www.chainfrog.com

chainfrog

INTRODUCTION

Find us at www.chainfrog.com

www.chainfrog.com

chainfrog

WHO ARE WE?

- Finnish blockchain software company
- Offering consultancy, workshops, project collaboration, product development
- 4 patents pending
- Demo software at https://wherecoin.com:555
- We know blockchains

Find us at www.chainfrog.com

Kiitos!

- Many thanks to:

  Tampere University of Technology

  Department of Pervasive Computing

  - Professor Jarmo Harju
  - Professor Kari Systä
  - Professor Tommi Mikkonen

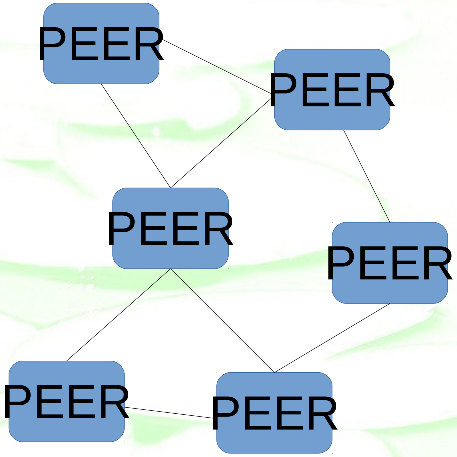
What is a Blockchain?

Simple answer: A DATABASE

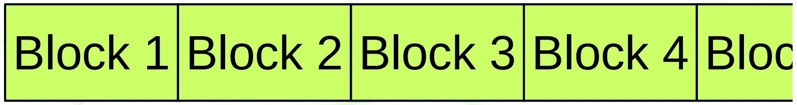
What is a Blockchain?

More complicated answer:

1: A peer-to-peer network



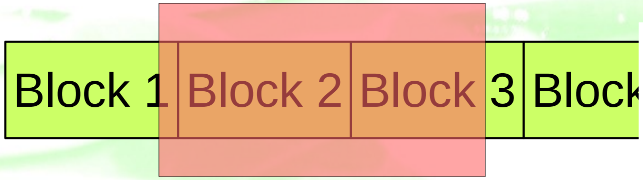
2: A blockchain file



3: An agreed set of protocols

```
sha256(sha256(block)) < difficulty
```

4: A blockchain parser



History Lesson

1960s: IBM introduces hierarchical databases (moonshot).

1970: Edgar Frank Codd, working at IBM, publishes the Relational Database Model. IBM sticks with the hierarchical model (RDBM too slow...).

1979: Oracle releases the first commercial RDMS. SQL starts to become popular. Oracle becomes rich.

2008: Nakamoto publishes “Bitcoin: A Peer-to-Peer Electronic Cash System”

2016: Most databases are RDMS. Oracle, MySQL, Microsoft SQL Server, PostgreSQL and IBM DB2 are the most popular implementations.

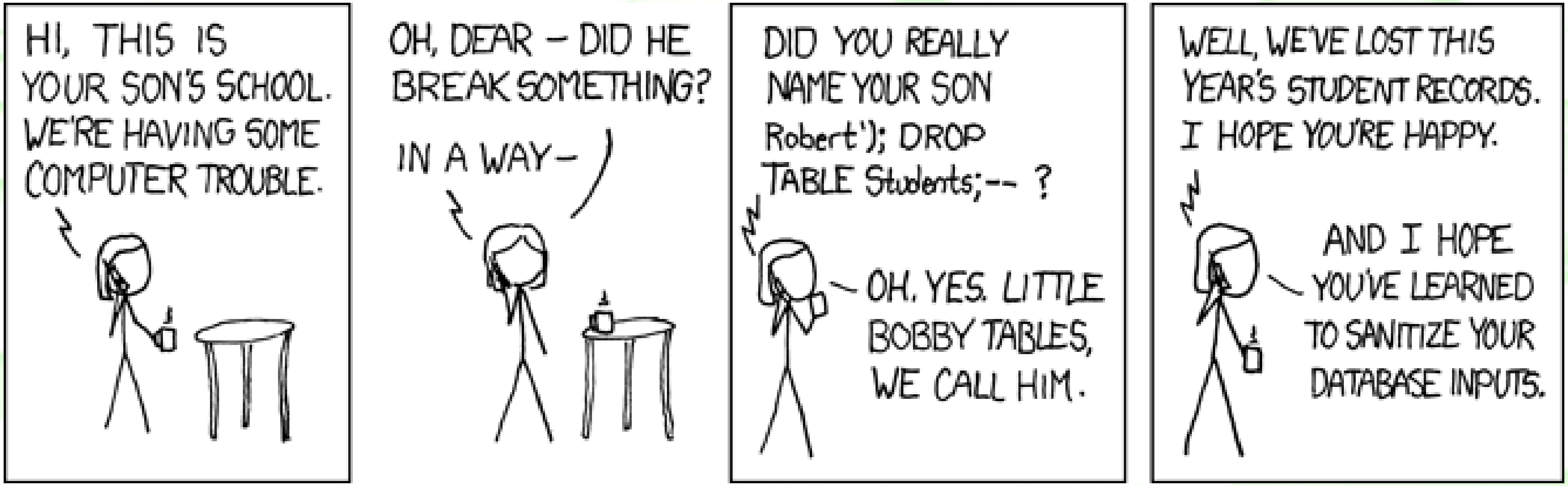
History Lesson

In the early 80s there were cases where a computer database salesperson would approach a company to encourage them to purchase and install one, only to be told:

“I have a perfectly good filing cabinet and secretary. Why do I need a database?”

Relational Database Weaknesses

- Records can be altered without a trace if incorrectly configured, or by a skilled administrator.
- Centralized by design, relying on client/server model.
- Problems with backups, synchronization across multiple database centers, concurrent record editing, and so on.


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

(Credit: http://xkcd.com)

See also: people with the surname Null

What is a Blockchain?

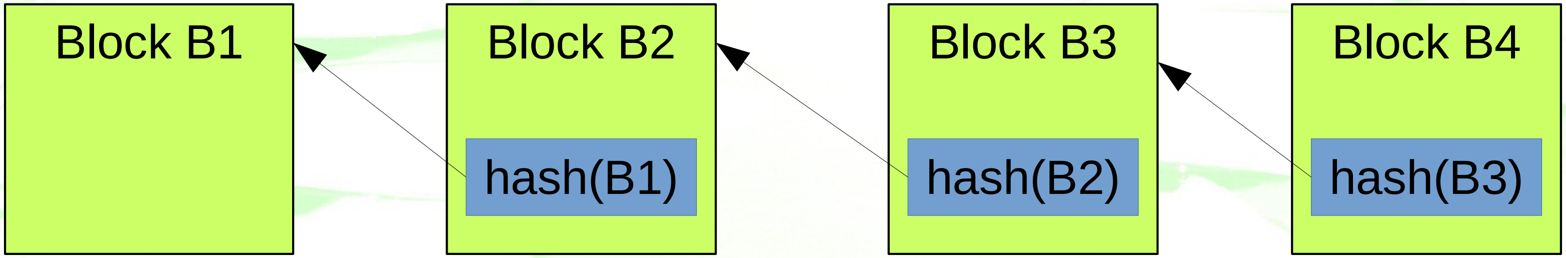
- A method of storing data in a sequential chain of blocks.

- Each block is a package of data created within a short consecutive window of time.

- A block has its own “hash”, based on the data it contains, which is like a fingerprint that uniquely identifies it.

What is a Blockchain?

- Each block (except the first “genesis block”) contains a reference to the block before it using the previous block’s hash, thereby forming a chain.



- The earlier blocks in the chain cannot be tampered with, because changing a block changes its hash, and this would break the chain of references.

How are Blocks Added to a Blockchain?

- Some of the devices on a peer-to-peer network regularly transmit data onto the network, to be included in the next block.

- Other devices receive and package the data into their own proposed block and then hold a lottery (consensus system) to see which device was lucky enough to create the block to be included.

- They do this because there is a reward for creating the next new block, or because they are run by entities who value the availability of the blockchain.

How are Blocks Added to a Blockchain?

- The lottery odds are adjusted occasionally to ensure that new blocks are accepted at roughly the same regular interval, for example every ten minutes or so.

- The most popular lottery methods are called:

  - “proof-of-work” (used by Bitcoin)
  - “proof-of-stake” (proposed for Ethereum)
  - “practical Byzantine fault tolerance” (Hyperledger Fabric)
  - “proof of elapsed time” (Hyperledger Sawtooth Lake)

Types of Blockchain

Type	Description	Example Use
Public	The blockchain is available freely on the internet. Software is generally open source or freely downloadable. Protocol specifics are usually published.	· Bitcoin · Public parking billing system · Global share trading platform · “Passport” system · Review/reputation system
Permissioned	The blockchain is accessed on the internet, but software is usually proprietary, and access is through keys issued by an authority.	· Asset tracking by consortium of shipping companies · Smart meters run by power company with multiple billing/admin companies · Location based game
Private	The blockchain is only available on an intranet/VPN, and access is through keys issued by an authority	· In-house notarizing of invention disclosures by R&D department · HR permanent records · Legal compliance records

Blockchain or RDM Database?

	Blockchain	Database
Integrity of data records	Records on the chain cannot be altered without an impossibly large amount of computing power	Records can be deleted or altered, and if logs are edited the changes cannot be detected
Audit trail	All actions are visible on the blockchain (although individual data within records may be encrypted)	Only administrators of the central system can view actions taken, and even then the logs may have been invisibly altered
Location	Stored in a distributed system across many (low powered) machines	Stored on a high power central server (possibly with secondary backup servers)

Blockchain or RDM Database?

	Blockchain	Database
Speed	Records can take minutes to be added to the system. Future systems may make millisecond blocks feasible.	Records are added in milliseconds
Partici-pants	A network of peers	A central authority granting or denying access to clients
Trust	Arises naturally between participants due to the actions required to add records and the rewards obtained for doing so	At a subjective level based on the perceived reliability of the database owner. Relies on a company’s reputation

Blockchain or RDM Database?

	Blockchain	Database
History	First emerged in 2009, new technology that is still evolving and developing. Need improvements in ease of use and ability to integrate.	Relational databases were proposed in 1970, and have been developed extensively ever since
Cost	Require custom development or integration.	Free high quality databases are available, but commercial ones for niche purposes can be expensive to use (eg SAP)

Blockchain or RDM Database?

	Blockchain	Database
Hardware	Easily scalable by adding new peers. Initial networks can be launched with cheap low power devices, and extended on an ad-hoc basis as more devices join	Cheap for simple low-user applications, expensive servers and support staff required for large user bases
Charging model	Folded-in due to cryptocurrency history	Requires integration and customisation
Collaboration	Emerges naturally from intrinsic design	Requires extensive access rights configuration, and is vulnerable to hacking