Høgskolen på Vestlandet

DAT159
Module3 – Blockchain technology

L18 - Blockchain Applications and Ecosystem

Lars-Petter Helland, 22.10.2018

Today

- Recap of last lecture
- Oblig3?

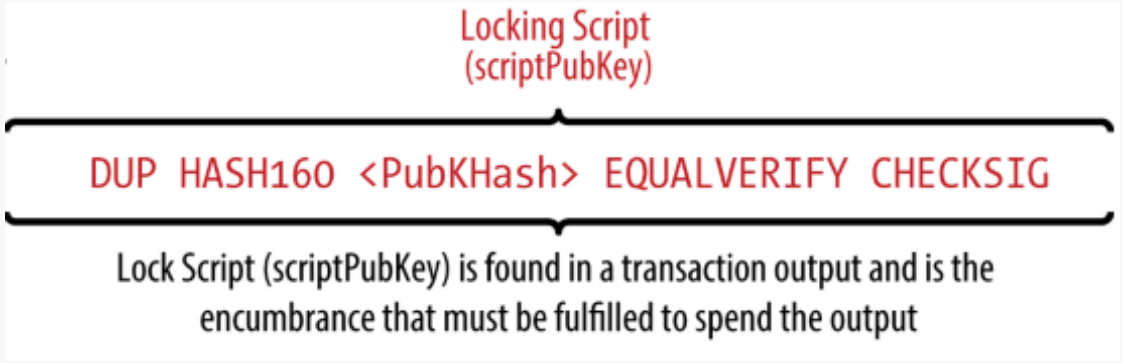
- Properties of blockchain technology
- Applications of blockchain technology
- The blockchain ecosystem

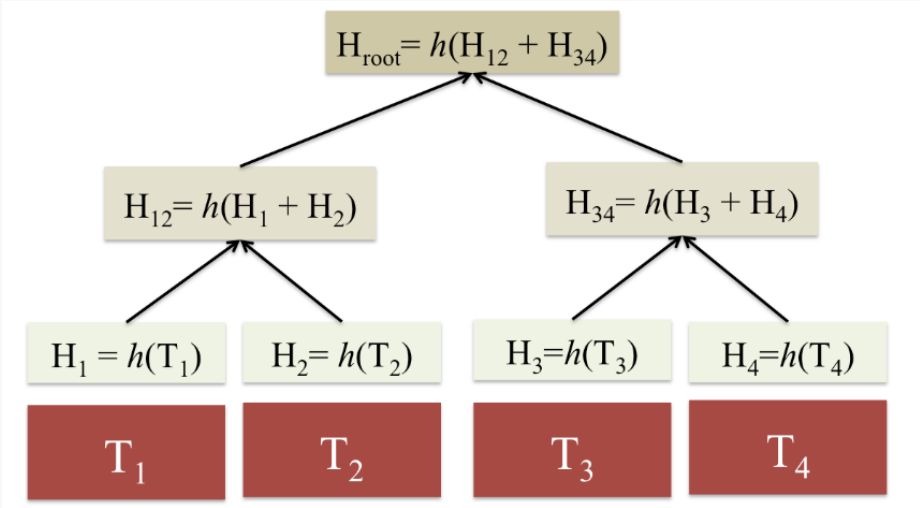
Reading material

- **[??]** ... https://rubygarage.org/blog/implementing-blockchain-in-business ??
- **[??]** ... http://www.visualcapitalist.com/the-bitcoin-universe-explained/ ??

Recap of last lecture

- Signing a transaction
- Transaction validation check list
- Locking and unlocking scripts
- Merkle tree / -root / -path
- Simplified Payment Verification (SPV)
- Block validation check list



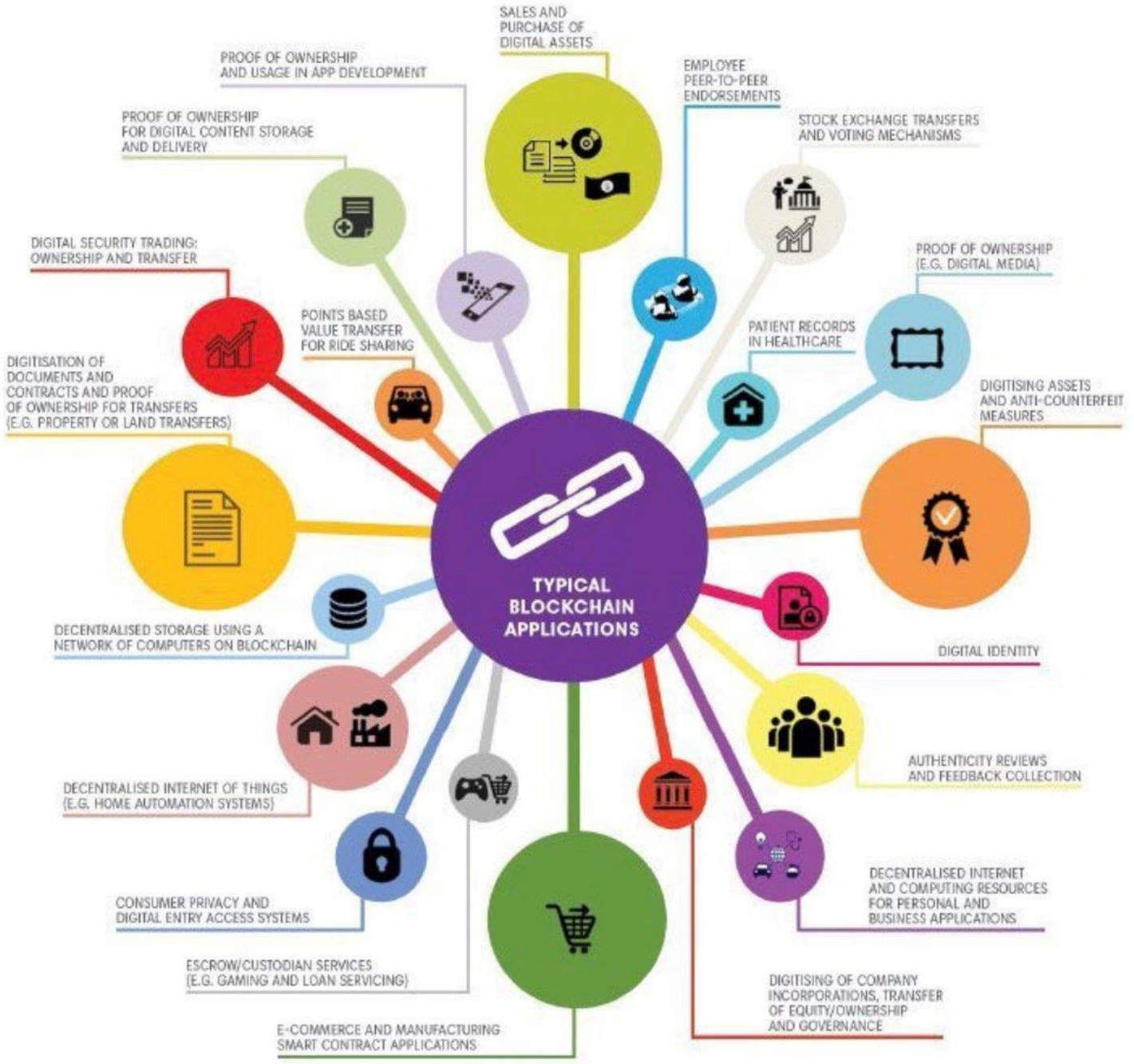


Oblig3 - questions?

```
Block3:
CoinbaseTx(HVkO3OLGTr1QzKsUKp3fxw/DVvheReRHbekCA1KuvBY=)
   message=Hello again, output=Output [value=100, address=kFn1+kOrdmbP...=]
Transaction(zzR7MngsWm/BzF9FQ8cKi67JwO2izO1Awj77i9ayPik=)
   inputs=
      Input [prevTxHash=OFTi85+GpUfxtFSwI0dca+854PoOtXRQuZckkvxyYcA=, prevOutputIndex=0]
      Input [prevTxHash=0Iz+qB65T3OCutB/dxyQBo2iORzFt2UkBFBnAlv2DHE=, prevOutputIndex=1]
   outputs=
      Output [value=20, address=f4WSHTd3/57vb7//EI8RF0L23J19f//rgozGAOFtnP0=]
      Output [value=160, address=kFn1+kOrdmbP/KHvrr9cD7wJ//QekWEuUQN29ayrI0w=]

UTXO:
Input [prevTxHash=0Iz+qB65T3OCutB/dxyQBo2iORzFt2UkBFBnAlv2DHE=, prevOutputIndex=0]
       --> Output [value=20, address=f4WSHTd3/57vb7//EI8RF0L23J19f//rgozGAOFtnP0=]
Input [prevTxHash=zzR7MngsWm/BzF9FQ8cKi67JwO2izO1Awj77i9ayPik=, prevOutputIndex=1]
       --> Output [value=160, address=kFn1+kOrdmbP/KHvrr9cD7wJ//QekWEuUQN29ayrI0w=]
Input [prevTxHash=HVkO3OLGTr1QzKsUKp3fxw/DVvheReRHbekCA1KuvBY=, prevOutputIndex=0]
       --> Output [value=100, address=kFn1+kOrdmbP/KHvrr9cD7wJ//QekWEuUQN29ayrI0w=]
Input [prevTxHash=zzR7MngsWm/BzF9FQ8cKi67JwO2izO1Awj77i9ayPik=, prevOutputIndex=0]
       --> Output [value=20, address=f4WSHTd3/57vb7//EI8RF0L23J19f//rgozGAOFtnP0=]

The miner's wallet:
Wallet [id=Miner's wallet, address=kFn1+kOrdmbP...=, balance=260]

My wallet:
Wallet [id=Lars-Petter's wallet, address=f4WSHTd3/57vb7...=, balance=40]
```

Blockchain Applications

(meaning: what blockchain tech. can be used for)



- Before we look at possible applications, I think **we should investigate the claimed properties** of blockchain technology.
- It is difficult to have a strong opinion about these things, but a break down and a discussion will always help.

- A also think that before we investigate the properties, **we also need to clarify what a blockchain is**.
- Opinions differ, and it is difficult to find a common definition.

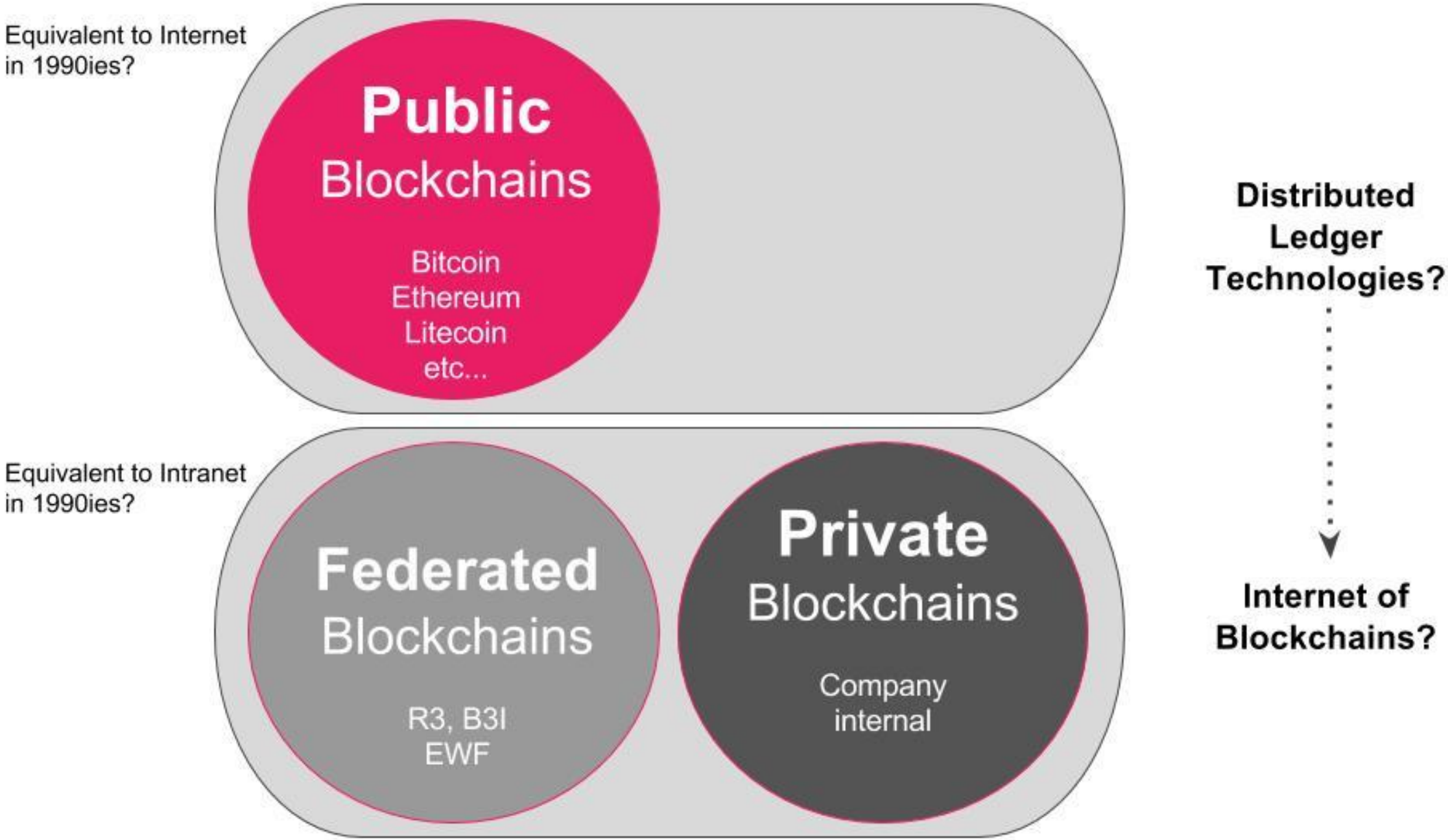
What is a blockchain

- It is a digital **ledger** recording transactions
- It is **cryptographically secured, tamper resistant chain** of records
- It is an **append-only** data structure
- It is **decentralized** / distributed
- It uses some **consensus protocol** on write/append

- See https://medium.com/@richbodo/common-use-of-the-word-blockchain-5b916cecef29 for a discussion about the term.

What is a blockchain, cont. ...

- Does it need to be publicly available?
  - Some are totally public (like Bitcoin), and some are totally private inside a company. **A private blockchain lacks some properties compared to a public one.**
- How decentralized does it need to be?
  - Some are quite decentralized (like Bitcoin), and some are more centralized. **A centralized blockchain lacks some properties compared to a decentralized one.**
- Does it need to have an associated cryptocurrency/-token?
  - Most uses a cryptocurrency as an incentive for securing the blockchain. **A blockchain will lack some properties if there is no crypto.**


Equivalent to Internet in 1990ies?
Public
Blockchains
Bitcoin
Ethereum
Litecoin
etc...
Equivalent to Intranet in 1990ies?
Federated
Blockchains
R3, B3I
EWF
Private
Blockchains
Company
internal
Distributed Ledger Technologies?
Internet of Blockchains?

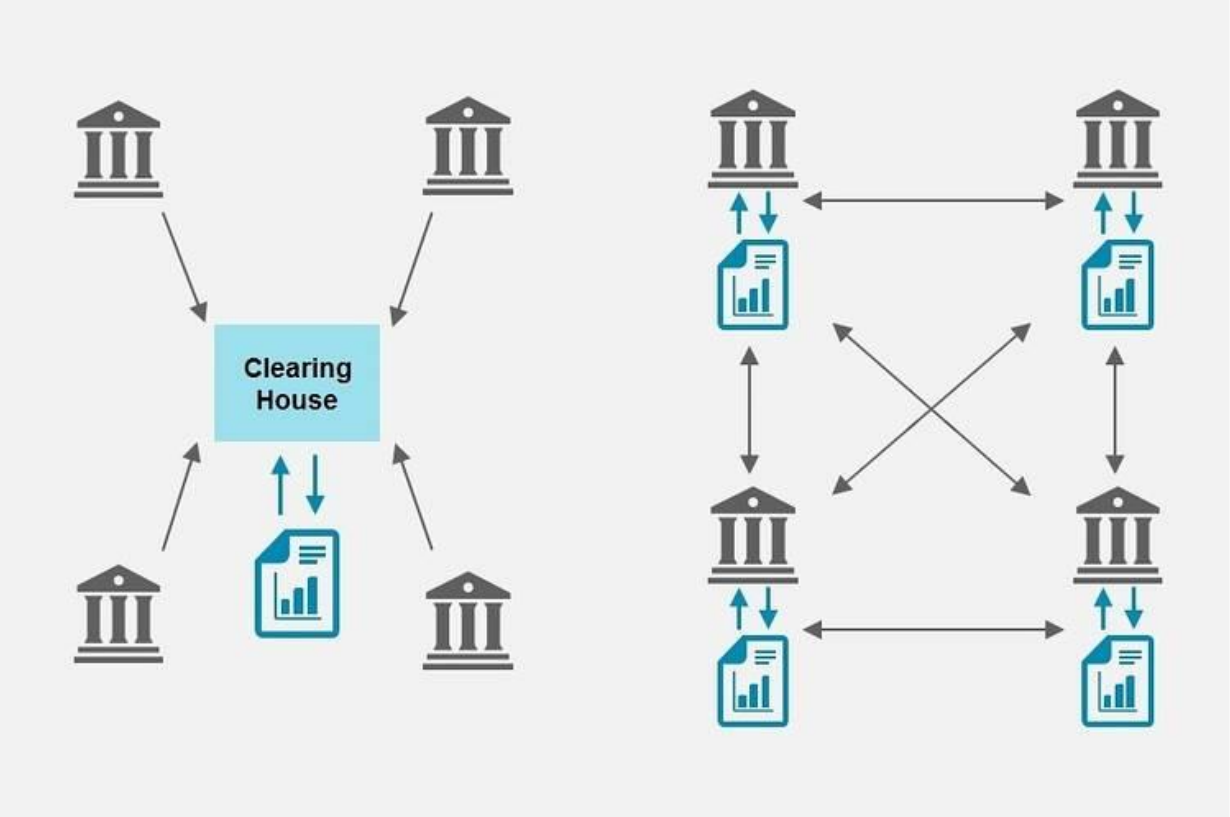
A list of common "claimed" properties

https://rubygarage.org/blog/implementing-blockchain-in-business

- Removing the need for a third party (disintermediation)
- Permissionless use / transactions
- Transactions without trust
- Transparency
- Immutability
- Privacy
- Giving the users ownership over their transactions and data
- Time and cost efficiency
- Security and robustness
- Fraud reduction

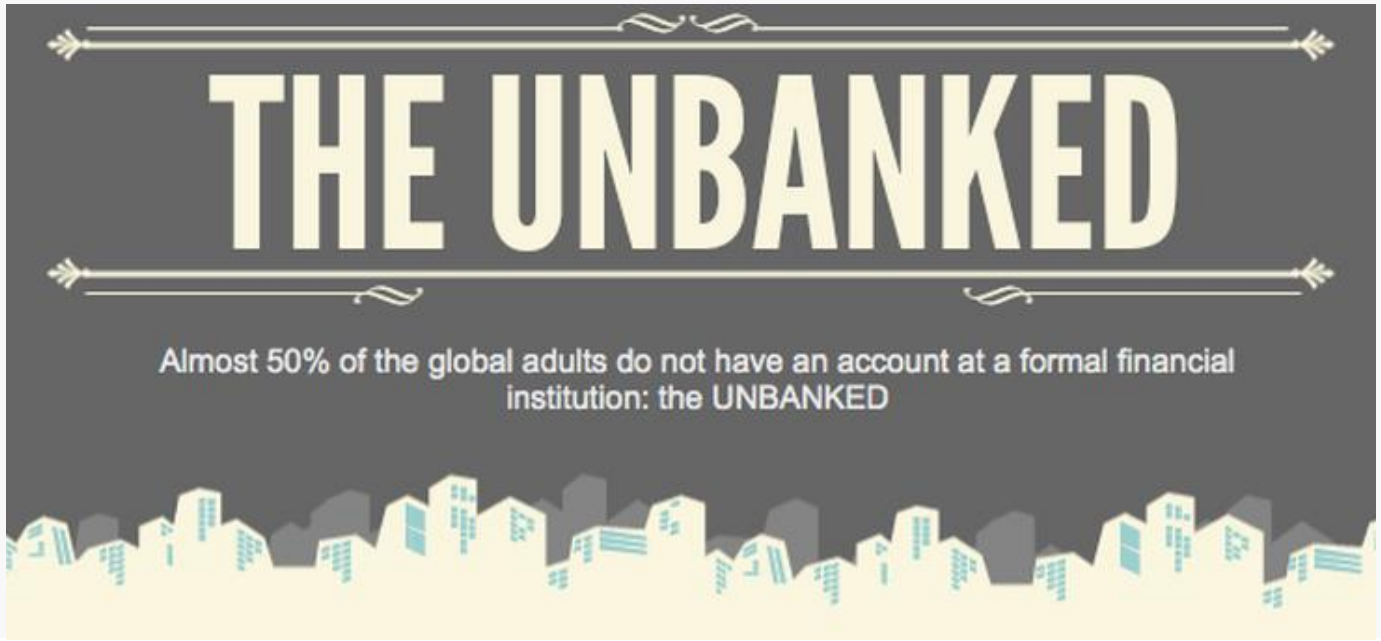
Removing the need for a third party

- This was one of the original main selling points.
- The ability to do direct peer-to-peer transactions without needing a clearing house (bank).
- This property enables the community of users to set the policy of how things are done (rules, fees, ...) .
- A truly **disruptive** property.



Permissionless use / transactions

- Permissionless ledgers means **access for all**.
- Like the Internet, no consent is required from any central authority or group.
- This is a **democratic** property, empowering the people.
- *"Banking the unbanked".*

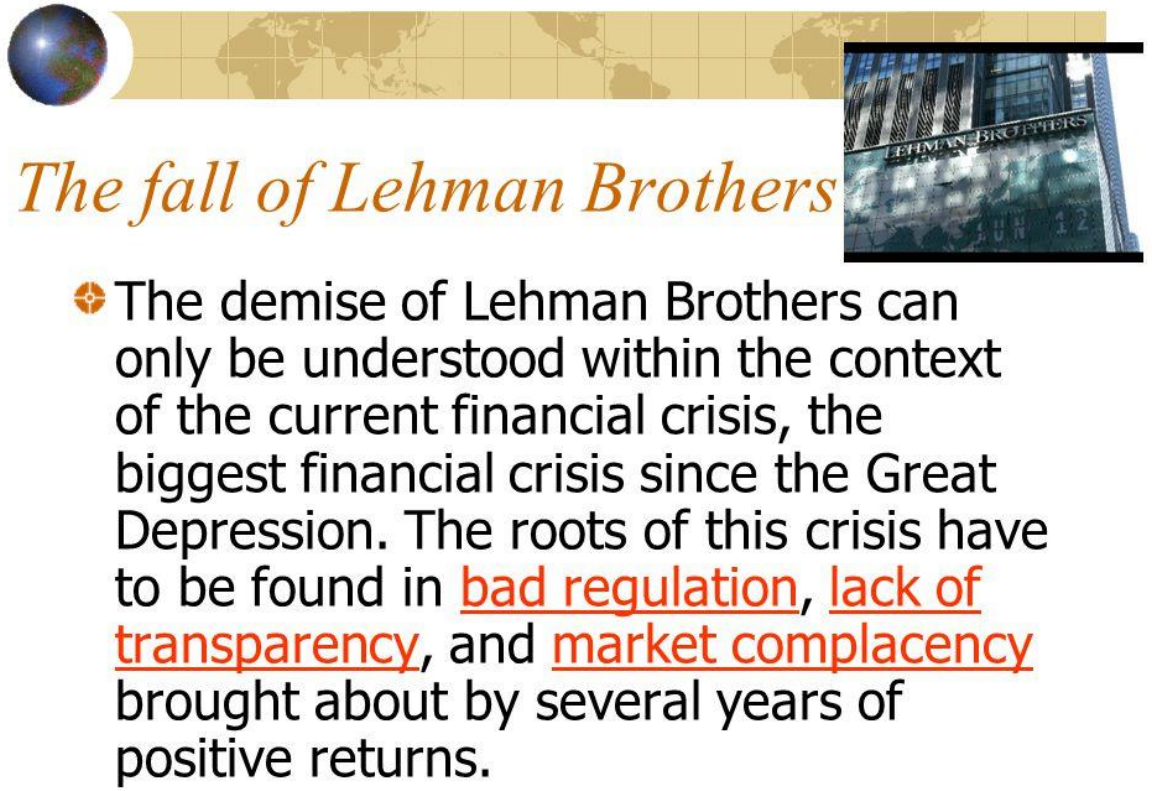


Transactions without trust

- Normally when you do transactions with someone, you need to trust each other or rely on a trusted 3rd party.
- The whole blockchain machinery, the algorithms, the crypto, the consensus protocol, make trustless transactions possible.
- You only have to rely on math and computer code doing it job.

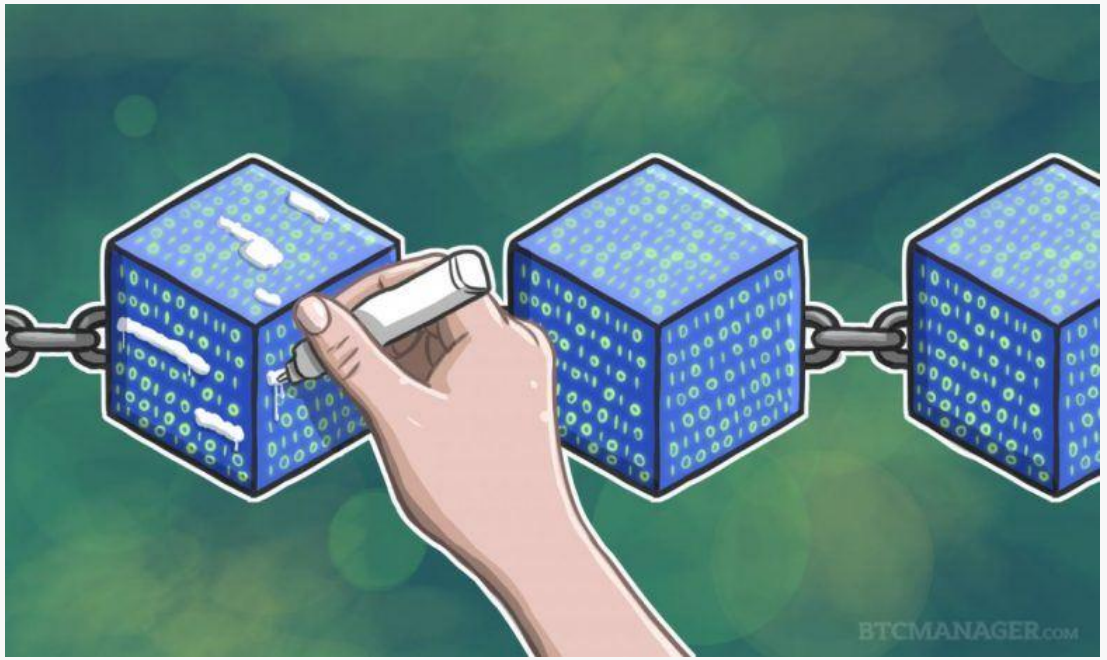
Transparency

- Transparency means that everyone can see what has happened.
- The transparency of a blockchain stems from the fact that the holdings and transactions of each public address are open to viewing.
- It adds a degree of accountability that has not existed before.



Immutability

- This means that the data is **tamper proof**.
- It should not be feasible to change data in a blockchain.
- The strength of this property is related to the **consensus mechanism**, but also to the **degree of decentralization**.
- Bitcoin's **Proof Of Work** is what makes it tamper proof.



Privacy

- Privacy becomes more and more important as we live our lives digitally.
- Why should the bank (or Rema1000) know how we spend our money?
- Why should Google know all our daily movements? ...
- Blockchain offers decentralized solutions that prevents central actors from collecting and analyzing data about our lives.
- By adding layers of cryptography, the data itself can also be protected from snooping.

Giving the users ownership over their transactions and data

- Why should we not own our own data? Why should Facebook own and monetize our data?
- A decentralized social network can f.ex. let the users decide how much personal data is shared and which advertisers they will support.

Time and cost efficiency

- Automation, global open standards

Robustness (withstands malicious attacks)

- Relies on a well functioning network ...
- Redundancy
- No single point of failure
- Strong consensus rules ...

Fraud reduction

- Transparency, ...
- Smart contracts, ...

Does a blockchain need a token?

https://hackernoon.com/why-use-the-blockchain-instead-of-a-database-what-gives-tokens-value-263449681153

- Blockchain embodies a lot of game theory and incentive models. In order for a blockchain network to be valuable or useful, it has to have participants.
- There needs to be some sort of incentive to attract them. The most common method is via issuance or reward of the token used in the network.
- Tokens are important to secure the network, both by rewarding block validators, and by preventing spamming.

- So, **yes**. (Unless you run a private blockchain.)

Different types of tokens

- **Currency tokens**—Tokens like Bitcoin, Monero, Nano, etc
- **Utility tokens**—Tokens that allow you to essentially use or perform an activity on a network, such as Ether or OX. On the Ethereum network you would need to spend Ether (aka gas), to run a smart contract, etc
- **Asset tokens**—Tokens that represent an actual asset or product
- **Equity tokens**—Tokens that basically act like a share, and gives you some kind of voting right or consensus participation

Blockchains without tokens

https://medium.com/swlh/does-a-blockchain-need-a-token-66c894d566fb

R3's Corda and IBM's Fabric.

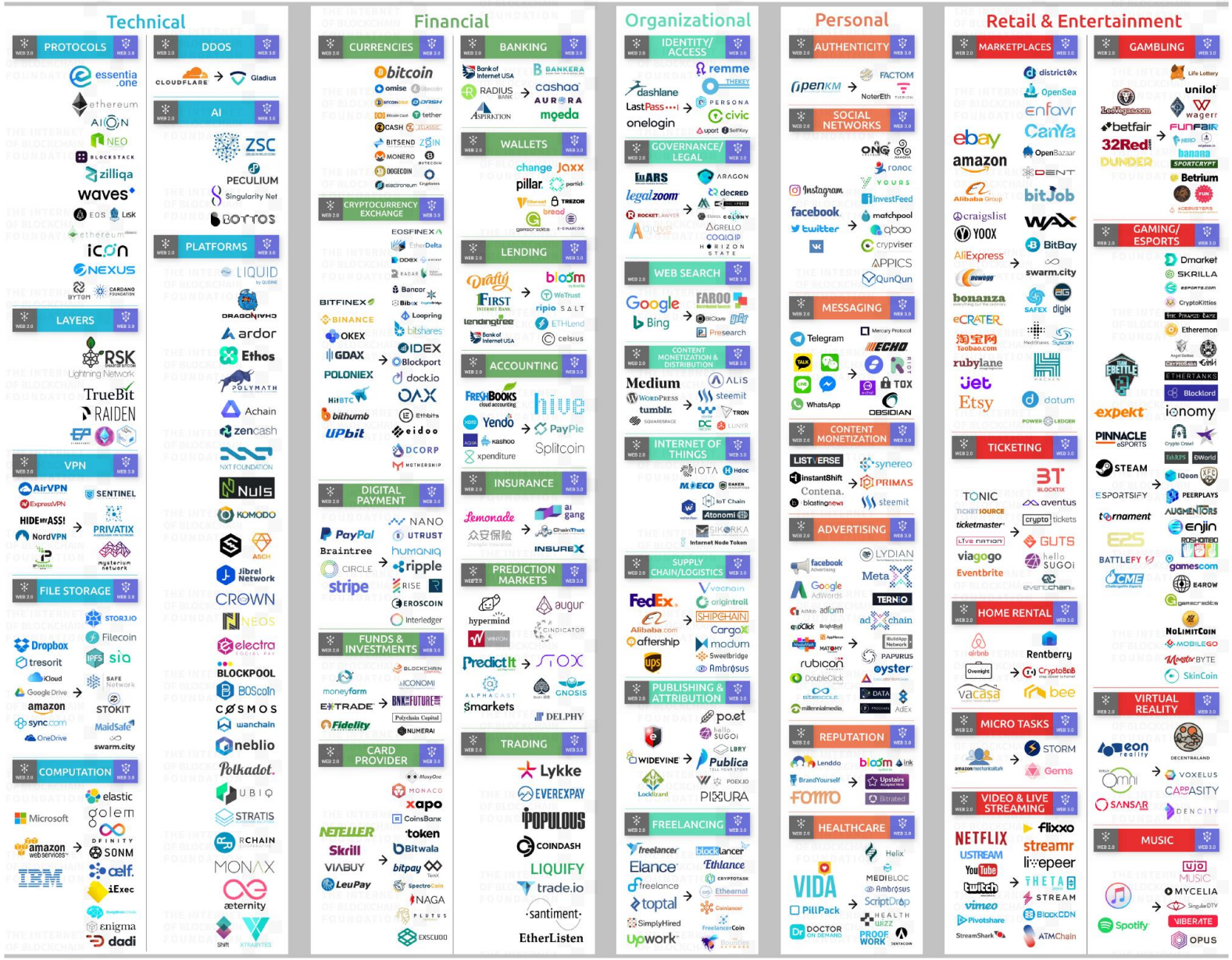
- Consensus on Corda is reached at a transaction level and only involves parties privy to a transaction. There is no "proof of work" or "miners" in order to verify transactions.
- As Philipp Sandner explains in his blogpost, *"Consensus is based on transaction validity and transaction uniqueness. Validity is ensured by running the smart contract code associated with a transaction, by checking for all required signatures and by assuring that any transactions that are referred to are also valid. Uniqueness concerns the input states of a transaction. Specifically, it has to be ensured that the transaction in question is the unique consumer of all its input states. In other words, there exists no other transaction that consumes any of the same states. The reason for this is to avoid double-spends."*


Pause


Blockchain Technology
Uses Beyond Cryptocurrency
SKOOKUM

WEB 2.0 → WEB 3.0 COMPARISON LANDSCAPE.

WELCOME INTERNET OF BLOCKCHAINS



THE INTERNET OF BLOCKCHAIN FOUNDATION

Matteo Gianpietro Zago

50+ BLOCKCHAIN
REAL WORLD USES CASES

GOVERNMENT
Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government

essentia.one

IDENTIFICATION
Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by **Uport**.

uport

MOBILE PAYMENTS
The blockchain ledger that **Ripple** uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.

ripple

INSURANCE
A smart contract-based blockchain is being used by Insurer **American International Group Inc** as a means of saving costs and increasing transparency.

AIG

ENDANGERED SPECIES PROTECTION
The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.

CARBON OFFSETS
IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.

IBM HYPERLEDGER

ENTERPRISE
Ethereum's blockchain can be accessed as a cloud-based service courtesy of **Microsoft Azure.**

Microsoft Azure

BORDER CONTROL
Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.

essentia.one

SUPPLY CHAINS
IBM and **Walmart** have partnered in China to create a blockchain project that will monitor food safety.

IBM Walmart

HEALTHCARE
A number of healthcare systems that store data on the blockchain have been pioneered including **MedRec.**

MEDREC

SHIPPING
Shipping is a natural fit for blockchain, and **Maersk** have been trialling a blockchainbased project within the maritime logistics industry.

MÆRSK

REAL ESTATE
Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by **Propy**.

PROPY

ENERGY
Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.

essentia.one

LAND REGISTRY
Land registry titles are now being stored on the blockchain in Georgia in a project developed by the **National Agency of Public Registry**.

NATIONAL AGENCY of PUBLIC REGISTRY

COMPUTATION
Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.

DIGITAL CURRENCY GROUP

ADVERTISING
New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.

NYIAX

BORDER CONTROL
Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.

essentia.one

JOURNALISM
Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as **Civil** has shown.

CIVIL

WASTE MANAGEMENT
Waltonchain is using **RFID** technology to store waste management data on the blockchain in China.

ENERGY
Food importation is another industry where blockchain is proving its worth, with **Louis Dreyfus Co** trialling a soybean importation operation using this technology.

LDC

DIAMONDS
The **De Beers Group** is using blockchain to track the importation and sale of diamonds.

De Beers GROUP OF COMPANIES

FINE ART
By storing **certificates** of authenticity on the blockchain, it's possible to dramatically reduce art forgeries, as one blockchain project is proving.

NATIONAL SECURITY
For the past two years, the **US Department of Homeland Security** has been using blockchain to record and safely store data captured from its security cameras.

TOURISM
In a bid to boost its tourism economy, **Hawaii** is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.

TAXATION
In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by **Miaocai Network**.

ENERGY
Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.

CNE COMISIÓN NACIONAL DE ENERGÍA

RAILWAYS
Russian rail operator **Novotrans** is storing inventory data on a blockchain pertaining to repair requests and rolling stock

ХОБОТРАНС

ENTERPRISE
Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by **Alphabet Inc**

Google Alphabet

MUSIC
Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.

arbit

FISHING
Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.

THE INTERNET OF BLOCKCHAIN FOUNDATION

IMPLEMENTING BLOCKCHAIN IN BUSINESS

The blockchain is based on principles of disintermediation, transparency, time and cost efficiency, process integrity, and security.
And this is how exactly businesses benefit from the blockchain principles:

Time & cost efficiency | Security | Transparency | Records keeping | Fraud reduction | Smart contracts | Privacy | Decentralization

BANKING

- Reduced transaction costs and settlement time
- Improved transactions security and data quality

PREDICTION MARKETS

- Low fees
- Safe automated payment
- Accurate forecasting & crowdsourced reporting

INSURANCE

- Eliminating the cost and time of processing insurance claims
- Transparency and relevant records keeping
- Reducing the opportunity for insurance fraud

HEALTHCARE

- Reduced time and increased efficiency in providing insurance quotes
- Tamper-resistant means

GOVERNANCE

- Reducing corruption at state level
- More opportunities for businesses to manage their assets

SUPPLY MANAGEMENT & RETAIL

- Proof of ownership & resale
- Transparency in logistics, storing & real-time tracking each stage
- Increased trust due & information evidence

CAR LEASING

- Reducing time for procurement process
- Simplified leasing process
- Blockchain as the foundation for smart assets

EDUCATION

- Eliminating claims of un-earned educational credits
- Improved verification procedures

https://coincheckup.com/category/digital-currency

Applications of blockchain technology

- There are **so** many applications / use cases to choose from, so I am just going to pick a "few":
  - Electronic Cash / Remittance
  - Logistics / Supply chains
  - Digital Identity management
  - Tokenization
  - Social media
  - Education (courses, grades, diplomas)
  - Supporting the Internet of Things
  - Energy Market
  - Healthcare

Electronic Cash / Remittance

- This is maybe the most obvious case.
- Bitcoin has proved itself over 10 years now as an alternative to traditional money.
- The big hurdle now is scaling. Bitcoin can only process 7 transactions per second, while Visa can process > 1000 t/s. (people work on it)
- Remittance means sending money home. Today, this is a very cumbersome process involving many instances. With cryptocurrencies, this is made really easy.
- Examples:

Bitcoin  Litecoin  Dash  Monero  and many more..

Logistics / Supply chains

https://www.investinblockchain.com/supply-chain-blockchain-projects/

- Traditional supply chain management is inefficient, cumbersome, lacks transparency, traceability and audits.
- Many think that blockchain (and IoT) can solve all of these problems due to properties like:
  - Storing and real-time tracking
  - Transparency
  - Increased data quality
  - Immutability
- Examples:

VeChain  Ambrosus  Waltonchain  OriginTrail  WaBi 

Video supply chain?

- Ambrosus https://www.youtube.com/watch?v=DftD5gTPvWA
- WaltonChain https://www.youtube.com/watch?v=mcxSe56jXqY
- OriginTrail https://www.youtube.com/watch?v=g3gcQAYIMGQ
-

Digital Identity management

https://www.forbes.com/sites/forbestechcouncil/2018/07/27/how-blockchain-can-solve-identity-management-problems/#6a9d5a8413f5

- Most online activities require that you register and disclose personal information (name, address, email, credit card number, etc.).
- This information is stored in many databases, is a problem to keep updated, and is a security/privacy risk.
- Further, this information can be shared with third parties without the user's consent.
- Blockchain can remedy this by letting individuals create and maintain a self-sovereign identity which is used to authenticate the user.
- Examples:

Civic Metaverse ETP TheKey Namecoin Bloom





Video civic/bloom?

- Civic https://www.youtube.com/watch?v=2XDGX41nr1o
- Bloom https://www.youtube.com/watch?v=ntNKcBlw9FU
-

Tokenization

https://blockonomi.com/tokenization-blockchain/

- Tokenization means recording ownership of real world assets (stocks, gold, cars, houses, ...) on a blockchain. The ownership of a token prove the ownership of the real asset.
- Both intangibles, fungible and non-fungible goods can be tokenized
- Some say that "everything will be tokenized"
- This will give undisputed record keeping and easy transfer of ownership.
- It also enables dividing assets into smaller parts. For example can a token represent 1mg of Gold.
- Examples:

DigixDAO 

Cryptokitties (ERC-20) 

Social media

https://www.investinblockchain.com/blockchain-social-media/

- The most popular Social Media platforms today (Facebook, Twitter, Youtube, etc..) are company owned and centralized.
- That also means that they use and sell your personal information (you are the product, the advertisers are their customers)
- That also means that they can censor your posts / comments.
- New distributed Social Media Platforms built on blockchain set out to solve these problems and create alternatives.
- Examples:

Steem

Sapien

Indorse

DTube

Education (courses, grades, diplomas)

- "Using the power of blockchain technology and its smart contract-based payment platform, ODEM will enable students and educators to interact directly and participate in the exchange of education and learning, without the involvement of intermediaries. Our goal is to make quality education more accessible and affordable to a broader audience."
- "BitDegree ... blockchain based reward system and achievement tracking."

- Examples

  ODEM BitDegree

Video ODEM?

- ODEM https://www.youtube.com/watch?v=B278U-V__gs

Supporting the Internet of Things

- Examples
  - IOTA

Energy Market

- Examples:

  PowerLedger WePower Restart Energy Electrify.Asia

Video energy?

- Power Ledger https://www.youtube.com/watch?v=jMqMRs34_u8

Healthcare

- Examples

  Ontology Dentacoin MEDX Medibloc Docademic

- Norwegian? (nødhjelp?, Obos, ...)
- Seminar next week?
- Federated?
- Private?

Technical solutions that enables these applications

- Data storage on the block chain (or just the fingerprint)
- Integration with other systems!
- (IoT-) Devices that provide data.
- Smart contracts! (Ethereum / EOS / i morgen)
- An market for valuation / exchange / trading of tokens.
- Infrastrucure (mobile apps, web apps, wallets, ...)

- Second layers? for scaling
- DAG / Tangle? for scaling

Kursbevisgreiene til Svein / MIT

- Se på noen passasjer (fra erfaringsdokumentet) og se om de forstår det.
- Et eksempel på at man faktisk kan bruke Bitcoin-nettverket til å lage kursbevis som ikke kan forfalskes

The blockchain ecosystem

- The is a whole industry that is built up around these new blockchain solutions.
- For developers, the job opportunities will not only be in blockchain companies, but also in companies in this ecosystem.

- I found some infographics from 2015 that lists some of types of emerging businesses.
  (There are probably more, and the growth since 2015 has been exponential)

http://www.visualcapitalist.com/the-bitcoin-universe-explained/

WALLETS

"At Coinbase, we're excited about the progress made thus far but we're still in the early days of the technology and even more excited about the app ecosystem and what the future of Bitcoin applications will look like."

Adam White
VP of Business Development, Coinbase

http://www.visualcapitalist.com/the-bitcoin-universe-explained/

STORAGE

"Bitcoin paved the way to decentralized security, and will jumpstart the usage of personal privacy devices."

Eric Larchevêque
CEO, Ledger

"Today there are more than 100,000 Bitcoin transactions per day for more than $100 million and there are more than 5,000 servers acting as nodes of the network. Bitcoin is a lot less likely to disappear today than it was 2 years ago when the price was over $1,000 per Bitcoin."

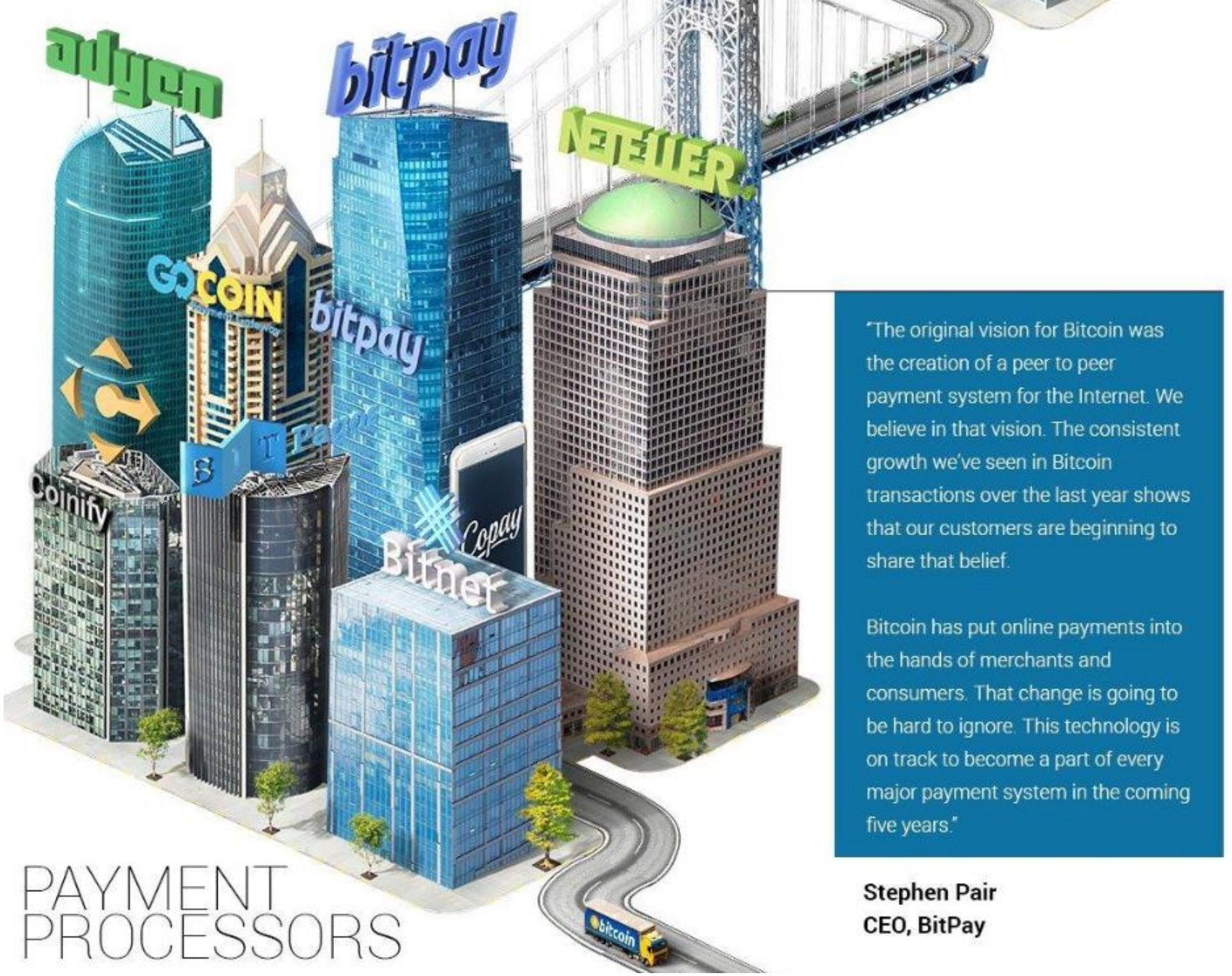
http://www.visualcapitalist.com/the-bitcoin-universe-explained/

EXCHANGES

"Bitcoin startups like Gemini are ushering in a new chapter of legitimacy and integrity that will allow Bitcoin to go mainstream and fulfill its ultimate promise."

Tyler Winklevoss
Co-Founder and CEO, Gemini

http://www.visualcapitalist.com/the-bitcoin-universe-explained/



http://www.visualcapitalist.com/the-bitcoin-universe-explained/

http://www.visualcapitalist.com/the-bitcoin-universe-explained/

http://www.visualcapitalist.com/the-bitcoin-universe-explained/

MEDIA & ADVOCACY

"We are privileged to be at the nexus where information meets technology, using a multimedia platform to support the adoption and innovation of Bitcoin and the blockchain. In only two years, the audience for digital currency news has exploded from Fintech specialists to the man on the street. This is now a mainstream media topic, and what happens in Bitcoin happens to the world."

David Bailey
CEO, BTC Media

http://www.visualcapitalist.com/the-bitcoin-universe-explained/

DEVELOPER TOOLS

"It's exciting to be a part of the growth and maturation of the blockchain and Bitcoin ecosystem. Previously we saw products geared towards true believers or technical wizards. We are beginning to see practical, intuitive applications being built for real mainstream users with intuitive, consumer friendly user experiences. This shift has allowed financial institutions, corporations and regulators to take a second look, embracing a platform they once resisted."

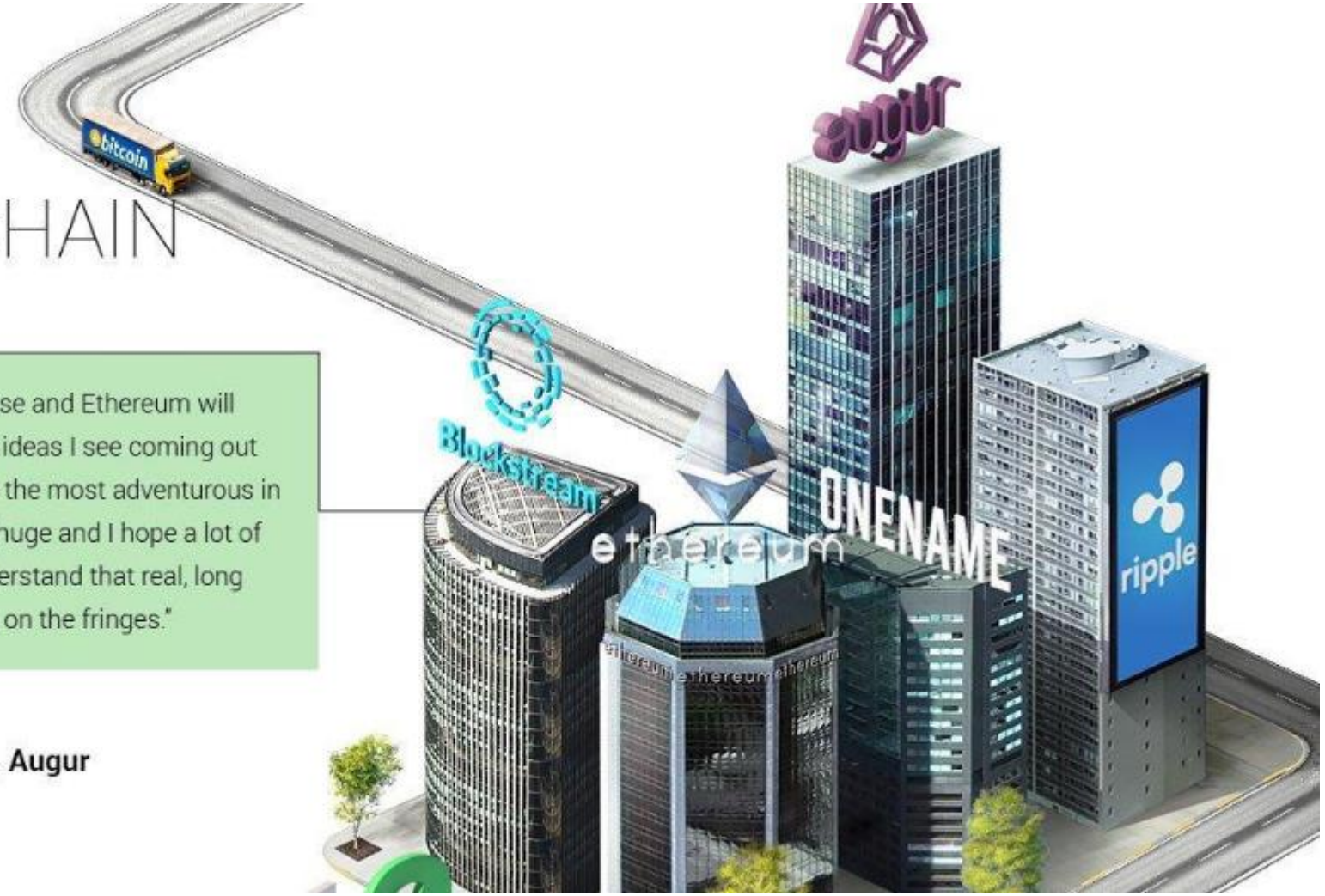
Justin Newton
CEO, Netki

http://www.visualcapitalist.com/the-bitcoin-universe-explained/

BLOCKCHAIN TECH

"Bitcoin will serve a purpose and Ethereum will serve a different one. The ideas I see coming out of it are immense and are the most adventurous in years. The opportunity is huge and I hope a lot of the investment types understand that real, long term money is happening on the fringes."

Tony Sakich
Director of Marketing, Augur



http://www.visualcapitalist.com/the-bitcoin-universe-explained/

FINANCIAL SERVICES

"Bitcoin use is continuing to grow across borders. 12% of our users, all of whom are international receiving wages from US employers, encompass over 50% of our volume. While we continue to see growth with domestic employees receiving wages from the like of Google, Microsoft or even the U.S. Navy, we foresee the international use-case growing significantly over the next few years until the value of Bitcoin stabilizes."

Jonathan Chester,
Founder & President, BitWage

http://www.visualcapitalist.com/the-bitcoin-universe-explained/

Next

- Tomorrow
  - Smart contracts ++
- Oblig3 ... in by the end of the week