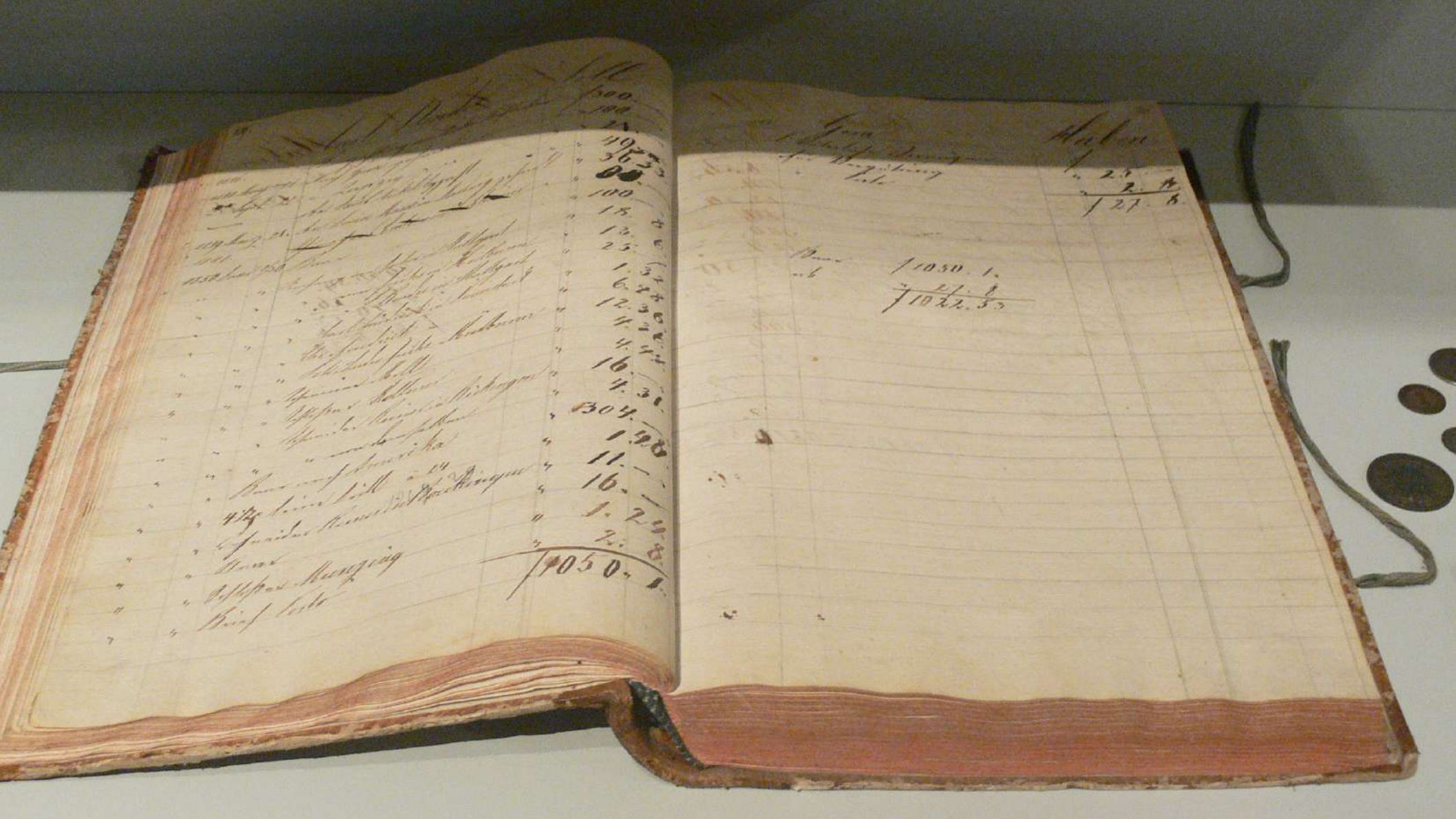
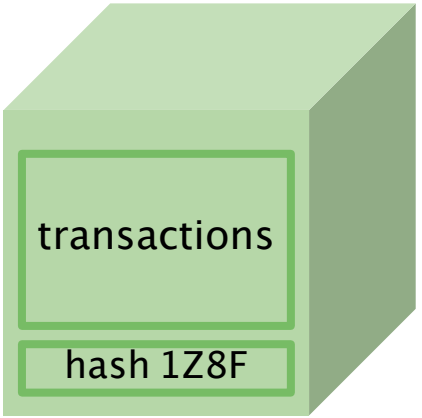
A BLOCKCHAIN IDENTITY

COMPUTER AID INTERNATIONAL
Keith Sonnet, CEO

Supported by Netriver

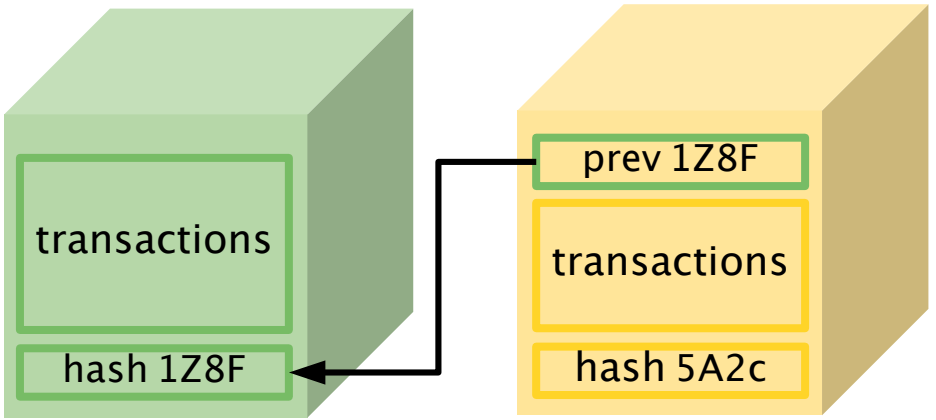


BLOCKCHAIN SIMPLIFIED



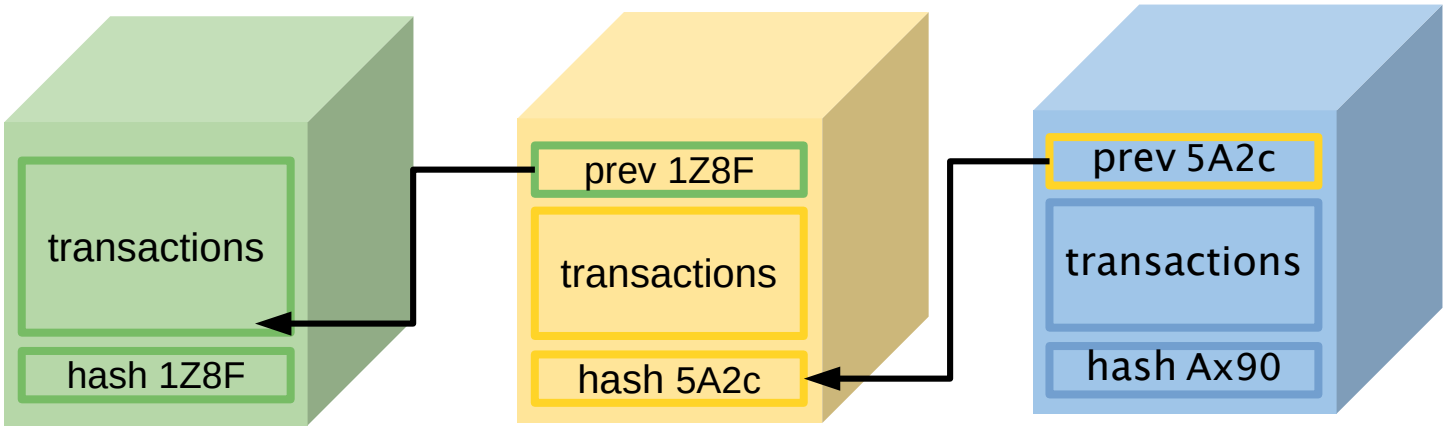
- First block is genesis block
- Contains:
  - **transactions**
  - **hash** of block data

BLOCKCHAIN SIMPLIFIED



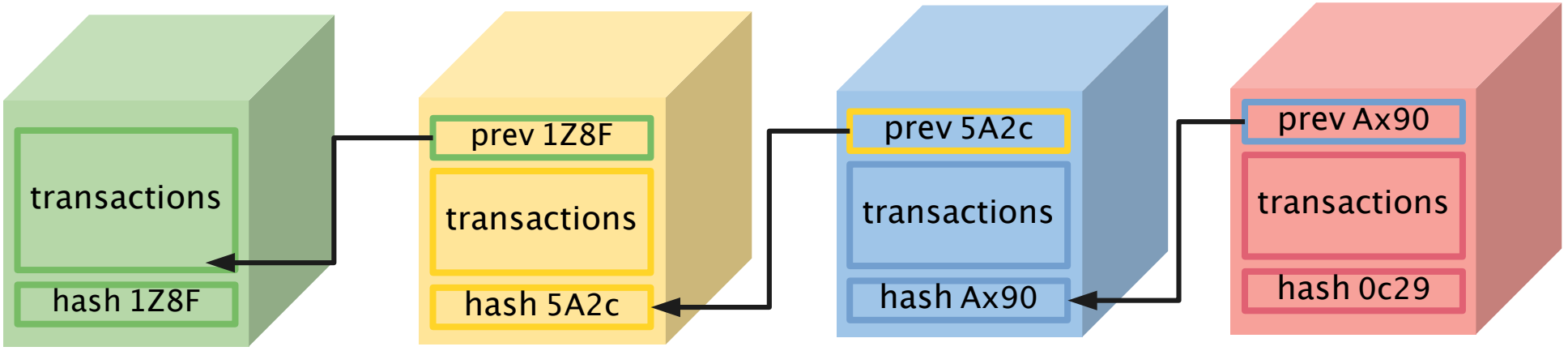
- Second block references first block
- Contains:
  - **previous block's hash**
  - **transactions**
  - **hash** of block data

BLOCKCHAIN SIMPLIFIED



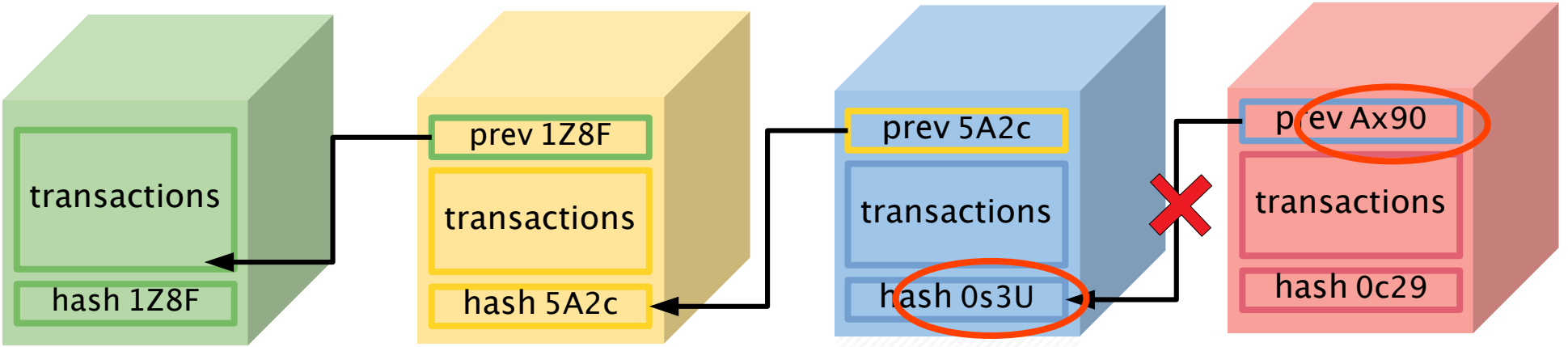
- Third block references second block
- Contains:
  - previous block's **hash**
  - **transactions**
  - **hash** of block data

BLOCKCHAIN SIMPLIFIED



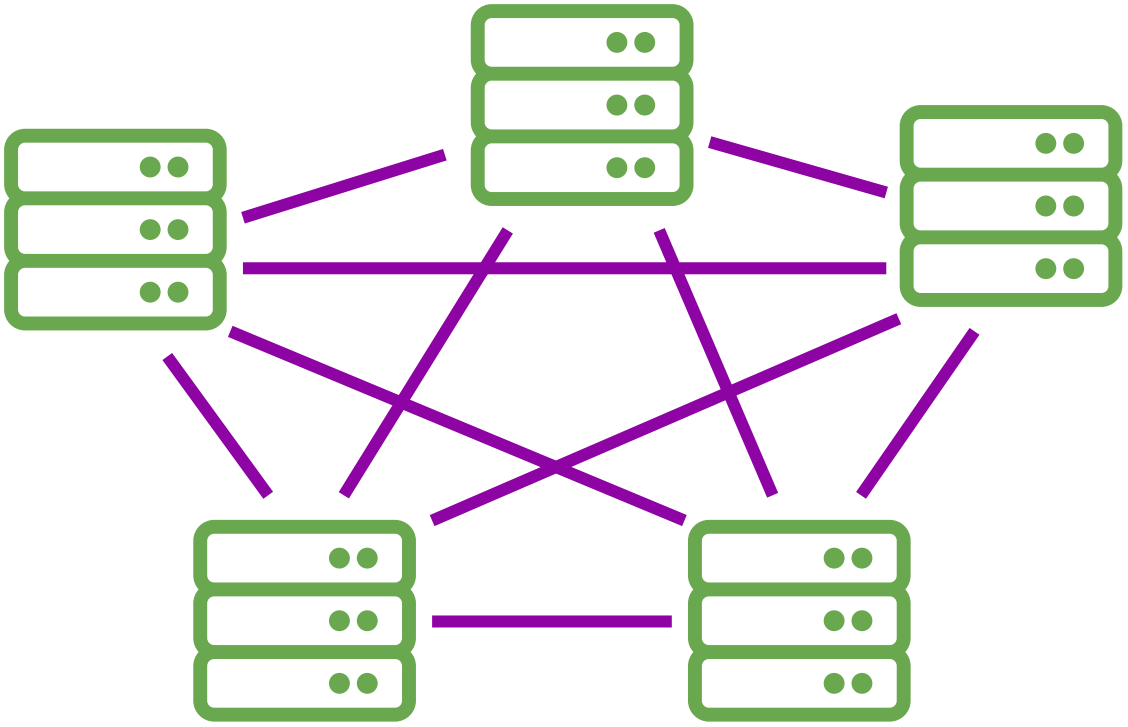
- Fourth block references third block
- Contains:
  - previous block's **hash**
  - **transactions**
  - **hash** of block data

BLOCKCHAIN SIMPLIFIED



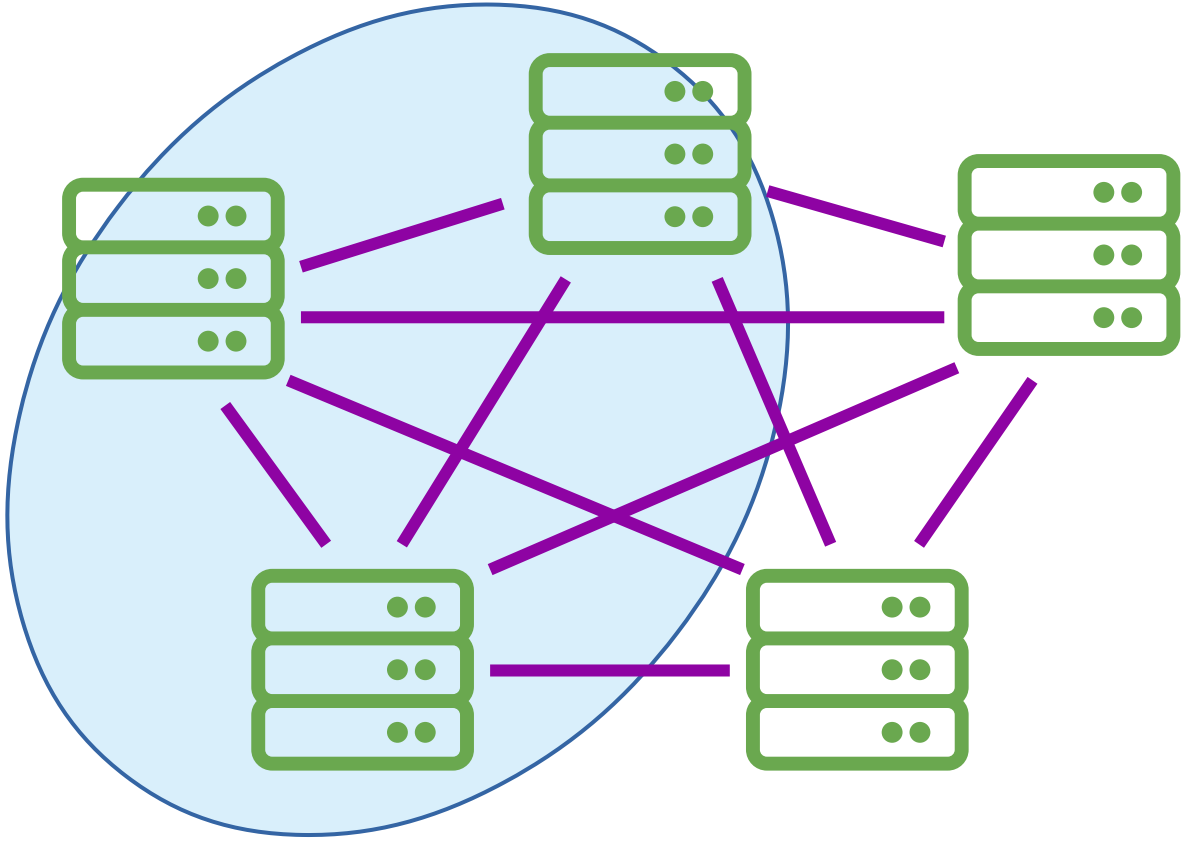
- An attempt is made to change 3rd block
- The change in data changes the block's hash
- The fourth block's previous hash no longer matches
- The chain is therefore broken

DECENTRALISED LEDGER TECHNOLOGY



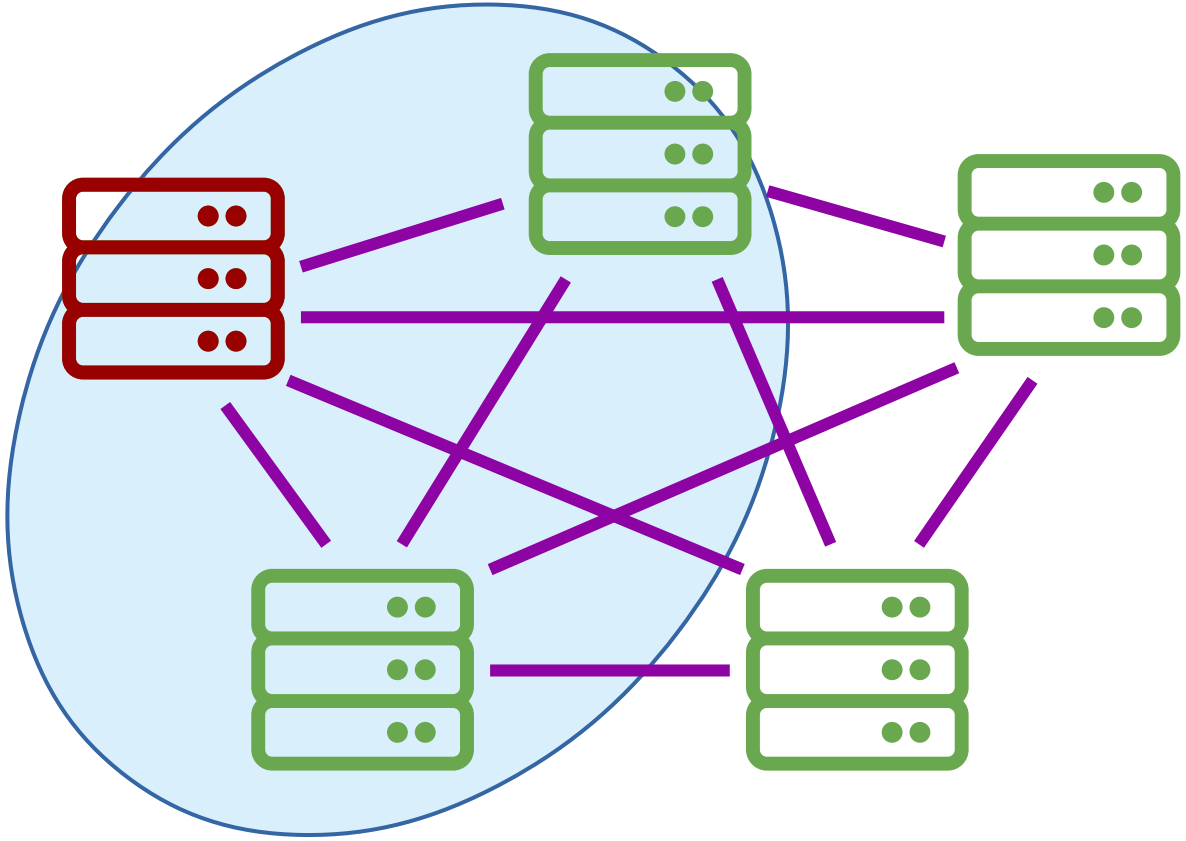
- Peer to peer computing creates a decentralised ledger
- Transactions are verified by each peer to gain consensus
- Introducing an invalid transaction is extremely hard due to consensus

DECENTRALISED LEDGER TECHNOLOGY



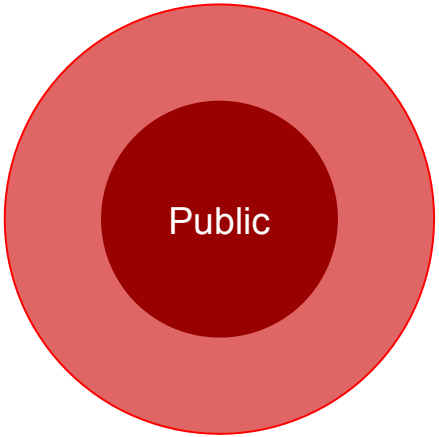
- Peer to peer computing creates a decentralised ledger
- Transactions are verified by each peer to gain consensus
- Introducing an invalid transaction is extremely hard due to consensus

DECENTRALISED LEDGER TECHNOLOGY



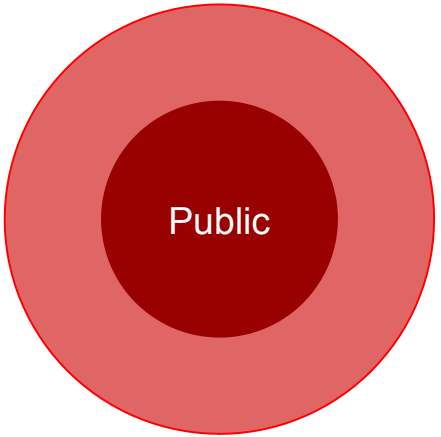
- Peer to peer computing creates a decentralised ledger
- Transactions are verified by each peer to gain consensus
- Introducing an invalid transaction is extremely hard due to consensus

TYPES OF BLOCKCHAIN

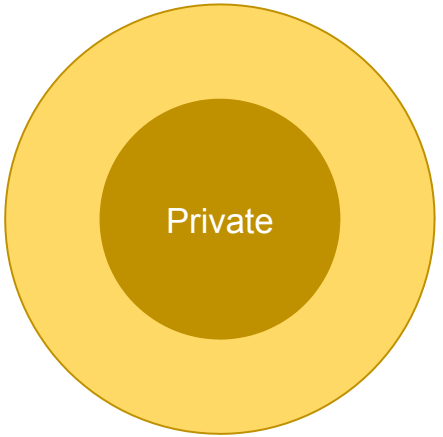


- Anyone can see and inspect the ledger
- Trust comes from the generation of consensus

TYPES OF BLOCKCHAIN



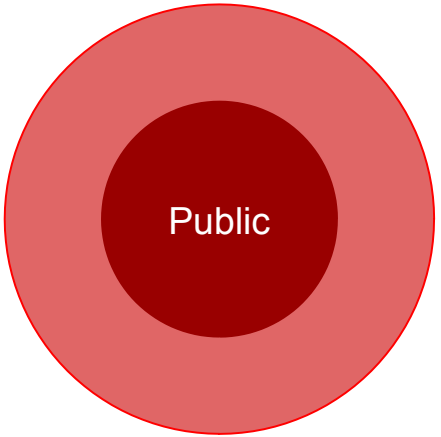
- Anyone can see and inspect the ledger
- Trust comes from the generation of consensus



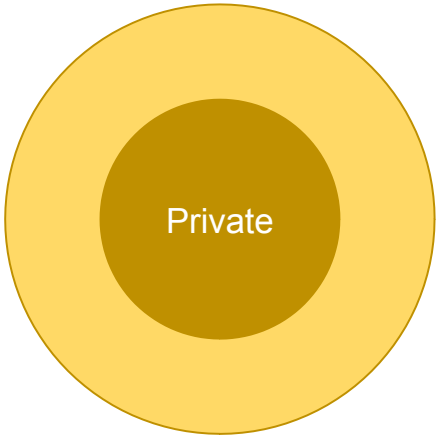
Agora

- Private to an organization
- Useful where privacy is a concern

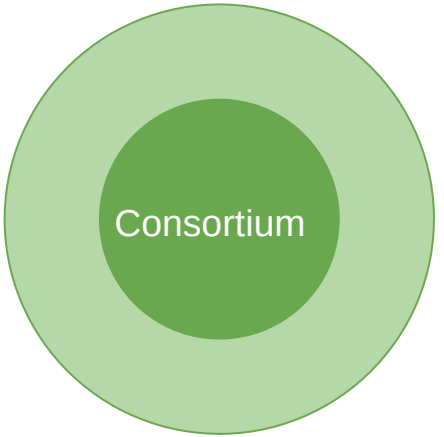
TYPES OF BLOCKCHAIN



- Anyone can see and inspect the ledger
- Trust comes from the generation of consensus



- Private to an organization
- Useful where privacy is a concern



- Hybrid type of blockchain
- Ran by multiple organizations, thus de-centralising the system


THIS LAND IS NOT
FOR SALE

From the **1st edition of Black's Law Dictionary**:

identity =

the sameness of the ***person*** to their ***references***


SAMENESS

PERSON

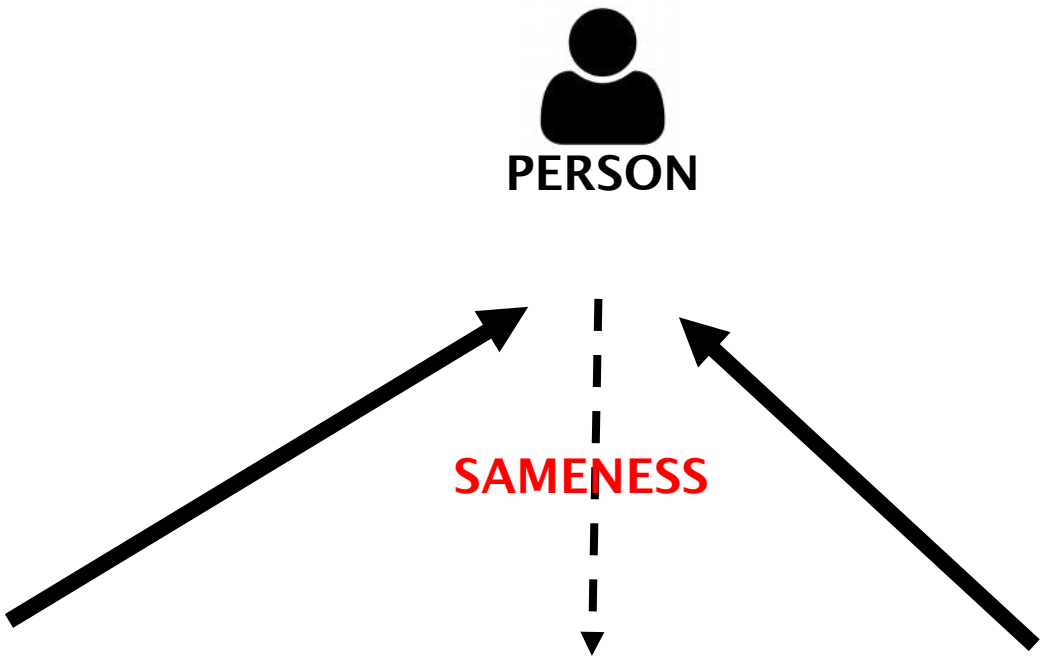
SAMENESS

PERSON

SAMENESS

REFERENCE 1
NAME. The designation of an individual person

REFERENCE 2
DESIGNATION. A description or descriptive expression by which a person or thing is denoted (without using the name)



REFERENCE 1
NAME. The designation of an individual person

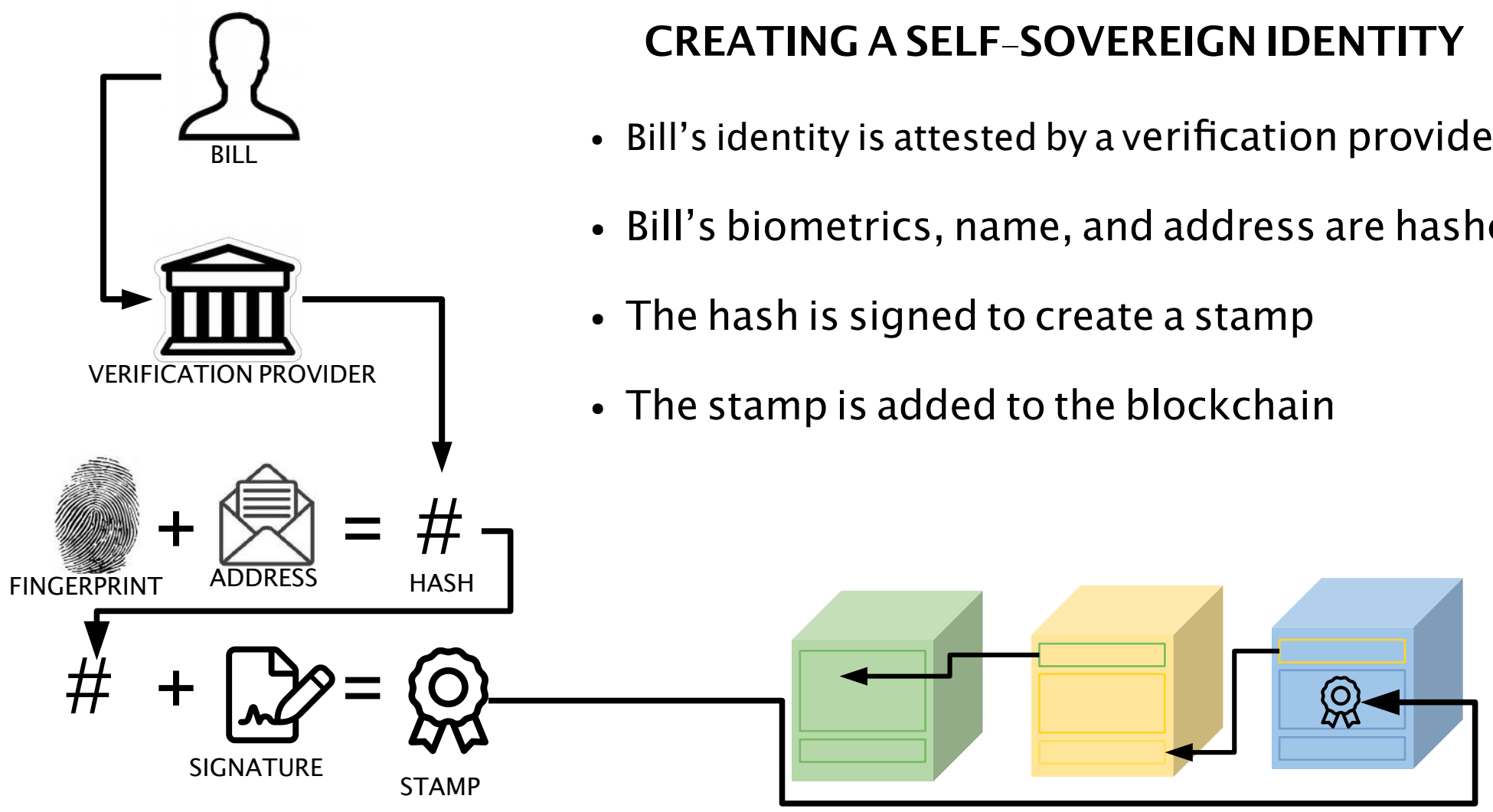
REFERENCE 2
DESIGNATION. A description or descriptive expression by which a person or thing is denoted (without using the name)

references on the ledger → one and only one thing?

If yes → possible to authenticate an individual using their characteristics, **without** knowing all details about that individual

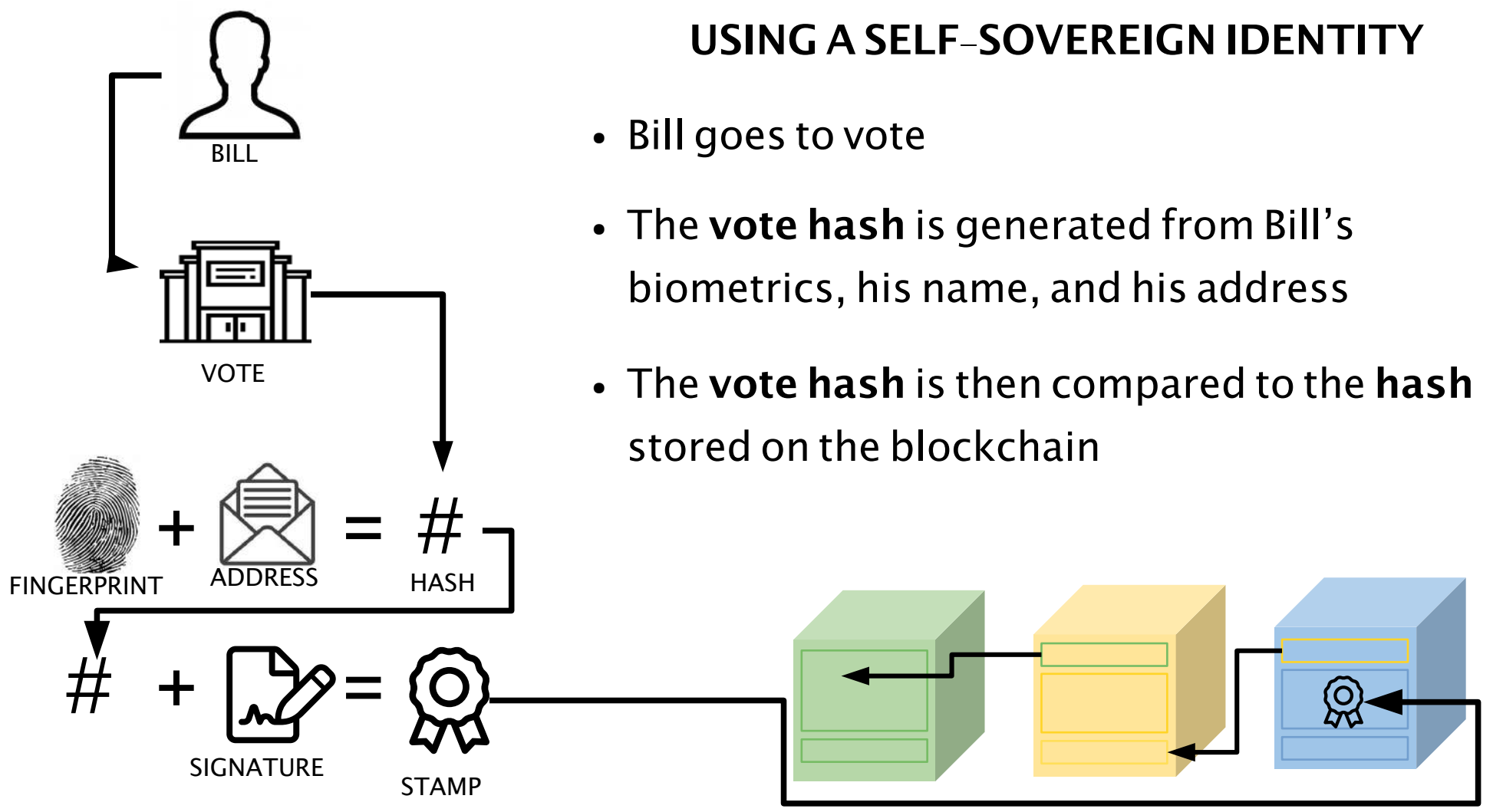
CREATING A SELF-SOVEREIGN IDENTITY

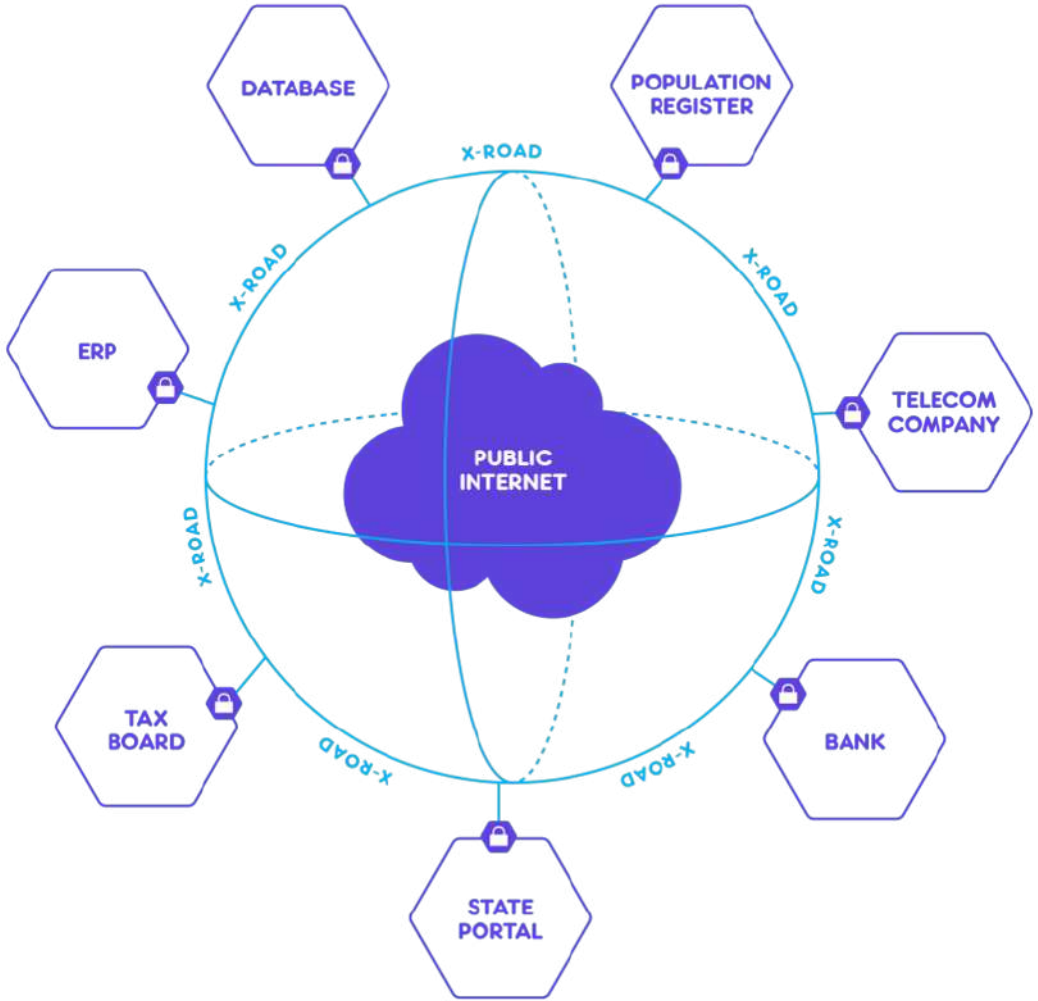
- Bill's identity is attested by a verification provider
- Bill's biometrics, name, and address are hashed
- The hash is signed to create a stamp
- The stamp is added to the blockchain



USING A SELF-SOVEREIGN IDENTITY

- Bill goes to vote
- The **vote hash** is generated from Bill's biometrics, his name, and his address
- The **vote hash** is then compared to the **hash** stored on the blockchain




DATABASE
POPULATION REGISTER
X-ROAD
X-ROAD
X-ROAD
ERP
TELECOM COMPANY
PUBLIC INTERNET
X-ROAD
X-ROAD
TAX BOARD
BANK
X-ROAD
X-ROAD
STATE PORTAL

e-estonia

LIMITATIONS

- Speed

LIMITATIONS

- Speed
- Environmental Cost

LIMITATIONS

- Speed
- Environmental Cost
- Unavoidable Security Flaw

LIMITATIONS

- Speed
- Environmental Cost
- Unavoidable Security Flaw
- Lack of standardization

LIMITATIONS

- Speed
- Environmental Cost
- Unavoidable Security Flaw
- Lack of standardization
- Lack of regulation

INTRODUCTION

We know that about 1.5 billion people can’t formally prove their identity. As an objective of the sustainable development goals, everyone should have an identity by 2030. Historically records of identity or other information about people, have been kept on manual files, also called “a ledger”. But in the current electronic age, any identity database is going to be digital. People are naturally concerned about having their personal details recorded in files and databases over which they have no control. They are concerned about the possibility of identity theft and the information being used for purposes for which it was not intended.

Therefore any system of identity recording must inspire confidence and trust.

One of the most discussed technologies today is Distributed Ledger Technology known as “DLT” and Blockchain.

Companies and governments are investing millions of dollars in developing this technology. It’s a fast-developing area. Many argue that block chain technology will usher in revolutionary changes whilst others see it as offering more opportunities for criminal behaviour.

At its simplest blockchain allows participants to trust a system without necessarily trusting anyone to validate it. It should enable the sharing of information among parties who do not trust one another, providing confidence that no one individual or participant can alter the information recorded in that system.

In this short presentation I will seek to explain the principles of a Distributed Ledger Technology (DLT) and a form of DLT known as blockchain, highlight their strengths and shortcomings, and application to identity authentication, and draw some lessons from this experience so far.

LEDGER

Information, particularly financial information has usually been recorded in ledgers like this 19th century German ledger.

However, how much can you trust this information, which is all held centrally over which one person may well have full control? Pages can be altered or removed from books.

In the present day, physical ledgers have not really changed but have only been digitized in the databases. But whilst databases might be reliable, the data can be changed. How do we ensure that the data hasn't been tampered with or amended in any way?

To overcome these weaknesses, Haber and Stornetta in their 1991 paper came up with the idea of cryptographically signing series of blocks of information. But the idea wasn’t taken seriously until 2008 when an individual or individuals Satoshi Nakamoto posted a white paper on a cryptocurrency called “Bitcoin”. This introduced a significant innovation, compared to earlier work, by introducing a distributed

network of peer-to-peer nodes to track and verify transactions. This forms a decentralised immutable ledger for recording information and transactions with mechanisms for processing, validating and authorisation.

So what is a blockchain? Let’s break the process down, of how basic blockchain data structure works. [Click to next slide.]

BLOCKCHAIN SIMPLIFIED

This is the genesis block, the first one, the word doesn’t mean anything. It’s the first of its kind in a blockchain and contains the initial set of transactions or information. The genesis block, being the first, doesn’t reference a previous block.

We assemble the block and then work out a hash value. A hash is an algorithmically derived signature, which is calculated by processing the block’s data. Any change in the data causes the hash value to be completely different.

BLOCKCHAIN SIMPLIFIED

A new block is created and shared across the network. From now on each block has three main properties. The transaction data with in it, the hash of the block and the hash of the previous block.

The previous hash will always link up with the hash of the block before it. This is what creates the chain.

The hash of the new block is calculated from all the data in the block including the transactions and the previous block hash.

When a third block is added the same process as before happens, its previous block hash points to the second block thus forming the next part of the chain.

And so on.

What makes a blockchain so secure? If a user was to tamper with the data in block three, this would then change the hash of that block. However the next block would still have the original hash value of the third block thus breaking the chain. You could conceivably then tamper with all subsequent blocks to remake the chain but there are other protections in place. For example, if we make the calculation of the hashes computationally hard enough, it becomes uneconomic to attempt recalculating the blocks.

Therefore a blockchain is a particular way of recording information, and is a data structure or data storage system, which sequentially links chunks of information in a way that can’t be altered. Blockchain system is a collection of computers running software that maintains a blockchain in a consistent state called “consensus”. It is a chain of blocks designed to create an immutable ledger of transactions.

A blockchain on its own is a data structure, which provides tamper resistance. We now need to verify that the data we are storing is correct and can be trusted.

THE DECENTRALIZED LEDGER TECHNOLOGY (DLT)

A key feature of blockchain systems, and probably why Bitcoin succeeded, is the use of decentralised peer-to-peer computing and consensus, in order to solve the trust problem. Peer-to-peer computing is where you have computers based all over the world providing a service. The fact that there are many computers, or “nodes”, means that the system is very rugged, with no single point of failure.

Using peer-to-peer computing makes blockchain a type of decentralised ledger. Other types of decentralised ledger technology exist but blockchain adds in tamper proofing.

How does decentralisation help solve the trust problem? When a transaction is to be added to the blockchain, the transaction must first be verified by enough nodes to gain consensus. In our example here that is three nodes out of the five.

Requiring consensus makes introducing an invalid transaction extremely hard. With a single trusted server, you only need to hack that one server to introduce an invalid transaction. With a peer-to-peer validation network, you could introduce a hacked peer but you wouldn't be able to gain consensus because the other peers would reject the transaction.

In a real deployment, the peer-to-peer network would be large enough, and the level of consensus high enough, that you'd never be able to introduce enough hacked peers to force consensus. It would simply cost too much.

Peer-to-peer computing also distributes the blockchain data across multiple sites, so if you were to try to distribute blocks with tampered data you would never be able to build a consensus that your data is correct. There are too many copies of the valid data.

Having multiple sites also means that the data is highly available. Services built on top of blockchain don't need to rely on the up-time of a single hosting platform, because there is a large network of peer-to-peer nodes. Thus the services become highly available.

The advancements in blockchain aren't only useful in digital currencies. The core technologies of a cryptographically secure chains of blocks, containing transactions verified via a distributed peer-to-peer network, can be used in other situations, where having a tamper-proof ledger is critical. You can use blockchain technology for voting systems, land registry, digital contracts and identity verification.

TYPES OF BLOCKCHAIN

There are 3 main types of blockchains.

There is the public blockchain, where anyone can see and inspect the ledger and add to it. The trust comes from the generation of consensus from peer-to-peer nodes. A public blockchain has the highest level of security but in order to be viable it requires a business model where peers can make an income.

Bitcoin is an example of a public blockchain.

Private blockchain. This type of blockchain is as the name suggests private to an organisation. It is hosted and managed by a single organization and only accessible by that organisation. Private blockchains can be useful where privacy is a concern but lack the level of security which comes from a more open architecture. Uses of a private blockchain could be vote counting, banking communications or supply chain management.

Agora runs a private blockchain that can record votes during elections.

Consortium, is a hybrid type of blockchain. It's very similar to the private blockchain but there's a significant difference. A consortium blockchain is run by multiple organizations, thus de-centralising the system.

R3 Corda created a blockchain that has been built especially for business and consortium's

A very practical example of how blockchain can make a difference is in land registry. [CLICK to next slide.]

LAND AND PROPERTY OWNERSHIP

Land and property ownership are a vital store of wealth that is passed down through generations, often with little documentation of the true owner.
In parts of the world you can walk down the street and see hand written signs like this image. Does the person that wrote the sign have the true title deed to that land? Making all land records publicly available online using blockchain could eliminate contention over who owns a piece of land, reduce corruption and raise confidence in property markets.

In Ghana for example, Seso Global is building a trusted real-estate market using blockchain. The idea is to enable secured lending in emerging economies, where centralised land-registry data can be unreliable. Their aim is to accelerate access to capital through securing land ownership. Seso is partnering with leading property developers and mortgage lenders to launch the country's first digital mortgage registry. Governments and businesses around the world are exploring ways to use blockchain tostore legal data, such as contracts and assets.
Blockchain-based land-titling systems store ledgers of property transactions in immutable digital registries, which are cross-checked by a network of peer-to-peer nodes.

Let's look at the application to identity. [CLICK to next slide.]

IDENTITY

From the 1st edition of Black's Law Dictionary, identity is the sameness of the person to their references.

Take a look at two possible values. First of all it is a NAME.
The second is a DESIGNATION.

If identity is the sameness of a person to the information that points to them, and if we store this information on a ledger, we have a method for authenticating identity. Are the references on the ledger each a reference to one and only one thing?

If we can prove this is the case, then it is possible to authenticate an individual using their characteristics, without knowing all details about that individual.

There are numerous ways in which people can identify themselves but many methods involve disclosing more information than is required for a particular purpose. For example, a simple identification database may be able to prove your bank account details and your address, but how do you avoid revealing your bank account details when you are just trying to prove your address?

One method of resolving this problem is self-sovereign identity. With self sovereign identity, the individual is fully in control of the information disclosed.

CREATING A SELF-SOVEREIGN IDENTITY

So how does this work in a blockchain system? Let's explore a simple scenario. This is Bill. He would like his name and address to be attested (first time/onboarding) by a verification provider, such as a government authority, licensing authority, or passport office.

"Hello verification provider, I am Bill and this is my address. (First time meeting.) Please attest it. (I need you to know that this is true.)

"Here is my thumbprint." (First time.) (For the hash generation.) (The address points to him. The name points to him. The fingerprint points to him.)

The verification provider would first prove that ~~Bill is who he says he is~~ (avoid this, as this contradicts the concept of identity we propose. It never 'is', it can only be 'compared' and the sameness of the comparison gives assurance or doubt. Instead...) what Bill says does point to him. ~~and that he resides at the address given.~~ How this is done depends on the standard of proof required by the verification provider, but it could involve meeting Bill, or reviewing documentary evidence that Bill provides. Once the verification provider is confident that the information is correct, it then uses the thumbprint, name and address to create a hash. The **hash** is then encrypted with the **verification provider's private key** to create a **signature**. Finally, the **hash** and **it's signature** make a **stamp** which is added to the blockchain.

Even if you can read this stamp on a public blockchain, it is impossible to obtain Bill's name, his address or his thumbprint from it, so his data cannot be stolen and his privacy is maintained. The stamp can only be used to verify that Bill's name and

address is correct, and only when Bill chooses to provide this information plus his thumbprint.

USING A SELF-SOVEREIGN IDENTITY

So, how would Bill prove his name and address are correct?

Bill goes to vote in his local elections where, in this simple scenario, Bill needs to prove his name and address.

“Hello, I'm here to cast my vote. I am Bill, this is my address and here is my thumbprint.”

The clerk will take the name and address Bill has provided, along with his thumbprint. This information will then be used to generate a hash value.

If the **hash value in the stamp on the blockchain** matches the **hash value generated by the clerk**, Bill has successfully verified his address to the clerk. The clerk can check the verification provider’s signature with a public key.

Notice that the clerk didn't obtain Bill's name or address ***from*** the blockchain, instead Bill ***chose*** to provide that information to the clerk. The blockchain is only providing verification of identity data, proving **the sameness** of Bill to the address he provided. The blockchain is not providing storage of identity data and so Bill's privacy is maintained.

ESTONIA EXPERIENCE

Estonia has been testing blockchain technology since 2008 and is credited with being the first country to use such technology on a national level. An Estonian company, Guardtime, launched in 2007 developed a verifiable security system called Keyless Signature Infrastructure (KSI) which uses only hash-function cryptography. This allows verification to rely only on the security of hash-functions and the availability of a public ledger, commonly referred to as a blockchain. KSI has been continually developed and improved since it’s initial development. Since 2012 blockchain has been in operational use in Estonia’s registries such as national health, judicial, legislative and security.

A user interacts with the KSI system by submitting a hash-value of the data to be signed into the KSI infrastructure and is then returned a signature which provides cryptographic proof of the time of the signature, integrity of the signed data, as well as attribution of origin i.e. who created the signature. The number of participants in the KSI system is limited thus making reaching consensus far quicker than say, under Bitcoin.

99% of Estonia state services are online. 98% of Estonians have an ID card and can provide digital signatures to identify themselves and use services. The identity service has a mobile-ID not reliant on a card reader. The Population registry contains the names, ID codes, dates of birth, place of residency, nationality, native language, education and profession of all residents.

Underpinning the various national databases is a platform called X Road which enables communication and information sharing between users on different software platforms and data service providers. Thus, a resident who changes their address for their driving license can have that change recorded in all other databases such as health and social security. The system also allows electronic. voting from any location.

Individual citizens own their own data and can access information about themselves, see who, if any, other person or organisation has accessed the data and can prevent future access.

Many countries turning to blockchain for systems for voting. A few examples [CLICK]

BLOCKCHAIN AND VOTING

Russia

In December 2017 officials developed a pilot system for tracking votes via blockchain. The government made the code behind the open-source on GitHub. In an effort to diminish the likelihood of electoral fraud, which is a huge issue despite the prevalence of electronic voting systems, the system started to be tested in November 2017. In regional elections to elect new governors, sixteen regions in September last year tested the system. The technology keeps the information not just on one server but on all of the computers of the voters. The more voters there are the more secure the system is. Records are added sequentially and all copies are stored and refreshed on each voter's computer. The only real successful example of a wide electronic voting system is in Estonia where online voting accounts for around 30% of the population.

Japan

The tsukuba, ibaraki pref. introduced an online voting system based on their My Number identification system and blockchain technology. The system allows voters to cast ballots via a computer display after placing the My Number card on a card reader. Blockchain technology is used to prevent the voting data from being falsified or read.

In Africa

The African Union signed a cooperation agreement with the government of Estonia in 2017 to pilot the introduction of e governance and in Kenya president Uhuru Kenyatta recently launched a blockchain and artificial intelligence task force for the purpose of deploying blockchain technologies within the country's existing economic framework over a 15 year timescale including for voting and land registry purposes. In South Africa the South African Central Securities Department, announced an agreement for Nasdaq (the SA stock exchange) to deliver a blockchain solution to bring electronic voting to the South African capital markets. The solution is intended provide general meeting services and give to shareholders an easy, user-friendly and secure tool for voting remotely.

LIMITATIONS

I’ve spoken a lot about the advantages of blockchain and decentralized ledgers and not mentioned it’s limitations and possible problems. Cryptocurrency platforms like Bitcoin have certainly had their critics. Key issues:

Speed

Most high grade blockchain network clients store an entire transaction history. Which in the case of bitcoin is huge. The data has to be downloaded. Thus it requires a large amount of memory to store but the speed is necessarily compromised. Thus transactions tend to take much longer than using other platforms and systems. Bitcoin transactions can take several hours to finalise. This in turn increases costs.

Environmental Cost

Blockchain relies on encryption and complex algorithms, which in turn require large amounts of computing power. This comes at a cost. The high energy requirements are also a stumbling block for mass adoption. It was estimated last year that the computing power required for the bitcoin network consumes as much energy as was used by 159 of the worlds nations!

Unavoidable security flaw

There is one notable security flaw: if more than half of the computers working as nodes to service the network tell a lie, the lie will become the truth. This is called a ‘51% attack’ and was highlighted by Satoshi Nakamoto when he launched bitcoin.

Lack of Standardisation

The number of companies and blockchain players is expanding rapidly and as no standardisation exists, there is an important issue of interoperability and their ability to interact with each other. On coding site GitHub there are over 6500 active blockchain projects using different coding languages, consensus mechanisms, protocols and privacy measures.

Lack of Regulation

This creates a risky environment for users and, particularly in the cryptocurrency market, manipulation and scams have been common.

SUMMARY

In conclusion, it is the reality of identity that is important.
Blockchain can provide a secure and private platform for identity management, so long as the data stored is in a form of hashes to verify identity, rather than actual personal data. Identity in its true form is inherent in who we are and we can’t move identity into technology. We can only reference it. Using technology for identity purposes is advantageous but it can never describe everything about us.
Bitcoin's success came from it's peer-to-peer nature, and it is now one of many

cryptocurrencies. If you can choose which cryptocurrency you use, shouldn't you also be able to choose which verification system you subscribe to?