BLOCK CHAIN BASICS

Peter Cochrane
cochrane.org.uk

معهد قطر لبحوث الحوسبة
Qatar Computing Research Institute

COCHRANE associates

University of Hertfordshire

BLOCK CHAIN

A very brief history

- BC is a distributed ledger
- 2009 saw the first manifestations
- No one knows the inventor/origins for sure
- Designs, protocols and code are open source
- Security agencies suspected to be on a similar tack
- Specialised Block Chains dedicated to just one task
- Generalised Block Chains will likely become a platform
- A next step in the logical progression toward decentralisation
- Inherently more secure than any previously realised transaction system
- Sidelines institutions and centralised control making all transactions simpler

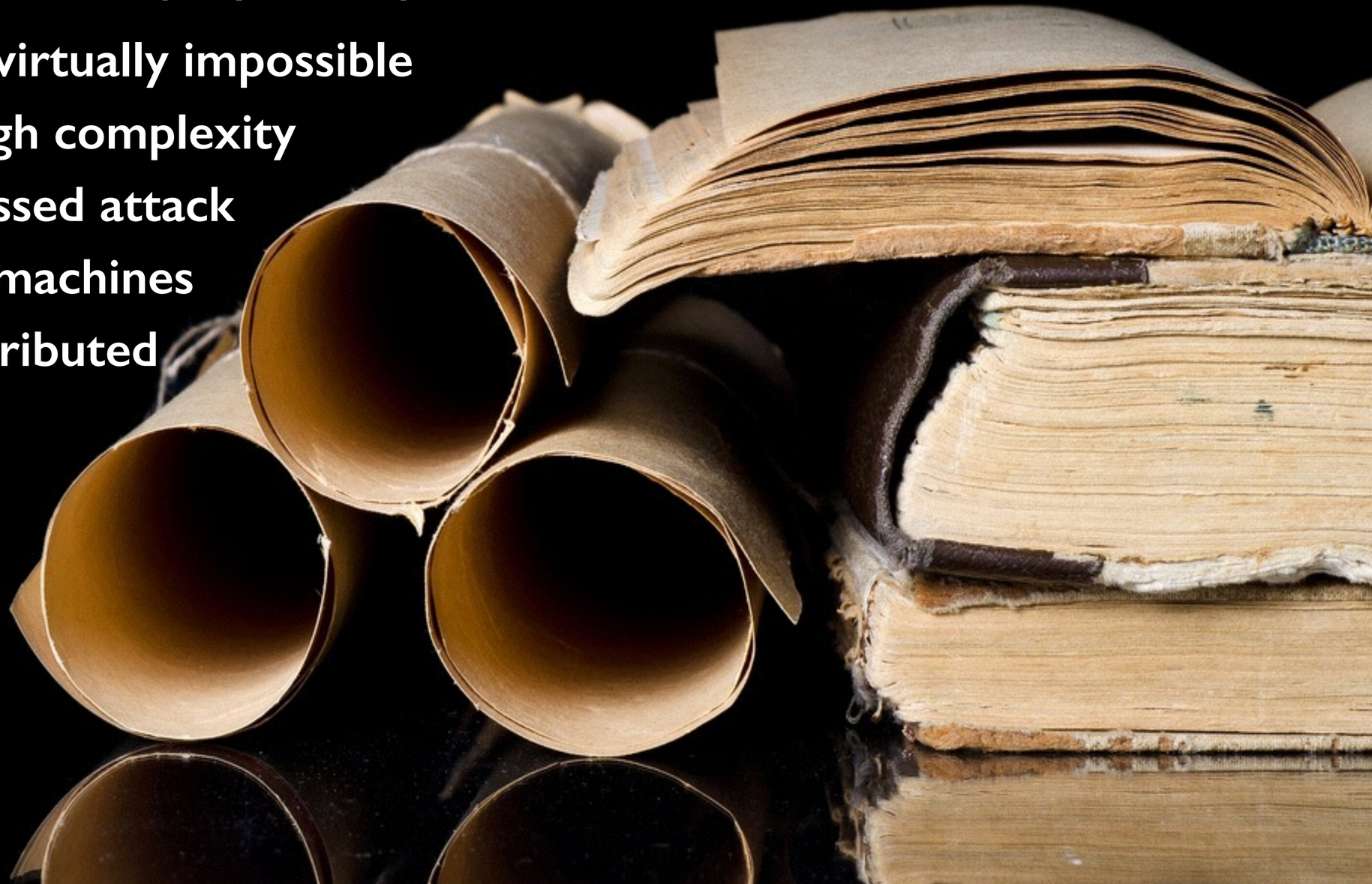
The technology to hack and crack Block Chains is not yet available

A DISTRIBUTED LEDGER

Digital, Encrypted, Highly Complex

- Distributed attack virtually impossible
- Obscuration through complexity
- Impervious to focussed attack
- Spread over many machines
- Geographically distributed
- Inherently secure
- Format variable
- Vastly scaleable
- Multiple forms
- Multi-key

Yet to be cracked!



NOT JUST CURRENCY

All forms of transaction and record

- Every variety of value exchange
- Legal documents of every form
- Property, Deeds ,Ownership
- Ultra secure communication
- Licences and permissions
- R&D, production detail
- Patents and copyright
- Multi-media vault
- Medical records
- Voting

++++++++

NO CENTRALISED CONTROL

Sans Institutions - Banks and Companies

- Beyond the reach of governments
- Confounding for regulators
- Available to everyone
- Multi-species
- Truly global

++++++++

- User driven
- Open or closed
- Public or private
- No external controls
- A universal application
- Freedom of use and application

++++++++

TECHNOLOGY FRIENDLY

Agnostic, adaptive & broadly applicable

- IoT
- Mobile
- Fixed
- Mobile
- Clouds
- Internet

- Big
- Vast
- Small

- Groups
- Military
- Personal
- Corporate
- Government

IMPLICATIONS

Expansive & confounding

- Greater and easier access to financial services and funds
- Openly available to be used by anyone for any purpose
- Greater security of records and personal information
- Improved book keeping and asset management
- The sidelining of established institutions
- Far easier access to global markets
- The potential to by-pass regulation
- An enabler of distributed teams
- Allows new business models
- Extremely disruptive

HOW DOES IT ALL WORK

Shrouded in complexity and jargon !

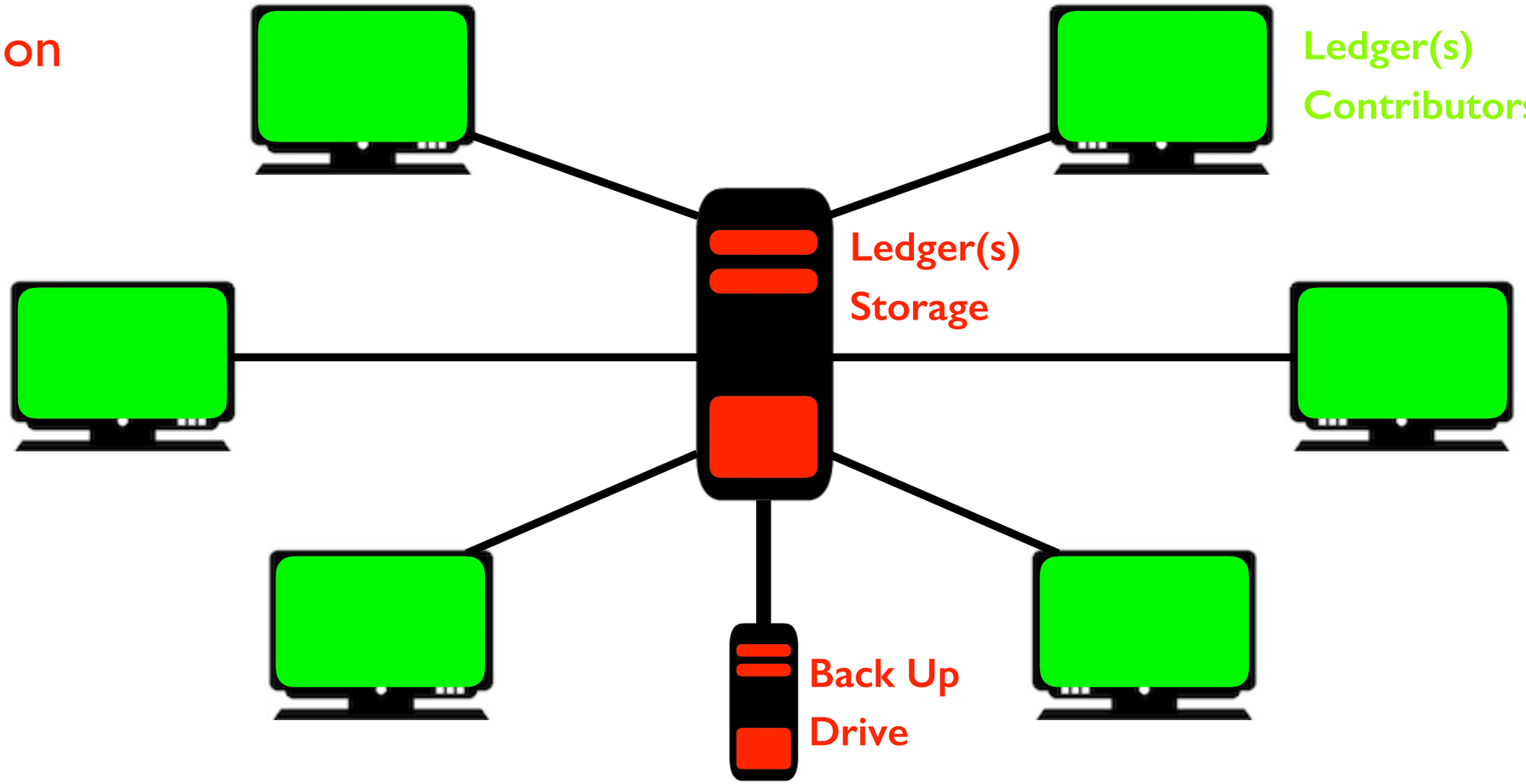
Demystification of the complex
is often very difficult,
but not in this case
if we address each
step one at a time

…each step is a known
process and not a giant leap !

CENTRALISED LEDGER

Step 1: *Dominant mode for decades*

Flow of information and operational control by one central point

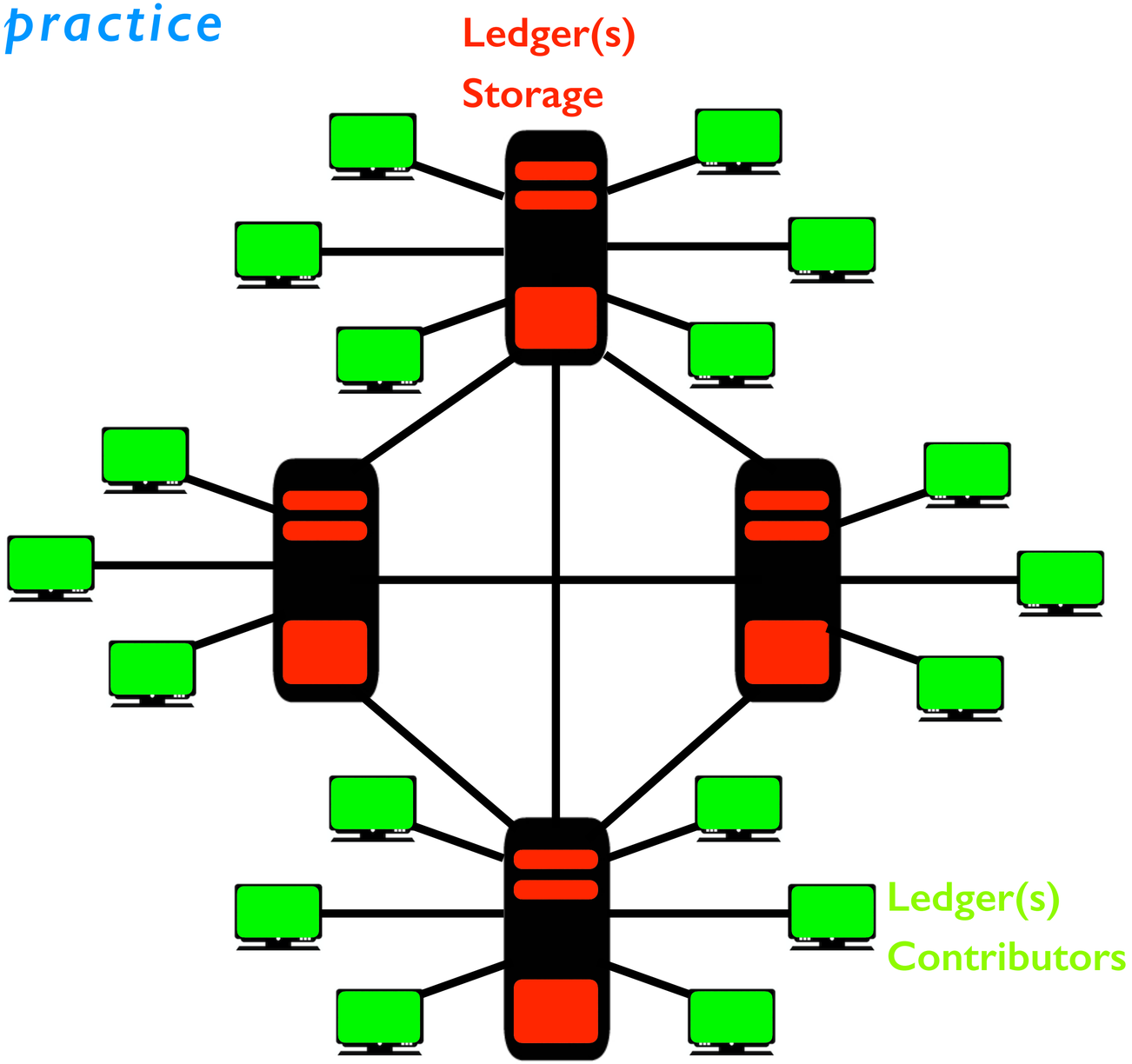


DISTRIBUTED LEDGER

Step 2: *Still very common practice*

Spreads computational and storage workload across multiple network nodes

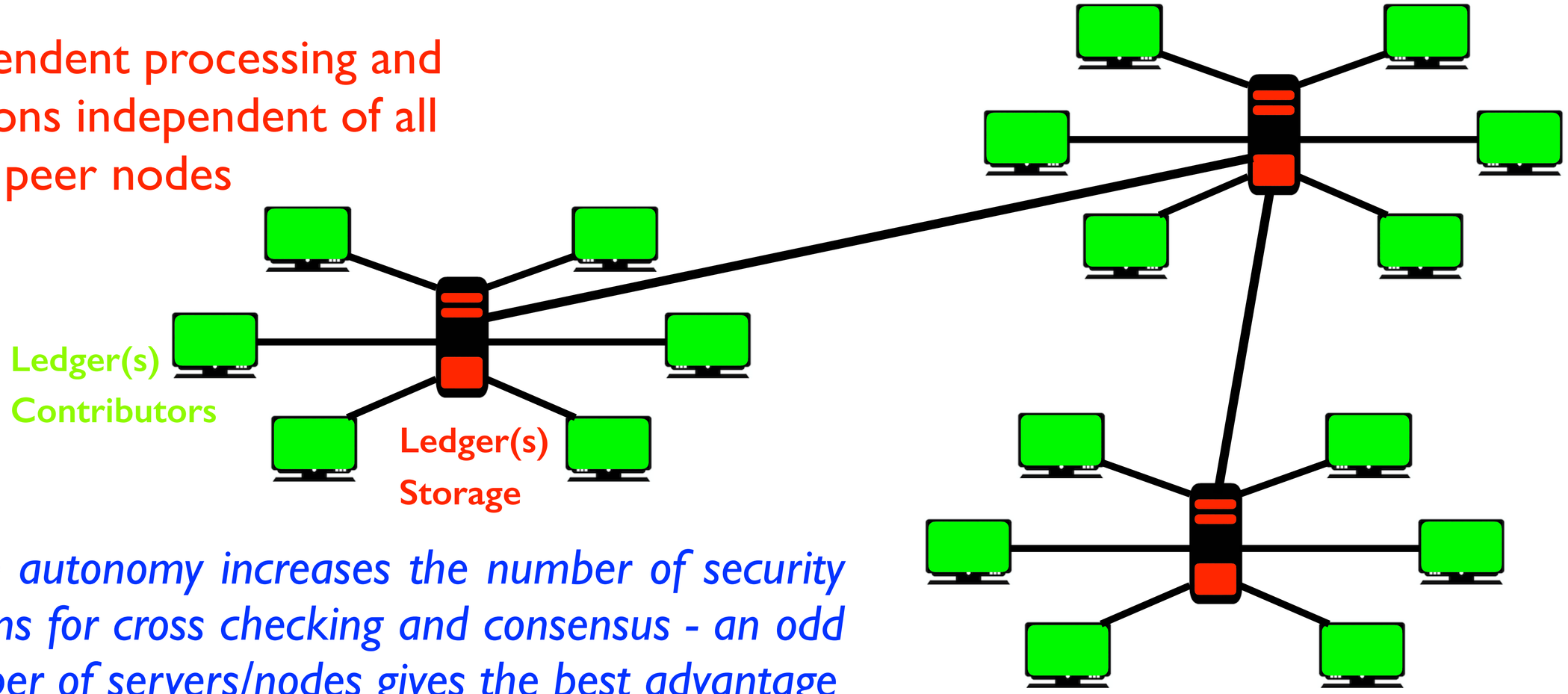
Generally employ 'mirror site' dependent decision to ensure distributed duplication and greater security and reliability



DISTRIBUTED LEDGER

Step 3: *Typical of 'evolved' systems*

Independent processing and decisions independent of all other peer nodes

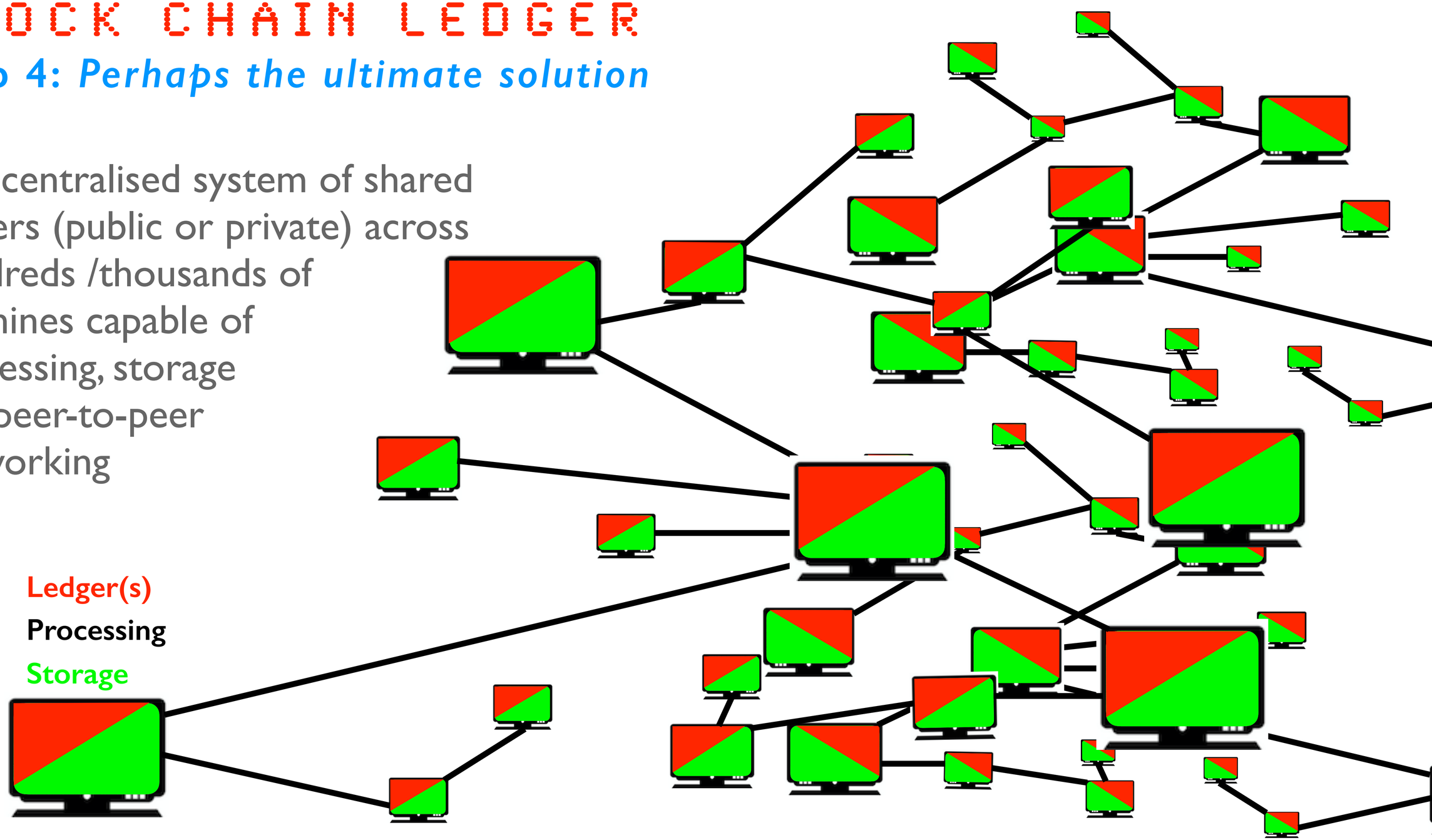


Node autonomy increases the number of security options for cross checking and consensus - an odd number of servers/nodes gives the best advantage

BLOCK CHAIN LEDGER

Step 4: *Perhaps the ultimate solution*

A decentralised system of shared ledgers (public or private) across hundreds /thousands of machines capable of processing, storage and peer-to-peer networking



BLOCK CHAIN LEDGER

Very briefly stated

- An immutable record of any form of transaction
- No middle man, institutions, government, regulator
- A highly scalable, decentralised peer-to-peer (P2P) network
- File integrity based on a consensus, rather than a trust-basis
- A ‘proof-of-work’ system model renders transactions irreversible
- Individuals or groups are unable to control the infrastructure or processes
- All participants (people and machines) are equal and use to the same protocols
- The system creates a chronological time stamp of all peer-to-peer transactions
- Encryption and hash value creation per file is followed by consensus before decode

BLOCK CHAIN LEDGER

Operation and securit

- All machines can cr… …edger file
- Any ledger c… …ore parties
- The l… …of the parti…
- … …p to aid la…
- … …ied' to cre…
- … …hen distrib…
- T… …ber, location and id… …e nidden
- The … identity is used to verify al… …d after recovery
- Any attempt to tamper with a file, now… …ll, will change the hash value
- Recovery and decode of a ledger involve… …check a consensus across many copies

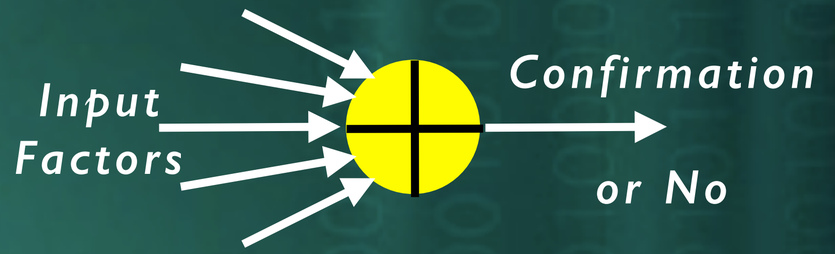
ALL MACHINES ARE EQUAL

HUH ??

Security is assured through encryption, distribution, hash, consensus and combinatorial complexity

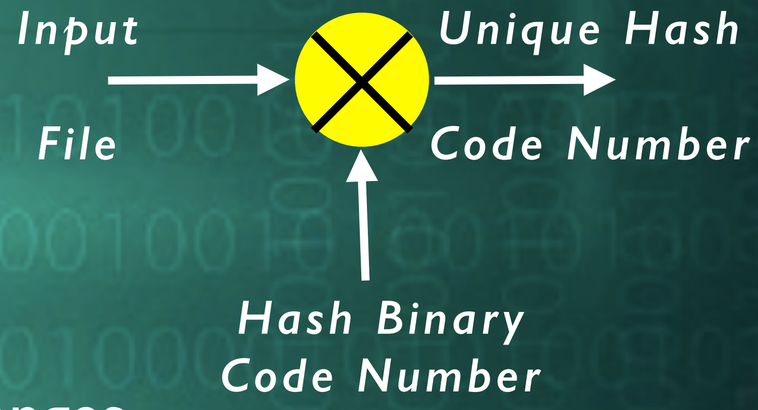
PROOF OF WORK & HASH

Simply put - proven algorithms



PROOF OF WORK - *Boiled Down*

Was a message sent ?
Was a transaction completed ?
Was everything acknowledged ?
Was everything checked and tested positive ?



HASH FUNCTION - *Boiled Down*

A simple mathematical operation
Uses a known seed/code binary number
This is multiplied by a binary file to be protected
A unique binary number is generated to reveal smallest of changes
Answers the question: is this the correct file or has it been tampered with ?

BLOCK CHAIN LEDGER

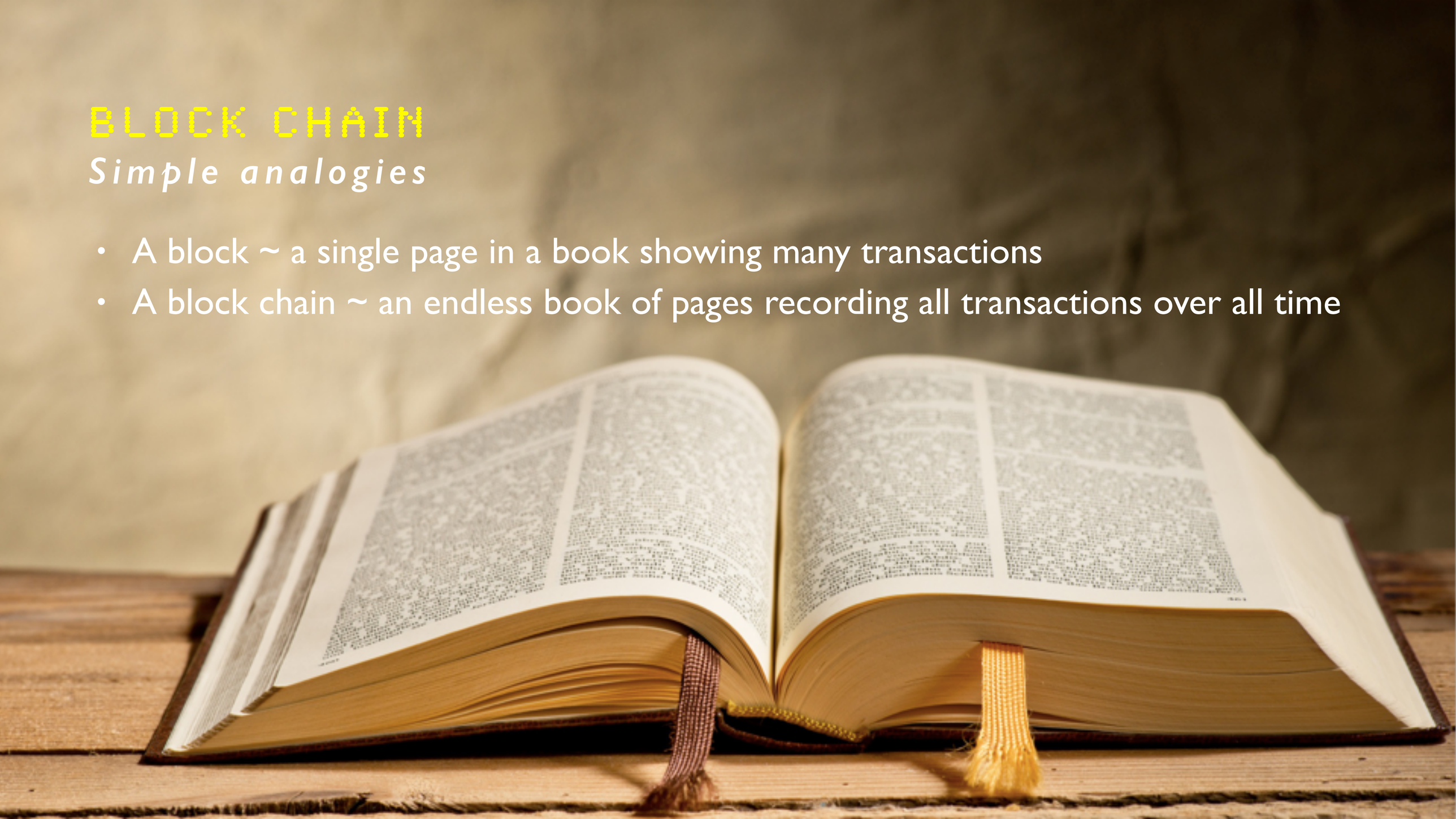
Security by option choices

- Machine types, system software and apps
- Fixed and mobile device choice uncertainty
- Encryption type, algorithm and choice of seed
- The choice of hash type, value and depth of application
- Public or private key, mode of communication, encryptions
- Chronological time stamp of file creation and network actions
- Variation in machines allocated to create files, process and store
- Random (or otherwise) rotation of machines used to perform consensus
- Hash word identity used to verify all copies before storage and after recovery
- Positioning and order of hashed files in an accumulated ‘chain’ of stored ledgers
- Recovery of a ledger involves a hash check and consensus across numerous copies

BLOCK CHAIN

Simple analogies

- A block ~ a single page in a book showing many transactions
- A block chain ~ an endless book of pages recording all transactions over all time



PROCESS WALK THROUGH

For only one simple set of choices

User 1 requests a transaction

Peer computers analyse past blockchain transactions with verification through proof of work and/or P2P consensus

Assets are exchanged

The entire transaction is recorded in the distributed ledger across many machines

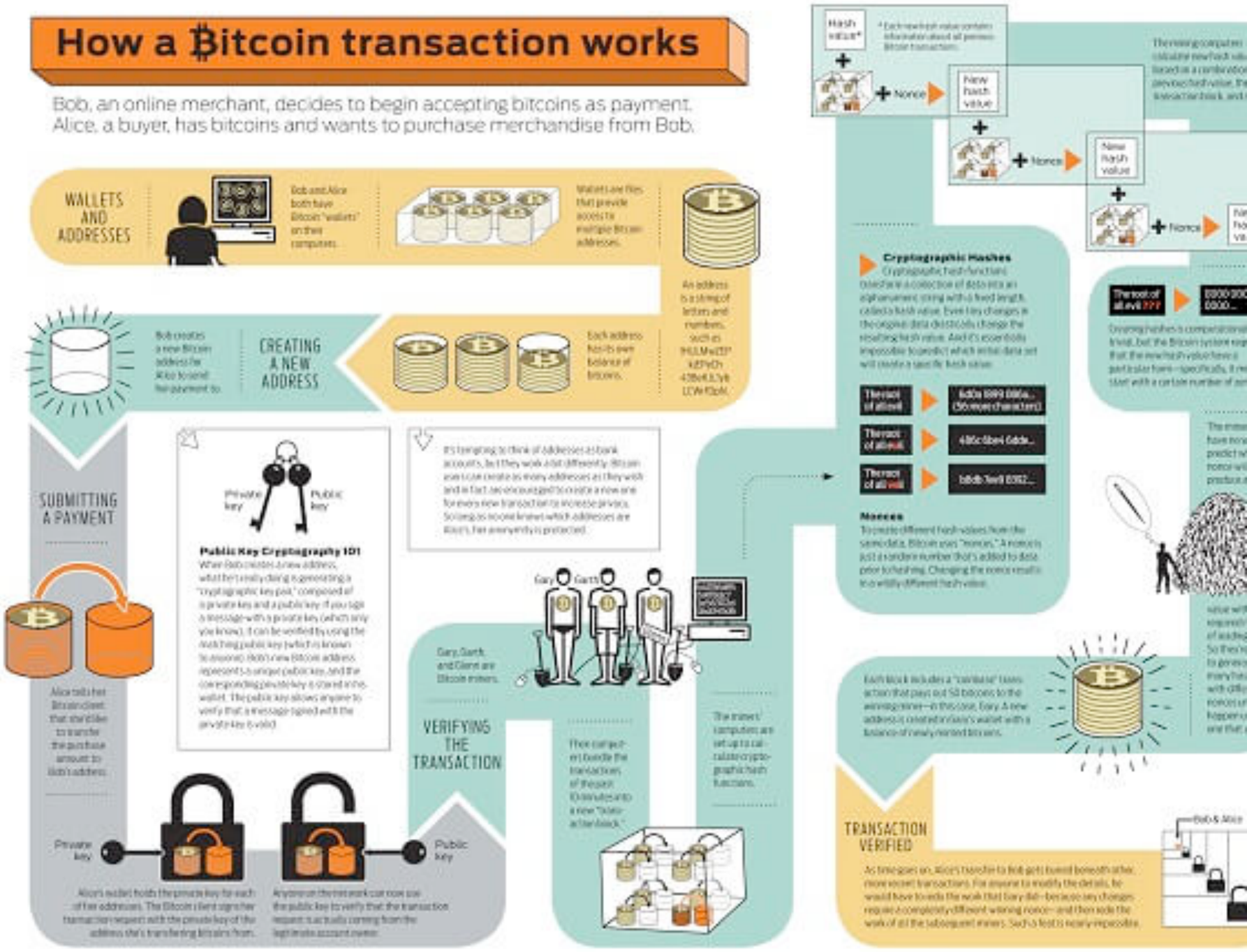
User 2 receives materials

MUCH MORE

Search the WEB

Beyond this slide set outlining the use and operating basics you will find numerous articles, movies and slide sets dealing with specific cases and implementations available on line

The depiction opposite is just one example of very many




Thank You
ca-global.org
cochrane.org.uk
معهد قطر لبحوث الحوسبة
Qatar Computing Research Institute
COCHRANE
associates
University of Hertfordshire
UH