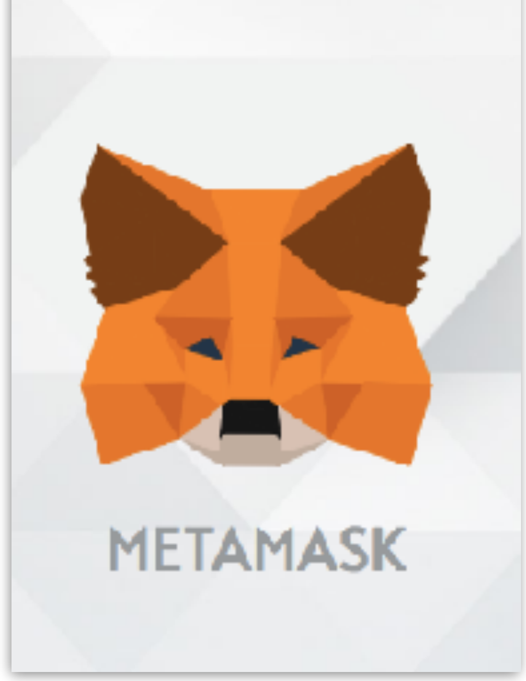
CRITICAL PERSPECTIVES ON THE

BLOCKCHAIN



INTERACTIVE WORKSHOP

GET METAMASK

50% OF THE GROUP WILL BE GIVEN **1 ETH**
(ON THE ROPSTEN TEST NETWORK)

TASK

SHARE ETH TO THE OTHER 50% OF THE GROUP

BLOCKCHAIN

Explore critical perspectives on 5 Key Aspects of the Blockchain

CONSENSUS ALGORITHMS

VALUE & VOLATILITY

DISINTERMEDIATION

SMART CONTRACTS

IMMUTABILITY

IDENTITY

Blockchain Workshop

ABOUT THE PRESENTERS

EDWARD BUCHI

@EDWARDBUCHI

With a background in Advertising and User Experience Design, I work directly with clients business problems. Raising the values of their brands and companies and making products user-centric and usable.

Recently my clients and work has revolved around Blockchain Networks, its applications, and its potential to reshape society.

DESIGN/MARKETING LEAD

bitcoin bay

ADVERTISING GRADUATE 2012

OCAD UNIVERSITY

DESIGN ADVISOR

COLLIDER·X

Token Funder

UNOCOIN

FINTECH CANADA

ABOUT THE PRESENTERS

NÉLIA TEIXEIRA

@OLIVEBRANCHLAW

Nélia is passionate about technology, design, and innovation. She is a researcher, strategist and lawyer practicing in Toronto, Ontario.

Prior to being called to the bar in 2016. Nélia was a Student-at-Law with Tangerine Bank. She received her Juris Doctorate degree from the University of Ottawa's Faculty of Law. She applies design thinking to the practice of law in a wide range of practice areas, with a special interest in blockchain technology.

She is also a nascent coder and has placed 2nd in the Blockchain Canada Summer Hack-a-thon and 3rd in the Ontario Securities Commission RegHack 2016. Nélia is a co-organizer of Toronto Legal Hackers, one of the largest of such groups in the world with over 1000 members.

FOUNDER

Olive Branch Law

ABOUT THE PRESENTER

MICHAELANGELO YAMBAO

@JELOTWEETS

Michaelangelo is a developer who has worked at and started numerous companies from crowdsourced photography platforms to game design studios. Gamification, technology for social betterment, and more egalitarian socioeconomic systems is at the heart of his interests. He has won prizes in various hackathons, including MIT's CODEX and the University of Waterloo's EthWaterloo, and has spoken and mentored at CanadaLearningCode and Tech2025.

His current focus is on smart contract development on the Ethereum blockchain.

DEVELOPER/CO-ORGANIZER

TECH2025

DEVELOPER/DIGITAL CURRENCY TEAM CO-FOUNDER

Infinigon Group

PAST WORK

Secret City Adventures

DISPOSABLE CAMERA PROJECT

Green Collar Initiative

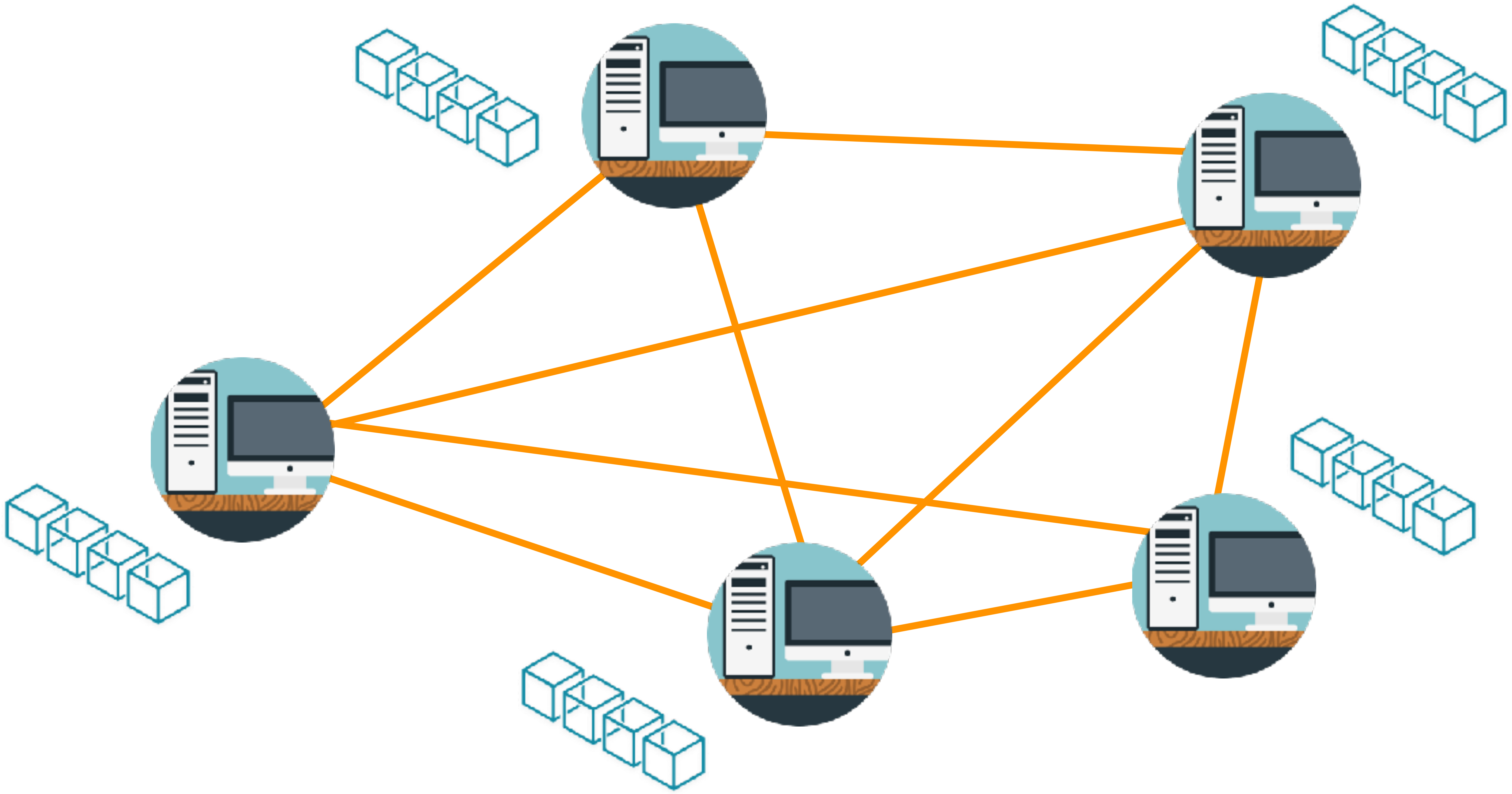
PRESENTATION GOALS

Bring to light key Blockchain Issues

Short Discussion after each section

Get everyone an address on the blockchain

CONSENSUS ALGORITHMS



FOR A BLOCKCHAIN NETWORK TO FUNCTION, THE NETWORK HAS TO DEMONSTRATE IT IS BYZANTINE FAULT TOLERANT

A MECHANICAL WAY OF MAKING SURE ALL NODES PROPAGATE AND MAINTAIN ONE TRUTHFUL COPY OF THE BLOCKCHAIN RECORD AND ARE INCENTIVIZED TO NOT LIE TO EACH OTHER

THIS IS ACHIEVED BY THE BLOCKCHAIN’S

CONSENSUS ALGORITHMS

CONSENSUS ALGORITHMS

Proof of Work

(BITCOIN)

Proof of Stake

(ETHEREUM 2018)

PROOF OF WORK

SH #

LAST

BLK#

+

NONCE

BLOCK HASH #

+

LAST

BLK#

+

NONCE

BLOCK HASH #

+

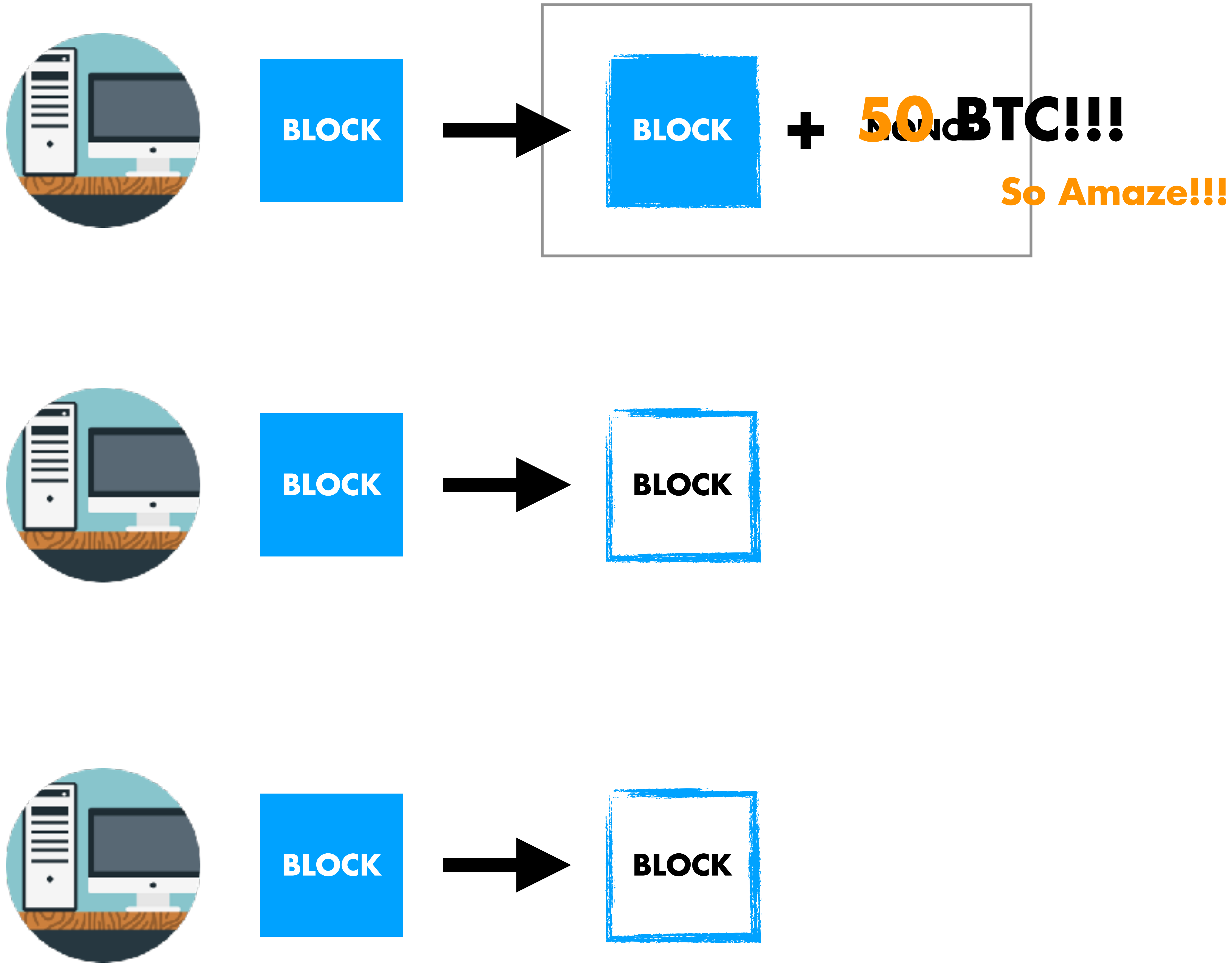
LAST

BLK#

+

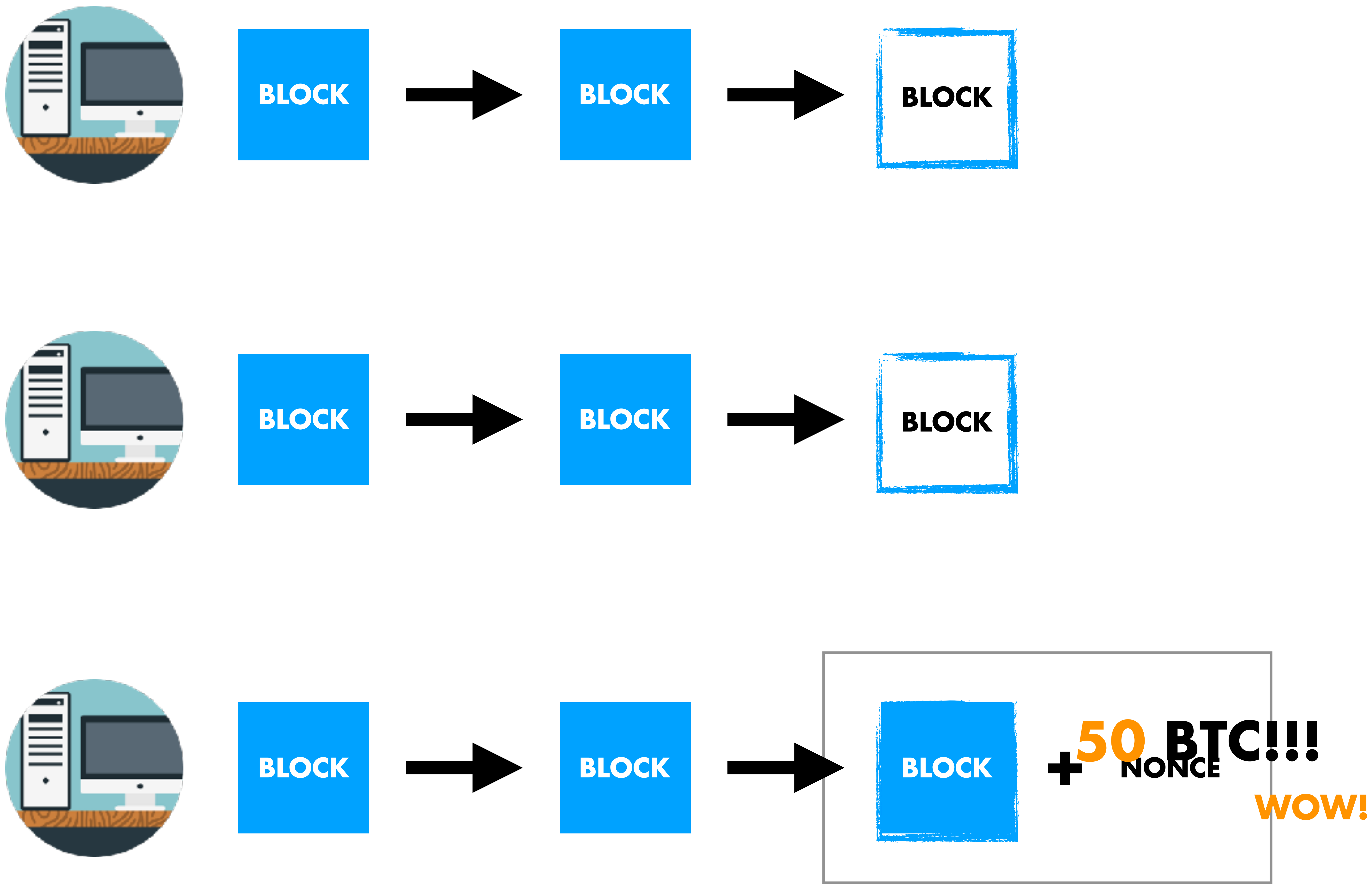
ESSENTIALS

PROOF OF WORK



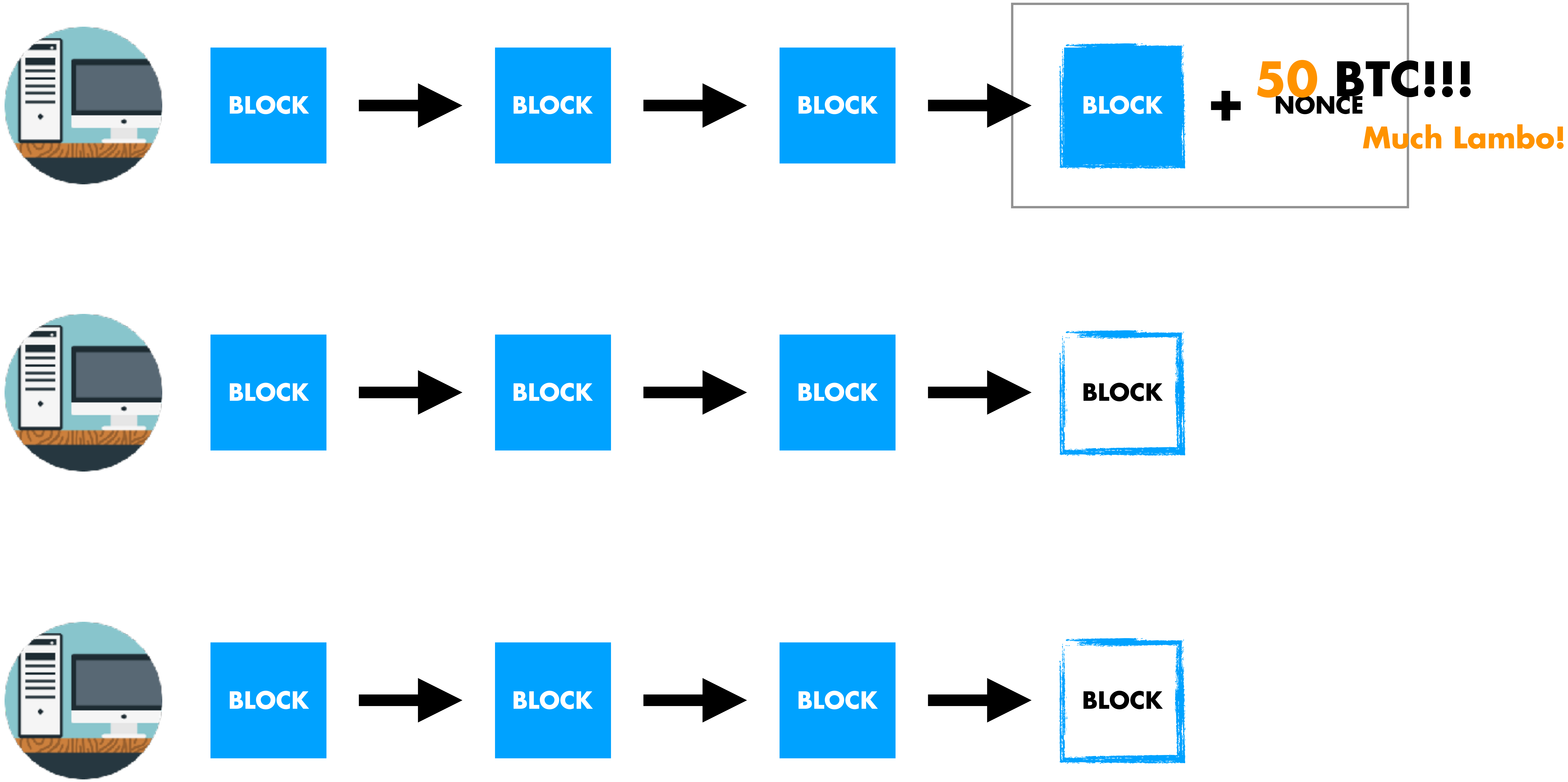
ESSENTIALS

PROOF OF WORK



ESSENTIALS

PROOF OF WORK



BLOCK → BLOCK → BLOCK → BLOCK + NONCE

50 BTC!!!

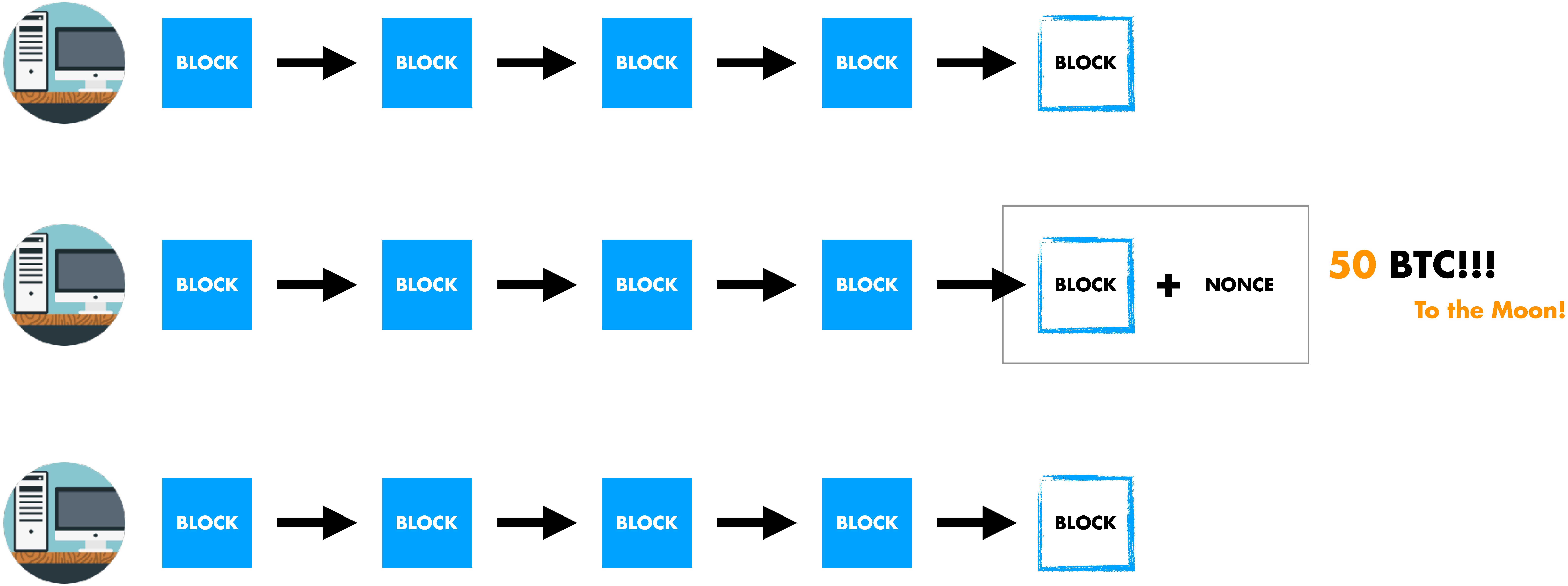
Much Lambo!

BLOCK → BLOCK → BLOCK → BLOCK

BLOCK → BLOCK → BLOCK → BLOCK

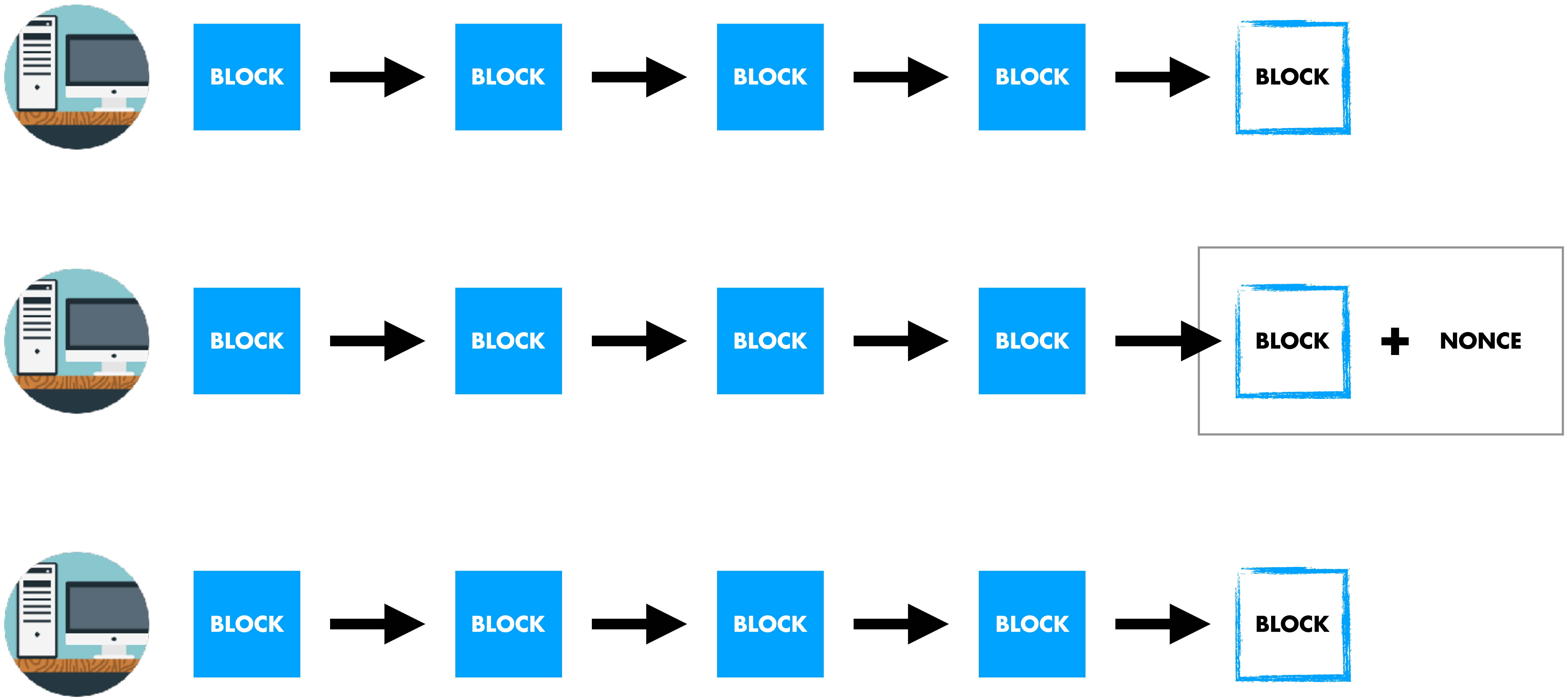
ESSENTIALS

PROOF OF WORK



ESSENTIALS

PROOF OF WORK

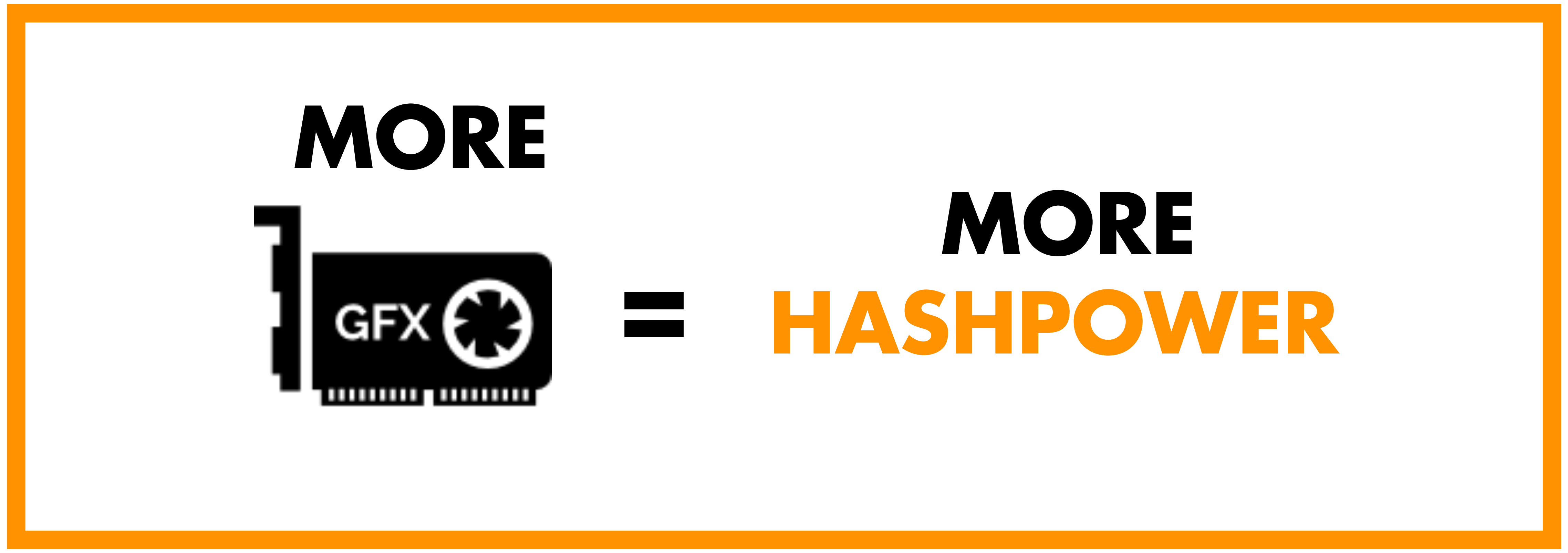


BLOCK → BLOCK → BLOCK → BLOCK → BLOCK

BLOCK → BLOCK → BLOCK → BLOCK → BLOCK + NONCE

BLOCK → BLOCK → BLOCK → BLOCK → BLOCK

A VALIDATOR NODE’S ABILITY TO GUESS THE NONCE IS MEASURED IN HASHPOWER



MORE = MORE HASHPOWER

AS SUGGESTED BY BITCOIN NETWORK

THIS IS FINE!

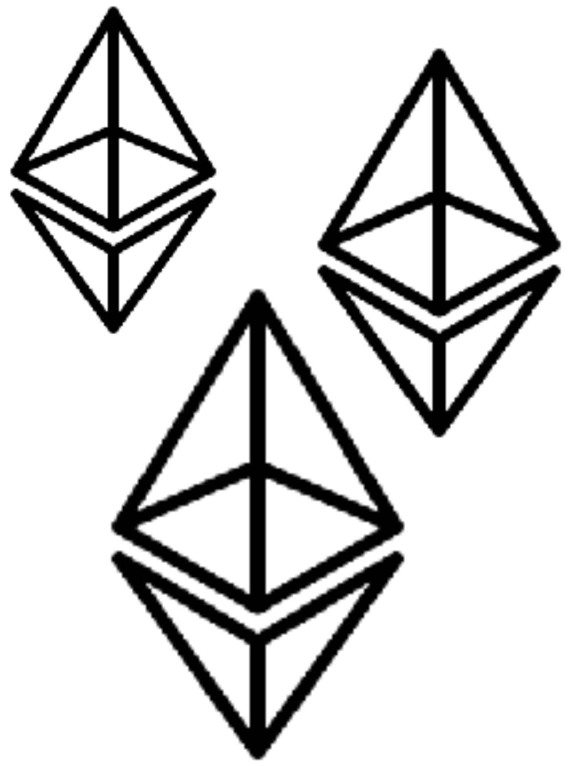
PROOF OF STAKE

VALIDATOR

(~1000 ETH TO SETUP)

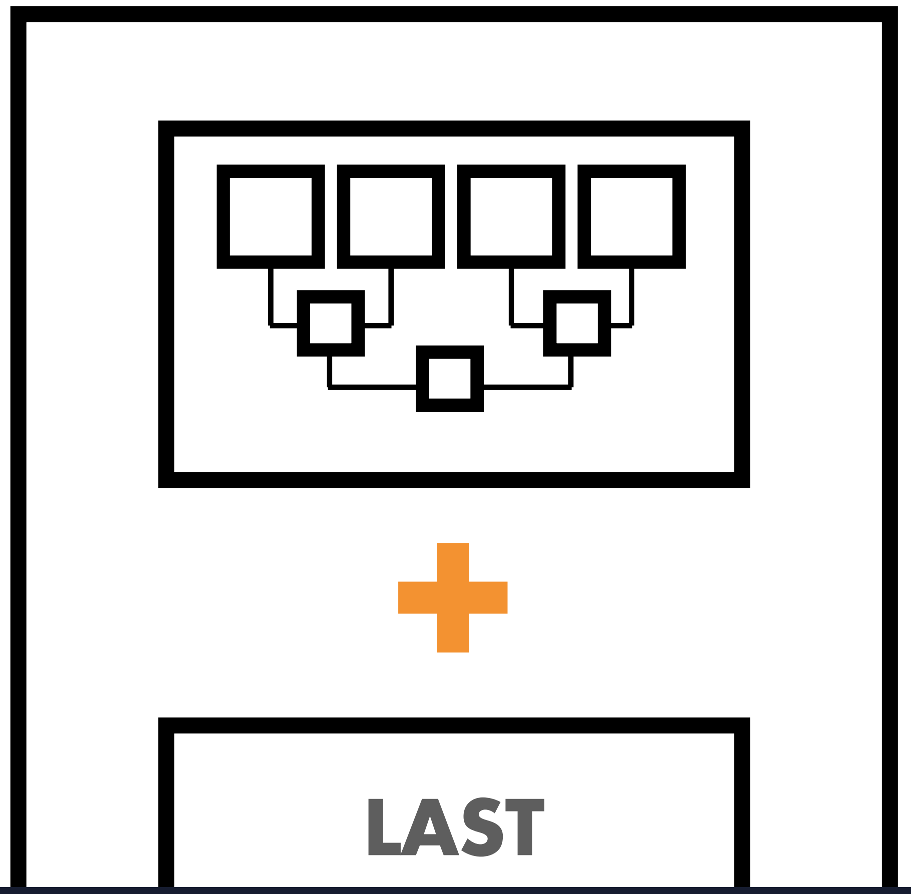
=

A NODE THAT HAS PUT CRYPTOCURRENCY AT STAKE



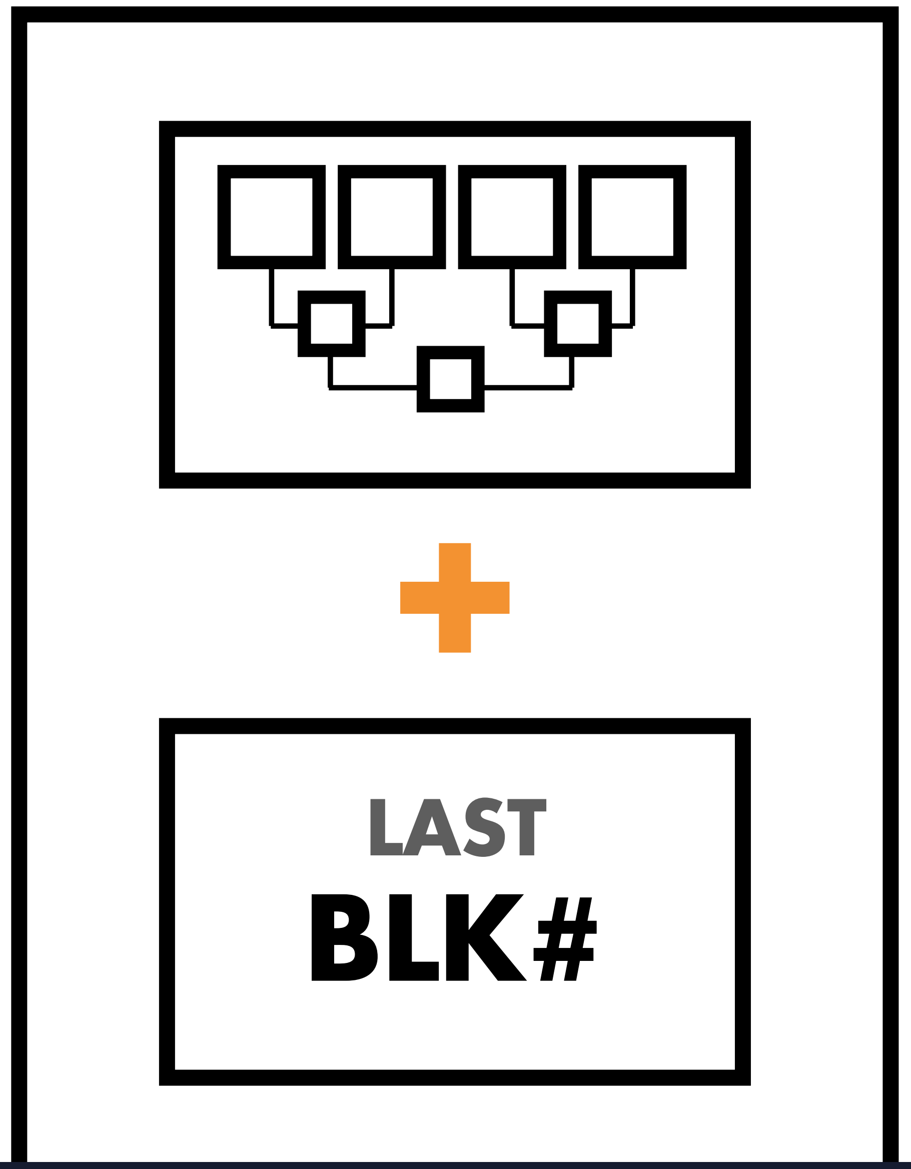
AS SUGGESTED BY ETHEREUM NETWORK

THE MORE CRYPTO YOU PUT AT STAKE ON A NODE = THE HIGHER PERCENTAGE OF THE BLOCK FEES YOU COLLECT



AS SUGGESTED BY ETHEREUM NETWORK

THE HIGHER PERCENTAGE OF THE BLOCK FEES YOU COLLECT



Ethereum blocks are generated roughly 15-20secs

30 transactions a second are typically handled

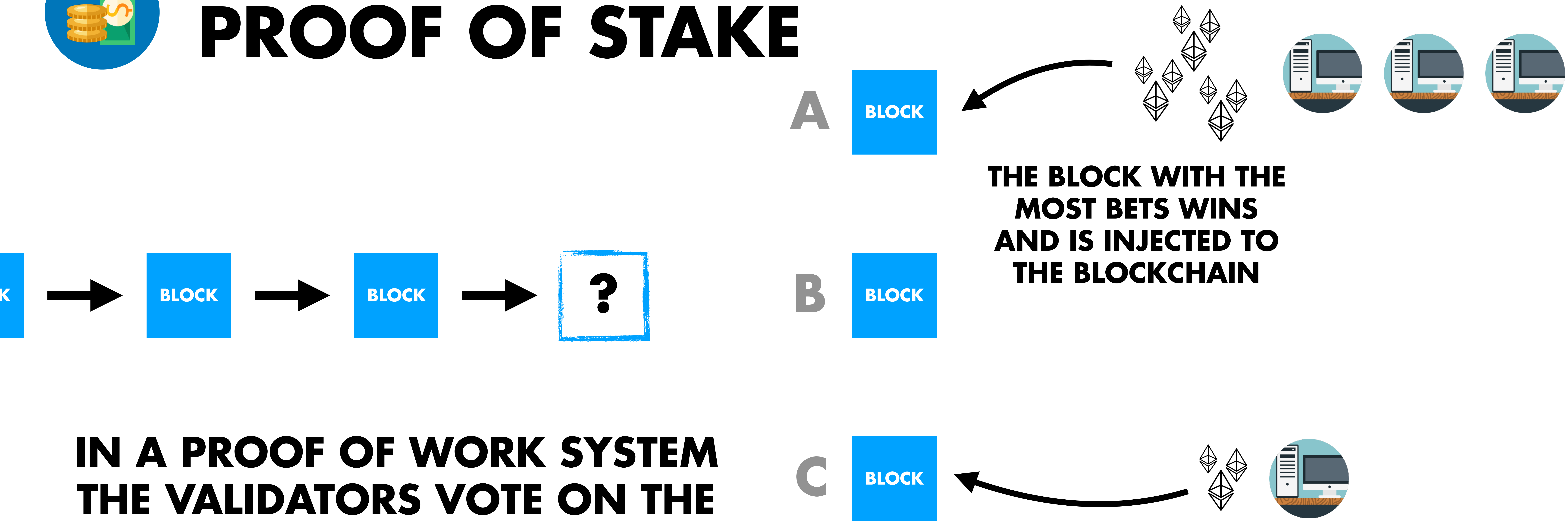
@2$ a fee

potential income per block = 1200$

AS SUGGESTED BY ETHEREUM NETWORK

ESSENTIALS

PROOF OF STAKE



THE BLOCK WITH THE MOST BETS WINS AND IS INJECTED TO THE BLOCKCHAIN

IN A PROOF OF WORK SYSTEM THE VALIDATORS VOTE ON THE NEXT BLOCK TO BE ADDED TO THE BLOCKCHAIN

AS SUGGESTED BY ETHEREUM NETWORK

ESSENTIALS

PROOF OF STAKE

K
BLOCK
BLOCK
A
BLOCK
B
BLOCK
C
BLOCK

Rewarded Fees are split amongst Validators proportionate to what was put at stake

Validators who staked ETH on a losing block lose it

AS SUGGESTED BY ETHEREUM NETWORK

CRITICAL PERSPECTIVES

Proof of Work

Resource Intensive

Costs 400M US$ Annually
Generates heat
Mining Hardware wears out faster

Vulnerable to 50% Attack

Only rewards individuals/groups who can afford specialized hardware

Proof of Stake

Mainly benefits individuals/groups who can afford to setup Validator nodes afford to stake ETH

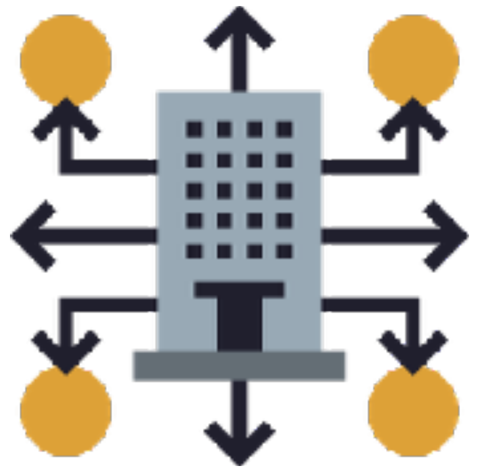
Cost is prohibitive to everyday users to become super validator nodes

Validator Nodes can easily be found by hackers and subject them to a DDOS attack

WHERE CAN WE START BUILDING BETTER CONSENSUS ALGORITHMS?

VALUE & VOLATILITY

TRADITIONAL



CURRENCY CREATION BY ONLY CENTRALIZED AUTHORITIES

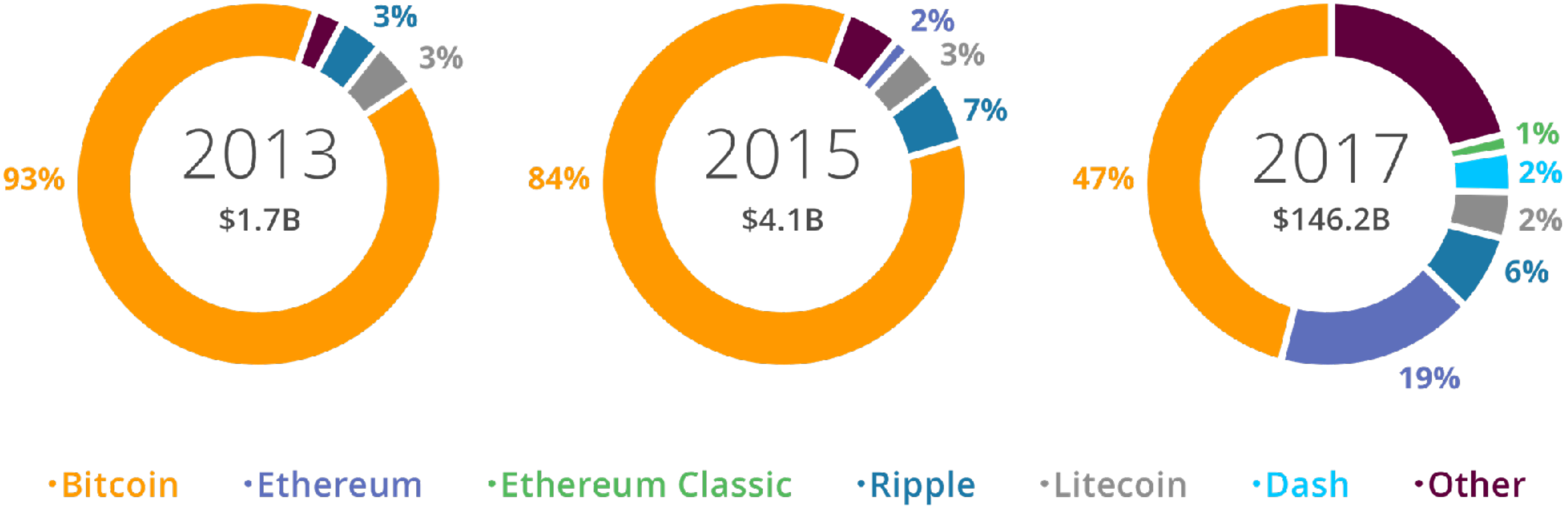
VALUE OF FIAT REGULATED BY CENTRAL BANKS

BLOCKCHAIN

CURRENCY CREATION EASILY DONE BY THE INDIVIDUALS

VALUE OF SERVICE/TECHNOLOGY REPRESENTED DIRECTLY BY VALUE OF TOKENS, DETERMINED BY MARKET/COMMUNITY SENTIMENT AND SPECULATION

MARKET CAP


2013
$1.7B
93%
3%
3%
2015
$4.1B
84%
2%
3%
7%
2017
$146.2B
47%
1%
2%
2%
6%
19%
•Bitcoin
•Ethereum
•Ethereum Classic
•Ripple
•Litecoin
•Dash
•Other

VALUE

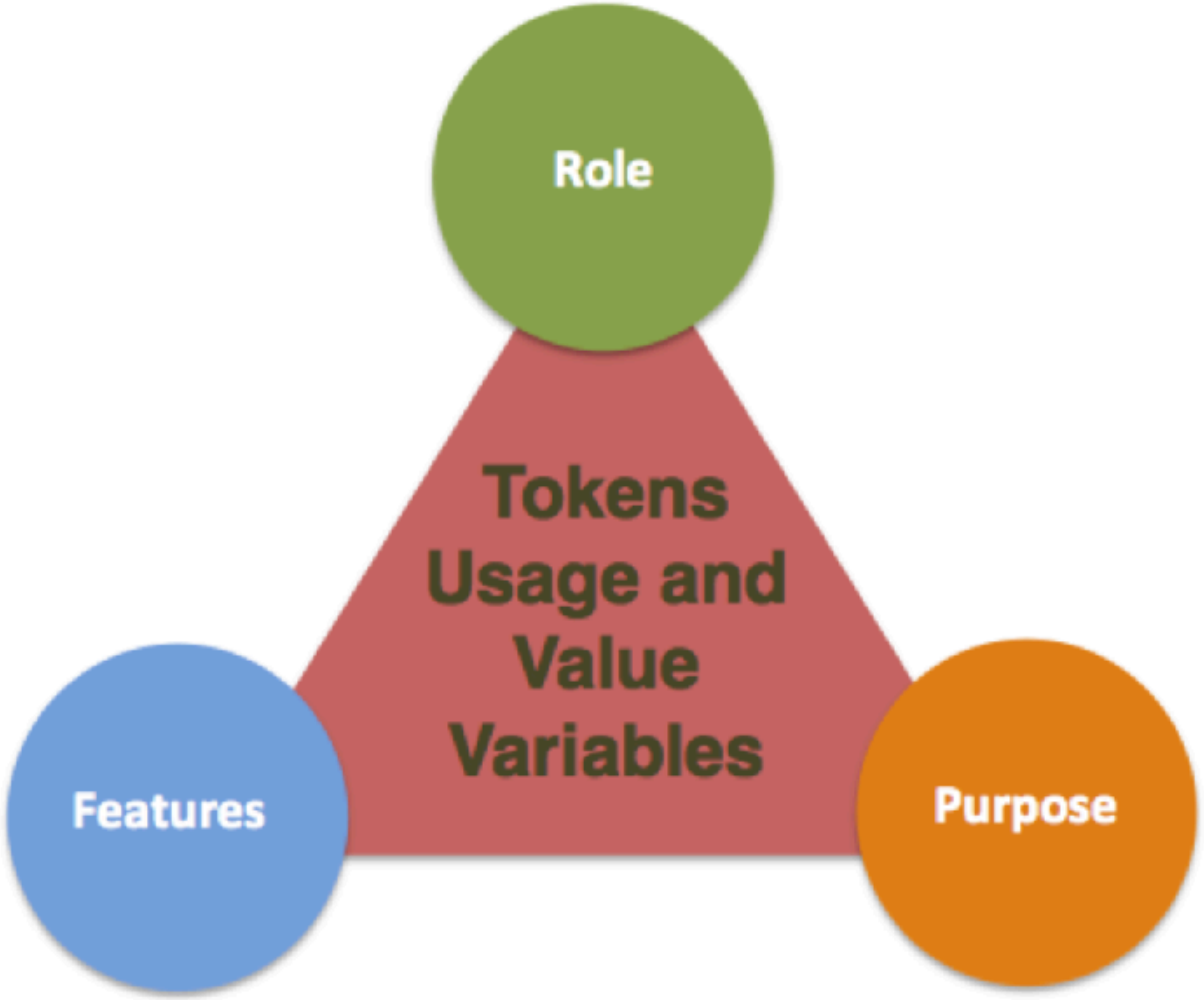
THE BLOCKCHAIN IS AN AMAZING DEMOCRATIZING TOOL THAT EMPOWERS INDIVIDUALS TO CREATE CURRENCY AND VALUE EASILY, AND TO CONNECT WITH USERS AND INVESTORS TO CREATE COMMUNITIES AND SERVICES IN OPEN, TRANSPARENT, AND NEW WAYS.

VALUE OF A SERVICE OR PRODUCT
REPRESENTED IN A TOKEN

INDIVIDUAL PRODUCTS & SERVICES
BECOME MARKETS IN AND OF THEMSELVES

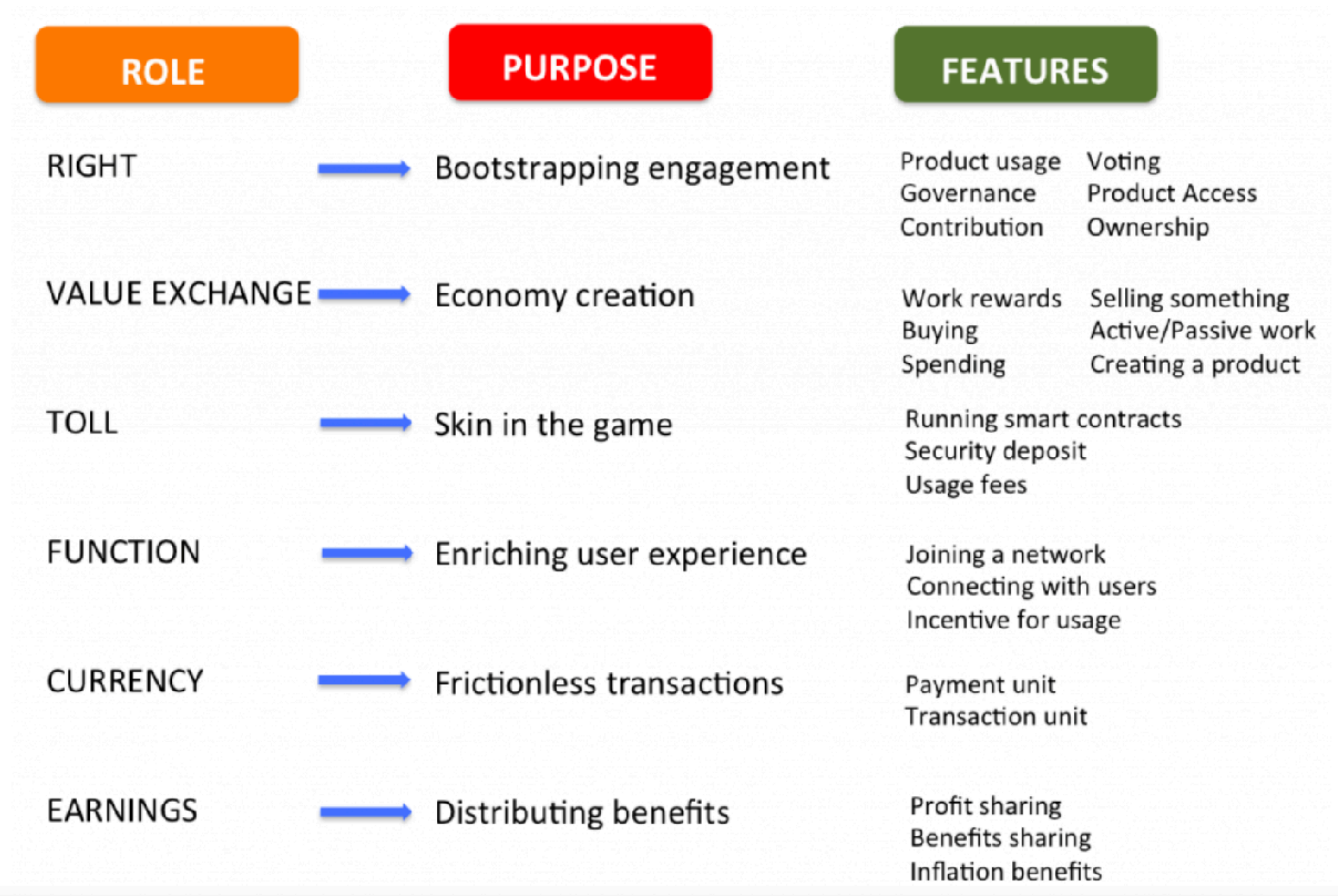
PERCEPTION OF VALUE IS A SUBJECTIVE AND
MANIPULABLE TRAIT

TOKEN VALUE DETERMINANTS



WILLIAM MOUGAYAR: AUTHOR OF THE BUSINESS BLOCKCHAIN

EXAMPLES



ROLE		PURPOSE	FEATURES	
RIGHT	→	Bootstrapping engagement	Product usage Governance Contribution	Voting Product Access Ownership
VALUE EXCHANGE	→	Economy creation	Work rewards Buying Spending	Selling something Active/Passive work Creating a product
TOLL	→	Skin in the game	Running smart contracts Security deposit Usage fees	
FUNCTION	→	Enriching user experience	Joining a network Connecting with users Incentive for usage	
CURRENCY	→	Frictionless transactions	Payment unit Transaction unit	
EARNINGS	→	Distributing benefits	Profit sharing Benefits sharing Inflation benefits	

THESE CRYPTOCURRENCIES ARE DIGITAL FIAT CURRENCIES WITH NOTHING TANGIBLE BACKING THE COINS.

PRESENTLY, MOST OF THE CRYPTO COMMUNITY IS FOCUSED PRIMARILY ON ISSUING DIGITAL TOKENS EXCHANGEABLE FOR ONLY OTHER DIGITAL TOKENS.

VOLATILITY

CRYPTOCURRENCIES DON’T REPRESENT DIRECT EQUITY IN ANY GOOD OR SERVICE, NOR ARE THEY BACKED BY TANGIBLE RESERVE ASSETS. PRICE IS DETERMINED BY MARKET SENTIMENT AND SPECULATION.

CRITICAL PERSPECTIVES

VALUE & VOLATILITY

Wildly volatile and unpredictable value is incompatible with real-world use

No protection against credit risk for investors

Individual savings can wildly grow or deplete

Token valuation is prone to market manipulation by whales and invested parties

No price floor (a token's value can theoretically go down to $0)

How can you design a stable-priced cryptocurrency?

DISINTERMEDIATION

DISINTERMEDIATION

PRESENTLY, INTERMEDIARY COMPANIES/AGENTS/ DEPARTMENTS TAKE CARE OF A LOT OF THE ADMINISTRATIVE FUNCTIONS OF A BUSINESS

– THE BLOCKCHAIN CAN AUTOMATE ALL OF THAT

TRADITIONAL

BANKS HOLD FUNDS

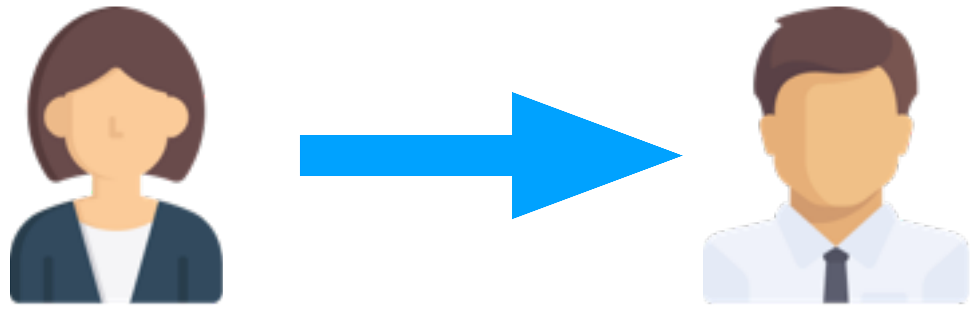
LAWYERS OFFICIATE CONTRACTS

SERVICES LIKE PAYPAL FACILITATE PAYMENTS

BLOCKCHAIN

YOUR SECURE WALLET IS YOUR BANK

SMART CONTRACTS ARE LAW



DIRECT INDIVIDUAL TO INDIVIDUAL PAYMENT

CRITICAL PERSPECTIVES

DISINTERMEDIATION

People will lose their jobs

There are no consumer protections on Blockchain services
(with the current state of blockchain tech)

Any consumer protection mechanisms have to coordinate globally

Is the consumer ready for the responsibility that comes with this independence?

WHAT, IF ANY, NEW JOBS CAN BE CREATED THAT COULD HELP WITH THESE ISSUES?

SMART CONTRACTS

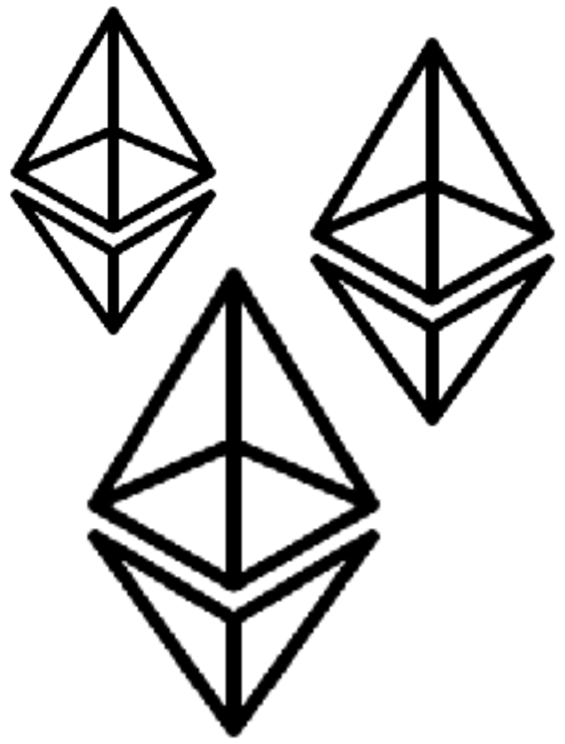
SMART CONTRACTS

A Smart Contract is a computer program that has some legal attributes.

SMART CONTRACT

=

PROGRAMS THAT LIVE ON THE BLOCKCHAIN

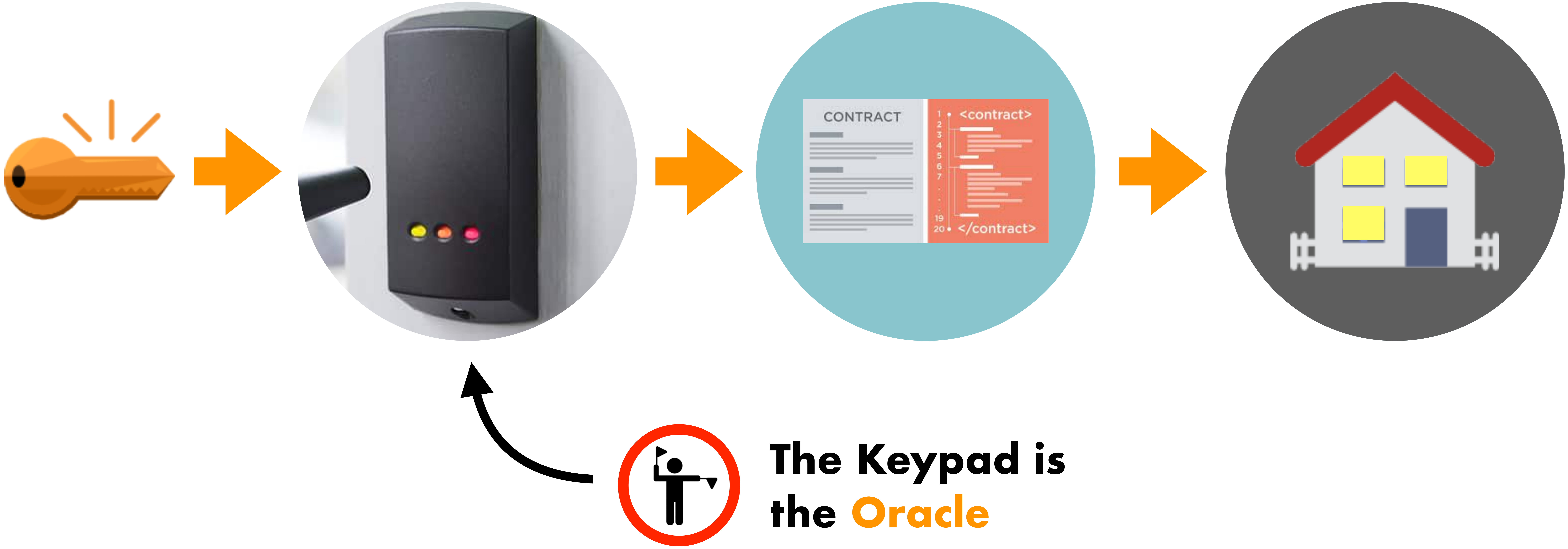


IMMUTABLE | ALWAYS ON
RUN ON GAS

IN SOME CASES SMART CONTRACTS NEED ORACLES

An Oracle is an agent that finds and verifies real-world occurrences and submits that information to the blockchain to be used by Smart Contracts.

ORACLES IN ACTION



The Keypad is the **Oracle**

EXAMPLES OF SMART CONTRACTS

LAND TITLES

CRYPTO KITTIES

WILLS & EMPLOYMENT CONTRACTS

CORPORATIONS

ICO

INITIAL COIN OFFERING

BLOCKCHAIN-BASED CROWDFUNDING

DAO FAILURE

- One of the first ICOs
- 11.5 million ETH were collected

- There was a money draining code bug
- A large sum of ETH was under the control of the Hacker
- Smart Contract wasn't properly audited by Slock.it team

- The network forked, creating Ethereum Classic, to remedy the situation

DAO FAILURE

IMPLICATIONS

JURISDICTION

DAMAGES

LIABILITIES

REMEDIES

How will issues of liability, jurisdiction and ownership be addressed in a decentralized world?

IMMUTABILITY

IMMUTABILITY

WHAT HAPPENS ON A BLOCKCHAIN STAYS ON A BLOCKCHAIN. A SINGLE POINT OF TRUTH IS ON THE CHAIN, DETERMINED AND BACKED BY THE CONSENSUS OF THE NETWORK. ONCE SOMETHING IS AGREED UPON AND WRITTEN ONTO THE BLOCKCHAIN, IT CANNOT BE EASILY ROLLED BACK.

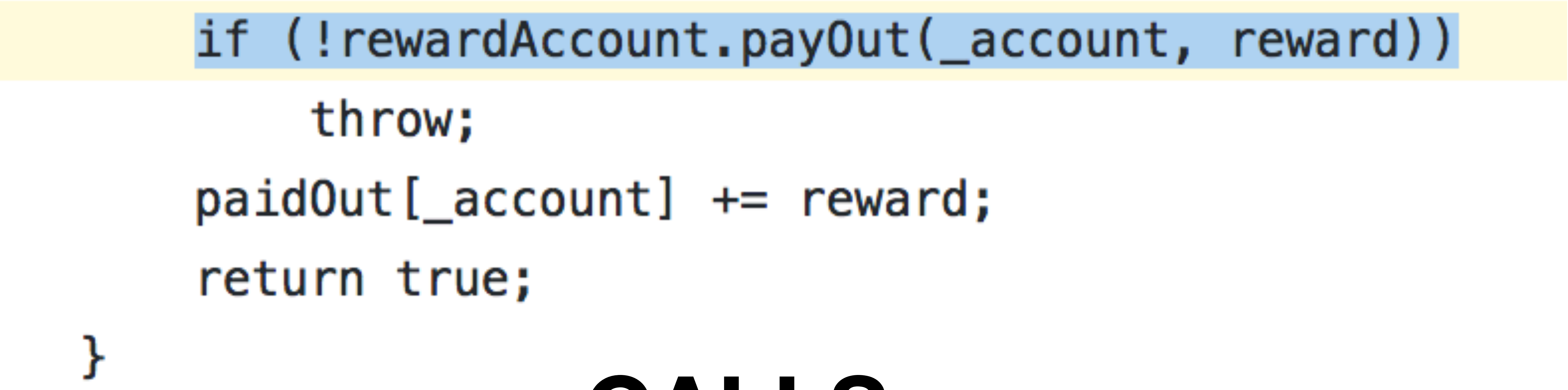
TRADITIONAL

1. **DATABASE RECORDS CAN BE ROLLED BACK**
2. **BUGGED SOFTWARE CAN BE PATCHED AND ITERATED ON**
3. **COMPANIES ARE HELD ACCOUNTABLE FOR SECURITY FLAWS OF THEIR SOFTWARE**

BLOCKCHAIN

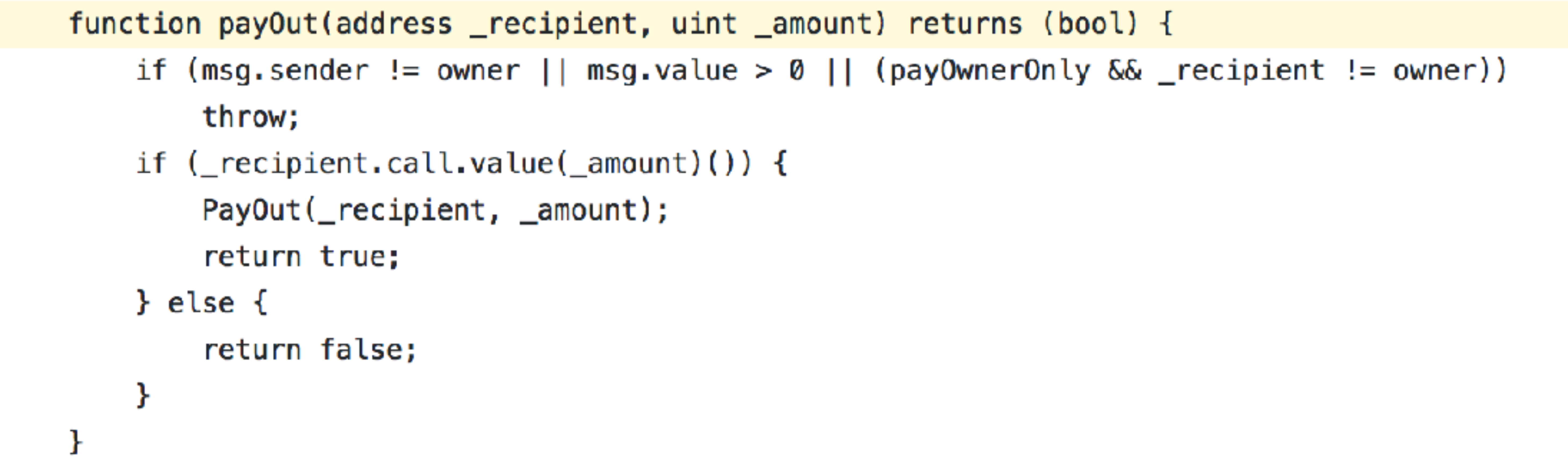
1. BLOCKCHAIN RECORDS CANNOT EASILY BE ROLLED BACK
2. SMART CONTRACTS ON THE BLOCKCHAIN CANNOT BE EDITED UNLESS A NEW COPY IS UPLOADED, AND THAT DOES NOT UNDO THE FAULTY CONTRACT'S EFFECTS
3. THE NETWORK/USERS ARE LEFT TO THEIR OWN DEVICES FOR HOW TO DEAL WITH ISSUES

EXAMPLE: THE DAO DEBACLE



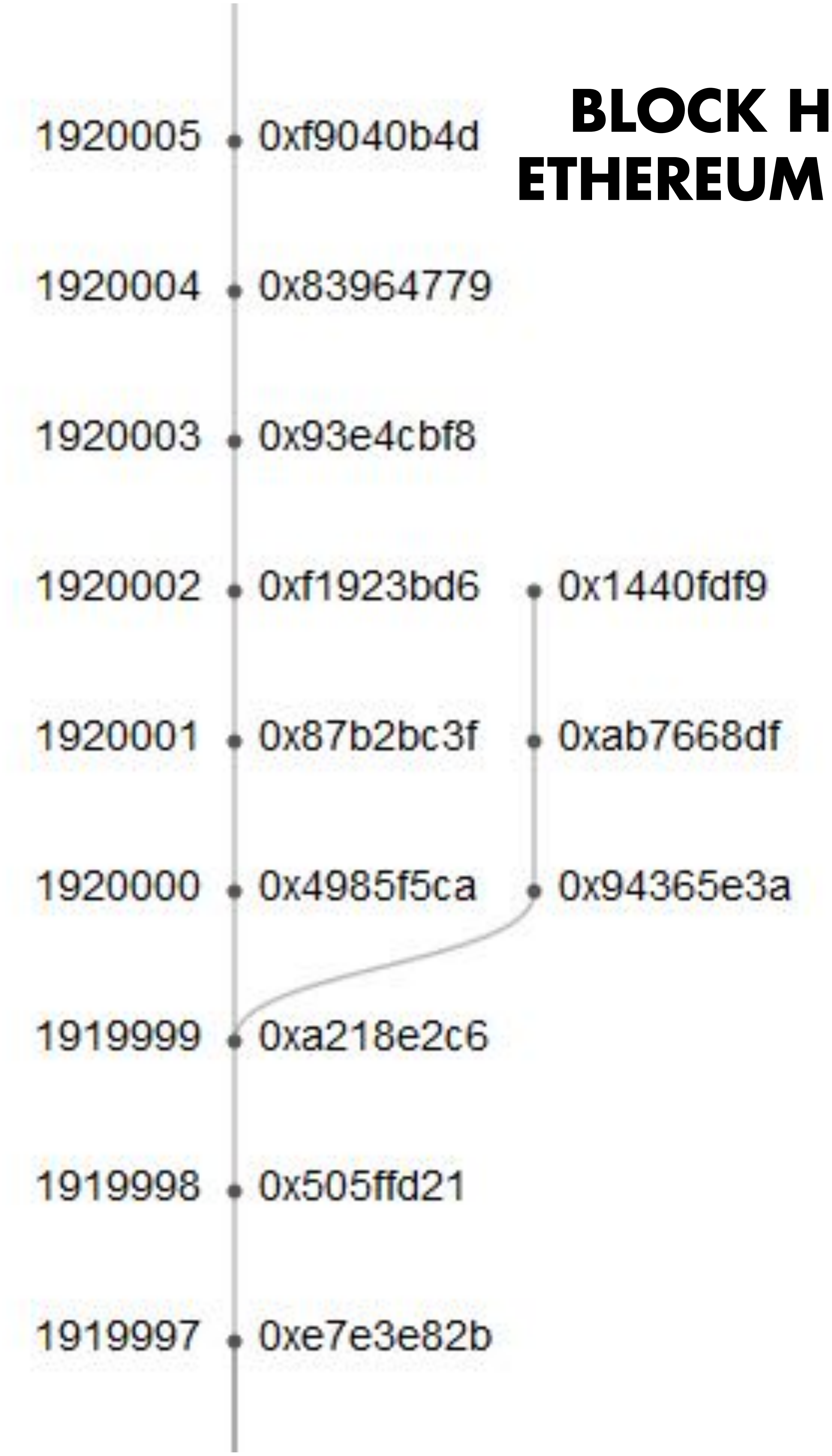
```
        if (!rewardAccount.payOut(_account, reward))
            throw;
        paidOut[_account] += reward;
        return true;
    }
```

CALLS...



```
function payOut(address _recipient, uint _amount) returns (bool) {
    if (msg.sender != owner || msg.value > 0 || (payOwnerOnly && _recipient != owner))
        throw;
    if (_recipient.call.value(_amount)()) {
        PayOut(_recipient, _amount);
        return true;
    } else {
        return false;
    }
}
```

RESULT: FULL NETWORK FORK



1920005	0xf9040b4d	
1920004	0x83964779	
1920003	0x93e4cbf8	
1920002	0xf1923bd6	0x1440fdf9
1920001	0x87b2bc3f	0xab7668df
1920000	0x4985f5ca	0x94365e3a
1919999	0xa218e2c6	
1919998	0x505ffd21	
1919997	0xe7e3e82b	

BLOCK HASHES ETHEREUM CLASSIC

BLOCK HASHES ETHEREUM

BLOCK NUMBERS

CRITICAL PERSPECTIVES

IMMUTABILITY

Humans (and their code) are still imperfect on a platform that demands perfection

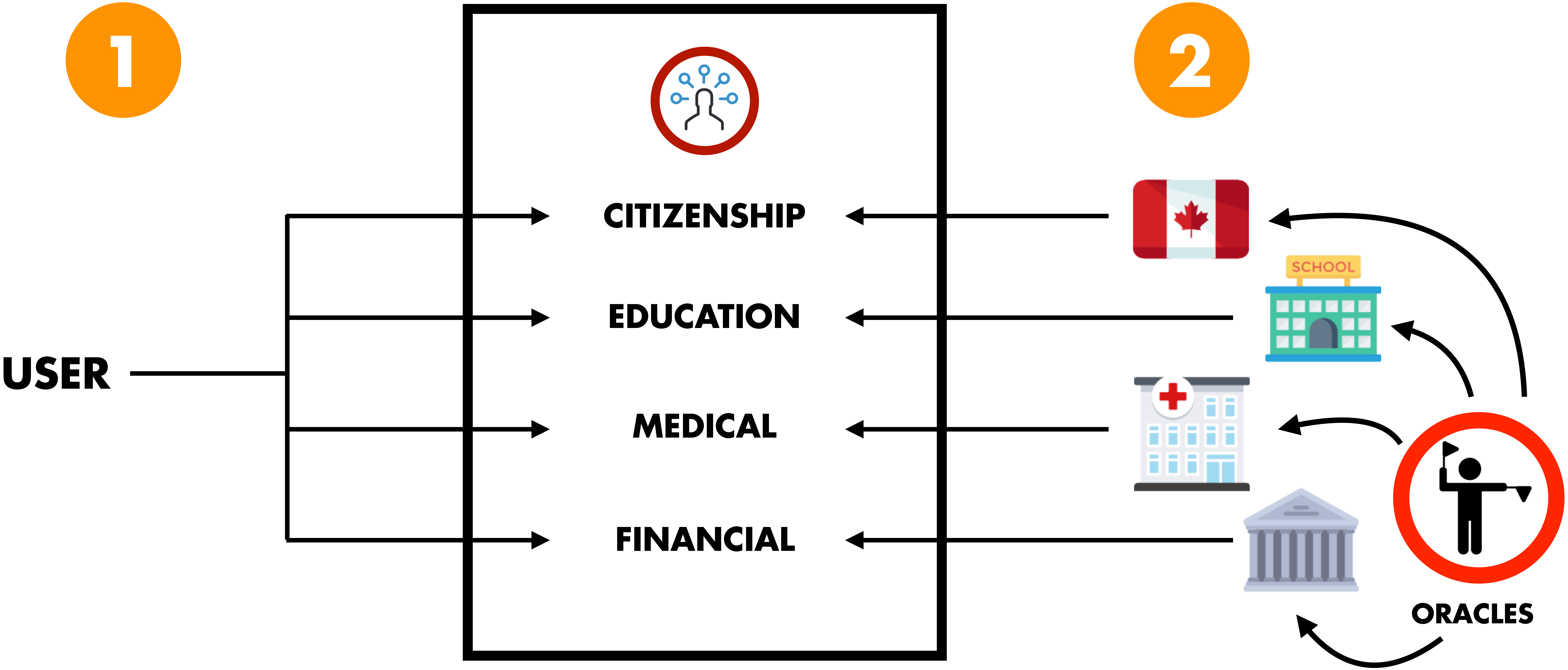
Transactions due to mistakes, fraud or hacks are not easily rolled back

**As the blockchain has one source of truth based on network consensus,
the entire network is affected in transaction roll backs**

How do we design out the limitations that limitations that we've talked about today?

IDENTITY

IDENTITY



1

2

USER

CITIZENSHIP

EDUCATION

MEDICAL

FINANCIAL

ORACLES

IDENTITY

BLOCK
BLOCK
BLOCK
BLOCK
BLOCK
BLOCK
BLOCK
BI

Individual who controls the private key owns the identity files

IDENTITY

BLOCK
BLOCK
BLOCK
BLOCK
BLOCK
BLOCK
BLOCK

Identity Documents would exist as a collection of smart contracts on the blockchain

A SINGLE BLOCKCHAIN IDENTITY
CAN ACT AS MULTIPLE IDs
SIMULTANEOUSLY

CRITICAL PERSPECTIVES

There is an increased emphasis for personal responsibility,
once private keys are lost there is no way of getting it back
- identity theft takes a whole new meaning

Institutions in control of the network can control livelihoods
of individuals by altering their records of identity

Nations, Institutions, Companies, and individuals have
to agree to a standard network and system for identity

Blockchain identities assume a privileged user, with access to the internet,
who is cognisant of the the technology and how to steward their records -
it is not clear how to scale the technology to the developing world

CRITICAL PERSPECTIVES

WORLDBOOK

It’s the year 2050, Blockchain identities are pervasive in society, a new service much like Facebook appears. anybody can join and partake in it – there is one caveat?

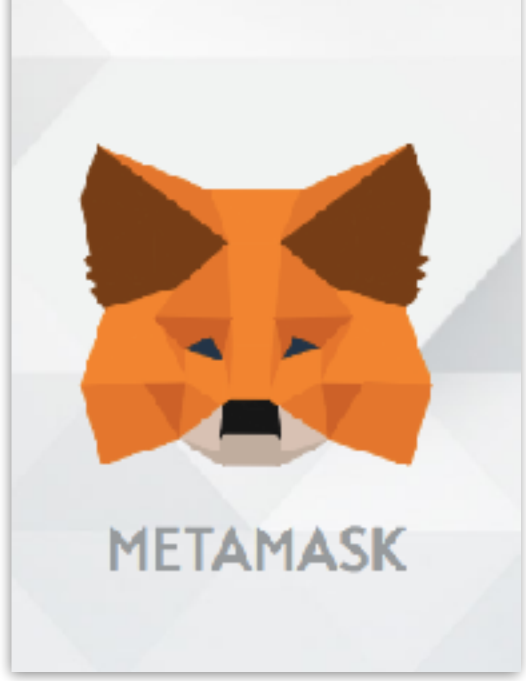
They need access to your ID data on the blockchain, data you’re not comfortable sharing on a whim.

WOULD YOU CONSENT TO THE EXCHANGE?

QUESTIONS?

THANK YOU FOR HAVING US!

@OLIVEBRANCHLAW | @EDBUCHI | @JELOTWEETS



INTERACTIVE WORKSHOP

GET METAMASK

50% OF THE GROUP WILL BE GIVEN **1 ETH**
(**ON THE ROPSTEN TEST NETWORK**)

TASK

SHARE ETH TO THE OTHER 50% OF THE GROUP