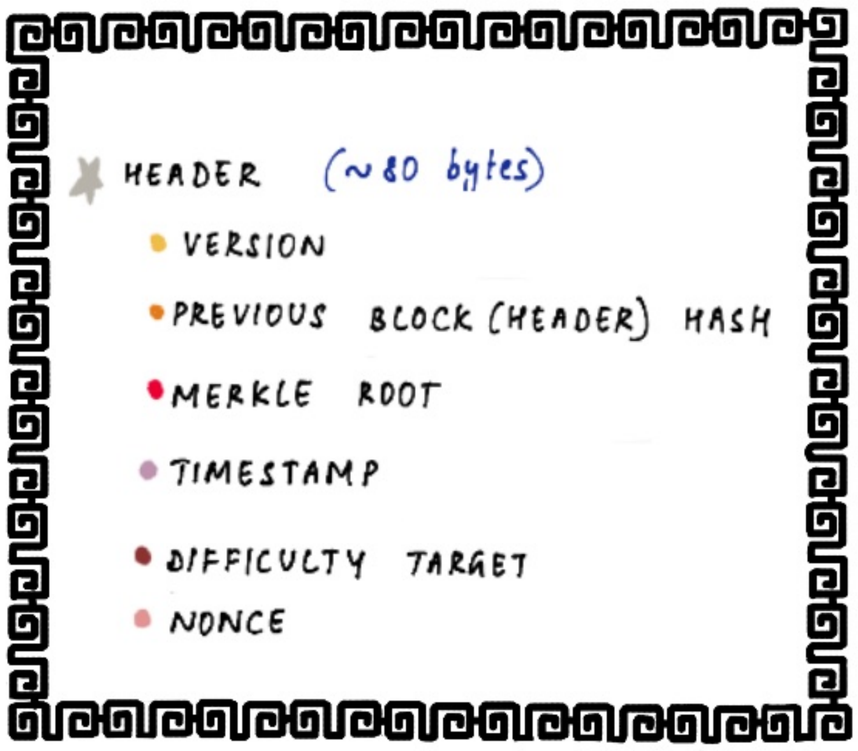
* The value changes frequently. Please look up the latest figures

NONCE - 2

THE NONCE IS VERY MUCH LIKE THE QUEEN'S GUESSES FOR RUMPELSTILSKIN'S NAME

IT IS SET TO ZERO INITIALLY





THE REST OF THE FIELDS IN THE BLOCK HEADER ARE PRETTY MUCH FIXED

ANY VARIATION TO ALTER THE HASH COMES FROM THE NONCE

PROOF OF WORK: ORIGINS



CYNTHIA DWORK AND MONI NOAR INVENTED THIS CONCEPT AROUND 1993

FORMALISED INTO A PAPER NOT LONG AFTER.

PROOFS OF WORK AND BREAD PUDDING PROTOCOLS 1999

By

Markus Jakobsson, Ari Juels

In a PoW, a prover demonstrates to a verifier that she has performed a certain amount of computational work in a specified interval of time

A way to deter junk/spam email and denial of service attacks

How to make a person indirectly pay?

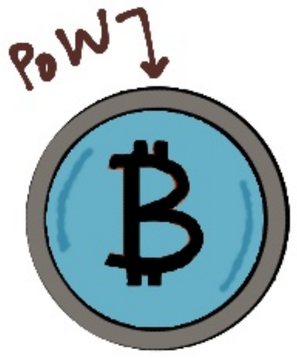
A payment method already signed up for...

Electricity Bill!

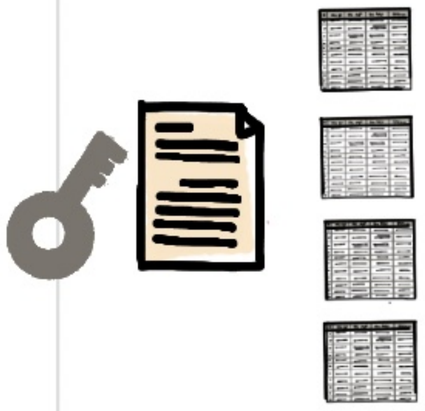
Get person to solve a problem that needs lots of processing power

A central authority would decide amount

WHAT BITCOIN DOES



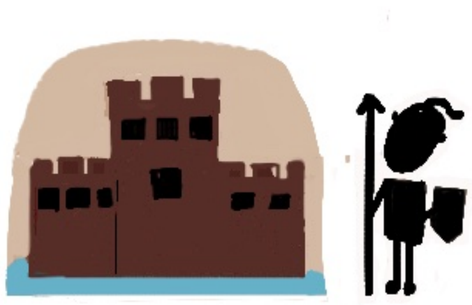
PROOF OF WORK WAS LATER ADOPTED INTO BITCOIN AS PART OF THE CONSENSUS MODEL



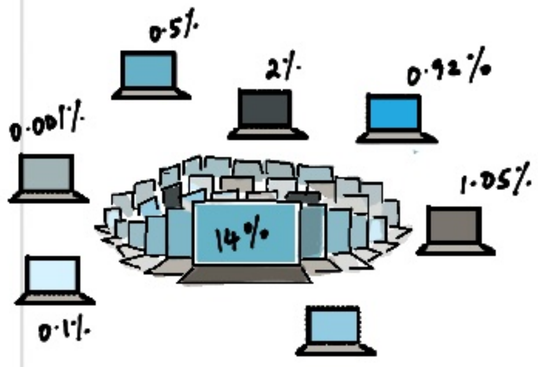
BITCOIN USES DIGITAL SIGNATURES TO TRACE OWNERSHIP AND A PUBLIC DISTRIBUTED LEDGER AS THE SOURCE OF TRUTH THAT NODES VERIFY



THE PROOF OF WORK PROCESS DURING BLOCK CREATION ENSURES THROUGH VERIFICATION AND OWNERSHIP THAT THE SAME BITCOIN IS NOT BEING DOUBLE-SPENT



BITCOIN SOLVES THE BYZANTINE GENERAL'S PROBLEM OF TRUST, WITHOUT EXPLICITLY SAYING SO, IN A PROBABILISTIC MANNER



PROBABILISTIC - AS MINERS COMPETE AMONGST EACH OTHER, THOSE WITH HIGHER HASHRATES ARE MORE LIKELY TO WIN THE MINING REWARD



REWARDS & FEES

REWARDS & FEES

THE MINER'S REWARD FOR CREATING A NEW BLOCK IS 50 NEW BITCOINS + TRANSACTION FEES

50

THIS REWARD IS HALVED AFTER EVERY 210,000 BLOCKS

25

MAXIMUM NUMBER OF HALVINGS ALLOWED TO MINT NEW BITCOIN

64

IN 2016, AT BLOCK 420,000, THE REWARD HALVED AGAIN

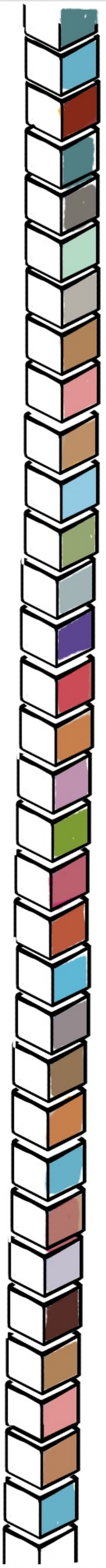
12.5

AFTER 64 HALVINGS, THE REWARDS WILL BE ONLY TRANSACTION FEES

∅

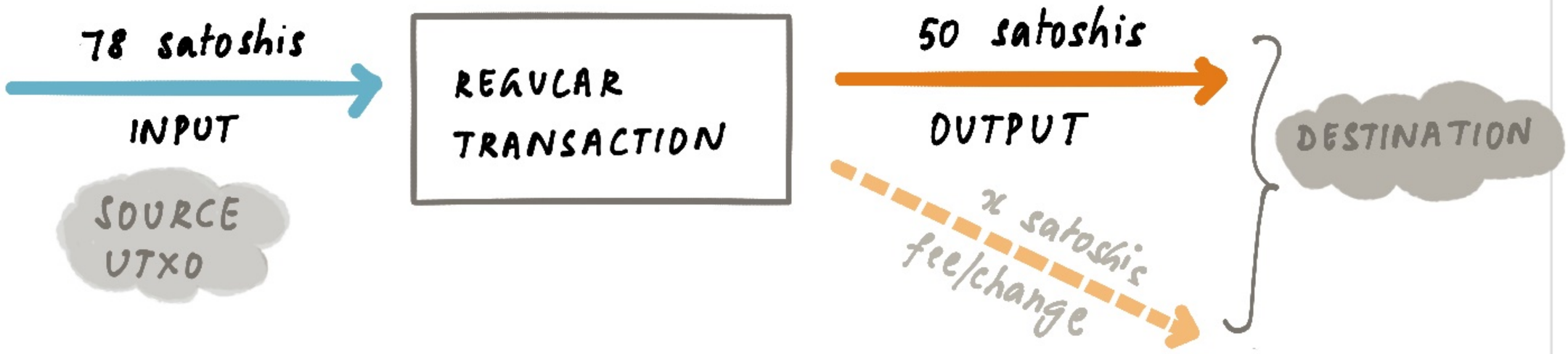
13.4 MILLION BLOCKS LATER, AROUND 2140, THERE WILL BE 21 MILLION BITCOINS IN CIRCULATION

FIXED MONEY SUPPLY

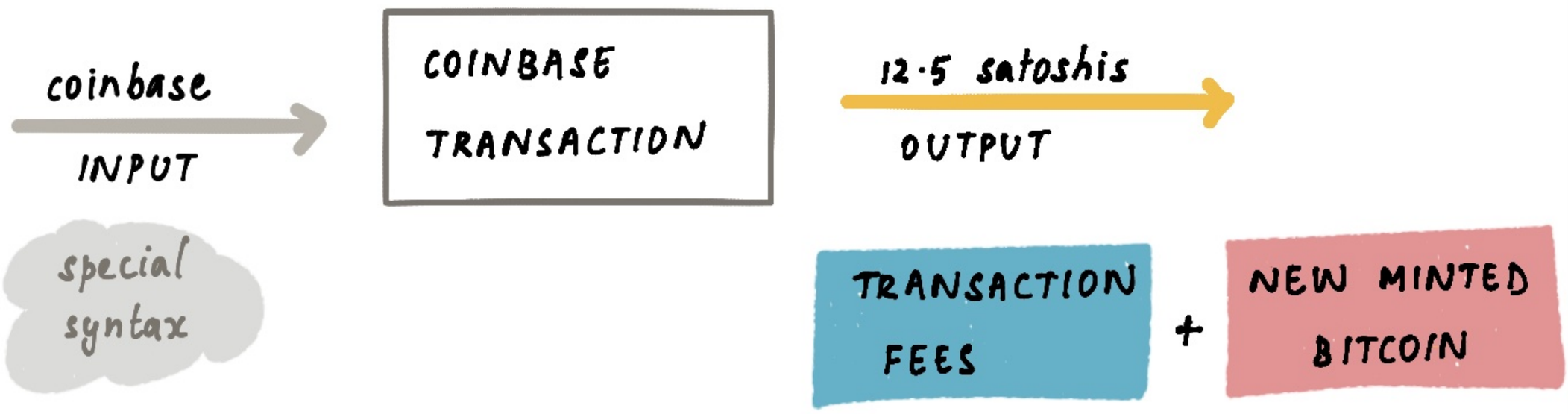


TRANSACTIONS FOR REWARDS/FEES

ALL TRANSACTIONS HAVE AN INPUT AND OUTPUT



A COINBASE OR GENERATION TRANSACTION HAS A DIFFERENT INPUT



WHAT MAKES IT SPECIAL?



IT IS THE FIRST TRANSACTION IN ANY BLOCK



IT IS THE REWARD FOR THE MINER WHO CREATED THE BLOCK

NOT TO BE CONFUSED WITH COINBASE, THE CRYPTO EXCHANGE



THE REWARDS/FEES WILL BE AVAILABLE 100 BLOCKS LATER

EVERY NODE VERIFIES EVERY TRANSACTION

NODES MAKE BLOCKS + SHOW PROOF OF WORK

EVERY NODE VERIFIES NEW BLOCK

NODES ADD TO THE CHAIN WITH HIGHEST DIFFICULTY

CONSENSUS!

VERIFY BLOCKS

VERIFYING BLOCKS

- ALL BLOCKS INDEPENDENTLY VALIDATE EACH BLOCK
- ONLY VALID BLOCKS ARE PROPAGATED

VALIDATION CRITERIA

- [ ] BLOCK SYNTAX /STRUCTURE
- [ ] PROOF OF WORK (HASH < TARGET)
- [ ] TIMESTAMP
- [ ] FIRST TXN IS A COINBASE TXN
- [ ] BLOCK HAS VALID TRANSACTIONS

WHEN NODES CHEAT, SAY, BY ATTEMPTING TO CHANGE REWARDS OR DOUBLE SPEND, IT IS THIS INDEPENDENT VALIDATION THAT GETS INVALID TRANSACTIONS OR BLOCKS TO STOP PROPAGATING. IT WASTES THE RESOURCES AND AIMS TO DEINCENTIVISE DISHONEST MINING.

EVERY NODE VERIFIES EVERY TRANSACTION

NODES MAKE BLOCKS + SHOW PROOF OF WORK

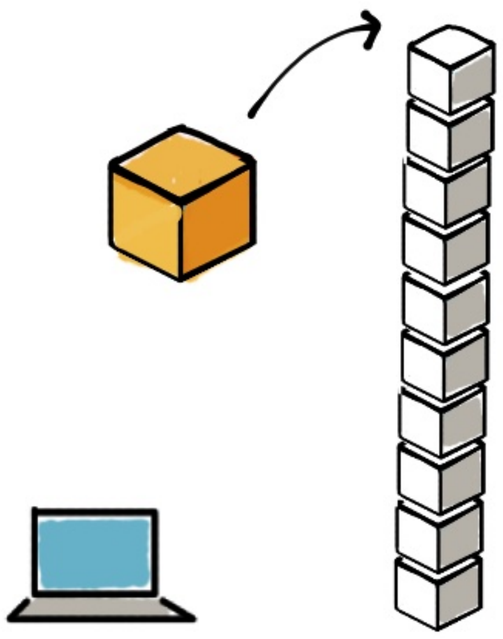
EVERY NODE VERIFIES NEW BLOCK

NODES ADD TO THE CHAIN WITH HIGHEST DIFFICULTY

CONSENSUS!

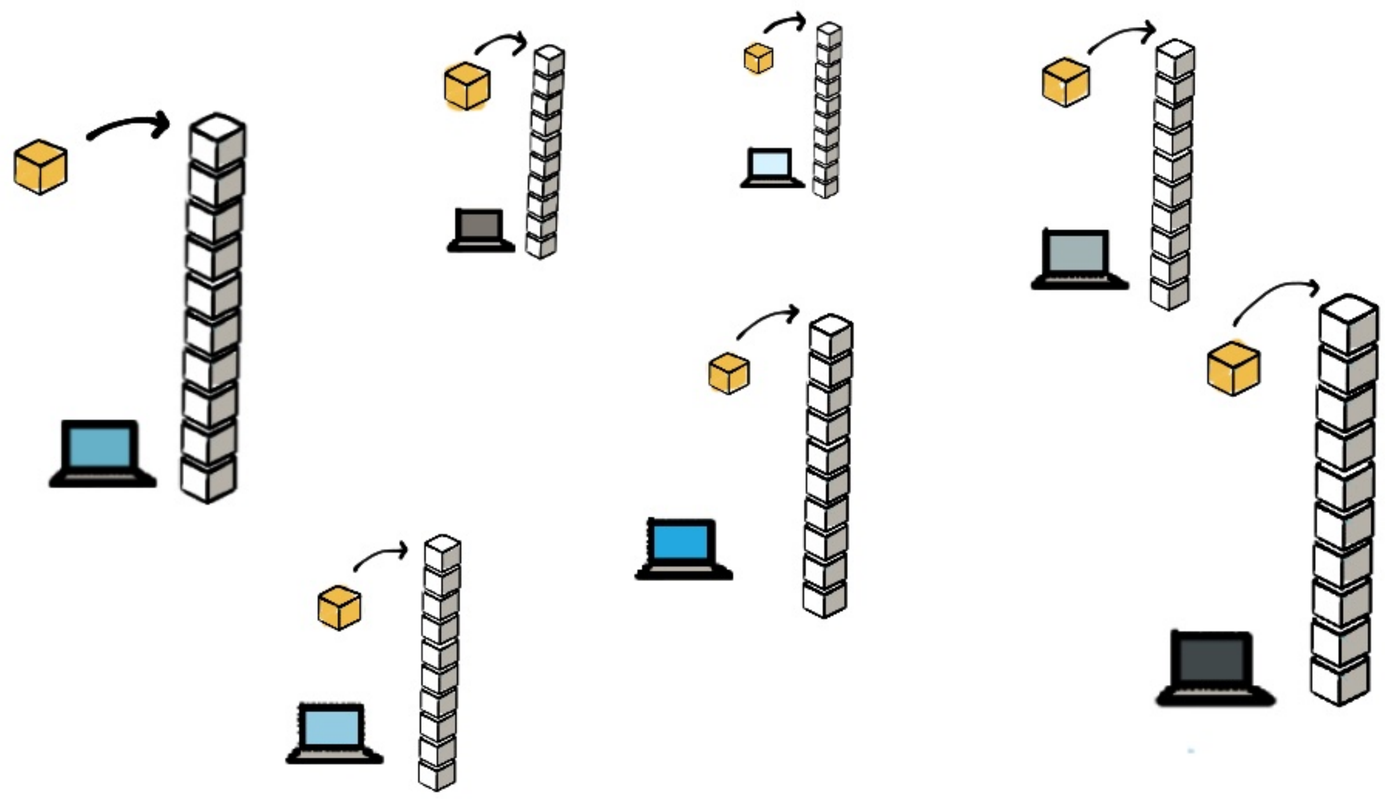
ADD BLOCK TO CHAIN

ADD BLOCK TO CHAIN



THE NODE MUST NOW ADD THE NEW BLOCK TO THE CHAIN

THE NODE WILL CHOOSE THE CHAIN CONTAINING THE BLOCK WHICH IS THE 'PREVIOUS BLOCK HASH' OF THE NEW ONE



THIS PARENT WILL LIKELY BE AT THE TOP OF THE CHAIN.

ALL OTHER BLOCKS WILL DO THE SAME

INCONSISTENCIES AND FORKS

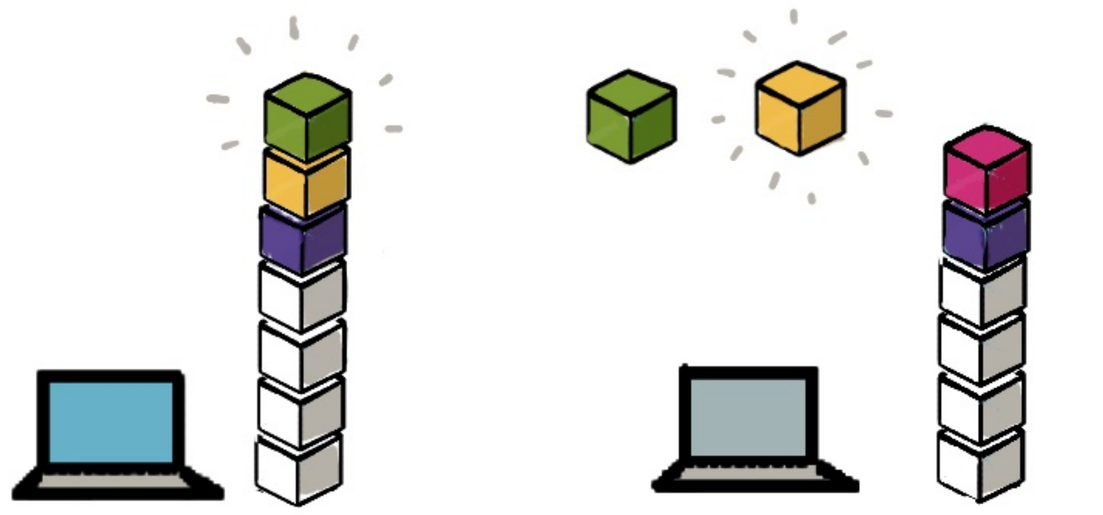
NODES HAVE A CONSISTENT VIEW OF THE BLOCKCHAIN — SOMETIMES THAT CHANGES.



DUE TO NETWORK DELAYS, NODES RECEIVE DIFFERENT BLOCKS & EXTEND THE CHAIN



SOME MINERS FIND AND PROPAGATE THE NEXT BLOCK, WHILE OTHERS JUST RECEIVE THE NEWLY MINED BLOCKS



THE MINERS CAN SEE TWO VERSIONS OF CHAINS AND ADD THE BLOCK(S) TO THE CHAIN WITH MORE PROOF OF WORK



USUALLY THESE FORKS ARE RESOLVED WITHIN A BLOCK AND ALL NODES RECONVERGE



TRANSACTIONS IN THIS BLOCK, BUT NOT IN THE SUBSEQUENT BLOCKS GO BACK TO THE MEMPOOL

ACHIEVE CONSENSUS

EVERY NODE VERIFIES EVERY TRANSACTION

NODES MAKE BLOCKS + SHOW PROOF OF WORK

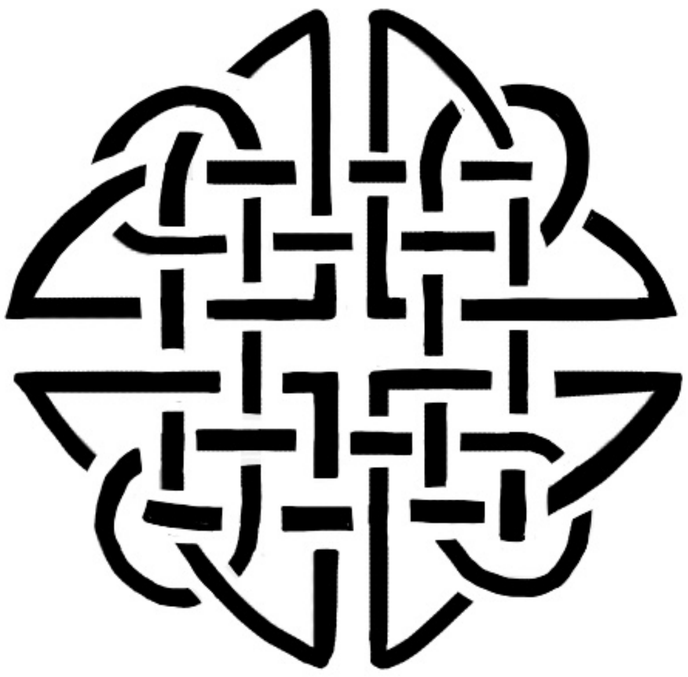
EVERY NODE VERIFIES NEW BLOCK

NODES ADD TO THE CHAIN WITH HIGHEST DIFFICULTY

CONSENSUS!

ON CONSENSUS

PURPOSE



CONSENSUS PROTOCOLS LIKE PROOF OF WORK ENSURE THE INTEGRITY OF DATA HELD IN A BLOCKCHAIN

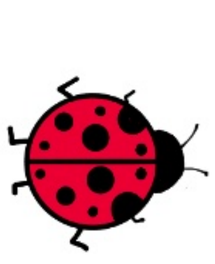
OTHER CONSENSUS PROTOCOLS

PROOF OF WORK
PROOF OF STAKE
DELEGATED PROOF OF STAKE
PROOF OF ACTIVITY
PROOF OF IDENTITY
PROOF OF ELAPSED TIME
PROOF OF CAPACITY
PROOF OF IMPORTANCE
PURE PROOF OF STAKE

INCONSISTENCIES



NETWORK DELAYS MAY CAUSE A TEMPORARY FORK





BUGS OR RULE CHANGES MAY CAUSE HARD FORKS - LEADING TO SEPARATE CHAINS

HOWEVER...

CONSENSUS PROTOCOLS CREATE SHARED AGREEMENT AND ENABLE DECENTRALISATION

THESE PROTOCOLS ARE MANAGED AND IMPLEMENTED THROUGH A GOVERNANCE STRUCTURE.

HOW DECENTRALISED IS THIS 'CORE' GROUP OF INDIVIDUALS OR ORGANISATIONS?

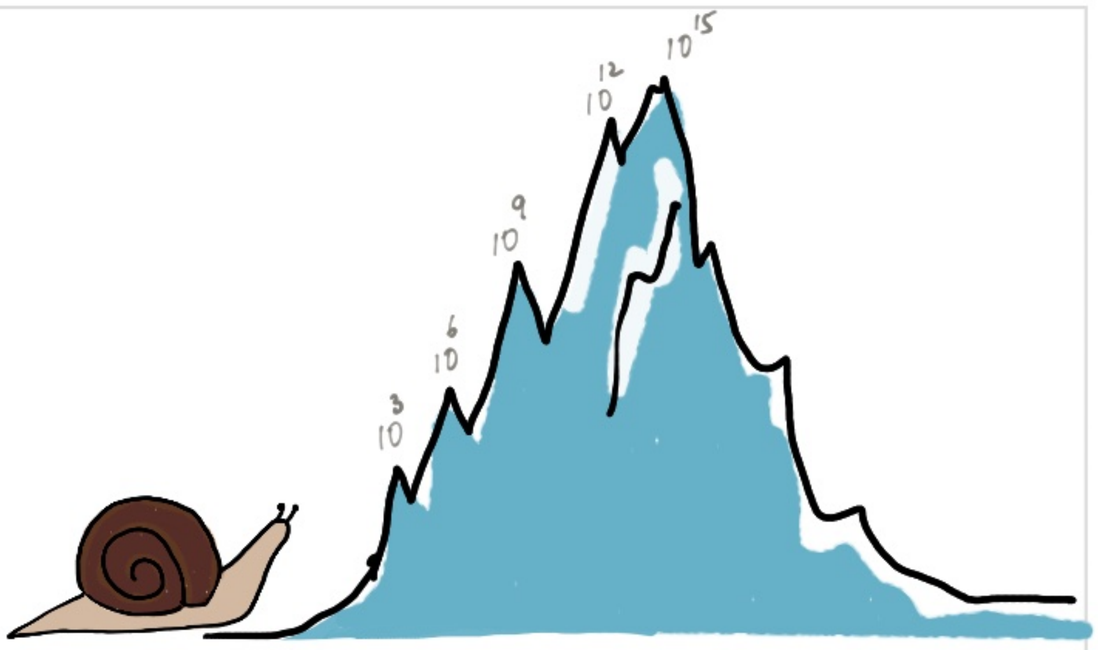
PROOF OF WORK



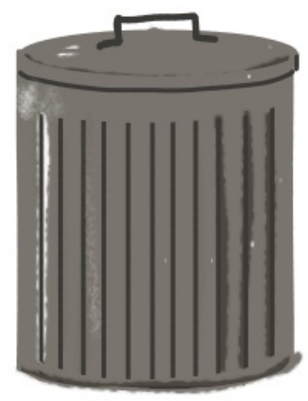
REQUIRES ENORMOUS
AMOUNT OF COMPUTATION



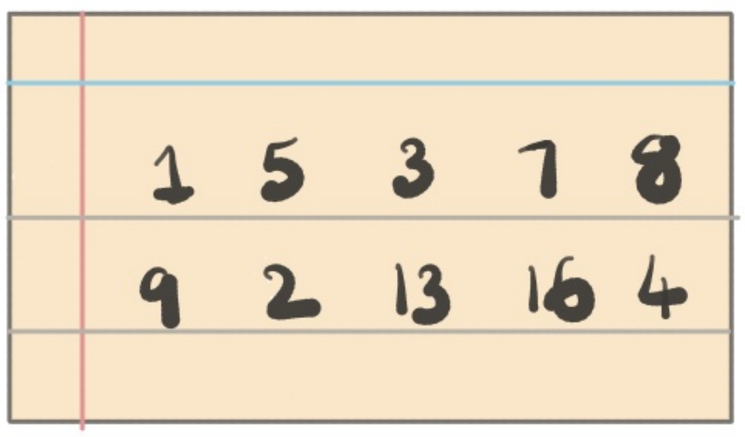
~5-20 TXNS PER SECOND
GET PROCESSED ON BLOCKCHAINS
VISA → 20,000/sec



SCALABILITY IS LIMITED
DUE TO COST OF
HARDWARE AND ELECTRICITY



RESOURCES ARE WASTED
WHEN A NODE TRIES
TO TAMPER WITH RECORDS
AS ALL HAVE TO AGREE



THE WINNING MINER GETS
TO CHOOSE THE ORDER OF
TRANSACTIONS - FAIR OR NOT



IT IS A STEP TO CONSENSUS
MINUS A THIRD PARTY.
THIS HAS SPARKED DEBATES
AROUND EFFICIENCY AND WASTE

COST OF MINING



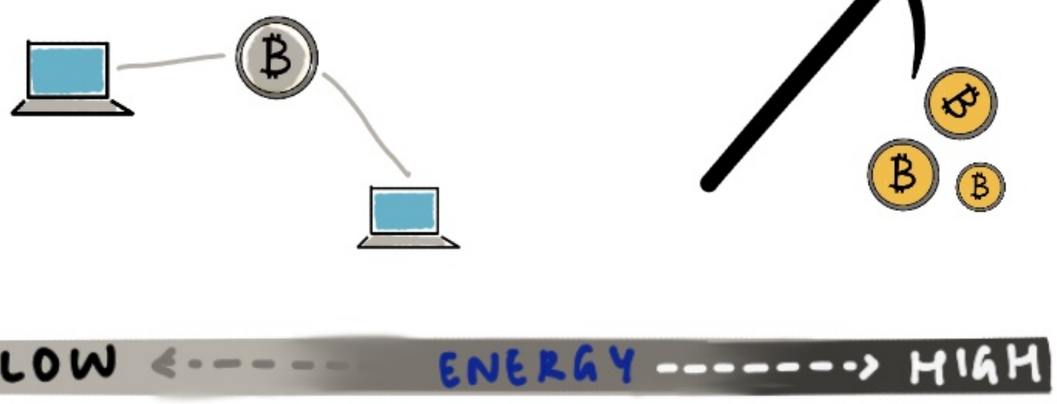
A MINING NODE OR RIG NEEDS CONSTANT POWER TO RUN AND TO KEEP COOL





BITCOIN CONSUMES THE ANNUAL ENERGY EQUIVALENT OF SWEDEN/PAKISTAN

ccaf.io/cbeci/index



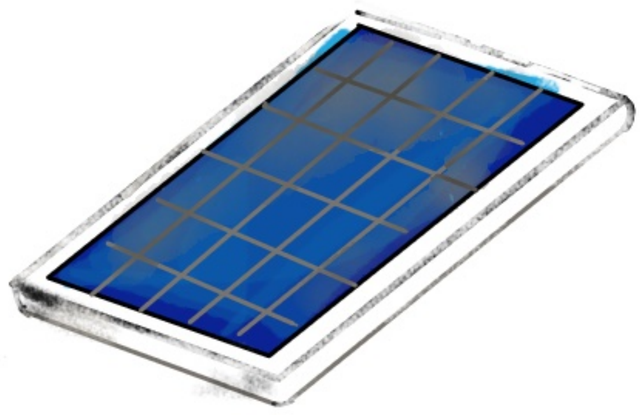
MINING BITCOIN CONSUMES MORE ENERGY THAN TRANSACTING WITH BITCOIN



ENERGY CONSUMED RELATES TO CARBON EMISSIONS WHEN 'DIRTY' ENERGY IS USED



THE EFFORTS OF ALL NODES THAT DID NOT WIN REWARDS ALSO GET WASTED



THIS INHERENTLY INEFFICIENT MODEL CANNOT BE IMPROVED WITH RENEWABLES

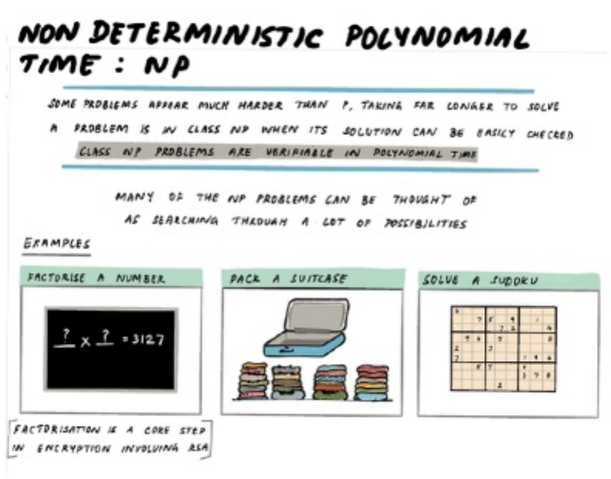
A COMPLEXITY ISSUE

IT TAKES A SIGNIFICANT AMOUNT OF TIME TO FIND A STRING OR NUMBER MATCHING THE CRITERIA FOR THE TARGET HASH





IT TAKES ONLY ONE COMPUTATION TO VERIFY IF A HASH CAME FROM A CERTAIN STRING



THIS PROBLEM FALLS INTO THE COMPLEXITY CLASS : NP SEARCH

Refer to the Thoughtworks Illustrated Guide to Quantum Computing for more detail

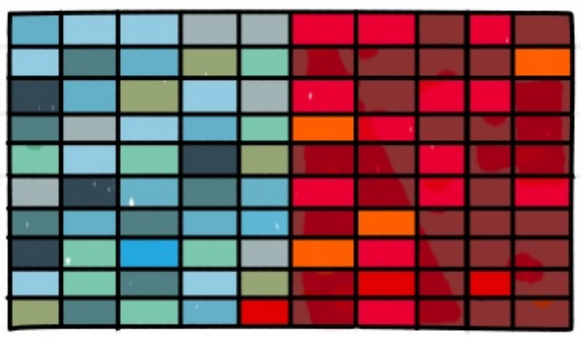
THUS, IT APPEARS THAT BLOCKCHAIN IS VULNERABLE TO

- A MATHEMATICAL PROOF THAT P=NP
- FUNCTIONING QUANTUM COMPUTERS THAT CAN USE
  - GROVER'S ALGORITHM TO SPEED UP FINDING HASHES
  - SHOR'S ALGORITHM TO BREAK DIGITAL SIGNATURES

CONSENSUS ATTACKS

A 51% ATTACK

WHAT IS A 51% ATTACK?



A MALICIOUS ATTACK

THREATENING THE INTEGRITY

OF A BLOCKCHAIN

BY A MINING GROUP

WITH 50% OR MORE

COMPUTING POWER

A 51% ATTACK CANNOT

✗ STEAL/SPEND OTHERS' BITCOIN

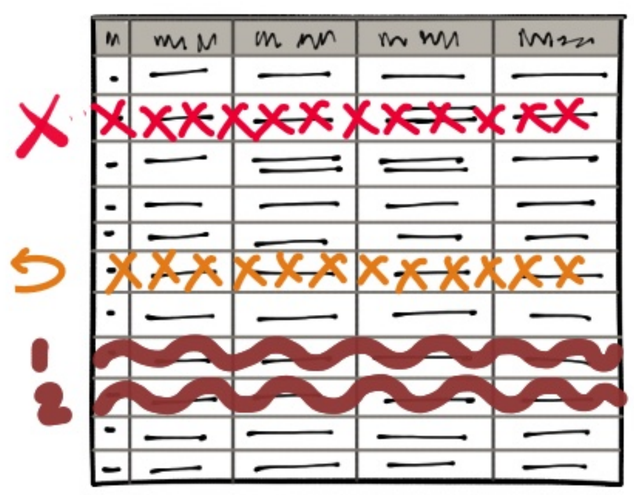
✗ VALIDATE INVALID TXNs

✗ REVERSE OTHER TRANSACTIONS

✗ CHANGE RULES/REWARDS/FEES

✗ CHANGE A BLOCK

A 51% ATTACK COULD



- EXCLUDE SOME TRANSACTIONS
- REVERSE OWN TRANSACTIONS
- DOUBLE SPEND TRANSACTIONS
- ATTACK AS DENIAL OF SERVICE

EXPENSIVE, NOT IMPOSSIBLE

REQUIRES MORE POWER IN

A BIGGER NETWORK

POSSIBLE MEASURES

INSTALL CHAIN REORGANISATION

TRACKERS - reorg tracker

(see dci.mit.edu/51-attacks)

A COMPARISON

A SIDE-BY-SIDE LIST OF SOME OF THE FEATURES OF THE BITCOIN AND ETHEREUM BLOCKCHAINS

BITCOIN V ETHEREUM

	BITCOIN	ETHEREUM
BEGAN IN YEAR	2009	2015
AS AN IDEA OF	SATOSHI NAKOMOTO	VITALIK BUTERIN
CURRENCY	BITCOIN	ETHEREUM
CONSENSUS METHOD	PROOF OF WORK	PROOF OF STAKE
BLOCK TIME	10 MINS	~14 SEC
CODE SUPPORT	SCRIPTING	TURING COMPLETE
LEDGER TYPE	TRANSACTION BASED	ACCOUNT BASED
USERS / HASHES	A LOT	A LOT LESS!
REWARDS	STEADY HALF OVER TIME	HAS VARIED
FEES	OPTIONAL	MANDATORY

BUILDING THE WEB3 ECOSYSTEM

WILL IT BE USEFUL?

TO RECAP, WEB3 IS BUILT ON THE FOLLOWING FEATURES

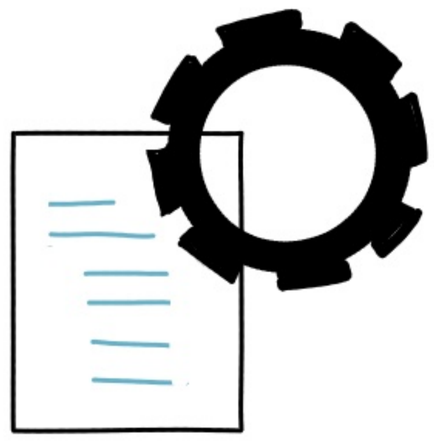
- VERIFICATION
- TRACEABILITY
- TRANSPARENCY
- SECURITY
- DISTRIBUTED OWNERSHIP
- MIGHT REDUCE COST } OF TRANSACTIONS
- MIGHT INCREASE SPEED }
- POSSIBLY BYPASS LAWS/CENSORSHIP
- NO INTERMEDIARIES
- A NEW WAY TO TRADE AND INTERACT

SETTING ASIDE THE ENERGY COSTS AND OTHER ILLS OF THE BLOCKCHAIN, LET US FOCUS ON ONLY THE TECHNOLOGY ASPECT.

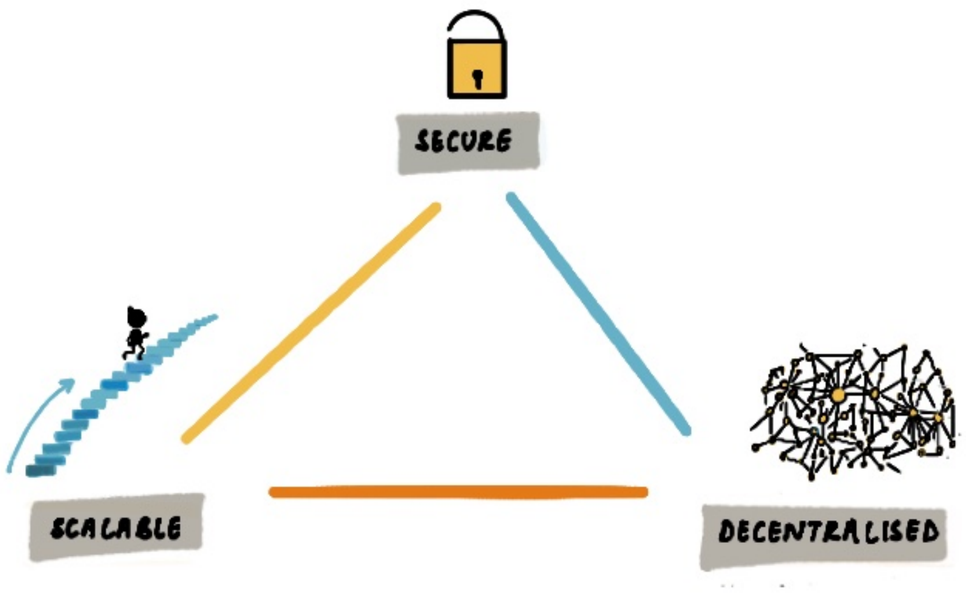
THIS SECTION EXPLORES THE DIMENSIONS THAT THE ADVOCATES SEE FOR IT TO BE APPLIED IN PRACTISE.

PATH WE TAKE

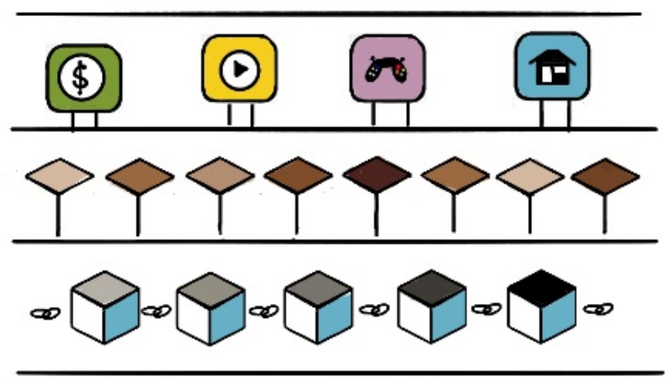
THIS SECTION BUILDS UP UNDERSTANDING OF SOME ADDITIONAL FEATURES THAT COMPRISE WEB3'S ECOSYSTEM



① SMART CONTRACTS



② BLOCKCHAIN TRILEMMA



③ BLOCKCHAIN LAYERS



④ DECENTRALISED APPS



⑤ TOKENS & MORE

1 SMART CONTRACTS

WHAT IS A CONTRACT?

A CONTRACT IS A PROMISE OR PERFORMANCE

IN EXCHANGE FOR PROMISE OR PERFORMANCE



LARRY LESSIG



A VENDING MACHINE IS OFTEN USED AS A WAY TO THINK OF A 'PERFORMANCE FOR A PERFORMANCE' CONTRACT

IF I PUT A COIN IN, I GET A DRINK

TERMS OF THE CONTRACT

✓ CORRECT DRINK
↳ AN OBVIOUS TERM

✓ SAFE DRINK
↳ IMPLIED BY LAW

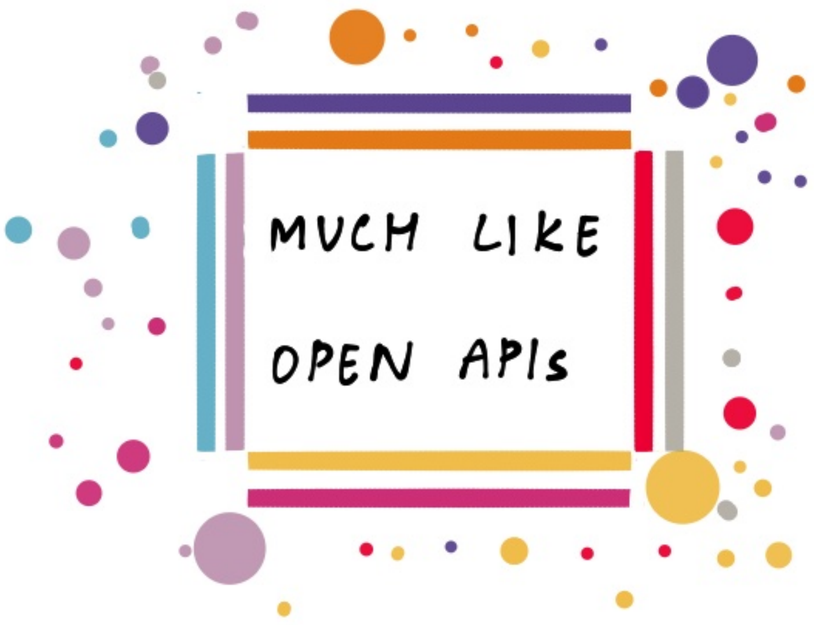
FOR IMPLICIT TERMS

THE LEGAL SYSTEM IS 'PRESENT' IN A CONTRACT -

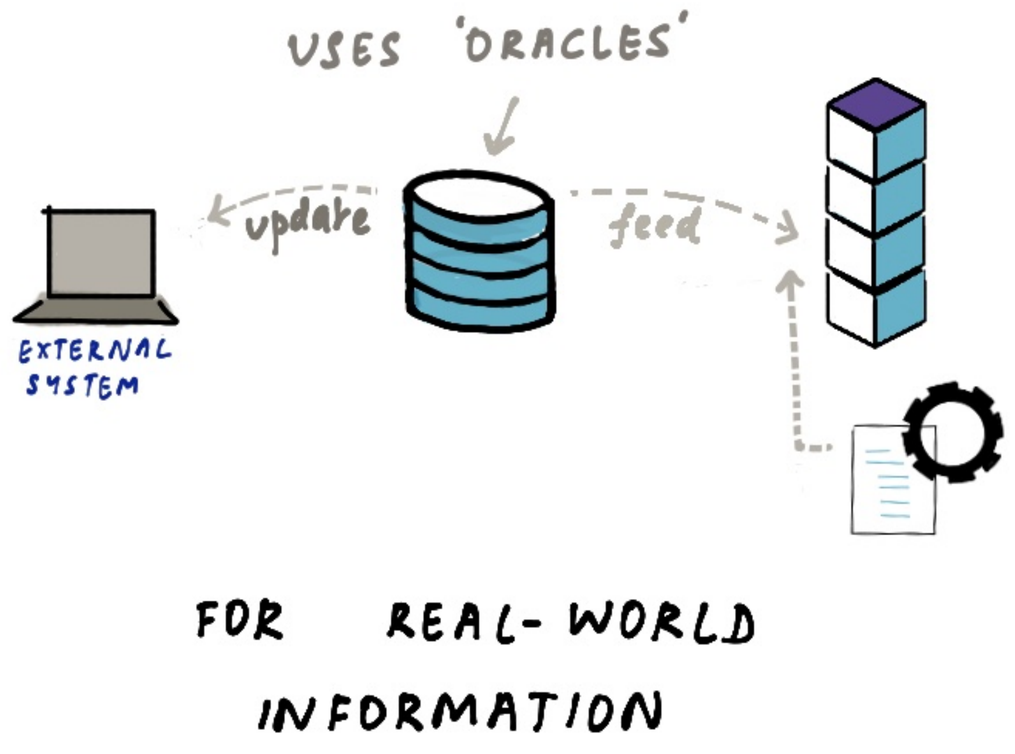
- TYPES
- TERMS
- ITS EFFECTS AND MORE

A SMART CONTRACT...

IS PUBLIC & EXTENDABLE



NEEDS DATA FEEDS



FOR REAL-WORLD INFORMATION

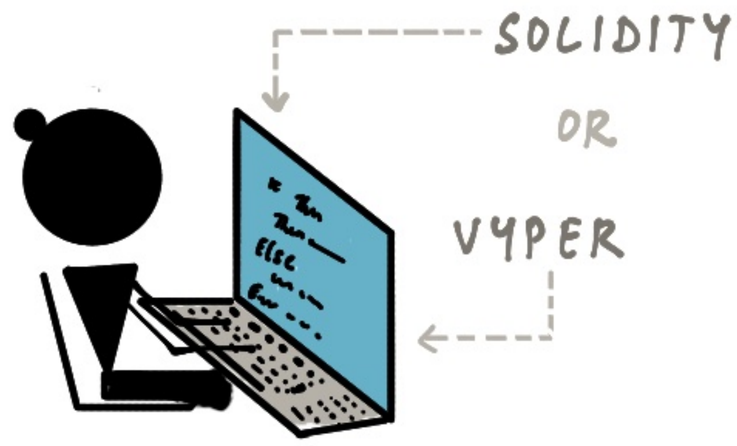
NEEDS NO INTERMEDIARIES

SUCH AS:

- LAWYERS
- BANKS
- MIDDLE PERSONS

ALLEGEDLY TO REDUCE COST/TIME

NEEDS PROGRAMMERS



INDEPENDENT THIRD PARTY TO CODE THE SMART CONTRACT

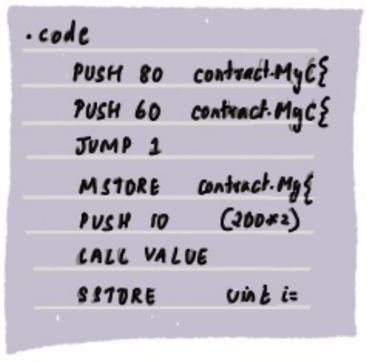
CANNOT BE DELETED



... CAN BE FUDGED

NOT IMMUTABLE

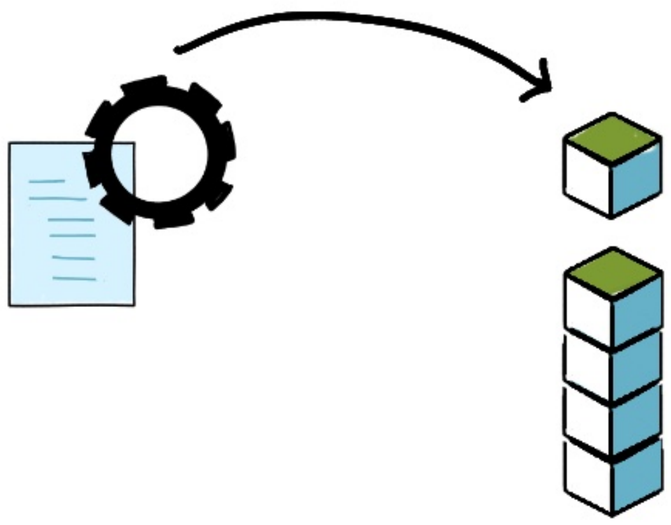




BYTECODE CAN BE UPDATED IN PLACE!

A SMART CONTRACT...

IS STORED ON A BLOCKCHAIN



IRREVERSIBLE
INTERACTION

IS MORE LIKELY TO BE ON



THE ETHEREUM
BLOCKCHAIN

... IN BITCOIN

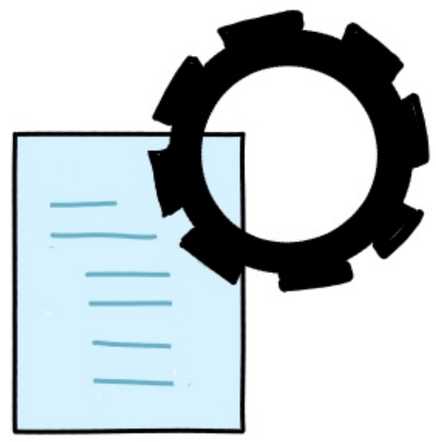
IS BASIC

NOT TURING
COMPLETE

SETS CONDITIONS
FOR SPENDING

IS A TYPE OF ETHEREUM A/C

called
CONTRACT
ACCOUNT



- HAS A BALANCE
- IS A TRANSACTION TARGET
- NOT HUMAN-CONTROLLED

DOES NOT RUN AUTOMATICALLY



AN EXTERNALLY OWNED ACCOUNT
HUMAN A/C MUST TRIGGER IT

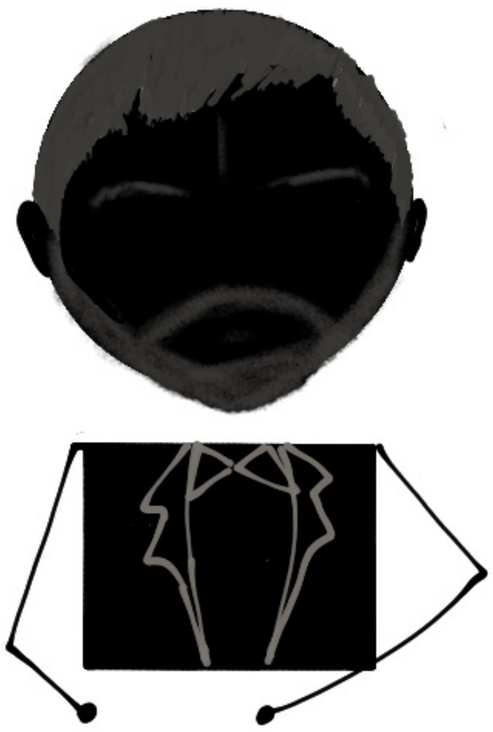
TRIGGERS CODE

transferToken()

createNewContract()

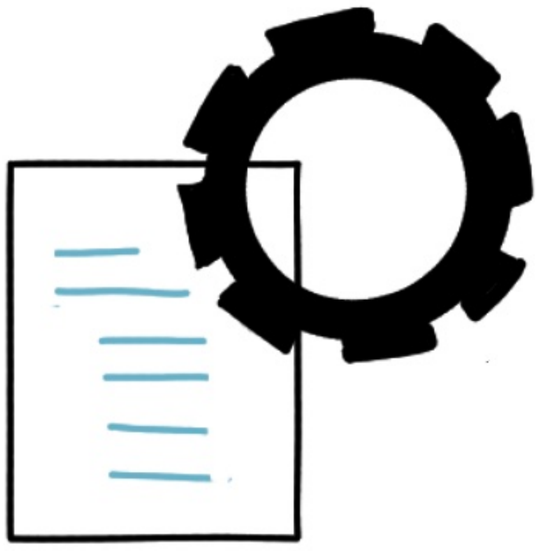
WHEN ANOTHER ACCOUNT
(HUMAN OR CODE)
INTERACTS WITH IT

WHAT IS A SMART CONTRACT?



A SMART CONTRACT IS
A COMPUTERISED TRANSACTION PROTOCOL
THAT EXECUTES
THE TERMS OF A CONTRACT

NICK SZABO



A SMART CONTRACT IS
A SET OF PROMISES
STORED ON A BLOCKCHAIN
IN PROGRAM FORM

HOWEVER IT IS ...

✗ NOT SMART

IT DOES NOT POSSESS
(AS OF NOW, 2023)
ARTIFICIAL INTELLIGENCE

✗ YET NOT A CONTRACT

SMART CONTRACTS ARE
NOT LEGALLY ENFORCED
IN CASE OF VIOLATION

WHAT A CONTRACT DOES AND DOES NOT

HANDLING RISKS

WHAT DOES CONTRACT LAW DO ABOUT RISK?

a) ELIMINATES RISK

b) ALLOCATES RISK

THE ANSWER IS **b)** **ALLOCATE RISK,** ASSUMING OF COURSE, A SENSIBLE LEGAL SYSTEM TO PROCESS ANY BREACHES.

LEVEL OF CLARITY

CONTRACTS COVER EVERY POSSIBLE SCENARIO —

a) TRUE

b) FALSE

THE ANSWER IS **b) FALSE** NOT ALL SCENARIOS ARE LIKELY. WHEN OPEN TO INTERPRETATION, THERE IS VALUE IN VAGUENESS.

WHEN CONTRACT LAW MEET TECHNOLOGY

TECHNOLOGY IS ALWAYS CONSISTENT WITH LAW —

a) TRUE

b) FALSE

THE ANSWER IS **b) FALSE.** TECHNOLOGY WILL VERY OFTEN CHALLENGE THE LAW.

A COMMON EXAMPLE IS COPYRIGHT LAW AND DRM WHERE DRM SOMETIMES PREVENTS FREE/FAIR USE.

SMART CONTRACTS: CONCERNS

WHERE CAN I USE A SMART CONTRACT?

IN A MORE WELL DEFINED SITUATION

BUT, USED IN

- DIGITAL ASSETS
- DECENTRALISED FINANCE

ARE SMART CONTRACTS ACCURATE?



HOW DO WE TRUST?

- PLATFORM
- PROGRAMMER
- ORACLE

WHAT ARE THE SERVICE LEVEL AGREEMENTS (SLAs)?



SMART CONTRACTS ARE SUSCEPTIBLE TO

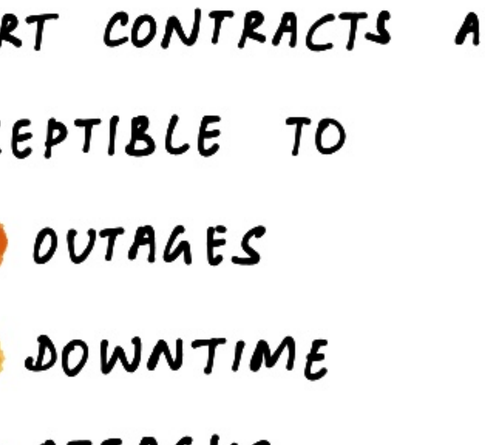
- OUTAGES
- DOWNTIME
- ATTACKS

HOW CAN I ROLLBACK FROM A SMART CONTRACT EXECUTION?



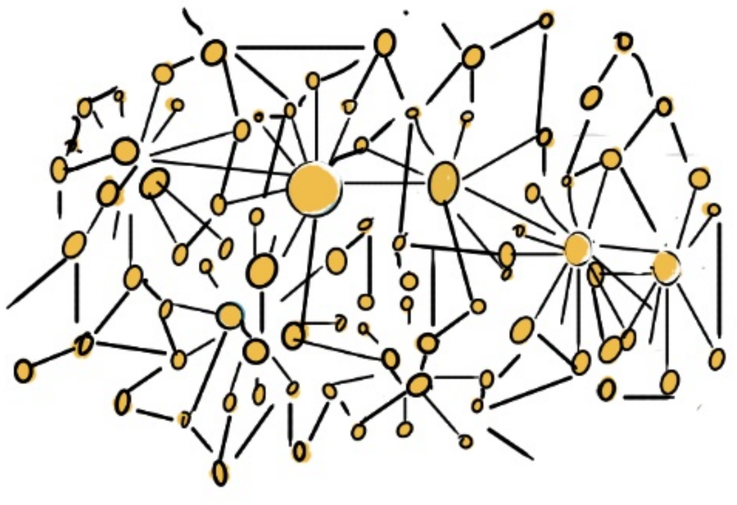
THE TRANSACTIONS ARE NOT REVERSIBLE EVEN IF IT IS IN ERROR

WHO OWNS THE 'ORACLE'?



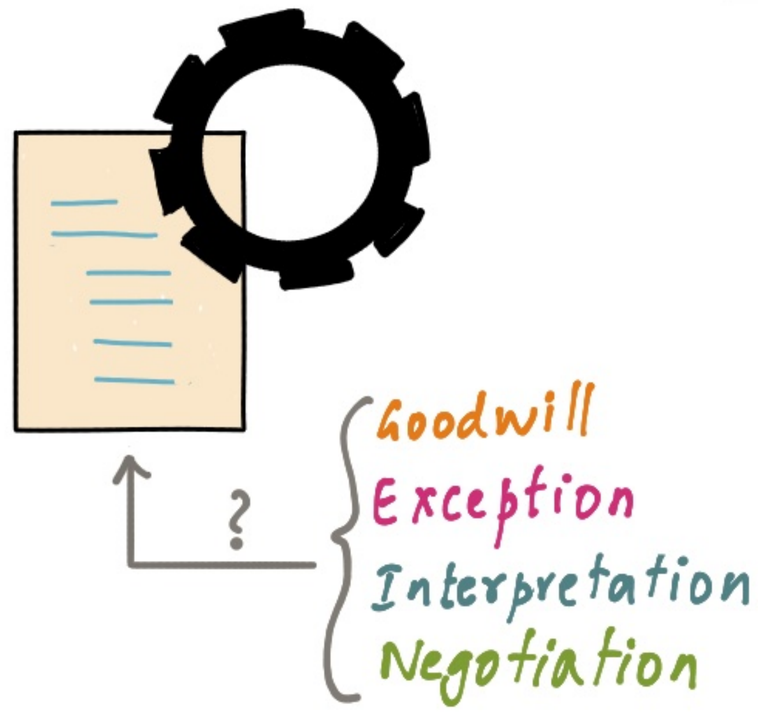
HOW DOES IT FIT WITH THE DECENTRALISED 'THEME'?

IS IT POSSIBLE TO ALWAYS/EVER HAVE DECENTRALISED ORACLES?



SMART CONTRACTS: CONCERNS

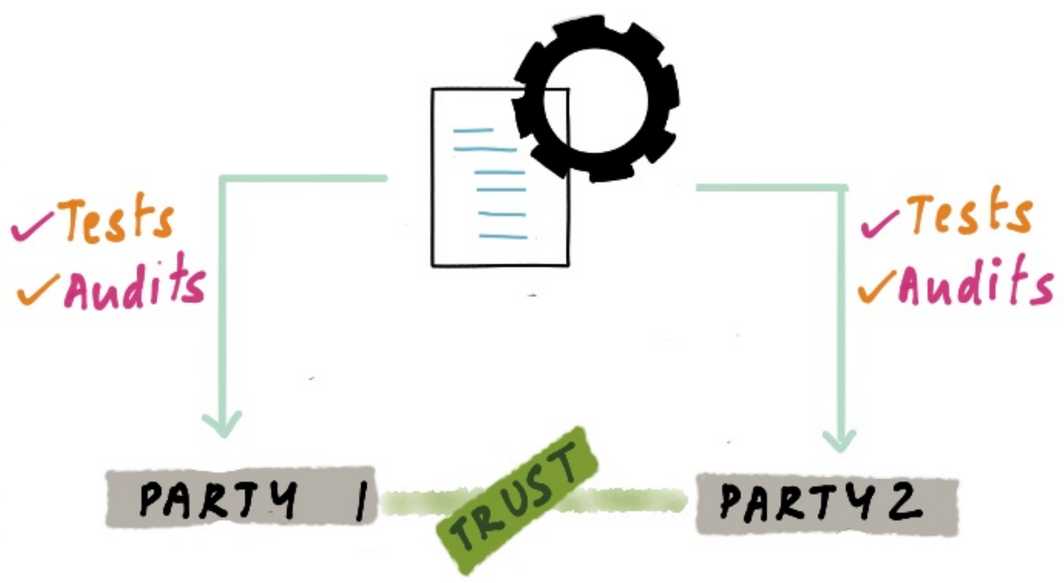
CAN OBJECTIVE CODE ACCOMODATE REAL-WORLD SUBJECTIVITY?



BYTECODE UPDATES COMPLETELY GO AGAINST EVERY TRUST MODEL!

SOFTWARE PROBES EXIST THAT DETECT IF CODE WAS CHANGED ON THE SLY

CAN PLATFORMS AND PROCESSES REPLACE HUMAN RELATIONSHIPS?



IS CODE TOO TECHNICAL FOR NON-PROGRAMMERS, LAWYERS?

FUNCTIONS
LIBRARIES
MODULARITY
ABSTRACTION
RECURSIONS
NESTED
CONDITIONAL
STATIC TYPIC
FRAMEWORKS
CLOSURE
VARIABLES
CONSTANTS
SCRIPTS
METHODS
DECLARE
LOOPS

ARE SMART CONTRACTS TAXED OR REGULATED IN ANY WAY?

VARIABLE BY COUNTRY
&
POSSIBLY NOT FULLY ACCOUNTED

ARE SMART CONTRACTS ENFORCEBLE BY LAW?



DEBATES BEGINNING TO HAPPEN

2 BLOCKCHAIN TRILEMMA

THE BLOCKCHAIN TRILEMMA

THERE IS A TRADE OFF BETWEEN 3 QVALITIES.

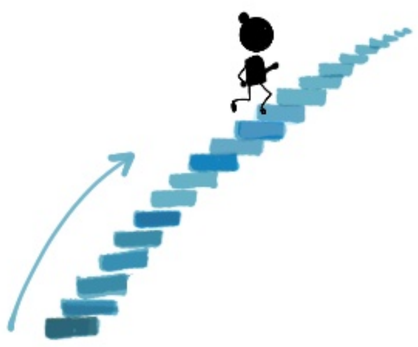
ONE MUST BE COMPROMISED TO GET THE OTHER TWO.

THIS IS THE BLOCKCHAIN TRILEMMA.



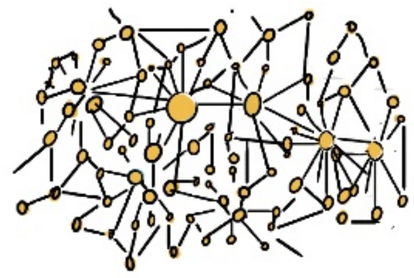
SECURE

HOW PROTECTED IS
THE DATA
FROM ATTACK / MISUSE ?



SCALABLE

HOW MANY
TRANSACTIONS PER SECOND
CAN IT PROCESS?



DECENTRALISED

TO WHAT EXTENT
DOES A SINGLE AUTHORITY
CONTROL OPERATIONS?

ARE ALL BLOCKCHAINS EQUAL?

WHO OWNS INFRASTRUCTURE?

- NETWORK MEMBERS → PUBLIC BLOCKCHAIN
- PRIVATE ORGANISATION → PRIVATE BLOCKCHAIN

WHO CAN JOIN?

- EVERYONE → PERMISSIONLESS BLOCKCHAIN
  - Incentives based security

WHO HAS RIGHTS?

- CHOSEN ONES → PERMISSIONED BLOCKCHAIN
  - NO proof-of-work
  - NO native currency



Are the private/ permissioned ones even 'blockchains'?

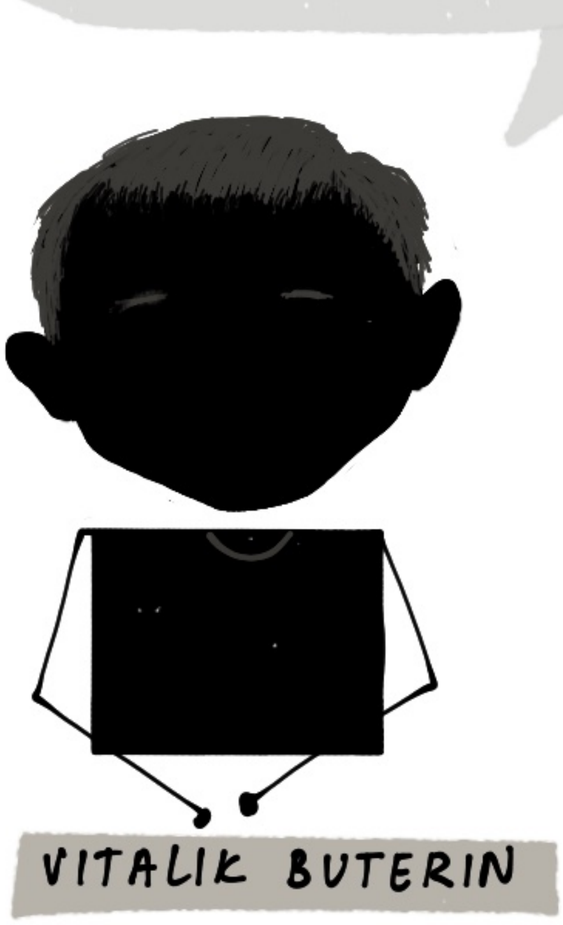


Distributed Ledger Technology DLT is a description that fits them all

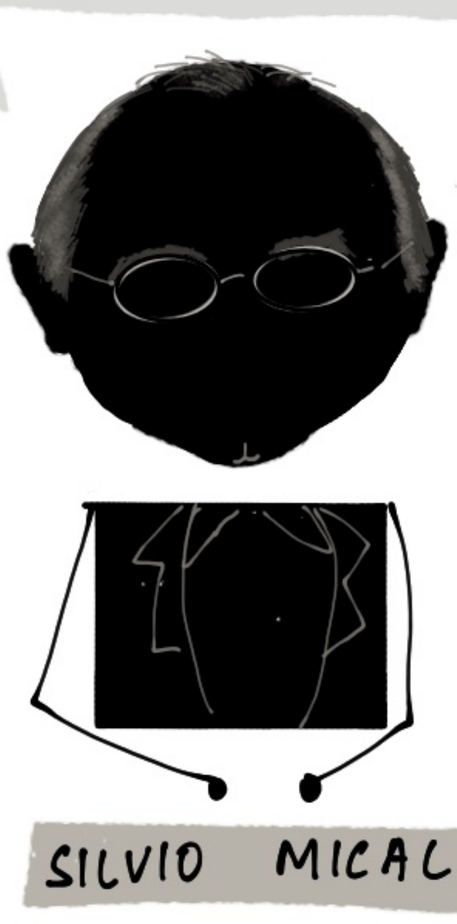
BLOCKCHAIN LAYERS

I came up with the trilemma. No blockchain can have these three qualities at once

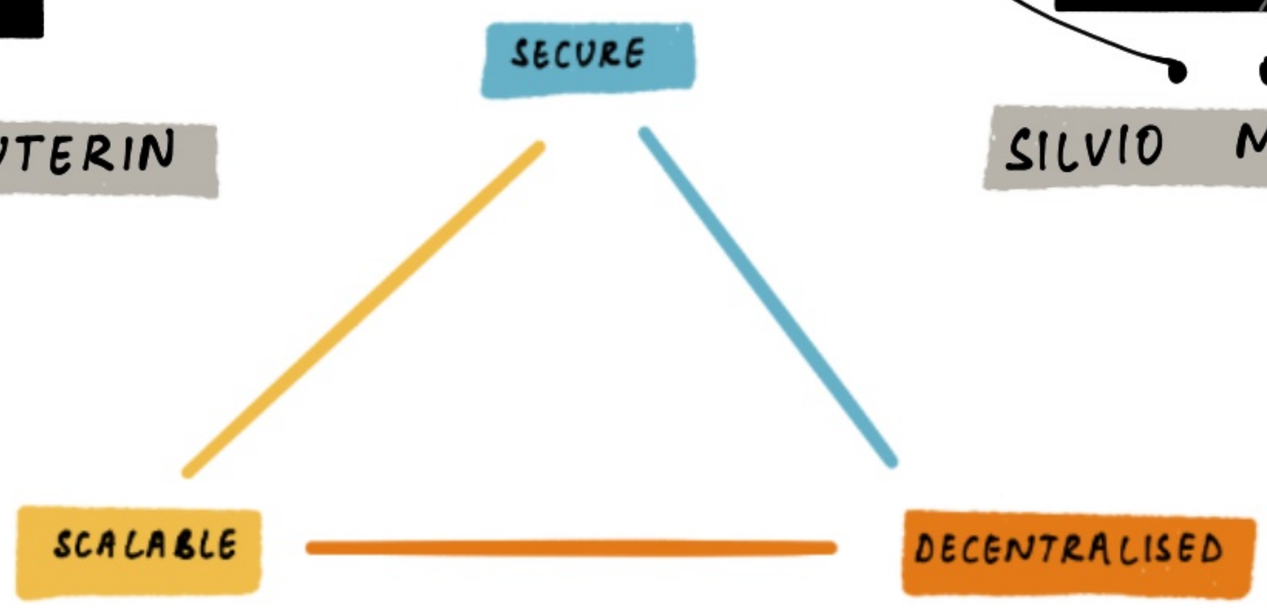
I disagree. We need some more mathematics to solve it. Otherwise why blockchain at all!



VITALIK BUTERIN



SILVIO MICALI



AS A RESPONSE TO SOLVING THE SCALABILITY ASPECT OF THE TRILEMMA, PEOPLE HAVE TRIED TO IMPROVE TRANSACTION SPEEDS

THE TERM LAYER IS MENTIONED IN THIS CONTEXT

---

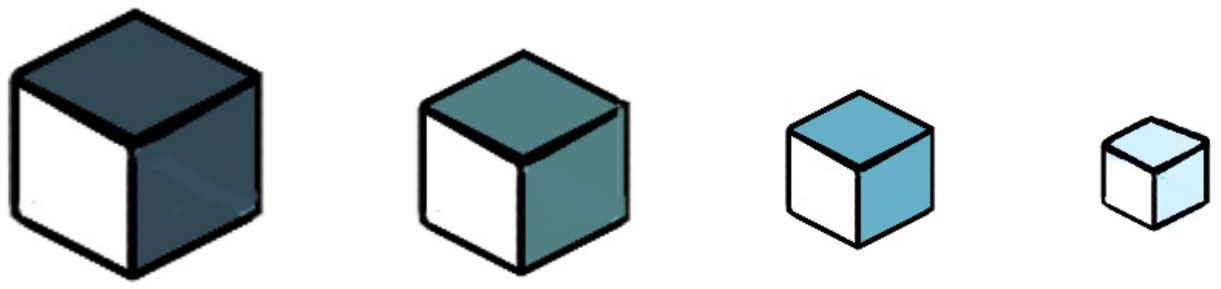
3 BLOCKCHAIN LAYERS

LAYER 1

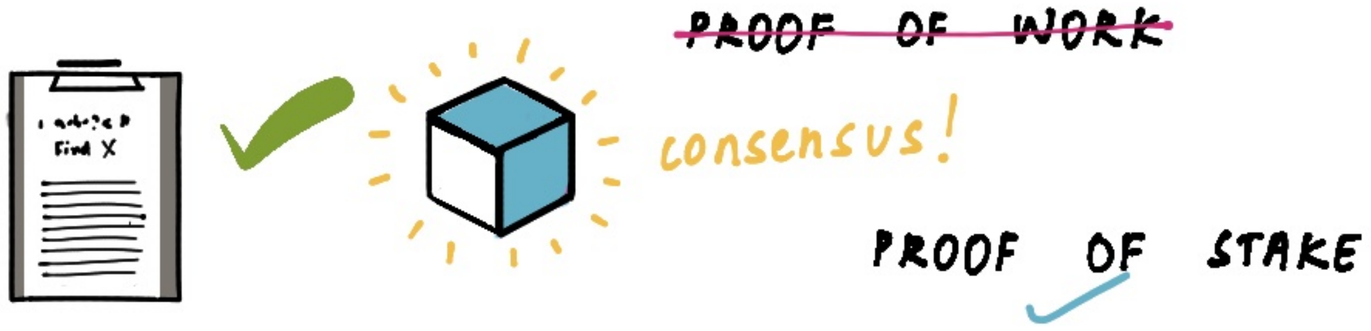
A LAYER 1 SOLUTION REFERS TO IMPROVEMENTS IN THE BASE BLOCKCHAIN

SUCH AS

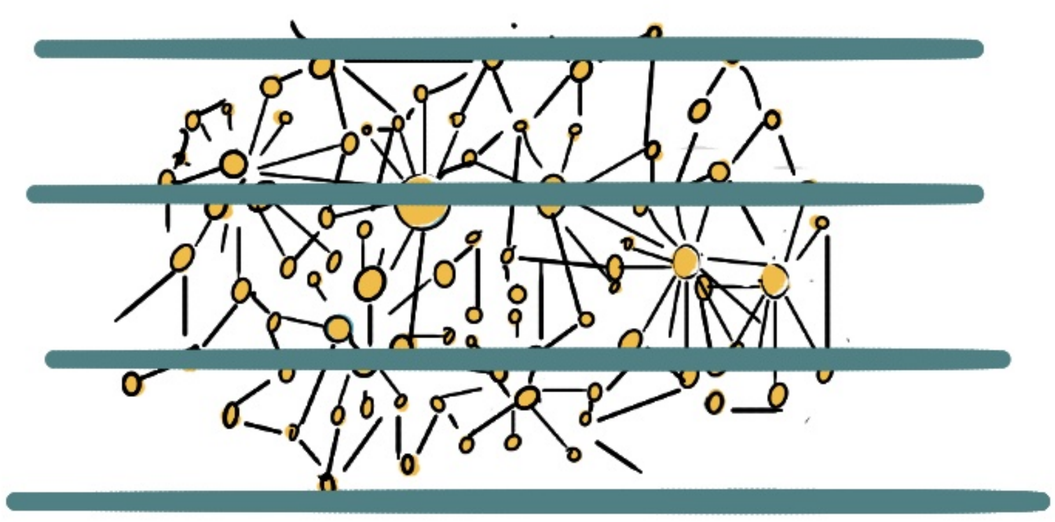
MODIFYING BLOCK SIZE



CHANGING CONSENSUS MECHANISMS



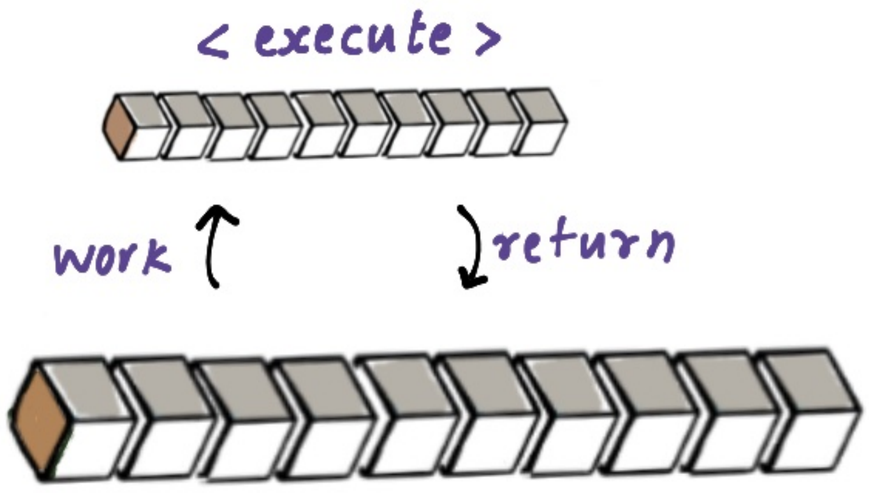
SHARDING - PARTITIONING INTO SMALLER NETWORKS



LAYER 2

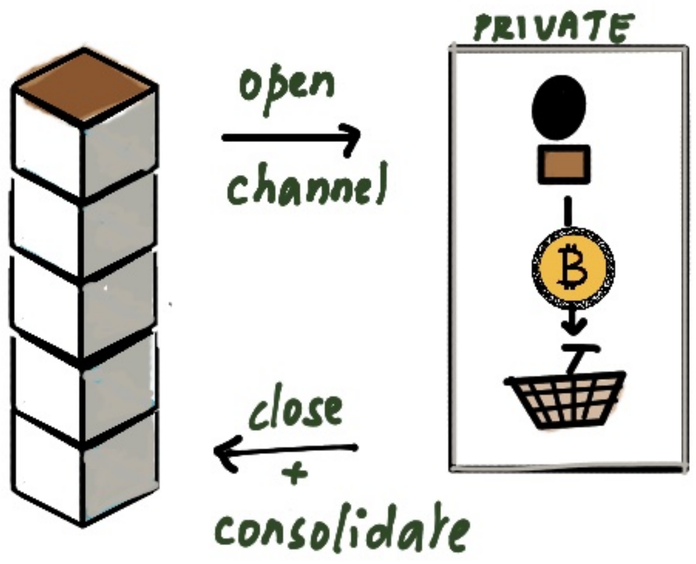
A LAYER 2 SOLUTION IS A PROTOCOL ALONGSIDE LAYER 1 PROVIDES OFF-CHAIN SERVICES TO MAKE TRANSACTIONS FASTER SUCH AS

NESTED BLOCKCHAINS



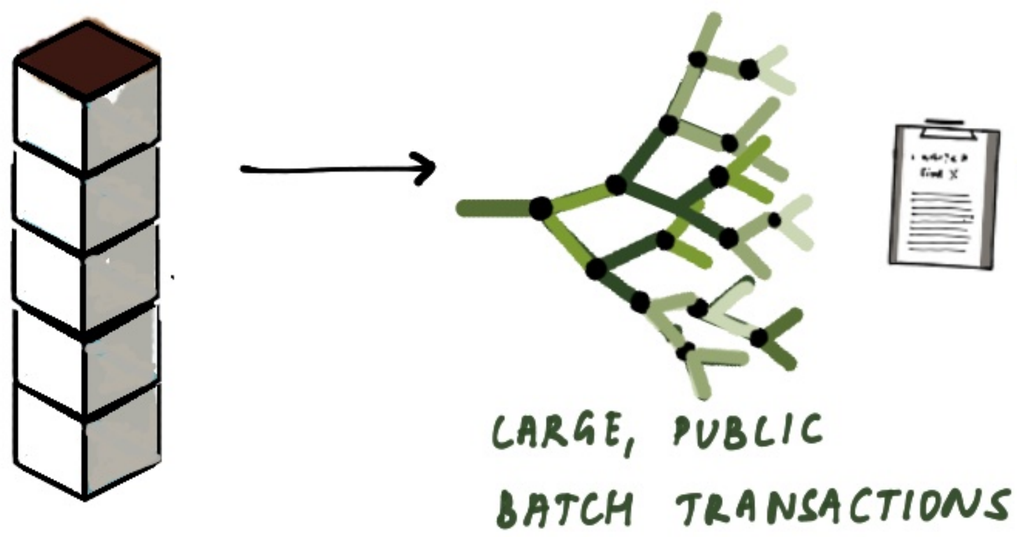
e.g ETHEREUM
OMG PLASMA NETWORK

STATE CHANNELS



e.g. BITCOIN LIGHTNING NETWORK

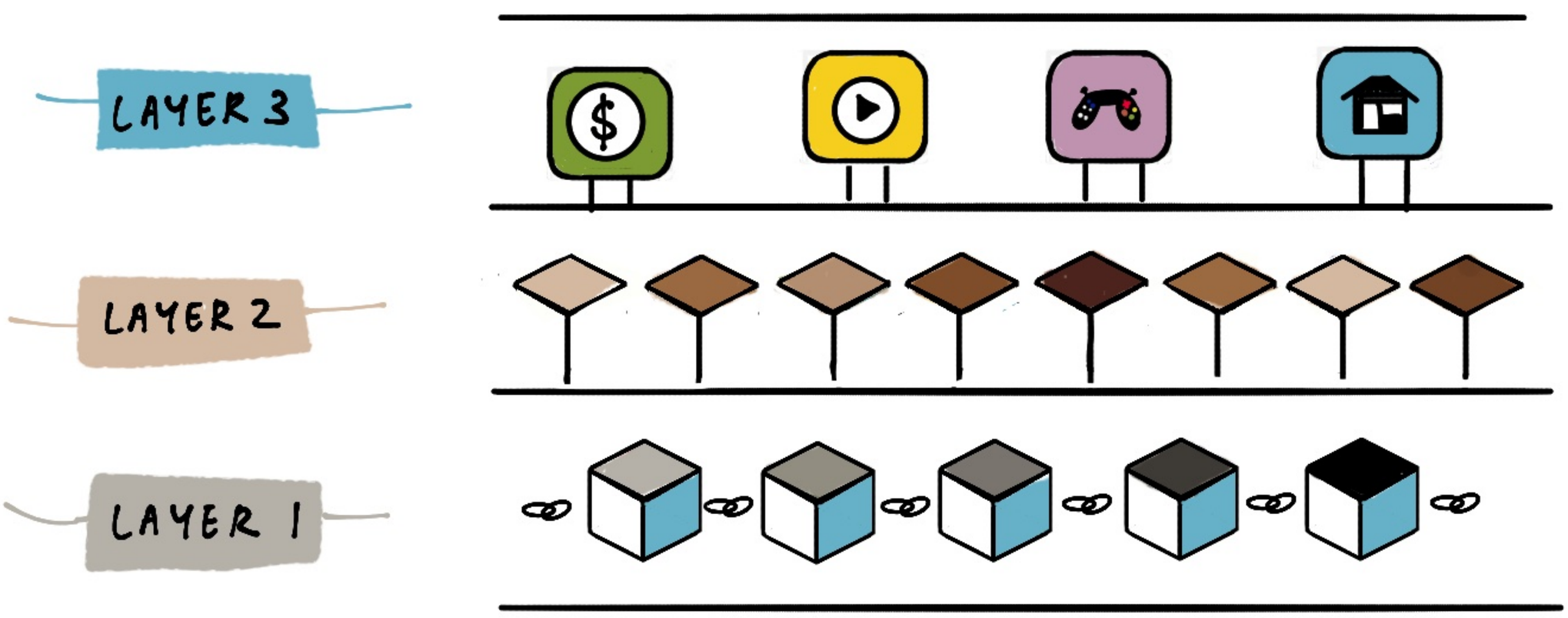
SIDE CHAINS



LARGE, PUBLIC BATCH TRANSACTIONS

LAYER 3

A LAYER 3 SOLUTION IS AN APPLICATION LAYER OVER LAYER 1 AND LAYER 2. IT IS POSSIBLE TO HAVE APPS OPERATING ACROSS BLOCKCHAINS



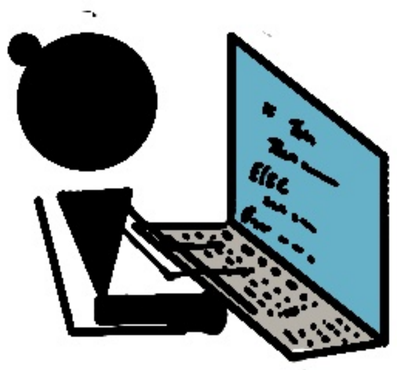
WE SEE APPLICATIONS SUCH AS DECENTRALISED APPS, GAMES FINANCE OR STORAGE APPS - THESE ARE LAYER 3.

BUILDS UPON THE LAYER 1 AND LAYER 2 IMPROVEMENTS TO BUILD INTEROPERABILITY BETWEEN BLOCKCHAINS BEYOND EXCHANGES THROUGH SAY ATOMIC SWAPS.

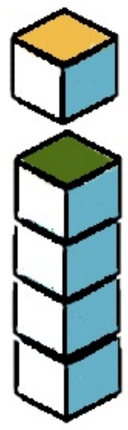
4 DECENTRALISED APPS OR DAPPS

DECENTRALISED APPS

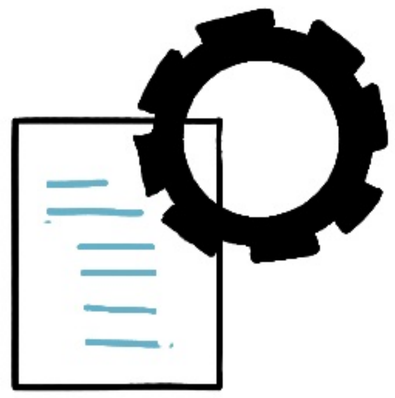
A DECENTRALISED APP OR DAPP IS AN APPLICATION



WITH A USER INTERFACE



BUILT ON A BLOCKCHAIN



THAT ALSO HAS SMART CONTRACTS

NOT ALWAYS HOSTED ON DECENTRALISED STORAGE

MORE LIKELY ETHEREUM

Definition of a DApp



COMPLETELY OPEN-SOURCE



DATA AND RECORDS OF OPERATION STORED IN A PUBLIC, DECENTRALISED BLOCKCHAIN



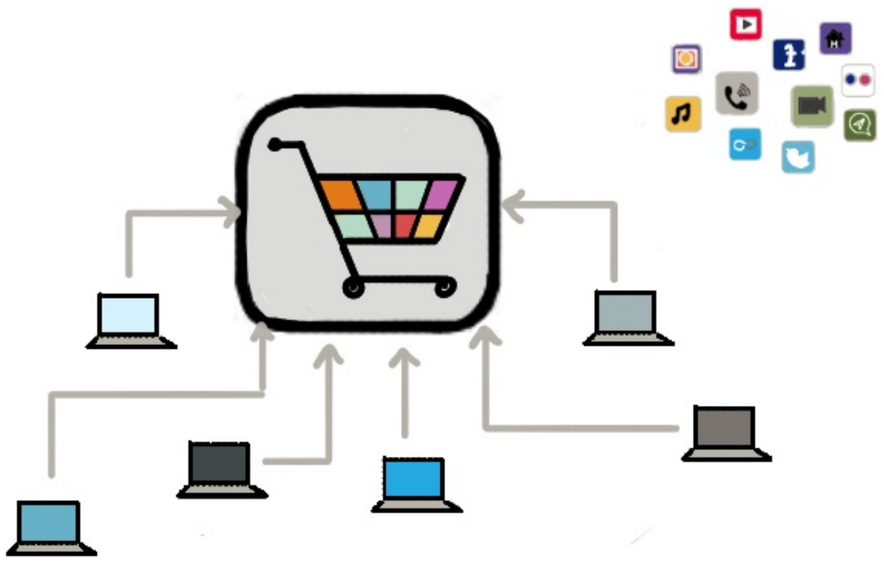
MUST USE A TOKEN (bitcoin or native) FOR ACCESS AND AS REWARDS



MUST GENERATE TOKENS USING A CRYPTOGRAPHIC ALGORITHM

github.com/DavidJohnstonCEO/DecentralizedApplications

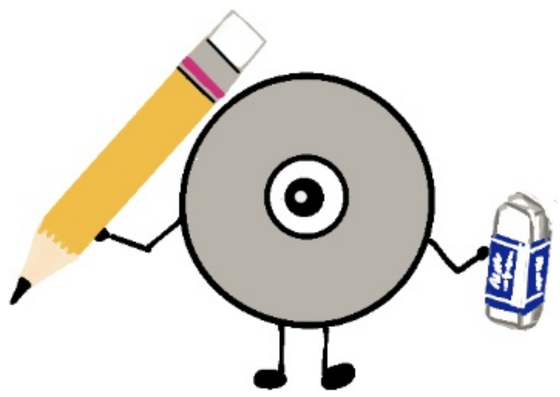
DECENTRALISED APPS



ARE NOT CONTROLLED BY A SINGLE ENTITY



CANNOT BE TAKEN DOWN FROM THE BLOCKCHAIN





ARE TURING COMPLETE

ON ETHEREUM VIRTUAL MACHINE

EXECUTE IN A VIRTUAL ENVIRONMENT



ACCESSED USING TOKENS



DO NOT NEED USERS TO REVEAL TRUE IDENTITY

DECENTRALISED APPS



ARE ABOVE CENSORSHIP

e.g. BLOCKING USERS

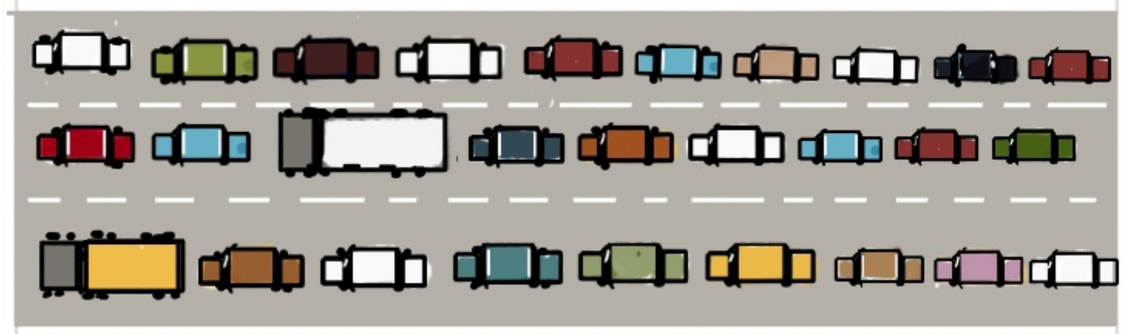
OR THEIR ACTIVITY



TRADE OFF

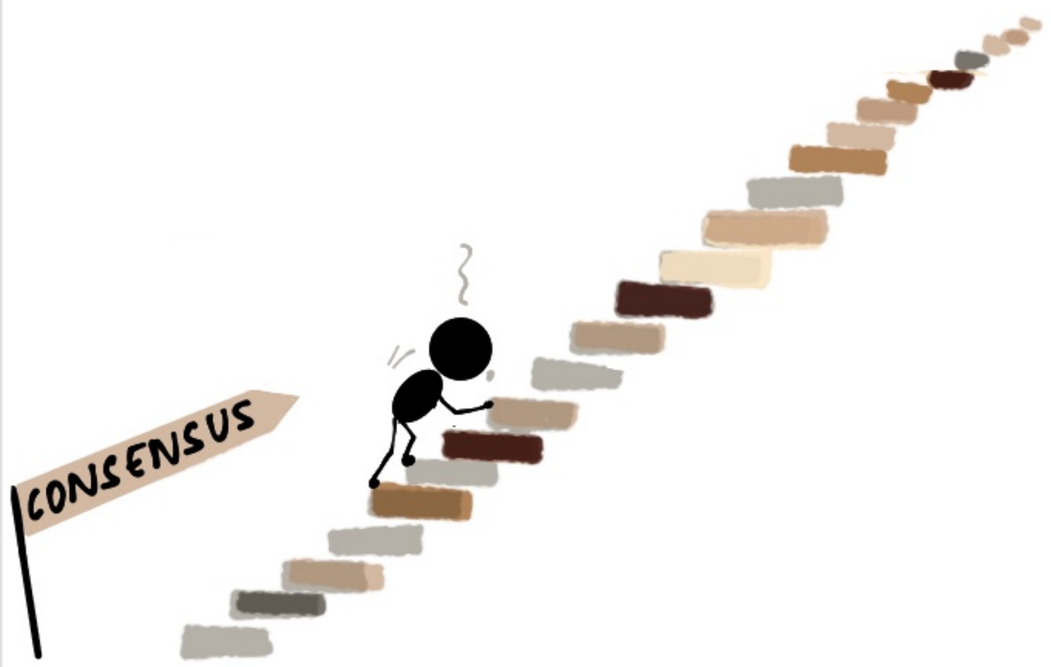
USER EXPERIENCE

WITH SECURITY



CAUSE NETWORK CONGESTION

WHEN OVER-USING RESOURCES



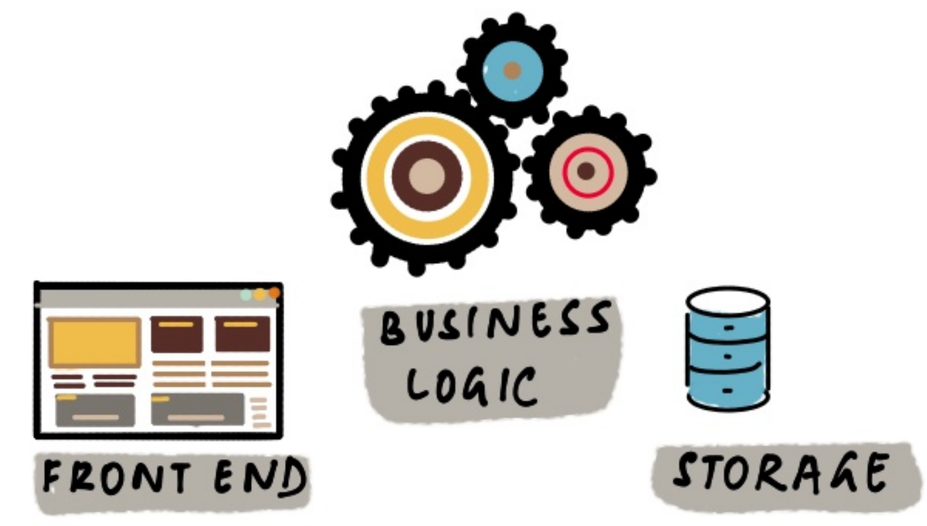
ARE MORE DIFFICULT

SCALE AND MAINTAIN



HAVE THE SAME DOWNTIME AS

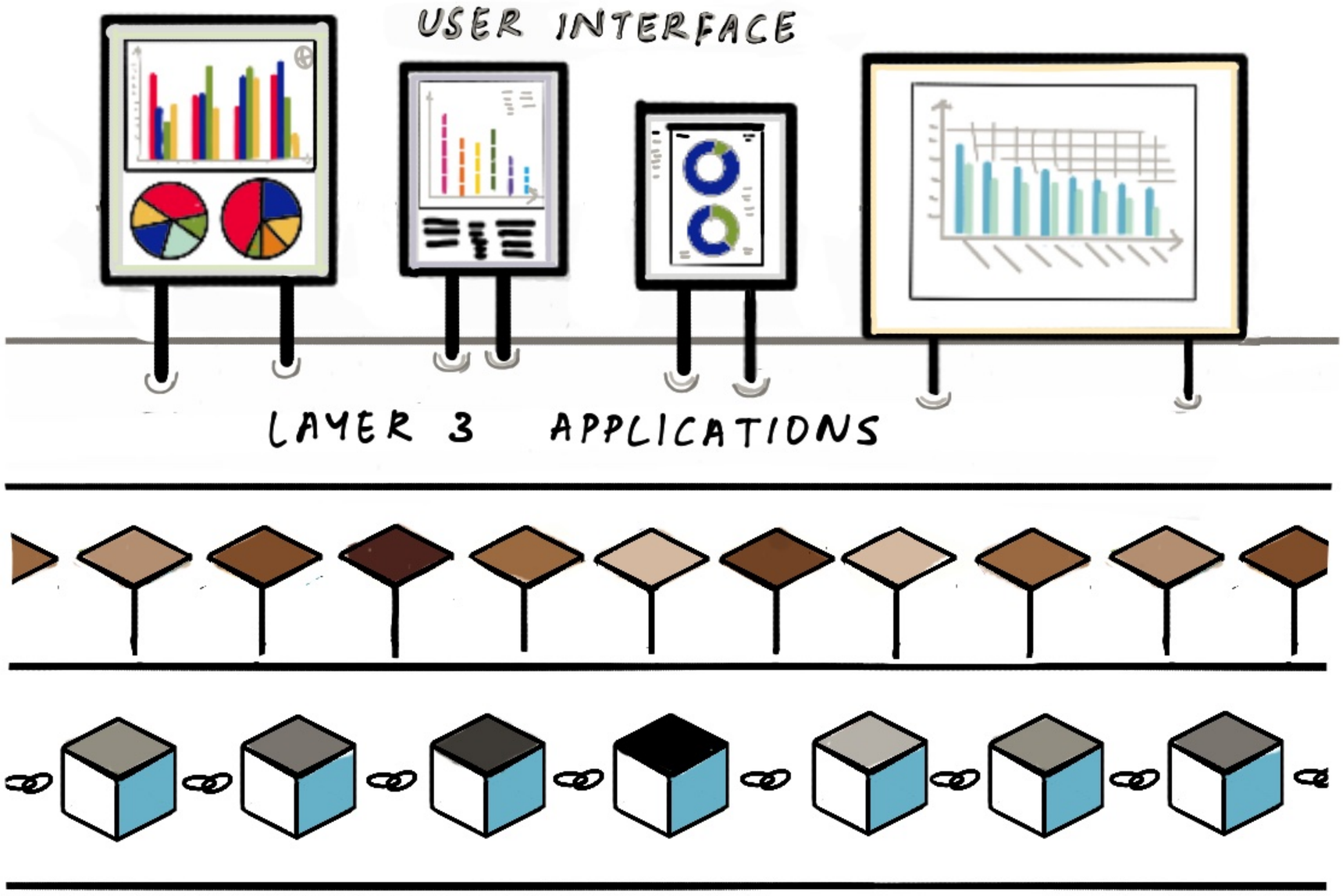
THE BLOCKCHAIN



MIGHT END UP WITH SERVICES

CENTRALISED...

DECENTRALISED FINANCE



DECENTRALISED FINANCE OR DEFI IS A TERM FOR FINANCIAL APPLICATIONS ON THE BLOCKCHAIN

HERE DIGITAL ASSETS ARE TRADED PROGRAMMATICALLY BETWEEN PEERS VIA DAPPS/SMART CONTRACT CODE

DEFI ENABLES NOVEL FINANCIAL INSTRUMENTS AND SOME DUBIOUS ONES SUCH AS FLASH LOANS, DERIVATIVES, MONEY LEGOS...

5 TOKENS, TOKENOMICS

WHAT DO YOU THINK?

MONEY IS

VALUABLE AND SCARCE



YET NOT FINITE IN SUPPLY

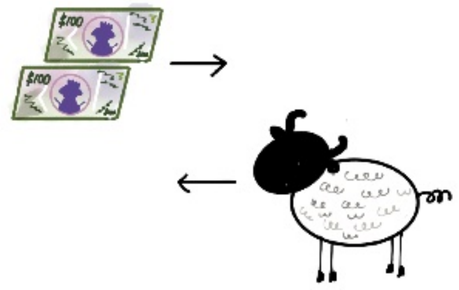
PORTABLE AND DIVISIBLE



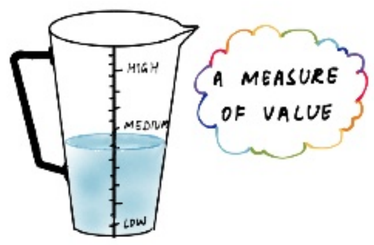
A STORE OF VALUE



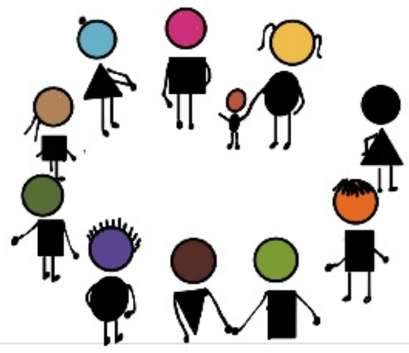
A MEDIUM OF EXCHANGE



A UNIT OF ACCOUNT



A SOCIAL CONSTRUCT



IS CRYPTOCURRENCY MONEY?

OR A SOCIAL EXPERIMENT?

?

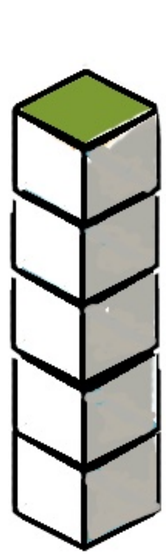
WILL IT REPLACE FIAT?

SHOULD THE BANKS BE AFRAID?

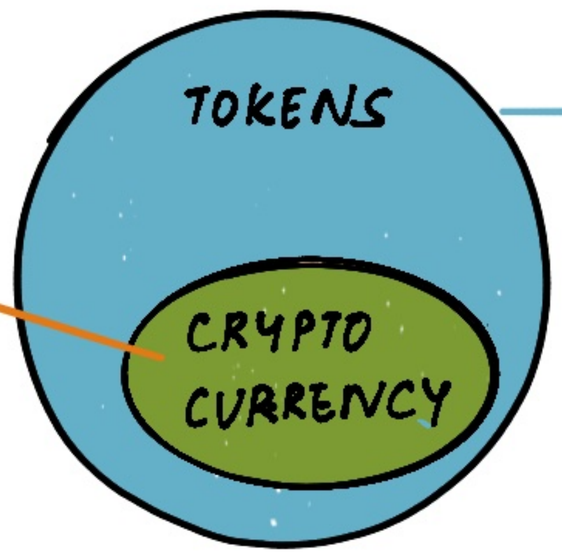
LET US TAKE A LOOK AT OTHER ASSETS ON THE BLOCKCHAIN

TOKEN OF VALUE

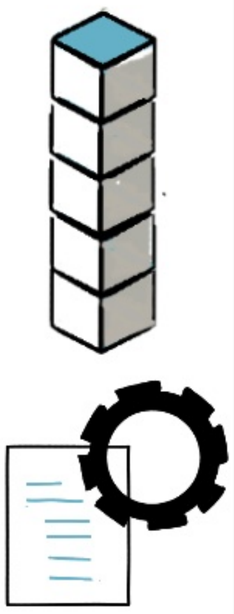
A TOKEN IN THE CONTEXT OF WEB3 IS A DIGITAL 'THING' OF VALUE BEING TRADED



BUILT ON NATIVE BLOCKCHAIN



BUILT ON OTHER BLOCKCHAINS AND PROGRAMMABLE



A TOKEN GIVES ACCESS / RIGHTS TO

- A PHYSICAL ASSET
- A DIGITAL ASSET

TOKENS CAN BE

- ISSUED
- TRADED

} RAPIDLY

TOKENS ARE NOT

- ✗ EARNED THROUGH MINING
- ✗ TRANSFERRED BETWEEN DEVICES

CONCERNS REMAIN : HOW TO

- VERIFY COUNTERFEITS ?
- REGULATE OR MONITOR ?
- STOP SCAMMERS ?

THE TERM **TOKENOMICS** COMES FROM STUDYING THE ECONOMICS AND INCENTIVE MECHANISMS OF CRYPTO-TOKENS

TOKENS ARE INCENTIVES

TO EFFECT CHANGE

- INFLUENCE THE SUPPLY AND DEMAND OF THE ASSET



- DELIBERATELY DESIGNED TO CHANGE BEHAVIOUR PATTERNS



TO RAISE FUNDS

- INITIAL COIN OFFERINGS - ICOs RAISE CAPITAL FOR A NEW CRYPTO-COIN/ASSET/APP

AN UNREGULATED MEANS



- NON-FUNGIBLE TOKENS - NFTs ARE ALSO USED TO RAISE FUNDS

TO CONTRIBUTE RESOURCES



ETHEREUM

- COMPUTING RESOURCES



HELIUM

- WIRELESS COVERAGE HOTSPOTS

TO CONTINUE ENGAGEMENT

- REWARDS TO





- MAINTAIN
- PARTICIPATE

Unfair 

(APPEARS TO) SETTLE THE UNFAIRNESS BETWEEN CONTRIBUTORS Vs EARNERS

EXAMPLES OF TOKENS

SOME TOKEN CATEGORIES

- PLATFORM TOKENS
- TRANSACTIONAL TOKENS
- SECURITY TOKENS
- GOVERNANCE TOKENS
- UTILITY TOKENS

THESE CATEGORIES ARE LOOSELY DEFINED

GOVERNANCE TOKENS



GRANT VOTING RIGHTS

SECURITY TOKENS

REPRESENT OFF-CHAIN ASSETS



- LAND RECORDS
- REAL ESTATE
- SHARES

UTILITY TOKENS

INTEGRATED AND USED WITHIN A PROTOCOL



FOR ADVERTISING

BASIC ATTENTION TOKEN



'COINS' FOR ONLINE GAMING

TRANSACTIONAL TOKENS

- ACT LIKE MONEY

PLATFORM TOKENS

- SUPPORT THEIR DAPPS
  e.g. UNISWAP
- MIGHT ACTUALLY HAVE A CENTRAL AUTHORITY

OTHER DIGITAL ASSETS

NON-FUNGIBLE TOKENS - NFTs

NFTs REPRESENT OWNERSHIP OF AN ORIGINAL DIGITAL ARTEFACT SUCH AS



CRYPTOKITTIES

- IMAGE
- AUDIO
- VIDEO

THEY CLAIM TO DIRECTLY BENEFIT THE CREATOR

STABLECOINS

STABLECOIN IS A CRYPTOCURRENCY WHOSE VALUE IS 'PEGGED' TO



US DOLLAR



ANOTHER CRYPTO



AN ALGORITHM

USED IN PAYMENTS, FOREX

CBDC

CENTRAL BANK DIGITAL CURRENCY

CBDC IS DIGITAL MONEY THAT A COUNTRY'S CENTRAL BANK ISSUES

- MORE LIKE CASH
- ENABLES FASTER, CHEAPER } PAYMENTS
- ENABLES TRACKING
- MAY (NOT) LIVE ON BLOCKCHAIN

MEME COINS

MEME COINS ARE CRYPTO THAT COME ABOUT FROM INTERNET JOKES



e.g. DOGECOIN
FLOKI
SHIBA INU

ECONOMICS OF (BLOCKCHAIN) WEB3

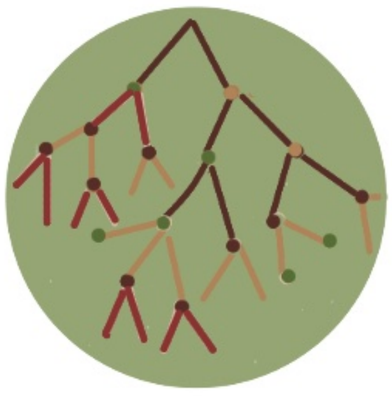
WHAT VALUE DO WE GET FROM BLOCKCHAIN WEB3 AND WHAT ARE THE ASSOCIATED CHALLENGES?

PROBLEMS FOR THE TOOL

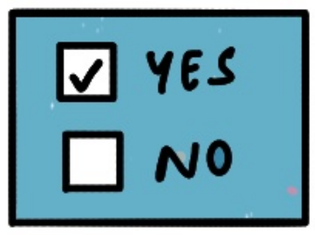
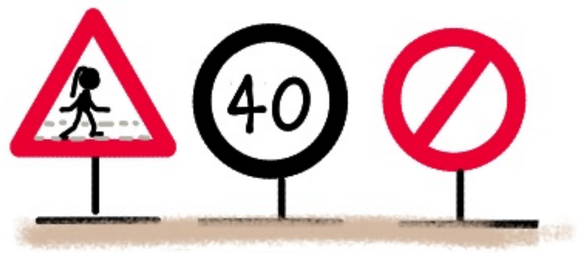
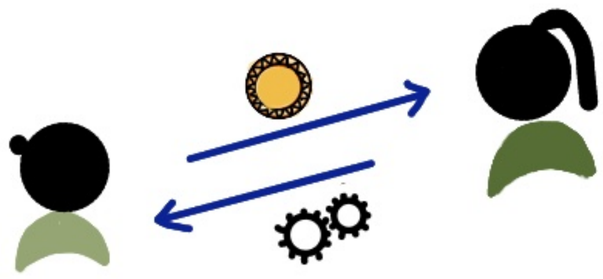
THIS IS FROM A PAPER BY TEPPO FELIN & KARIM R LAKHANI (MIT)

WHAT PROBLEMS WILL YOU SOLVE WITH A BLOCKCHAIN?

ACTION

RECORD	TRACK	VERIFY	AGGREGATE
			

VALUE CAPTURED

 INFORMATION	 VOTES	 ACCESS
 TRUST / REPUTATION	 CONTRACTS	 TRANSACTIONS

STAKEHOLDERS

CUSTOMERS	INVESTORS
SUPPLIERS	- - -
GOVERNMENT	- etc -

ECONOMICS OF THE BLOCKCHAIN

— SOME SIMPLE ECONOMICS OF THE BLOCKCHAIN —

CHRISTIAN CATALINI & JOSHUA GANS

NBER WORKING PAPER NO: 22952
(2019)

CONTEXT : HOW BLOCKCHAIN SHAPES INNOVATION AND COMPETITION IN DIGITAL PLATFORMS

BLOCKCHAIN AFFECTS TWO COSTS

COST OF VERIFICATION



WHEN IT IS CHEAPER TO VERIFY

TRANSACTION ATTRIBUTES

STATUS / SETTLEMENTS

CURRENT ASSET OWNERSHIP

BACK OFFICE RECONCILIATION

COST OF NETWORKING



WHEN CENTRAL CONTROL IS NOT ESSENTIAL TO

STARTUP
RUN
} A MARKETPLACE

ECONOMICS OF THE BLOCKCHAIN

LOWER COST OF NETWORKING

ECONOMIC INCENTIVES TO REWARD STATE TRANSITIONS



LOWER COSTS TO VERIFY/AUDIT

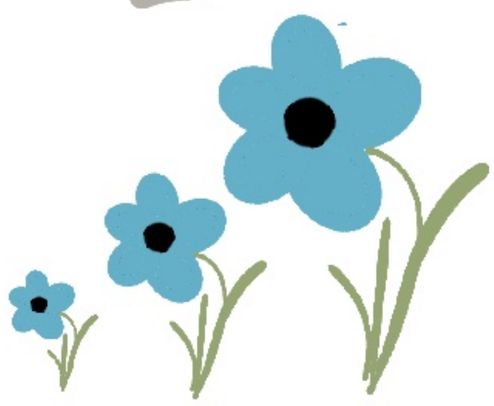


HELPS GETTING RESOURCES TO

OPERATE



SCALE



SECURE



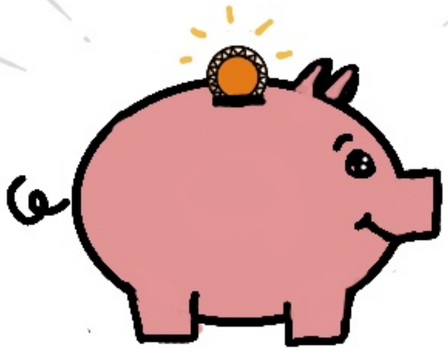
THE NETWORK

RESULTING IN A DIGITAL MARKETPLACE



WHERE MEMBERS JOINTLY INVEST IN

SHARED INFRASTRUCTURE



DIGITAL PUBLIC UTILITIES

- ENCOURAGING COMPETITION
- LOWERING ENTRY BARRIERS
- LOWERING PRIVACY RISK
- WITHOUT PLATFORM OPERATORS TO CENSOR/CONTROL

ALSO BRINGING

- NEW INEFFICIENCIES
- GOVERNANCE CHALLENGES

IMPACT ON INCUMBENTS

INTERMEDIARIES WILL HAVE

A DECREASE IN

- REVENUE SOURCES
- MARKET INFLUENCE

THEY CAN ADD VALUE THROUGH

CHECK OFF-CHAIN ACTIVITIES

- ✓ VALIDATE IDENTITY
- ✓ VALIDATE SERVICES
- ✓ VALIDATE PHYSICAL ASSETS

THEY WILL NEED TO CONSIDER



- PRIVACY
- OWNERSHIP
- PORTABILITY

IN THE CONTEXT OF HANDLING DATA

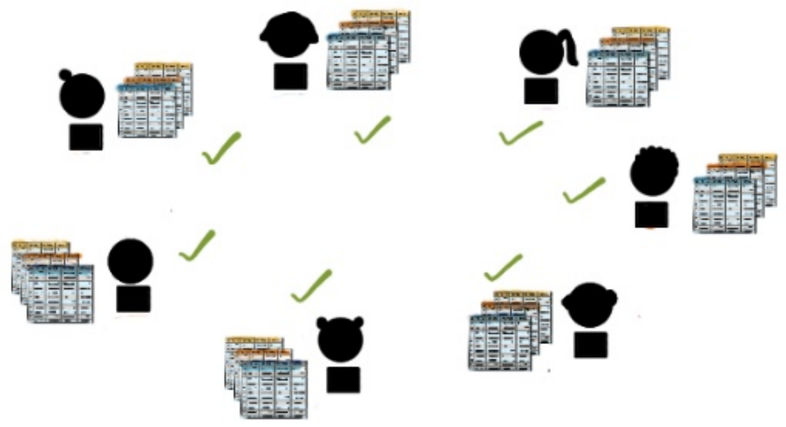
NEW OPPORTUNITIES OPEN UP

- REGULATION OF PUBLIC UTILITIES
- COLLABORATION BETWEEN INNOVATORS & INTERMEDIARIES

(FROM THE CATALINI-GANS PAPER ON ECONOMICS)

PERMISSIONED VS PERMISSIONLESS

PERMISSIONED BLOCKCHAINS





BENEFIT FROM
LOWER VERIFICATION COSTS

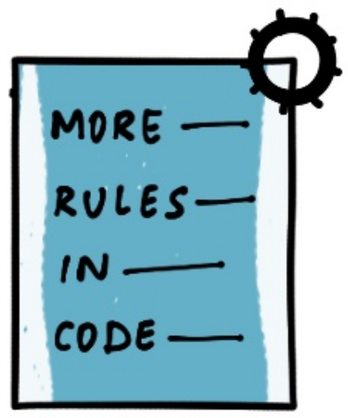
EARLIER MEMBERS LIKELY TO
HAVE MORE MARKET POWER

PERMISSIONLESS BLOCKCHAINS



USE INCENTIVES TO GET

LOWER
- VERIFICATION COSTS
- NETWORK COSTS



CORE DEVELOPERS ARE
RESPONSIBLE FOR GOVERNANCE



LOWER RISK OF ENTITIES HAVING PRIORITY/ACCESS TO
NETWORK INFORMATION TO MONETISE DATA

WHERE BLOCKCHAINS FAIL

THE LAST MILE

THE LAST PART OF THE JOURNEY TO MOVE

PEOPLE / GOODS / SERVICES

FROM THE HUB

TO THE FINAL DESTINATION

IT IS UNDERSTOOD TO BE

THE LAST DIFFICULT PART WITH CHALLENGES LIKE:

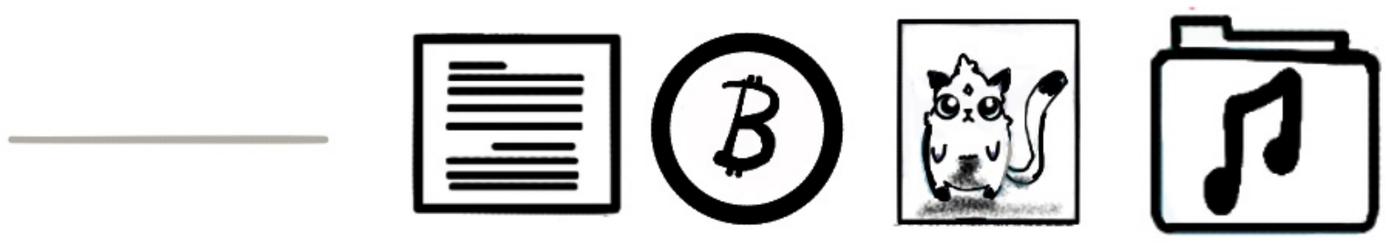
- EFFICIENCY
- TRANSPARENCY
- COST
- INFRASTRUCTURE

THIS IS A SUPPLY CHAIN TERM
WHOSE ORIGINS ARE FROM THE
TELECOMMUNICATIONS SECTOR

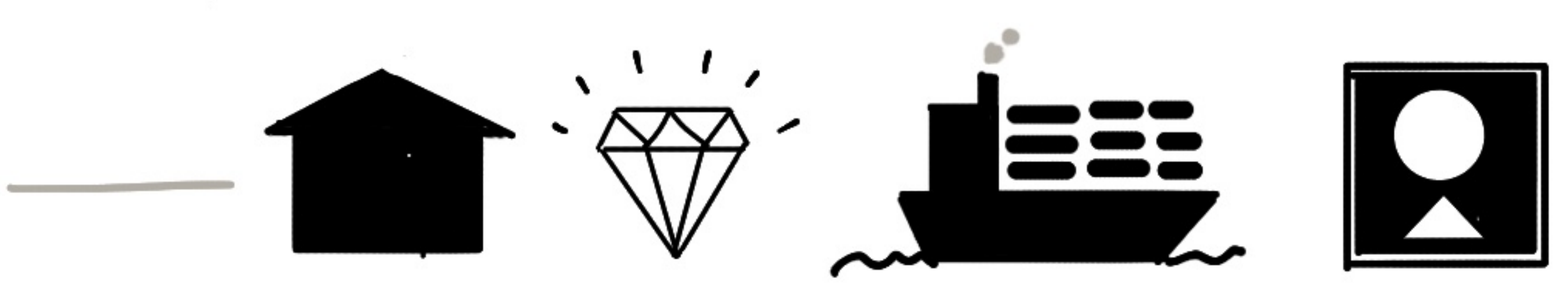
WE WILL SEE HOW THIS APPLIES TO BLOCKCHAINS

WHERE BLOCKCHAINS FAIL

COST OF VERIFICATION BECOMES ALMOST NEGLIGIBLE WHEN THE ASSETS/INFORMATION IN QUESTION ARE PURELY DIGITAL



HOWEVER, SOME ASSETS REPRESENT A PHYSICAL ENTITY



THE HANDOFF BETWEEN AN OFF-CHAIN ASSET & ITS DIGITAL FORM IS THE LAST MILE IN BLOCKCHAINS



ASSETS WITH LAST MILE FRICTION COME WITH HIGH COSTS OF VERIFICATION



UNLESS IT IS A PHYSICAL ASSET WITH AN IMMUTABLE PROPERTY WHOSE ATTRIBUTES ARE

- EASY TO CAPTURE
- EXPENSIVE TO FAKE

e.g. LAND RECORD + GEO LOCATION
DIAMOND + FOREVERMARK

WHAT MAKES BLOCKCHAINS COMPELLING?

NOT ALL PROBLEMS ARE SOLVED WITH BLOCKCHAIN TECHNOLOGIES.

TO HAVE A BLOCKCHAIN SOLUTION,
A PROBLEM HAS TO FIT MOST OF THE FOLLOWING CRITEREA



CENSORSHIP ISSUES



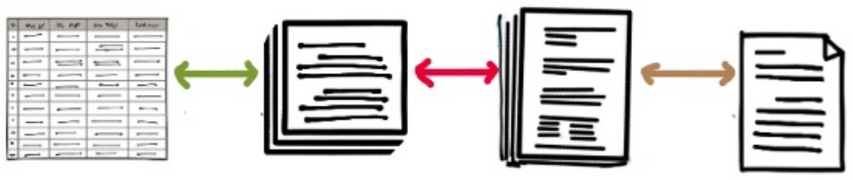
NO INTERMEDIARY



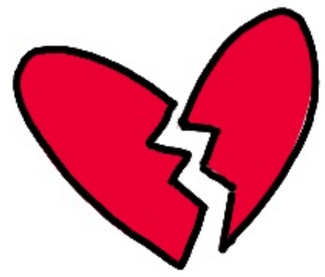
HIGH ECONOMIC RENTS



LOW VERIFICATION COSTS



BACK OFFICE RECONCILIATION



LOW TRUST ENVIRONMENT



PRIVACY REQUIREMENTS



INCENTIVISE ENGAGEMENT

IF NOT, IT MIGHT BE MORE EFFICIENT TO HAVE A
A 'TRADITIONAL' DATABASE AND CENTRALISED CONTROL

LET US LOOK AT A NARROW SET OF USE CASES

WHERE BLOCKCHAINS ARE COMPELLING

VERIFY + CONTRACTS

- MINIMUM LAST MILE COSTS
- LOW VERIFICATION COSTS
- NO INTERMEDIARY

BLOCKCHAIN - HYPERLEDGER

INDUSTRY - TRADE FINANCE

PURPOSE - DOCUMENT CHECKS

RECORD + TRANSACTION

- EFFICIENT/FAIR ALLOCATION OF FEES BETWEEN CREATORS ENABLED BY
- LOW COST OF NETWORKING

BLOCKCHAIN - MYCELIA

INDUSTRY - MUSIC

PURPOSE - PAY & CREDIT

FOUNDER - IMOGEN HEAP

RECORD + INFORMATION

- LOW VERIFICATION COST
- LOW NETWORKING COST
- ENABLING THE DEFINITION OF NEW TYPES OF
- DIGITAL ASSETS/PROPERTY RIGHTS

BLOCKCHAIN - EVERLEDGER

INDUSTRY - DIAMOND

PURPOSE - TRACK OWNERSHIP

RECORD + ACCESS

- USERS WANT

MORE [PRIVACY / CONTROL] OF THEIR DATA

ZERO KNOWLEDGE PROOFS

BLOCKCHAIN - DECO / CHAINLINK

INDUSTRY - HEALTH

PURPOSE - SELECTIVE ACCESS

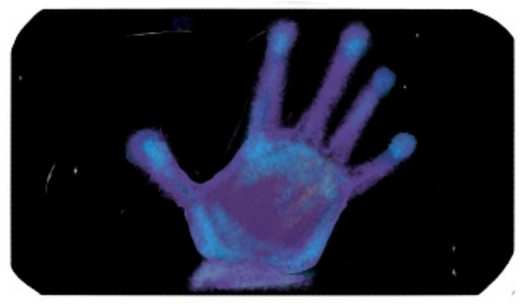
CHALLENGES OF OWNING CRYPTO

ILLEGAL

CRYPTO CURRENCIES

ARE NOT CONSIDERED LEGAL

IN MANY COUNTRIES.



THEIR USE AND TRADING

ARE NOT REGULATED

ENABLING CRIMINAL USE

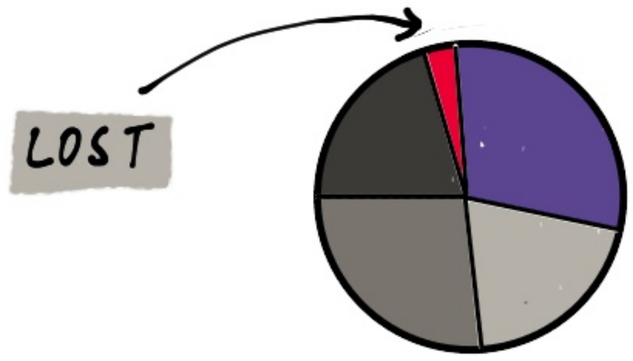


CRYPTO CURRENCY WEALTH

IS BECOMING MORE

CONCENTRATED — DEBUNKING

THE DECENTRALISATION MYTH

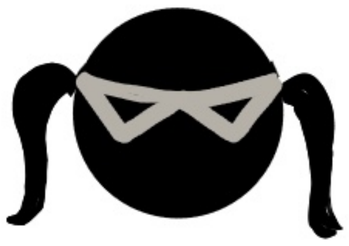


IRREVERSIBLE TRANSACTIONS

RESULTS IN UNCLAIMED CRYPTO

DUE TO LOST PASSWORDS

OR INCORRECT ADDRESSES



INTERSECTION BETWEEN

CRYPTO AND NON-CRYPTO WORLD

IS HIGHLY UNSECURED



CRYPTO AND DAPPS, LIKE

ANY CODE ARE SUBJECT

TO ERRORS & WEAKNESSES



PSEUDONYMOUS IDENTITIES CAN

BE TRACED BY THE LAW —

DEBUNKING THE PRIVACY MYTH

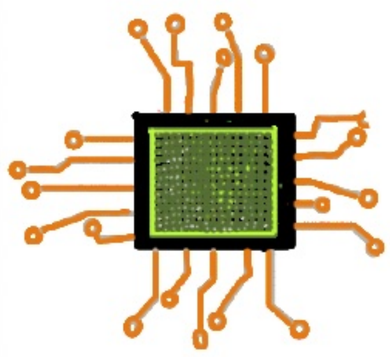


PRICES ARE VOLATILE

EXPENSIVE TO EARN/BUY

OTHER CHALLENGES

IN HIS BOOK CODE 2.0, LARRY LESSIG IDENTIFIES FOUR FACTORS THAT SHAPE USAGE AND ADOPTION OF ANY NEW PRODUCT - WHETHER PHYSICAL OR VIRTUAL



PRODUCT CONSTRAINTS



MARKET/ ECONOMY



LAW/ REGULATION



SOCIETAL NORMS

WHEN APPLYING THESE FACTORS TO BLOCKCHAIN - WEB3, HERE ARE SOME EXAMPLES OF CHALLENGES IN EACH CATEGORY

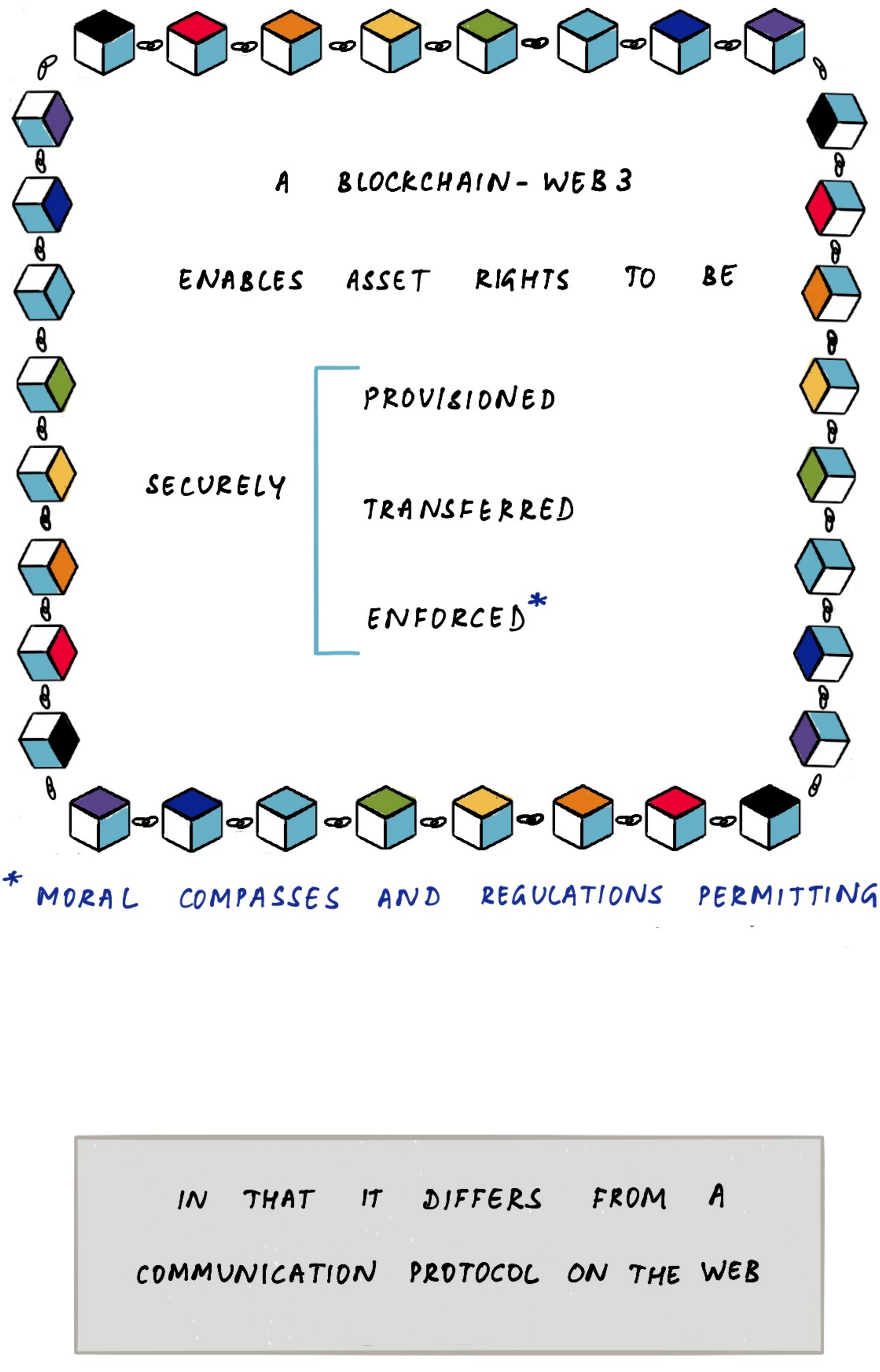
- KEY MANAGEMENT
- ENERGY USAGE
- USER EXPERIENCE

- INVESTMENTS
- RESEARCH
- ECONOMIC CLIMATE

- GOVERNANCE
- TRANSPARENCY
- REGULATION

- ACCEPTABLE
- TRENDY
- VALUABLE

FOCUS OF A BLOCKCHAIN-WEB3



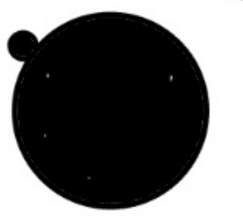
IN THAT IT DIFFERS FROM A COMMUNICATION PROTOCOL ON THE WEB

WHAT IS THE COST OF TRUST?

A FAMILIAR MODEL OF TRUST

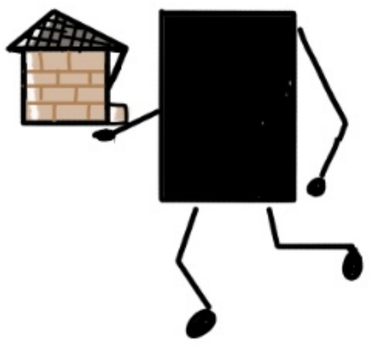


TRANSACTING PARTIES TRUST AN INTERMEDIARY









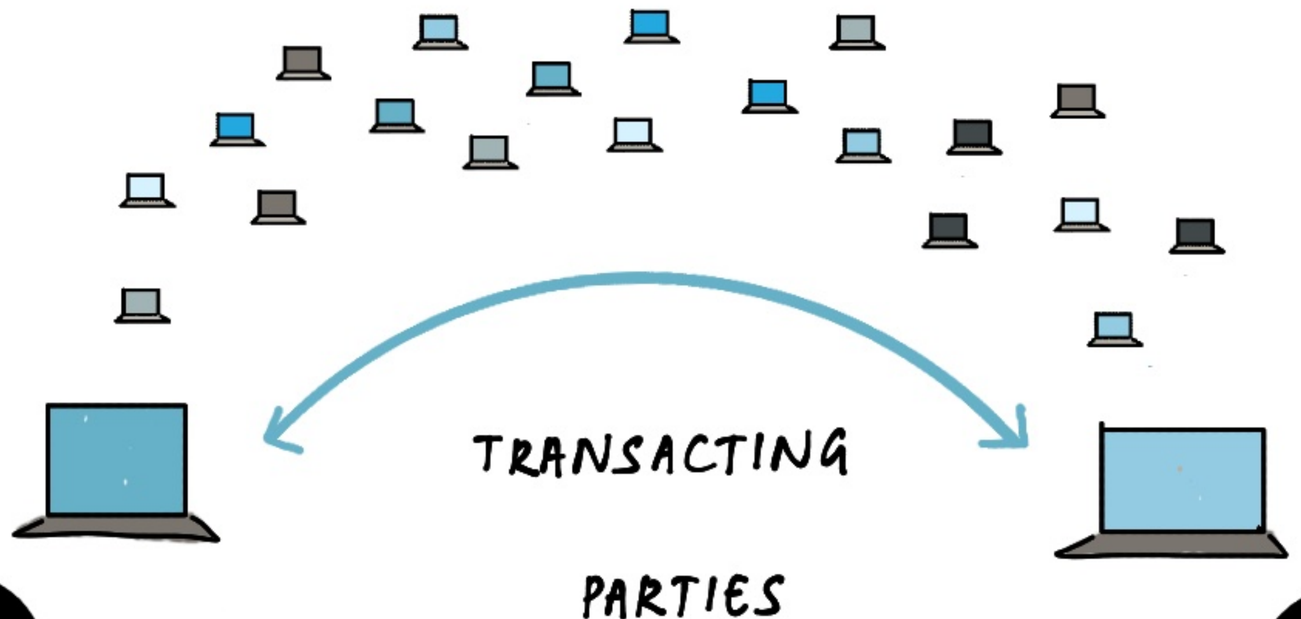
THERE IS **IMPLICIT TRUST** IN

- VAULT DOORS
- CYBERSECURITY
- RATES OF INTEREST
- CLEARING HOUSES
- SETTLEMENT PROCEDURES
- OFFICIALS
- PROCEDURES
- ANTI-FRAUD REGIME
- GOVERNMENT
- INTERNATIONAL LAW

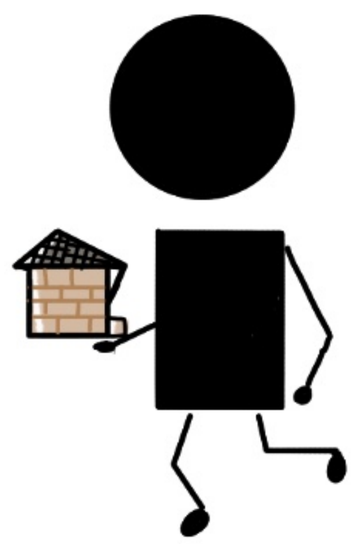
AND A **PRICE** TO PAY

- BANK CHARGES
- DELAYS
- PROCESSES/ADMIN

A NEW MODEL OF TRUST







THERE IS **IMPLICIT TRUST** IN THE

- CRYPTOGRAPHY
- BLOCKCHAIN LEDGERS
- CONSENSUS METHODS
- REWARDS MECHANISM
- VALUE BEING EXCHANGED
- INTEGRITY OF EXCHANGES/APPS
- RELATIVE ANONYMITY OF PARTIES
- INTENTION OF PARTICIPANTS

AND A **PRICE** TO PAY

- IRREVERSIBILITY OF TRANSACTIONS
- VOLATILITY OF PRICES
- MINING/ENVIRONMENT COSTS
- COMPLEX
- NOT WELL-REGULATED OR LEGAL
- LACK OF DISPUTE-SETTLEMENT

UNANSWERED QUESTIONS

THIS BOOK IS BY NO MEANS AN EXHAUSTIVE GUIDE. THERE ARE A GOOD FEW TOPICS I HAVE KEPT OUT OF SCOPE SUCH AS

- CYPHERPUNK ORIGINS OF BITCOIN
- THE MATHEMATICS OF ELLIPTIC CURVE CRYPTOGRAPHY
- OTHER BLOCKCHAINS/CONSENSUS PROTOCOLS
- THE WORKINGS OF EQUITY FINANCE
- FUNCTIONING OF DAOS FOR GOVERNANCE
- NON-FUNGIBLE TOKENS & HOW THEY WORK

HERE ARE SOME QUESTIONS I DID NOT FIND ANSWERS TO

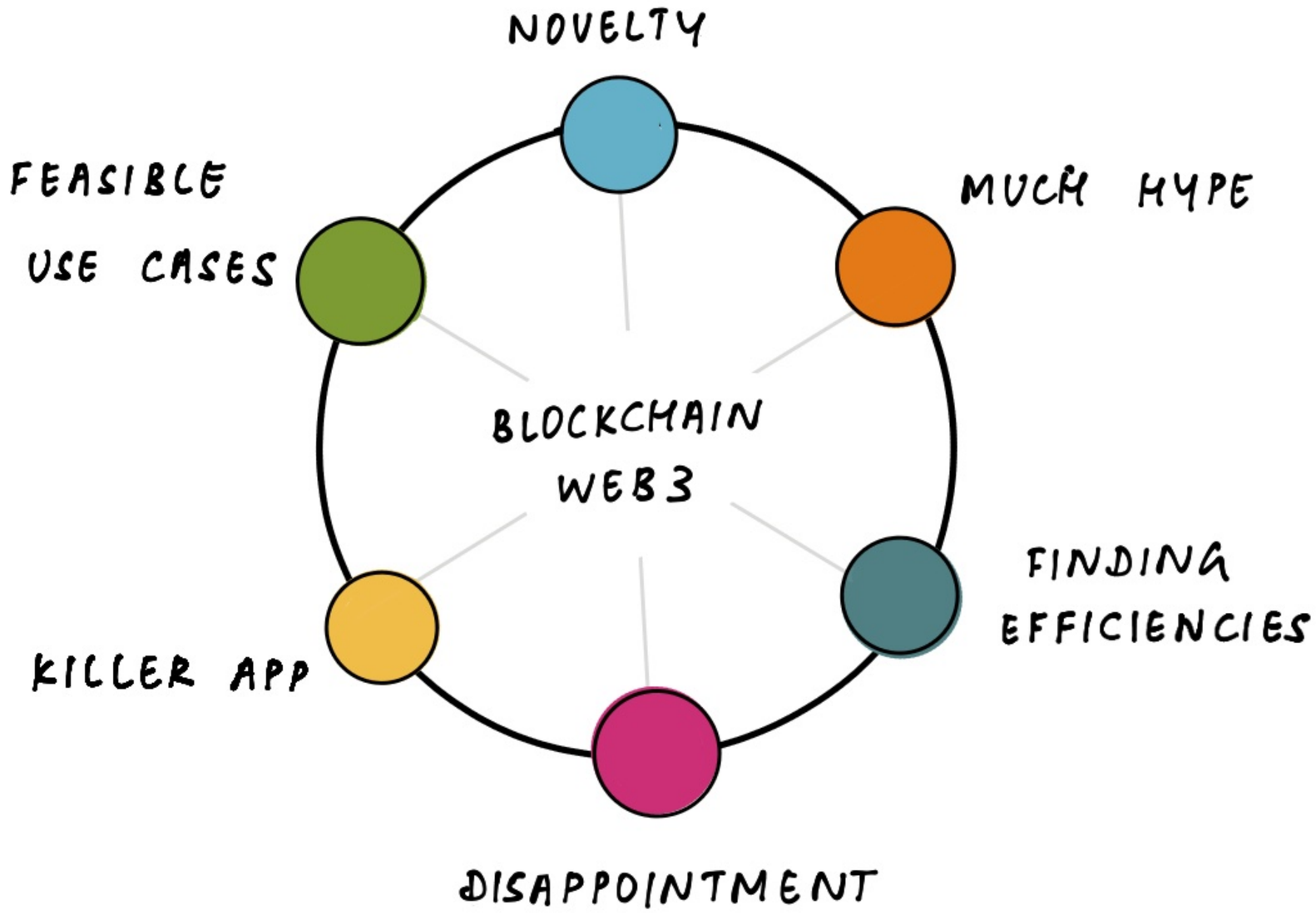
WILL BLOCKCHAIN/WEB3 TRANSFORM ANY OF THE WEB COMMUNICATION PROTOCOLS?

HOW MUCH OF A ROLE DOES THE METAVERSE/IOT/AI PLAY IN GROWING BLOCKCHAIN-WEB3 ?

WHAT AMOUNT OF REGULATION WILL MAKE DAPPS FRAUD-FREE?

WILL WEB3 ENABLE FINANCIAL INCLUSION TO THE UNBANKED BILLIONS THROUGH A CONNECTED MOBILE DEVICE?

LASTLY, WHERE ARE WE?



REGARDLESS OF THE SUBJECTIVITY OF THE QUESTION, THE BUILDING BLOCKS OF THIS TECHNOLOGY ARE HERE TO STAY

HOW THEY INFLUENCE/DISRUPT THE INDUSTRY DEPENDS ON HOW EACH OF ITS LIMITATIONS IS HANDLED.

MY REFERENCES

Semantic Web 3.0
- The Semantic Web PDF Tim Berners Lee + others
- The Semantic Web Revisited PDF Tim Berners Lee + others

Decentralisation/Web3.0
- Internet Policy Review: Decentralisation, a multidisciplinary perspective policyreview.info
- Dominic Tarr, ScuttleButt - What does decentralization mean? decentralizedweb.net
- How decentralisation and Web3 will impact the enterprise zdnet.com
- Three reflections regarding the re-decentralization of the web - Berkman Klein
- Review Web 3.0 – Coincu https://news.coincu.com
- From the Origins of the Internet to Decentralized Web 3.0 - hackernoon.com
- Web 3.0 Explained, Plus the History of Web 1.0 and 2.0 investopedia.com

Blockchain
- The Impact of Blockchain Technology on Finance: A Catalyst for Change: cepr.org Blockchain beyond the hype: What is the strategic business value? mckinsey.com
- Course Gary Gensler/MIT youtu.be
- Blockchain Trilemma - Silvio Micali wants to usher in the democratization of finance cointelegraph.com

Bitcoin
- Mastering Bitcoin O Reilly

Game Theory
- Game Theory Encyclopedia plato.stanford.edu
- Game Theory: A Basic introduction blockgeeks.com
- Definition and explanation: britannica.com
- Byzantine Generals Problem Lamport's paper lamport.azurewebsites.net

Public Key Cryptography
- Hash functions (via Consensys Blockchain Foundations course) coursera.org
- Digital Signatures (via Consensys Blockchain Foundations course) coursera.org
- Public Key cryptography: Illustrated Guide on How to Tell Secrets thoughtworks.com

Money, Currency and early digital currencies
- Explainers: Money/Currency basics bankofengland.co.uk
- What Was the First Cryptocurrency? Investopedia.com

History of bitcoin and crypto currencies
- A Short History Of Bitcoin And Cryptocurrency forbes.com
- History of Blockchain featuring Cynthia Dwork by Gregory Snelgar medium.com

MY REFERENCES

Intermediaries and Finance
- Financial Intermediaries – Meaning, Functions And Importance efinancemanagement.com
- Decentralised Finance: Blockchain, Ethereum, & The Future of Banking futurelearn.com

Transactions, Mining, Proof of Work, Difficulty, Hashrate
- Bitcoin Mining Difficulty: Everything You Need to Know coindesk.com
- Mining Difficulty and Network Hashrate Explained 2miners.com
- Bitcoin Mining Difficulty - What is it And How Does it Work? Blockgeeks.com
- Difficulty en.bitcoin.it
- Proof-of-work, and its flaws, explained hedera.com
- Bitcoin Proof of Work — The Only Article You Will Ever Have to Read levelup.gitconnected.com
- How Does Bitcoin Mining Work? investopedia.com
- How does a transaction get into the blockchain? Euromoney.com
- Hashrate: A measure of the computing power on a cryptocurrency network that is a key security indicator businessinsider.com

Double Spend and 51% Attacks
- Understanding Double-Spending and How to Prevent Attacks investopedia.com
- Blockchain explained: how a 51% attack works blog.goodaudience.com

Bitcoin and Energy Consumption
- How Much Electricity It Takes and Why People Are Worried cnet.com
- Cambridge Bitcoin Electricity Consumption Index (CBECI) ccaf.io
- Why Does Bitcoin Use So Much Energy_ – Forbes Advisor forbes.com
- Coinshares bitcoin mining report - Energy and Carbon Impact 2022 - coinshares.com

Smart Contracts
- Smart Contract in Nick Szabo's words uva.nl
- Identifying Real-life Use Cases of Smart Contracts blockgeeks.com
- [PDF] National Bureau of Economic Research: The Fine Print in Smart Contracts nber.org
- [Book] Code 2.0 by Larry Lessig
- Ethereum definition of smart contracts ethereum.org
- An Introduction to Smart Contracts and Their Potential and Inherent Limitations corpgov.law.harvard.edu
- Defend against "Wild Magic" in the next Ethereum upgrade by Jason Carver medium.com

MY REFERENCES

Layers
- Layer-1 and Layer-2 Blockchain Scaling Solutions gemini.com
- Everything there is to know about decentralized applications cointelegraph.com

Dapps, Regulation
- DeFi, Disintermediation, and the Regulatory Path Ahead by Jai Massari and Christian Catalini theregreview.org

Blockchain Economics
- Some Simple Economics of the Blockchain by Christian Catalini and Joshua Gans nber.org/papers/w22952

Use cases
- Blockchain and Digital Identity – A Good Fit? internetsociety.org
- What problems will you solve with the blockchain? (Felin/ Lakhani) researchgate.net