An introduction to blockchains

The Royal Academy of Engineering funded a Visiting Professorship in Practical Cybersecurity Insights at Northumbria University, 2019–2022. These slides are a slightly modified version of those delivered, intended to be available after the project has ended

Web `https://green-pike.co.uk/nvp`
Email p.brooke@northumbria.ac.uk (until it stops working. . .)
phil@green-pike.co.uk

If someone mentions “blockchain” we often think of the public, decentralised Bitcoin or Ethereum cryptocurrencies

Blockchains have more variety

- private or public
- inclusion of smart contracts
- different application areas, *e.g.*, non-repudiation of agreements

A blockchain

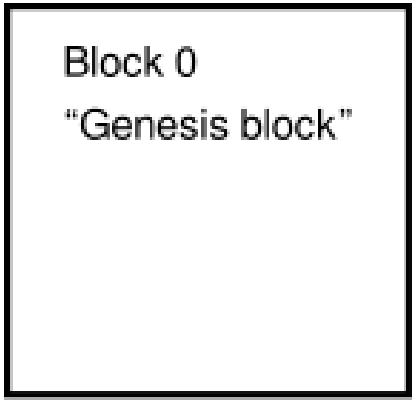
Blockchain

A series of blocks, each block cryptographically linked to the previous block, all the way back to the "genesis" block
Each block can be validated
Makes the blockchain "append-only"

A blockchain

Blockchain

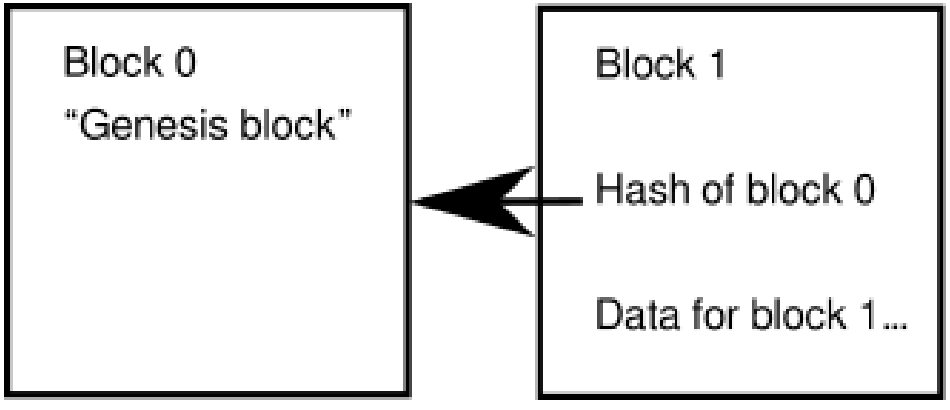
A series of blocks, each block cryptographically linked to the previous block, all the way back to the "genesis" block
Each block can be validated
Makes the blockchain "append-only"



A blockchain

Blockchain

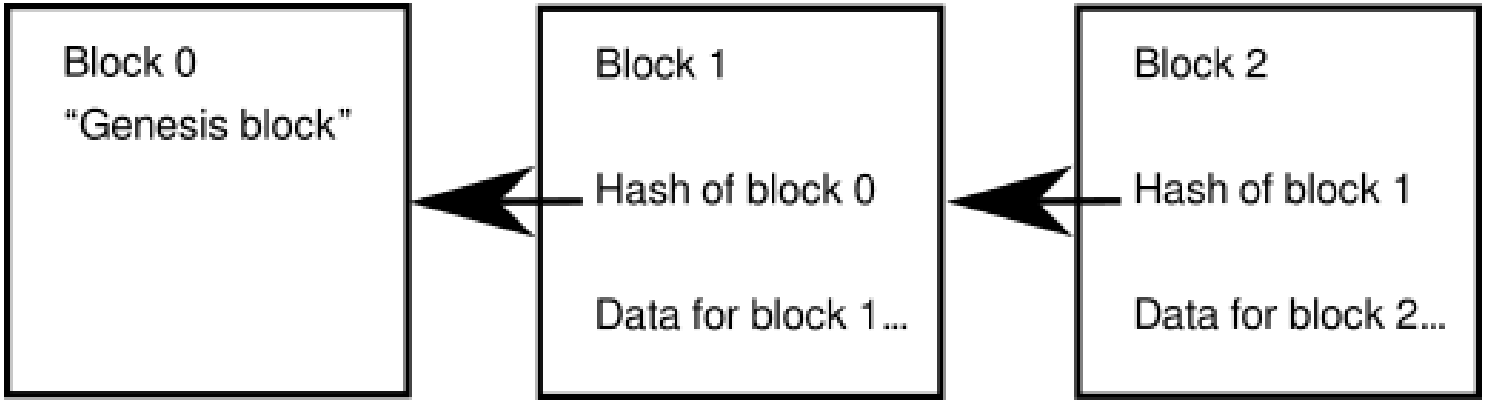
A series of blocks, each block cryptographically linked to the previous block, all the way back to the "genesis" block
Each block can be validated
Makes the blockchain "append-only"



A blockchain

Blockchain

A series of blocks, each block cryptographically linked to the previous block, all the way back to the "genesis" block
Each block can be validated
Makes the blockchain "append-only"



Modification

To modify any block other than the last should be visible to any validator

Example: `https://blockchaindemo.io/`

Classification of blockchains

Public decentralised, "permissionless", usually requires proof of work or proof of stake

Private non-transparent, "permissioned"

Hybrid *e.g.*, federations of organisations, consortiums

"Distributed ledger technology" (DLT) — sometimes applied to all blockchains, sometimes only for private or some hybrid blockchains

A simple blockchain using PGP

OpenPGP

Pretty Good Privacy (PGP) originated in 1991. It is standardised as OpenPGP (RFC4880) and the major open source implementation nowadays is Gnu Privacy Guard (GnuPG)
OpenPGP supports symmetric and asymmetric encryption

PGP Stamper `https://www.itconsult.co.uk/stamper.htm` is a service that automatically signs messages sent to it to provide proof of when a document was signed
Why do I call this a blockchain? "Stamper also stamps summaries of its own signatures from the previous day" as well as publishing the serial numbers and signatures
It has some characteristics of public and private blockchains

Currencies and cryptocurrencies

Currency

The UK, uses "Pound Sterling" aka British Pound (GBP)
Issued by the Bank of England (and others)

Virtual currencies...

...are unregulated and unguaranteed but may be exchanged for currency

Cryptocurrencies...

...are stored in digital ledgers, unregulated and unguaranteed, but may be accepted/converted by others, *e.g.*, Tesla (link)

Cryptocurrency

Lansky (2018) (link) specifies the following characteristics:

1. The system does not require a central authority, distributed achieve consensus on its state.
2. The system keeps an overview of cryptocurrency units and their ownership.
3. The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.

Cryptocurrency

4. Ownership of cryptocurrency units can be proved exclusively cryptographically.
5. The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
6. If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

Bitcoin uses a blockchain to achieve the properties of a cryptocurrency

Mining and energy consumption

Bitcoin and others "mine" by carrying out computationally expensive processes to append the next block to the chain — a "proof of work". If they "win" they earn some Bitcoin themselves — the incentive to mine

A major problem us the cost of mining and the associated energy consumption

It also has an impact on hardware, *e.g.*, cost/availability of GPUs! Ethereum value and GPU prices are roughly correlated recently...

Alternatives to mining / proof of work

- "Proof of stake" — proposed for Ethereum
  See `https://www.bloomberg.com/news/articles/2021-08-14/bye-bye-miners-how-ethereum-s-big-change-will-work-quicktake` and `https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/`
- Hyperledger Besu uses "Clique Proof of Authority"
  `https://eips.ethereum.org/EIPS/eip-225`

More generally, these are known as *consensus mechanisms*

Other issues with blockchains

- 51% attack — public blockchains
- Lack of transparency — private blockchains
- Forking
- Theft/fraud
- Privacy — bitcoin wallets are pseudonymous
- Embedded transactions
- Quantum attacks — depending on choice of algorithm(s)

Further reading/work

- Proof of work
- Proof of stake
- Geth https://geth.ethereum.org/
- Hyperledger Besu https://besu.hyperledger.org/en/stable/
- Proof of authority consensus protocols?
- Smart contracts
- OpenPGP

The end (of the slides)

Web	`https://green-pike.co.uk/nvp`
Email	p.brooke@northumbria.ac.uk (until it stops working. . .)
	phil@green-pike.co.uk