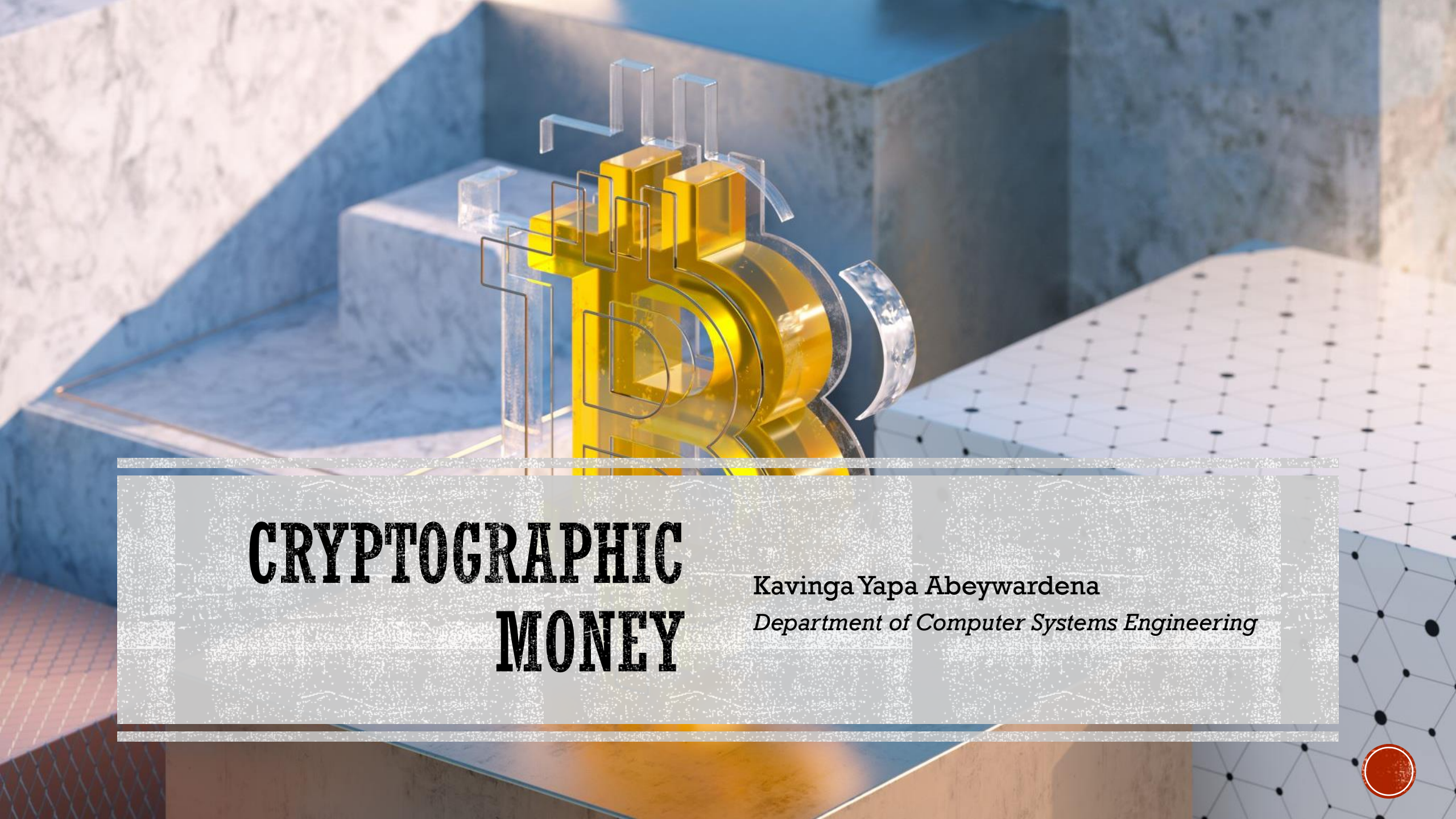


CRYPTOGRAPHIC MONEY

Kavinga Yapa Abeywardena
Department of Computer Systems Engineering

TOPICS COVERED

Origins of Money
Virtualization of Money
Cryptographic Concepts used in Bitcoin
Bitcoin Transactions
Recording Bitcoin Transactions
Bitcoin Mining
Bitcoin Inflation

ORIGINS OF MONEY

Part 1

WHAT IS MONEY?

- Hunter-gatherer tribe. Group of hunters kill mammoth. Mammoth cut up and meat taken home to feed tribe.
- Tribe “owes” each hunter for his part in killing mammoth.
- Debt settled by share of meat.
- Easy to remember who is owed what in small group.

WHAT IS MONEY?

Invention of agriculture:

- Domestication of plants and animals.
- Hunting declines - people settle - cities founded.

Specialization of trades:

- Farmers,
- Carpenters
- Metal smiths…etc.

Too many people now for informal debts easily to be remembered/enforced.

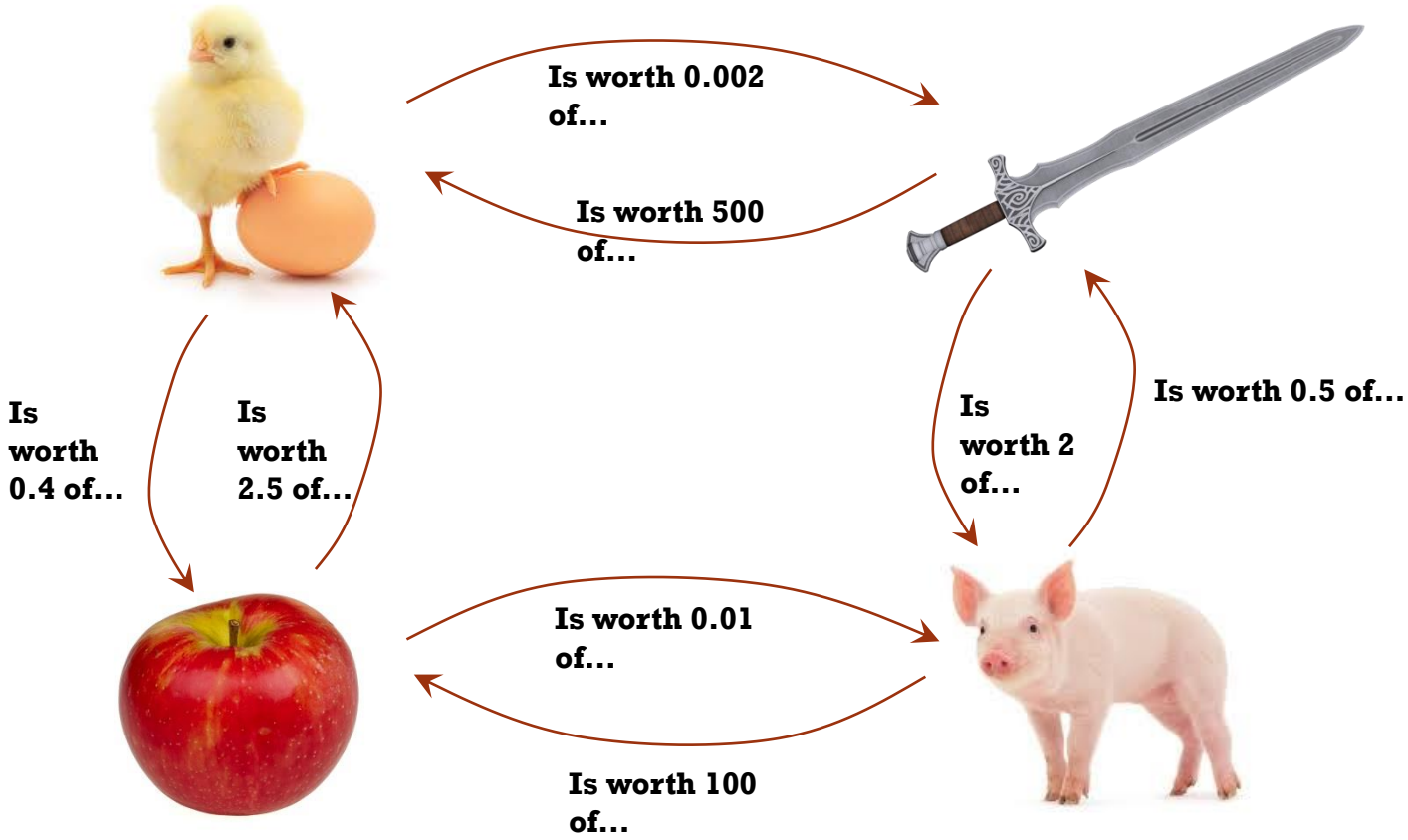
Barter systems develop:

- Exchange of eggs for apples.
- Grain for swords…etc.

<u>Aristotle (384-322BC) on the origin of money:</u>

Every commodity has a primary (original) use and a secondary use as an item of barter.

WHAT IS MONEY?



No universal measure of worth

A pig is worth 100 apples, but without the entire "web" of exchange rates that tells you nothing about the universal worth of pigs and apples.

Also all apples are not the same!

WHAT IS MONEY?

Is worth 0.5 of...

Is worth 250 of...

"Standard" Commodity

"Money"

Is worth 0.2 of...

Is worth 125 of...

WHAT MAKES GOOD MONEY?

- **<u>Aristotle:</u> the commodity must…**

1. Be durable

- Must not fade, corrode etc.

2. Be portable

- Must have a high worth relative to its weight and size

3. Be divisible/fungible

- May be separated, re-combined, exchanged, replaced without affecting value.

4. Have intrinsic value

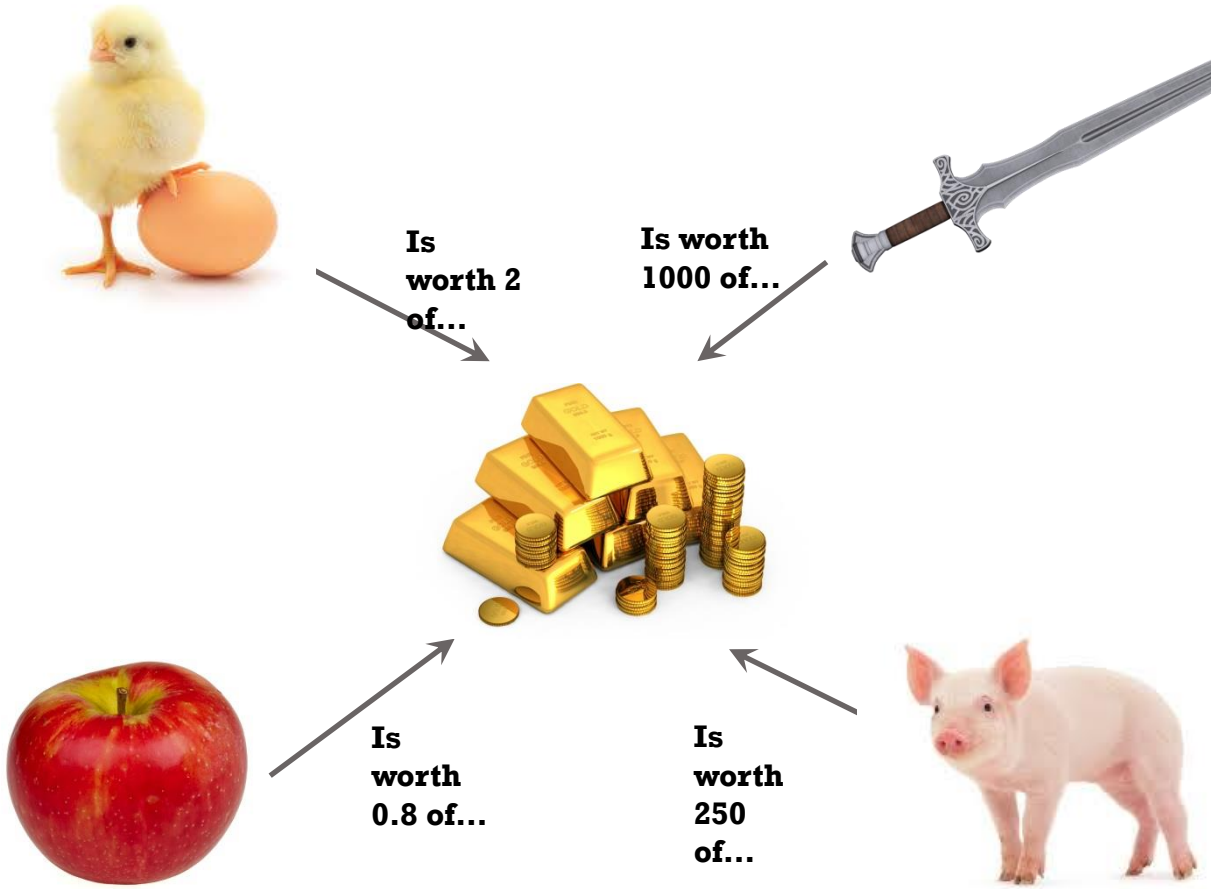
- The value of money must be independent of anything except the money itself.
- Usually linked to its <u>scarcity</u>.

GOLD AS MONEY

- **1. Durable - YES**
- Gold remains gold (though gold coins can be chipped – original reason why coins have "milled" edges).
- **2. Portable - YES**
- Gold is valuable relative to its weight. Gold coins can be carried
- **3. Divisible/fungible - YES**
- Different sized coins/ingots can be cast and recast.
- **4. Intrinsic value - PARTIALLY**
- Value of gold depends on the amount of gold there is in circulation. (As more gold is mined, value of existing gold falls.)

- Gold used to mint gold coins of standard weight/purity – payees know they are getting the amount of gold they think they are.

GOLD AS MONEY?

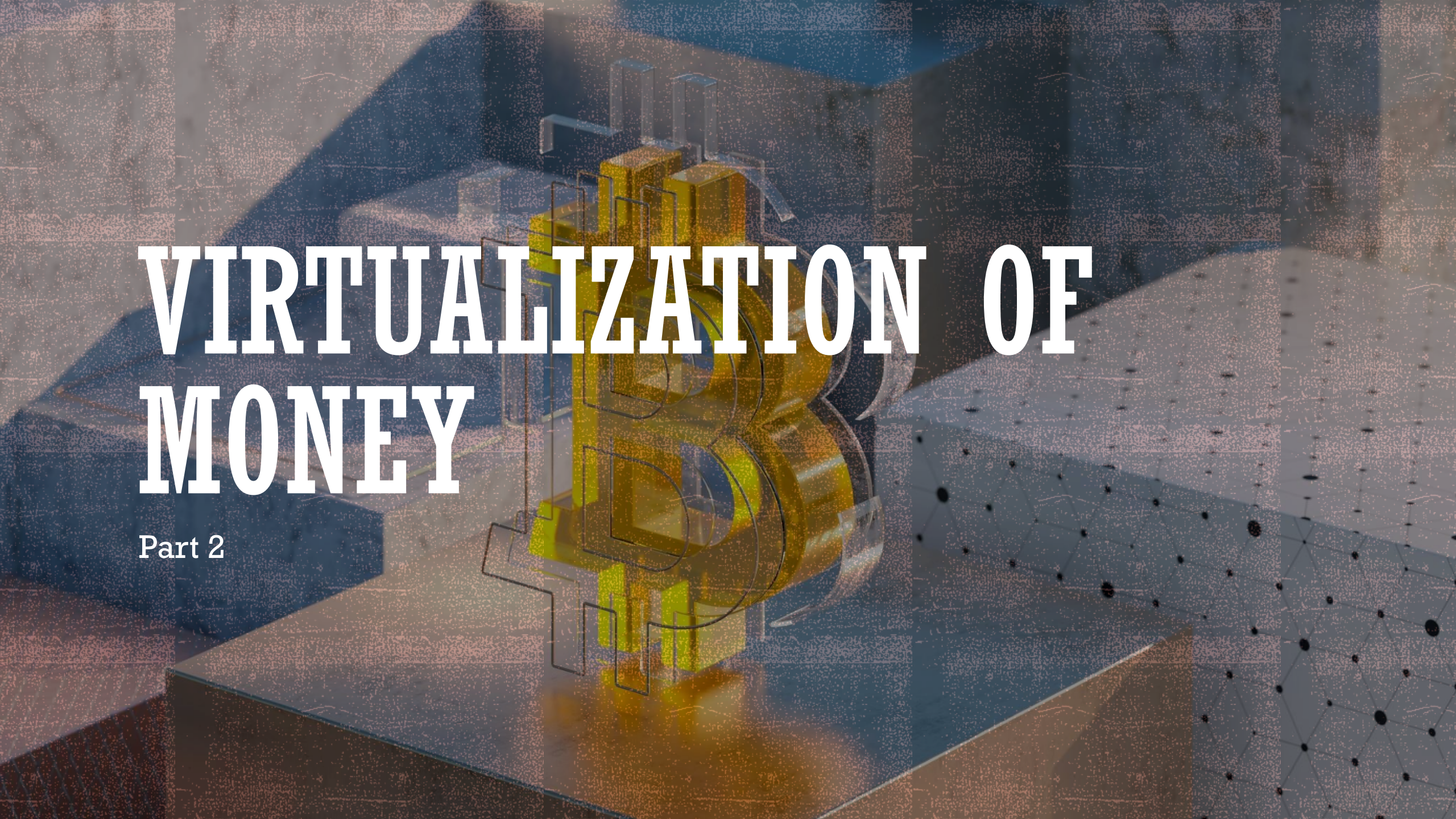


The worth of everything is now expressible in terms of a common "yardstick"

YOUTUBE VIDEOS…

- Sir Martyn Poliakoff talking about the gold in the Bank of England…
  - https://www.youtube.com/watch?v=CTtf5s2HFkA

- Professor Lawrence White on the "Gold Standard"…
  - https://www.youtube.com/watch?v=LdyHso5iSZI



VIRTUALIZATION OF MONEY

Part 2

FIAT MONEY AND VIRTUAL MONEY

- Gold replaced by promissory tokens/banknotes issued by governments and banks.
  - Under "gold standard" these could be exchanged for gold coin.
- **"Fiat" system nowadays more common.**
  - debt acknowledged, but not actually backed up with gold.
  - Value of notes/base-metal coins depends on authority of issuer, which **must** be trusted.
  - Can be counterfeited! (Counterfeit coins are becoming a nuisance!)
- **Now however…**
  - most money is "virtual" – it does not exist *even as fiat tokens*!
  - Exists as a balance in a bank account – acknowledgment of debt.
  - Most money is now merely information. (As it originally was!)

MONEY AS INFORMATION

- We no longer have physical tokens to record debt
- Their properties must be **replicated virtually**:
  - **Integrity**
    - Total amount of money must be conserved during every transaction. (Money may not be "double spent").
    - Transaction must be irrevocable; payer may not (unilaterally) reverse transaction afterwards.
  - **Scarcity**
    - "New" money cannot be created by anyone without appropriate authority.
- These features enforced by a trusted financial institution/ authority, which all participants trust.

YOUTUBE VIDEO…

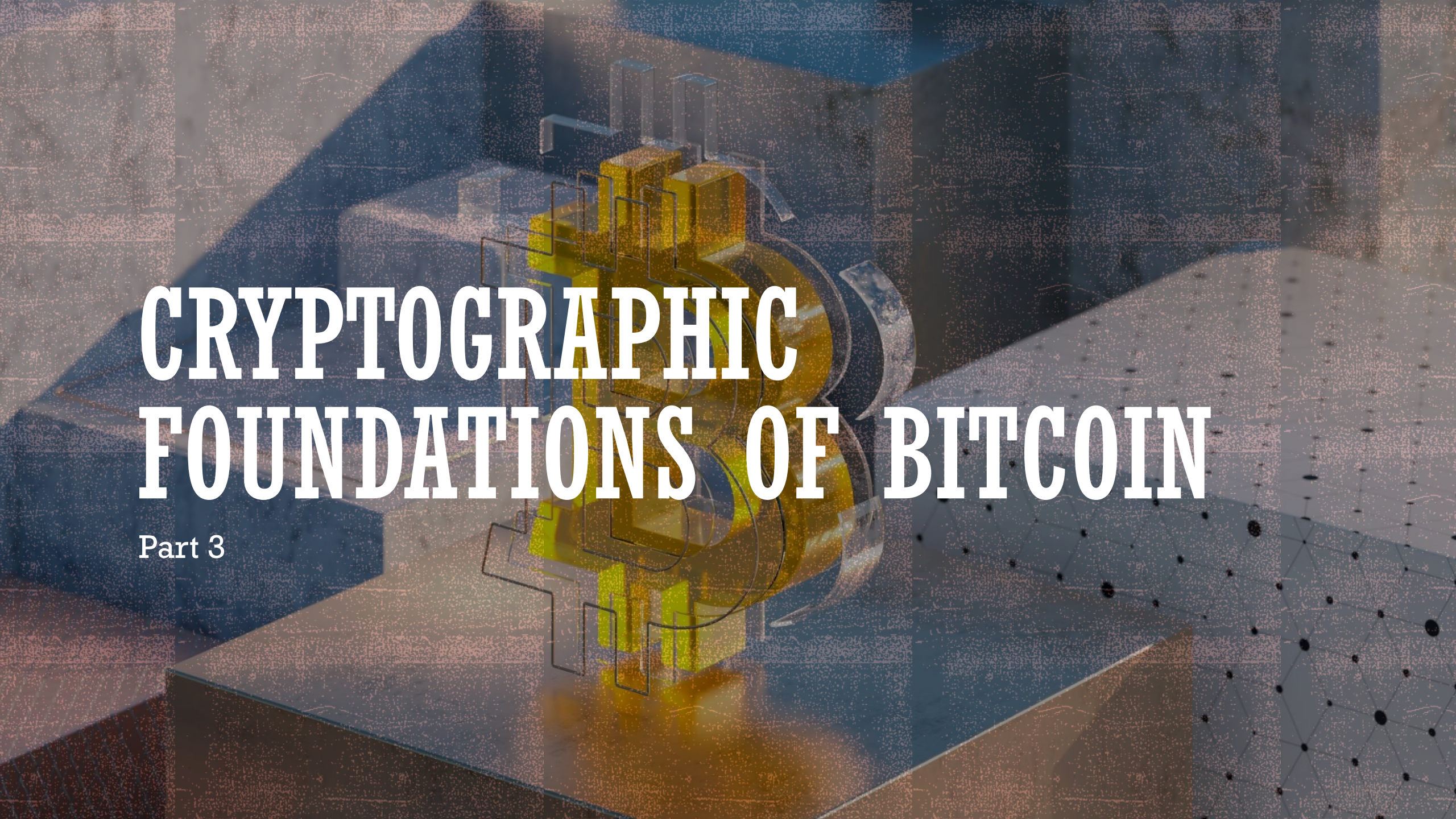
- "Money as Debt" – documentary by Paul Grignon…
  - https://www.youtube.com/watch?v=jqvKjsIxT_8

CENTRALIZED AUTHORITY

- "Payment" involves an authorized instruction to bank to transfer funds from one account to another.
  - Credit/Debit Cards
  - Cheques/Wire Transfer
- Contrast to paying with coins, banknotes etc.
  - These are issued by a central authority, **but transferred on a "peer-to-peer" basis.**

DECENTRALIZED CURRENCY

- Peer-to-Peer system – *no* centralized authority.
  - Mimics buying/selling with gold coins (also peer-to-peer).
  - We need an electronic equivalent to gold coins.
- Early attempts: "Hashcash", "B-money".
- Bitcoin introduced in 2009 by "Satoshi Nakamoto"
  - This is not his real name.
  - Sounds Japanese, but he is believed to be English or Norwegian.
- To understand how this works, we must first be sure to understand a few cryptographic concepts.



CRYPTOGRAPHIC FOUNDATIONS OF BITCOIN

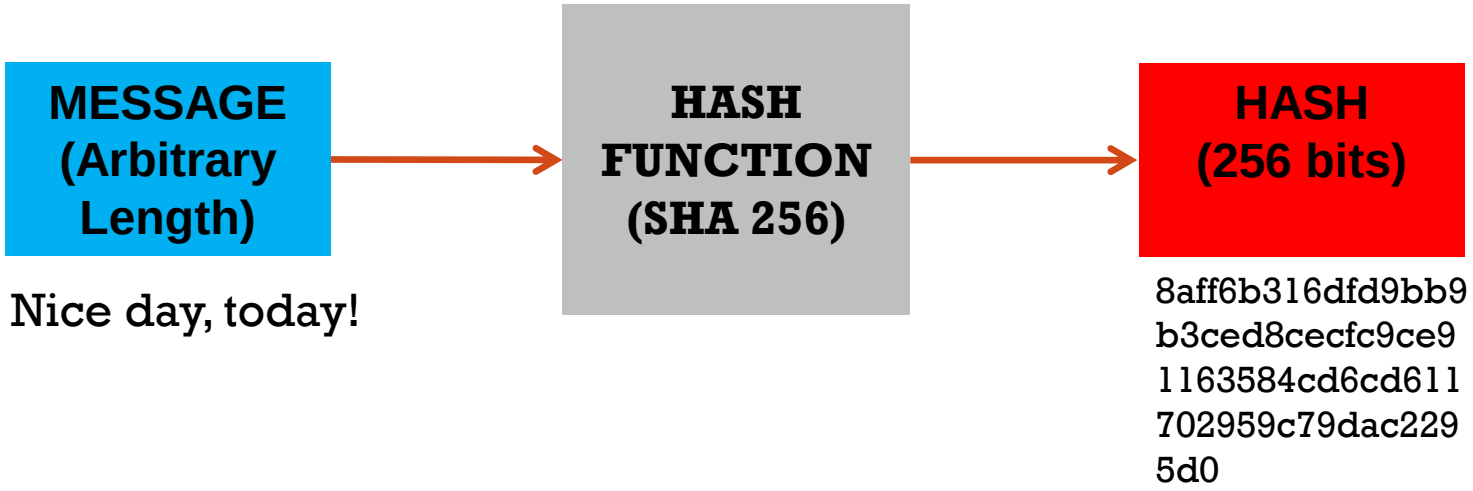
Part 3

CRYPTOGRAPHIC FOUNDATIONS

- To understand how this works, we must understand three basic cryptographic concepts:
  - Hash Functions
  - Digital Signatures
  - Proof-of-Work (PoW)

HASH FUNCTIONS

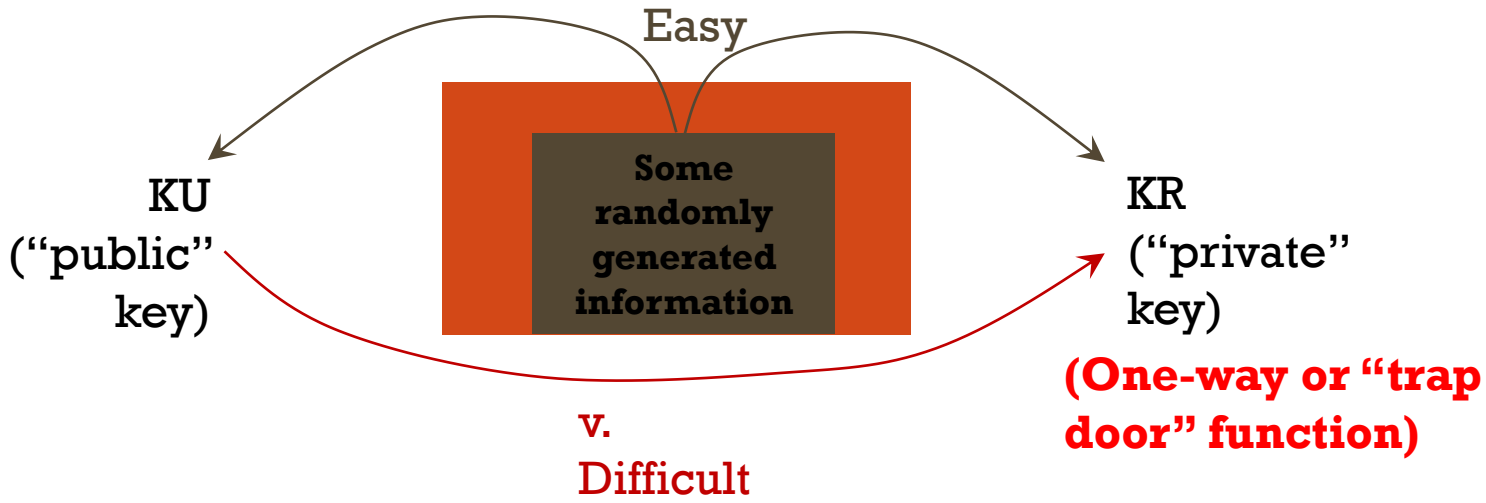
- A deterministic function *H*, mapping bit string of arbitrary length to fixed length string.
- Output bits are *seemingly* random.
- Algorithm needs to be:
  - Fast - many hashes may be generated in a very short time.
  - "Collision resistant": chance of 2 inputs producing identical output very very small.
  - "Pre-image resistant": infeasible to find input given output.
- Hash demo: http://www.xorbin.com/tools/sha256-hash-calculator



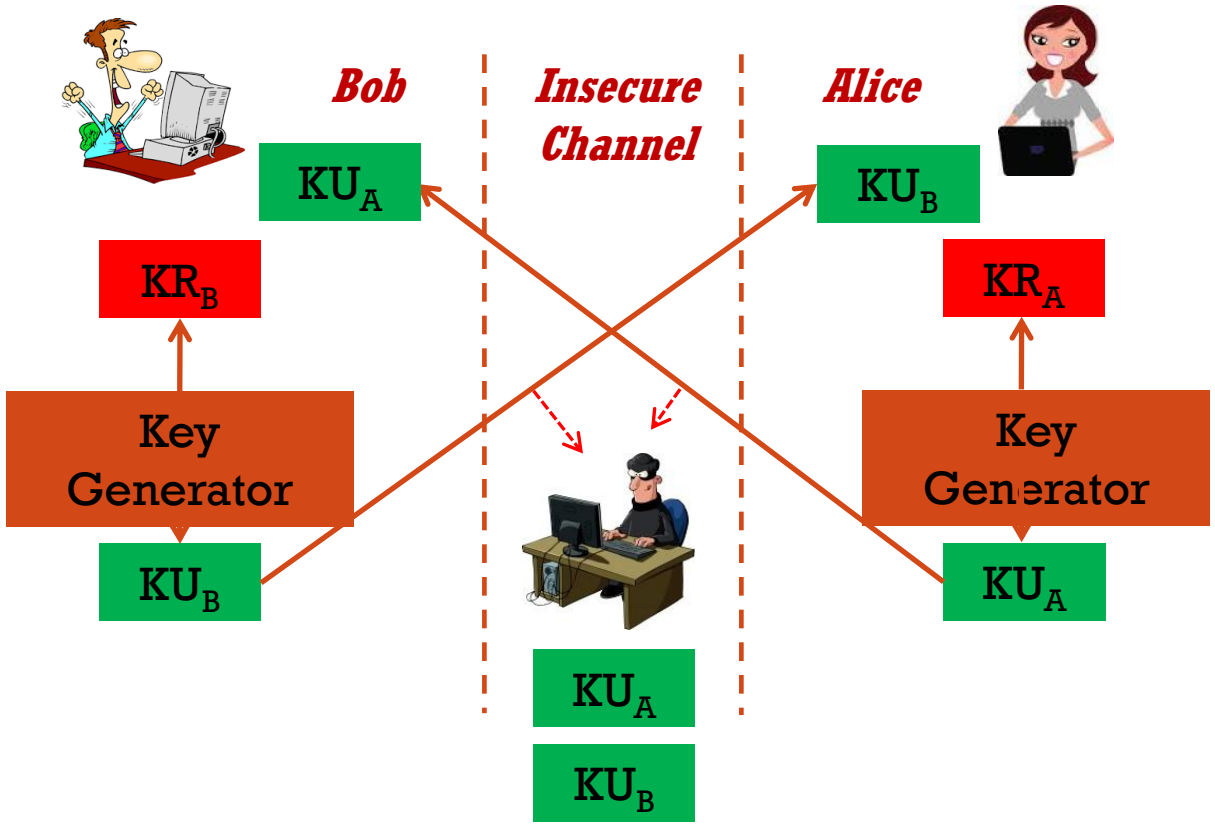
DIGITAL SIGNATURES (RSA TYPE)

Public Key Cryptography: keys are created in pairs:

- Messages encrypted using KU can only be decrypted using KR.
- Messages encrypted using KR can only be decrypted using KU.
- Neither key can (feasibly) be inferred from the other.

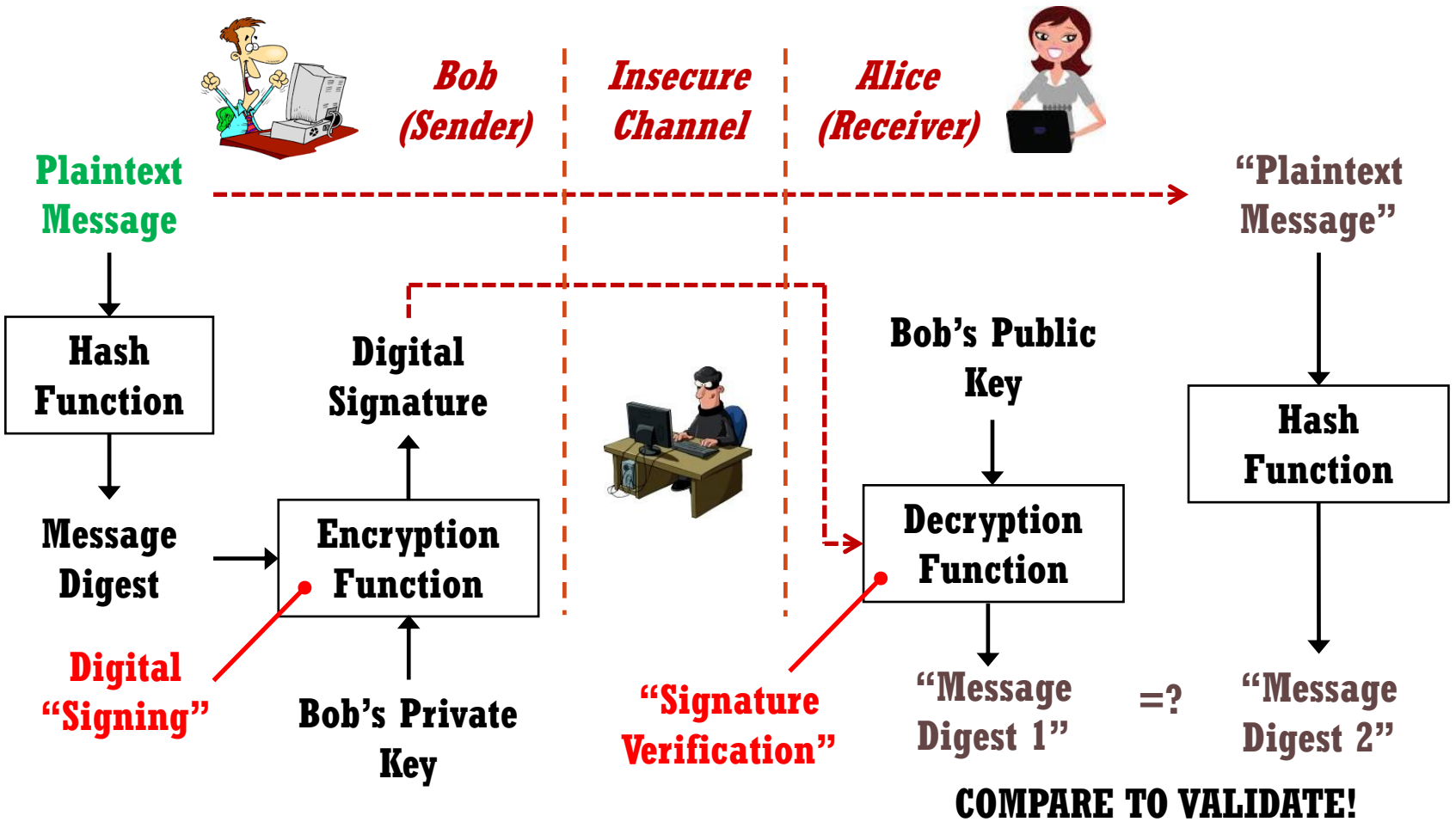


DIGITAL SIGNATURES (RSA TYPE)



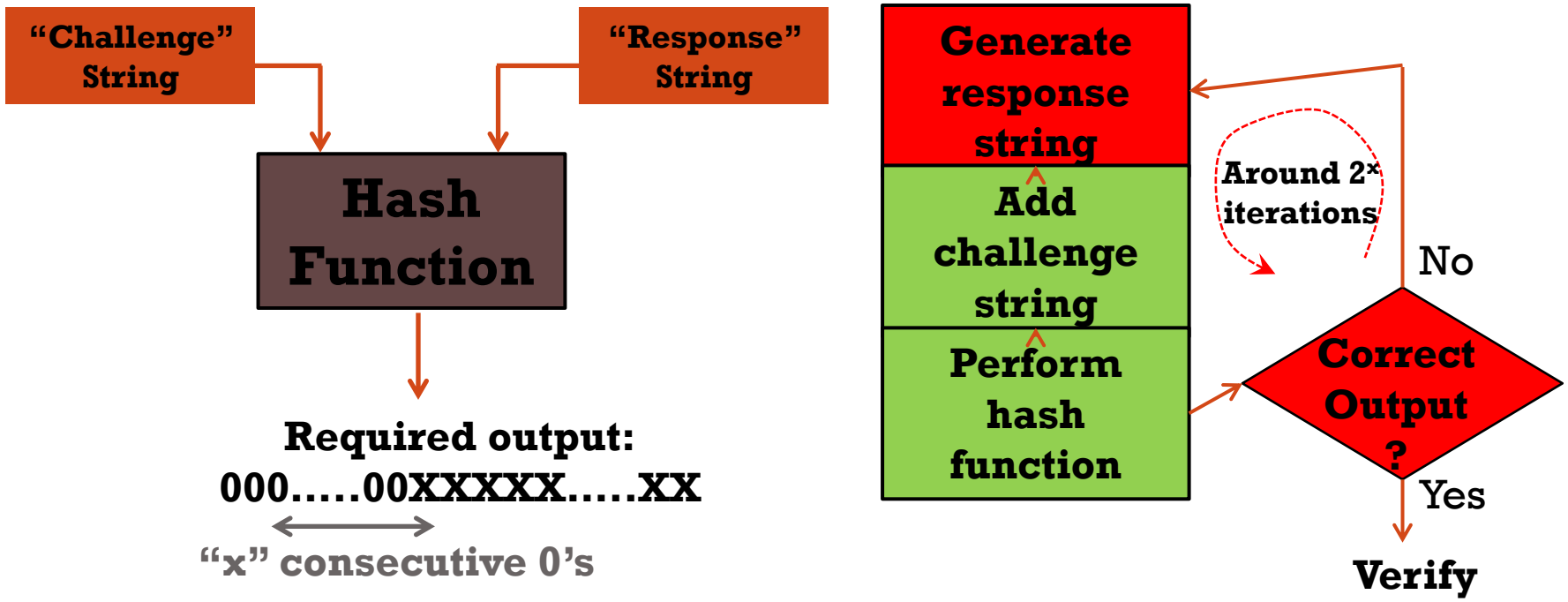
"Harry the Hacker" can only ever hope to intercept the public keys. The private keys are never transmitted.

DIGITAL SIGNATURES (RSA TYPE)



"Harry the Hacker" cannot sent messages to Alice pretending to be Bob, because he does not have Bob's private key.

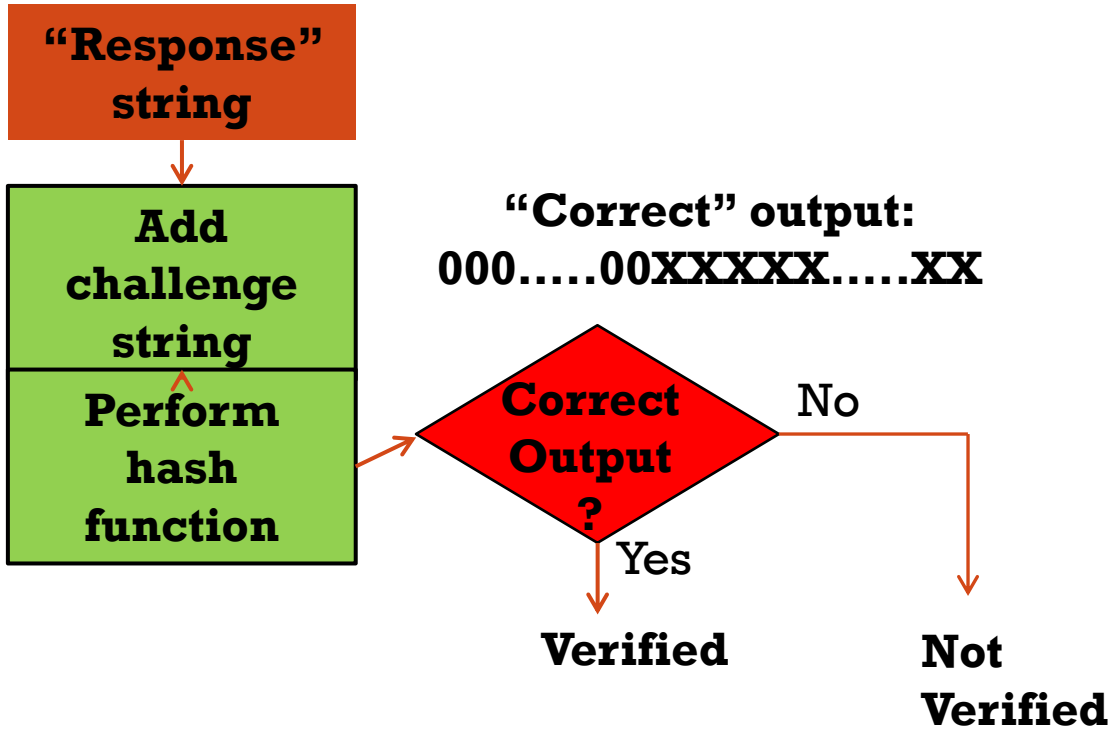
PROOF-OF-WORK (POW) PROBLEM



Forces the challenged party to "do work" – if x=40, he/she must perform about 2^40=1,000,000,000,000 hashing operations.

Imposes a "cost" on the challenged party, deterring him/her from over-using/ abusing services (if proof-of-work needed before access given).

PROOF-OF-WORK (POW) PROBLEM



Only one hashing operation is needed to check that this work has been done.

YOUTUBE VIDEO…

- Khan Academy – explanation of PoW
  - https://www.youtube.com/watch?v=9V1bipPkCTU
    - This video doesn't really add much to what I've said, but you may want an alternative description.

BITCOIN TRANSACTIONS

Part 4

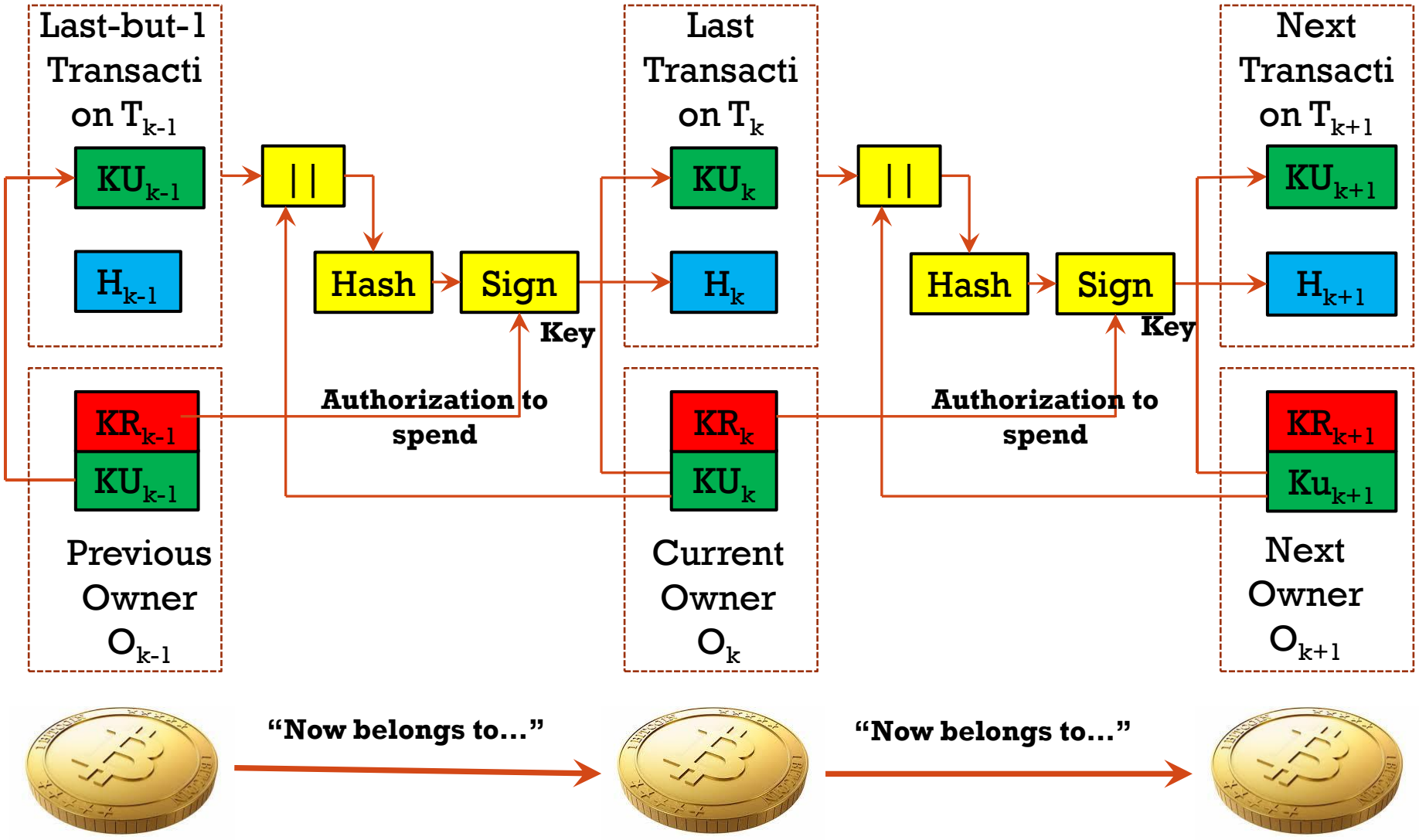
"BITCOIN" – TWO MEANINGS

- Bitcoin (BTC) is a unit of currency (has an exchange rate with Rs., $, yen etc.
  - Typically 1 bitcoin = $35,830 (Subject to huge fluctuations)
  - There are lots of different denominations of units – e.g. thousandths and millions of bitcoins.
- Bitcoin is the peer-to-peer protocol for the exchange of bitcoins between parties (players).
  - Also facilitates the "mining" of Bitcoins.
  - Participants compete to record "blocks" of transactions.
  - Winners rewarded with newly "minted" Bitcoins.
  - Like mining gold – introduces a mechanism for devaluation

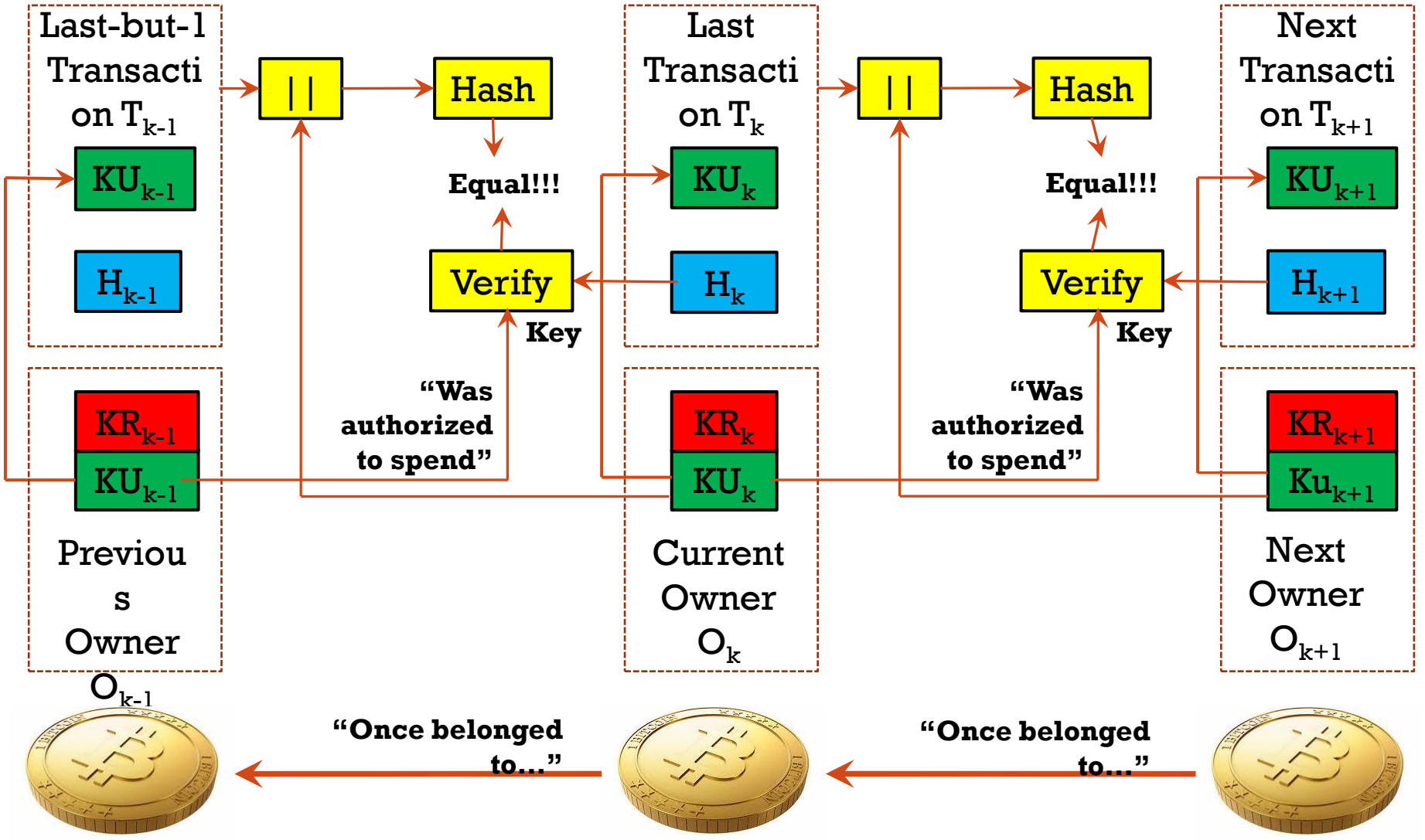
WHAT IS A BITCOIN?

- A virtual "coin" that can be exchanged.
- Exists as a chain of digital signatures representing all the transactions in the coin's history.
- Validated checked by verifying of these signatures.
- Contains a "bitcoin address" = public key of the coin's owner.
  - Owner has the corresponding private key.
  - Only owner can sign an instruction to transfer that Bitcoin to a new owner.

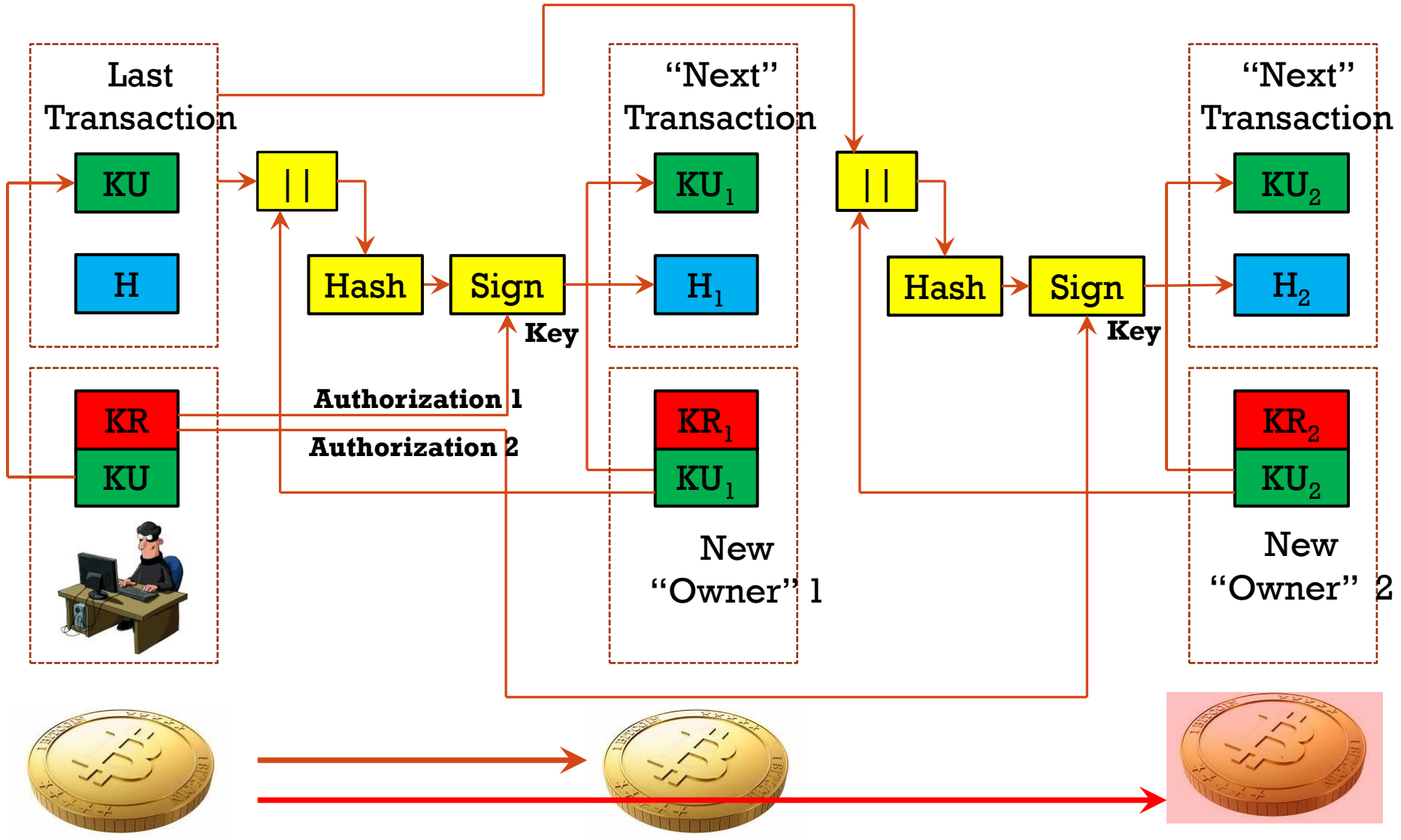
BITCOIN TRANSFER



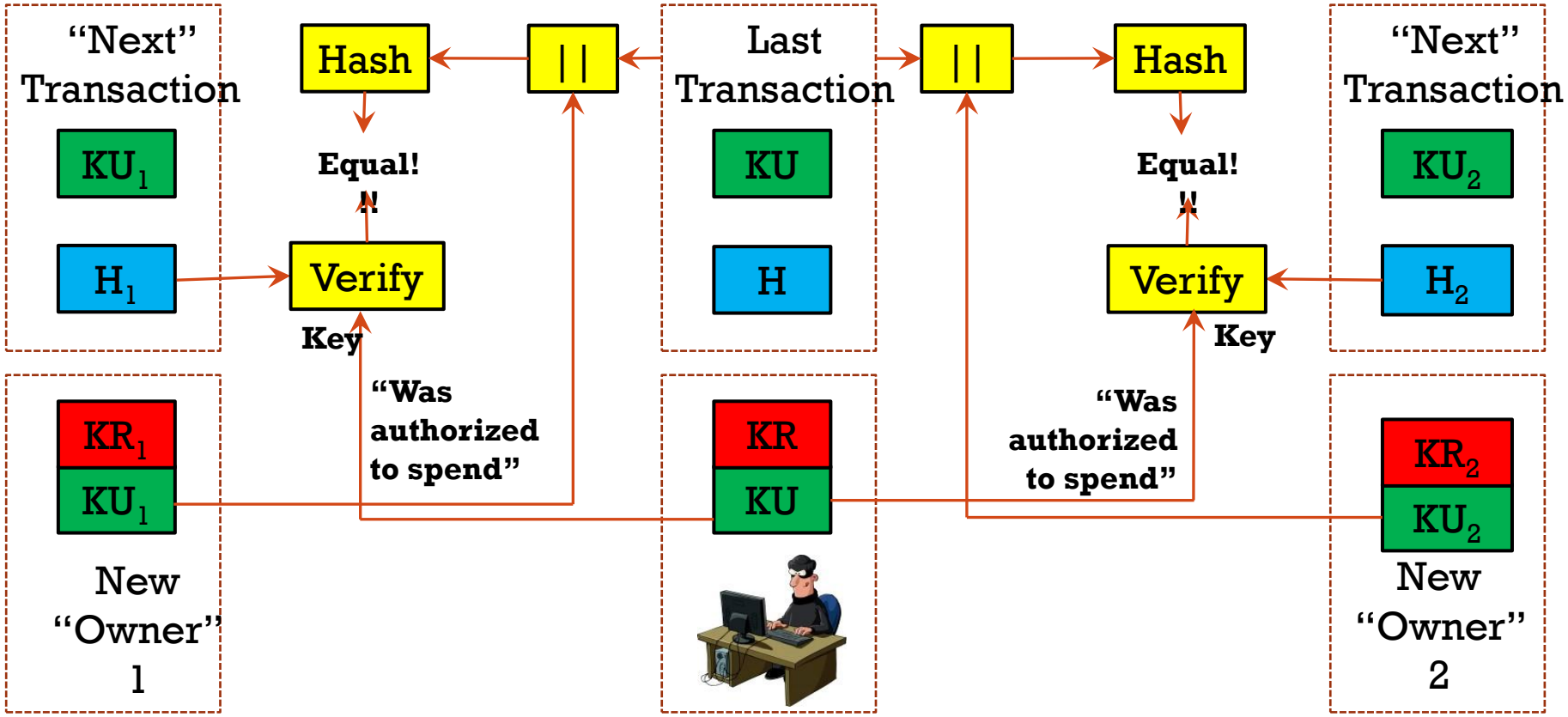
BITCOIN VERIFICATION



"DOUBLE SPENDING"



"DOUBLE SPENDING"



Both "owners" can also verify all earlier transactions in that bitcoin's history, and each believe they are its genuine owner. There is no mechanism to detect the previous owner's fraud.

THE "BLOCK CHAIN" AND BITCOIN MINING

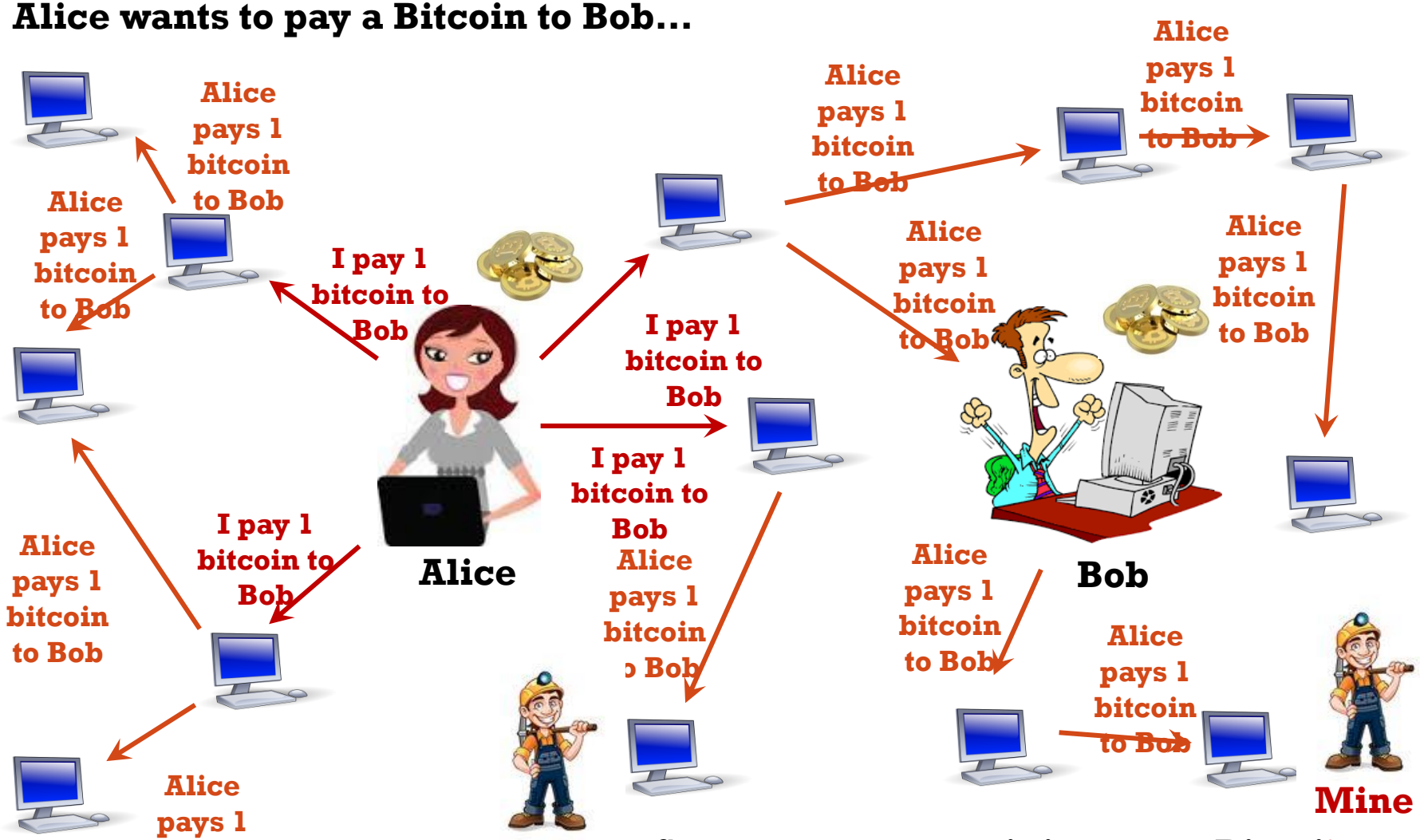
Part 4

THE PUBLIC LEDGER

- Record of all Bitcoin transactions.
- Must be kept up-to-date and agreed upon by all players.
- Receiver of a Bitcoin must be able to verify from the ledger:
  - That the payer genuinely owned the bitcoin with which he/she paid.
  - The payer did not use that same bitcoin to pay someone else.
- This "ledger" may be:
  - Held/maintained by a centralized authority.
    - Older solution. (Bank)
  - Maintained collectively by the entire community.
    - Newer solution implemented in Bitcoin algorithm.
  - The Bitcoin "ledger" is called the "Block Chain".
    - Maintained/updated by "Bitcoin Miners".

BITCOIN MINING

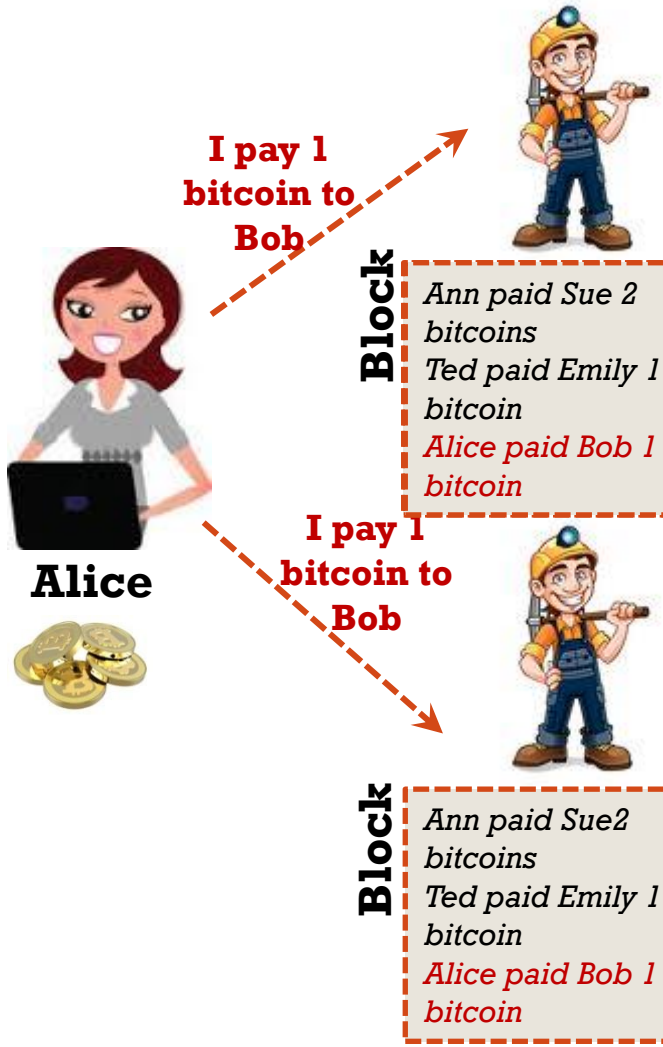
Alice wants to pay a Bitcoin to Bob…



Some message recipients are Bitcoin "Miners"…

BITCOIN MINING

The "Miners" add Alice's transaction to "blocks" which they are compiling…



Public Ledger ("Block Chain")

Bill paid Fred 4 bitcoins
Jim paid Jane 2 bitcoins
…
Blah blah….
…
Ann paid Sue 2 bitcoins
Ted paid Emily 1 bitcoin
Alice paid Bob 1 bitcoin

Miners "compete" to add their new block of records to the ledger!

BITCOIN MINING

Winner adds his block (including Alice's transaction) to the Public Le

"Winning" Miner

Gets prize of newly minted bitcoins!!!

Block

Ann paid Sue 2 bitcoins
Ted paid Emily 1 bitcoin
Alice paid Bob 1 bitcoin

Public Ledger ("Block Chain")

Bill paid Fred 4 bitcoins
Jim paid Jane 2 bitcoins
…
Blah blah….
…
Ann paid Sue 2 bitcoins
Ted paid Emily 1 bitcoin
Alice paid Bob 1 bitcoin

The is the only way in which new bitcoins are ever produced.

Block from winning miner is time-stamped and added to ledger

Analogous to digging gold!

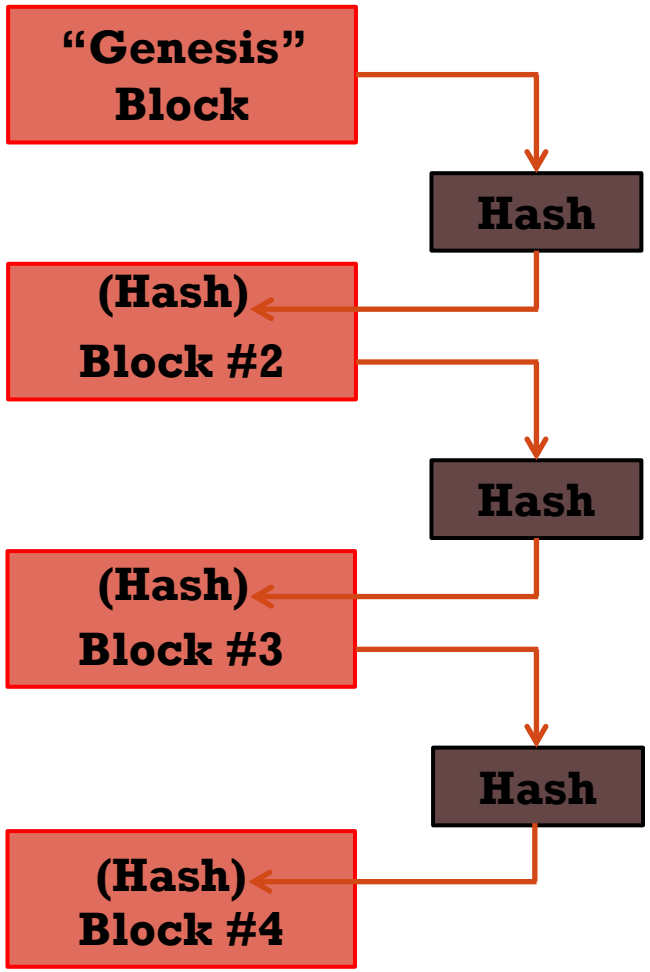
But…

- **Where is this "block chain" stored? (Remember, there is no central authority to hold it.)**
- **Who decides which miner "wins"?**

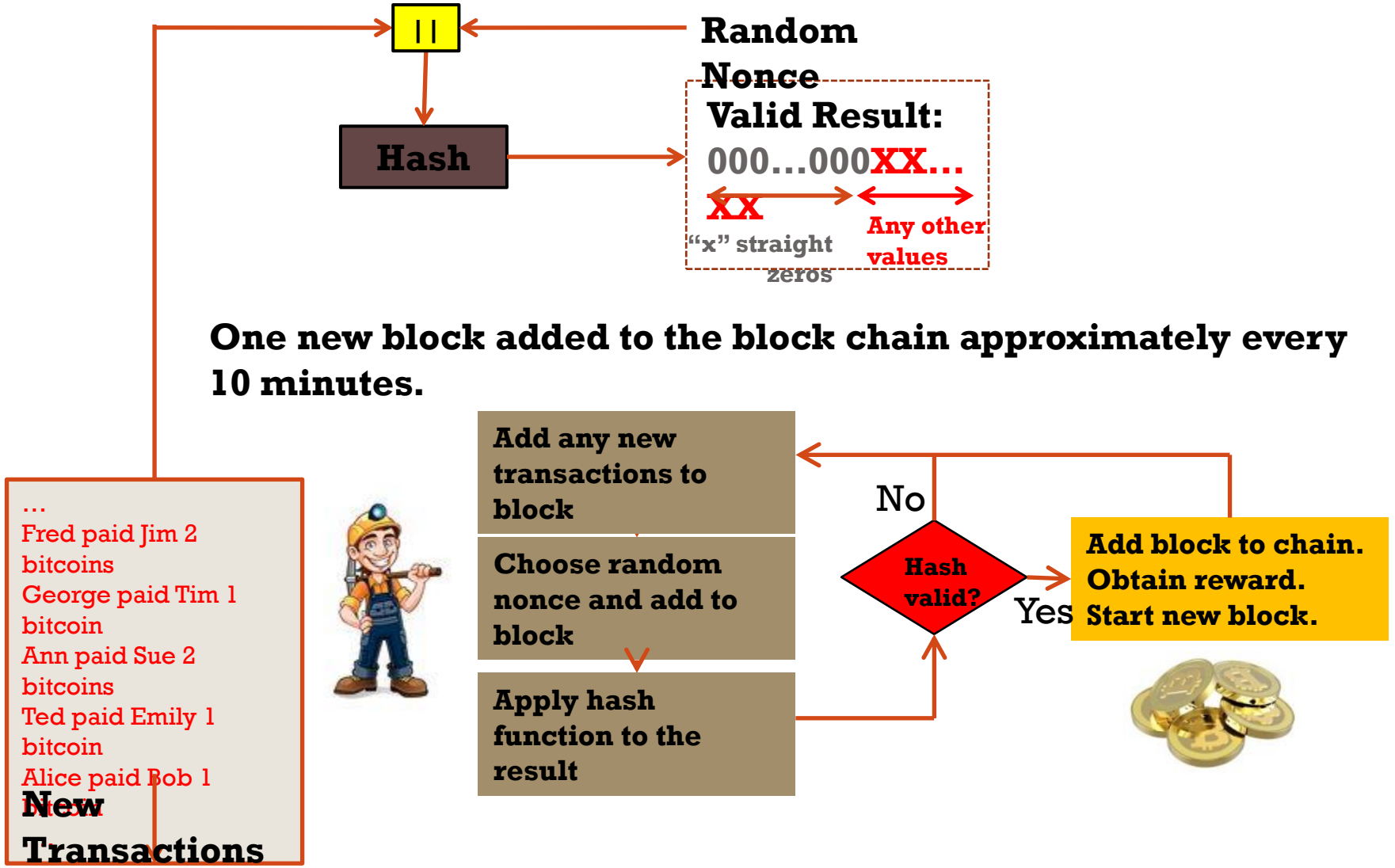
THE "BLOCK CHAIN"

Copy of the Block Chain is stored by all "Players" (participants in the Bitcoin network). Can take ages to download! 324GB

Each block contains a hash of its predecessor – anyone can verify no preceding block was modified!



MINING: THE POW PROBLEM



BITCOIN INFLATION

Part 5

CREATING SCARCITY…

- If Bitcoin mining goes on forever…
  - …the supply of bitcoins will steadily increase, and…
  - …the real value of each existing bitcoin will fall!
  - INFLATION!!
    - This is the usual result of the supply of money increasing faster than the quantity of goods available to be bought.
- Solution…
  - Implement a "law of diminishing returns"
  - Number of reward bitcoins programmed to half every time 210,000 bitcoins are mined.

- Eventually almost no new Bitcoins will be produced.
  - As if nearly all the gold in the world were mined
  - Rewards for mining more do not cover costs.
  - Former "miners" will need a new incentive to continue their work
- From then onwards, incentives will be provided in the form of "transaction fees" payable by users.

YOUTUBE VIDEO…

- US Philosopher Stefan Molyneux on Bitcoin…
  - https://www.youtube.com/watch?v=w4HGVJjqDVk
    - Note: I find Molyneaux's ideas interesting, but I disagree with most of them: please don't think that by recommending this video I'm advocating Molyneux's (or anyone else's) brand of anarcho-capitalism. I'm not!

SUMMARY

- Origins of Money
  - Debt, barter, gold
- Virtualization of Money
  - Fiat currency, bank accounts
- Cryptographic Concepts used in Bitcoin
  - Public key ciphers, hash functions and proof-of-work
- Bitcoin Transactions
  - Problem of "double spending"
- Recording Bitcoin Transactions
  - The "Block Chain"
- Bitcoin Mining
- Bitcoin Inflation

THANK YOU

Kavinga Yapa Abeywardena

Dept. CSE