

# Blockchain Technology: An Introduction (from an agrifood perspective)

Christopher Brewster

[christopher.brewster@tno.nl](mailto:christopher.brewster@tno.nl)

Workshop 'Blockchain voor Agrifood' Utrecht, 23 November 2016

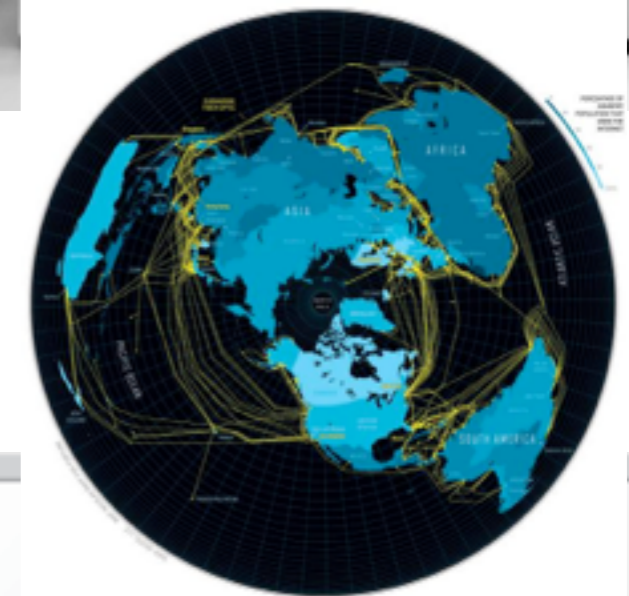
# Blockchain and Bitcoin

- ▶ Origins lie in Bitcoin - Bitcoin was developed as *cryptocurrency* - a technological alternative to *fiat* currencies (dollar, euro, pound)
  - ▶ An attempt to be an anonymous “Bank of the Internet” or Paypal
  - ▶ Finite number of Bitcoins supposedly provides *gold-standard* type guarantee against inflation
- ▶ Bitcoin depends on the *bitcoin Blockchain* to function
  - ▶ All Bitcoin transactions are recorded on the bitcoin blockchain
  - ▶ The blockchain is the infrastructure upon which bitcoin rests
  - ▶ Every 10 min a new block is add by “miners” (who consume huge amounts of energy)



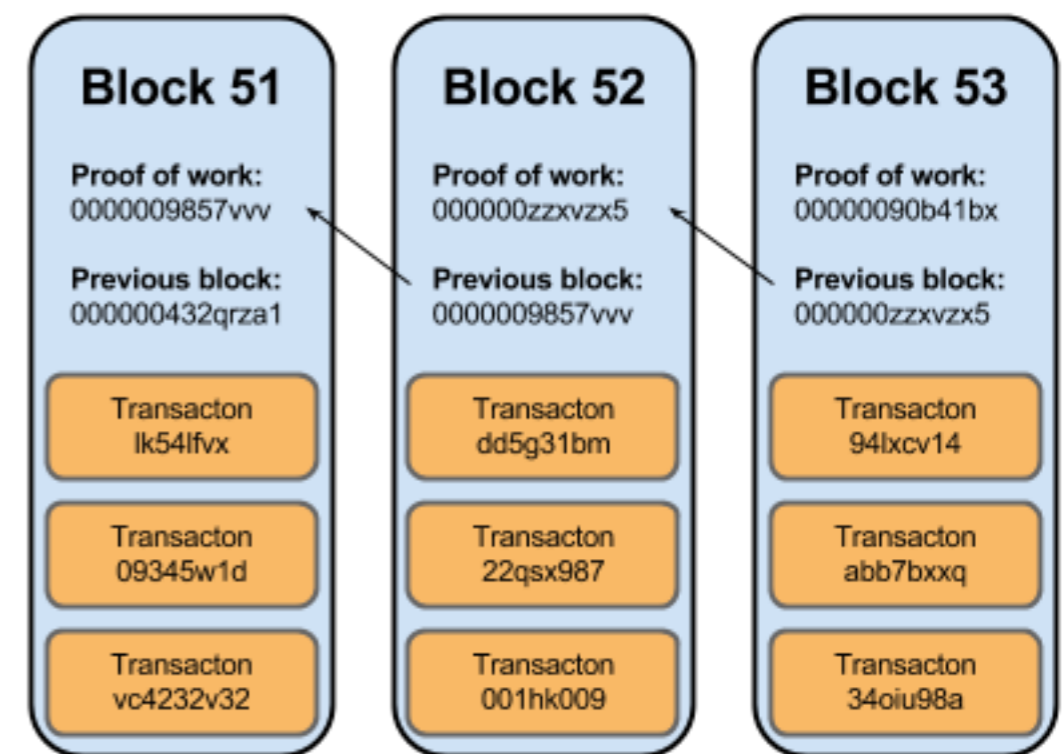
# In the beginning ...

- ▶ There was the database ....
- ▶ ... and then there was the network
- ▶ PUT THEM TOGETHER
- ▶ Gives us first “cloud computing”
- ▶ ... and now “blockchain” technology



# What is a blockchain?

- ▶ A blockchain is a simply **database** but ....:
  - ▶ Distributed across the network (Internet) - everyone has a copy
  - ▶ Auto-synced - every copy is the same almost instantly
  - ▶ Nothing can be deleted
  - ▶ Commonly open and public - everyone (authorised) can add
- ▶ **AND** currently *very slow throughput, very low capacity*

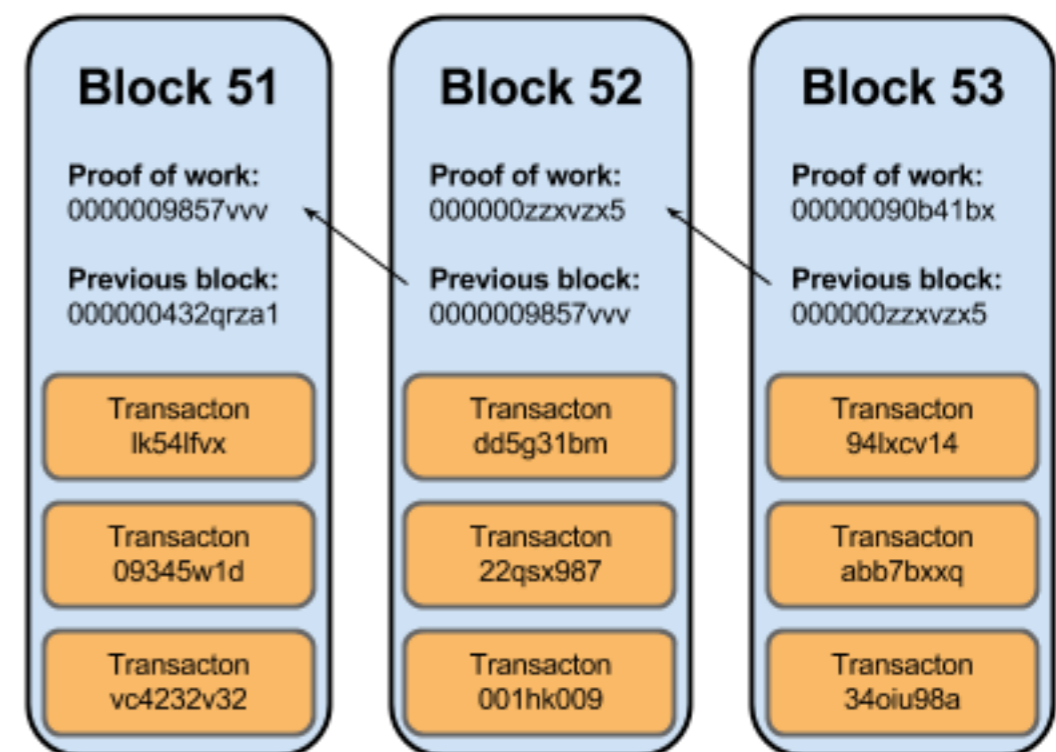


**Blockchain technology is otherwise known as Distributed Ledger Technology (DLT)**



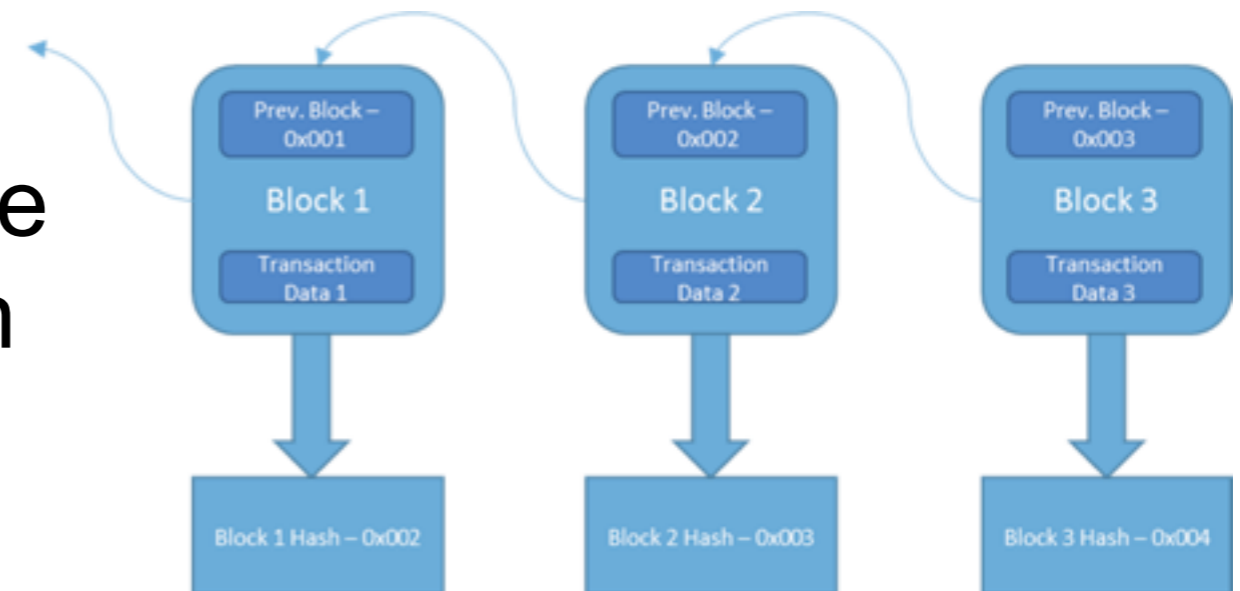
# What is a “block”?

- ▶ A block consists of a set of database transactions placed in a “block”
- ▶ The blocks are shared in a distributed and decentralised manner i.e. each “node” has a complete set of blocks
- ▶ In theory, everyone can see all transactions (complete transparency)



# What is a chain?

- ▶ Each block is linked to the previous block via a hash function. This means you cannot change a block without breaking the chain.
- ▶ Each block is cryptographically signed as well.



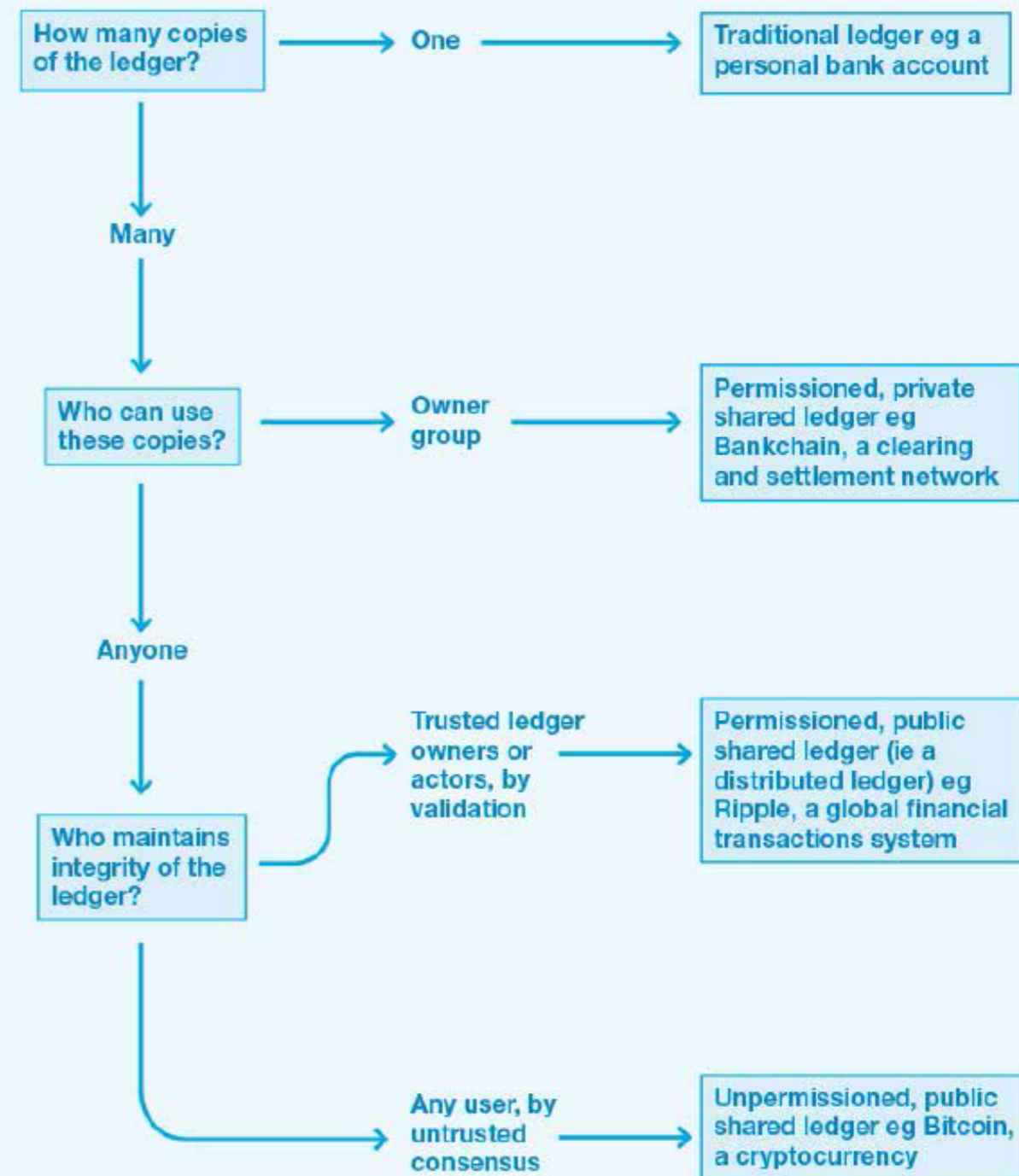
# Important Blockchain Characteristics

- ▶ Very secure due to use of cryptography
- ▶ Capable of near real-time synchronisation or settlement
- ▶ Very low transaction costs (only partially true)
- ▶ Typically based on open source software - changes are developed by the community
- ▶ Transparency and traceability of transactions is typically superior to current systems but user identification may be weaker or nonexistent

# Permissioned vs. Unpermissioned Blockchains

- ▶ Bitcoin uses an **public unpermissioned** blockchain meaning anyone can. Trust is achieved through mining.
- ▶ Other options possible including permissioned/public, permissioned/private, and a traditional ledger e.g. bank account.

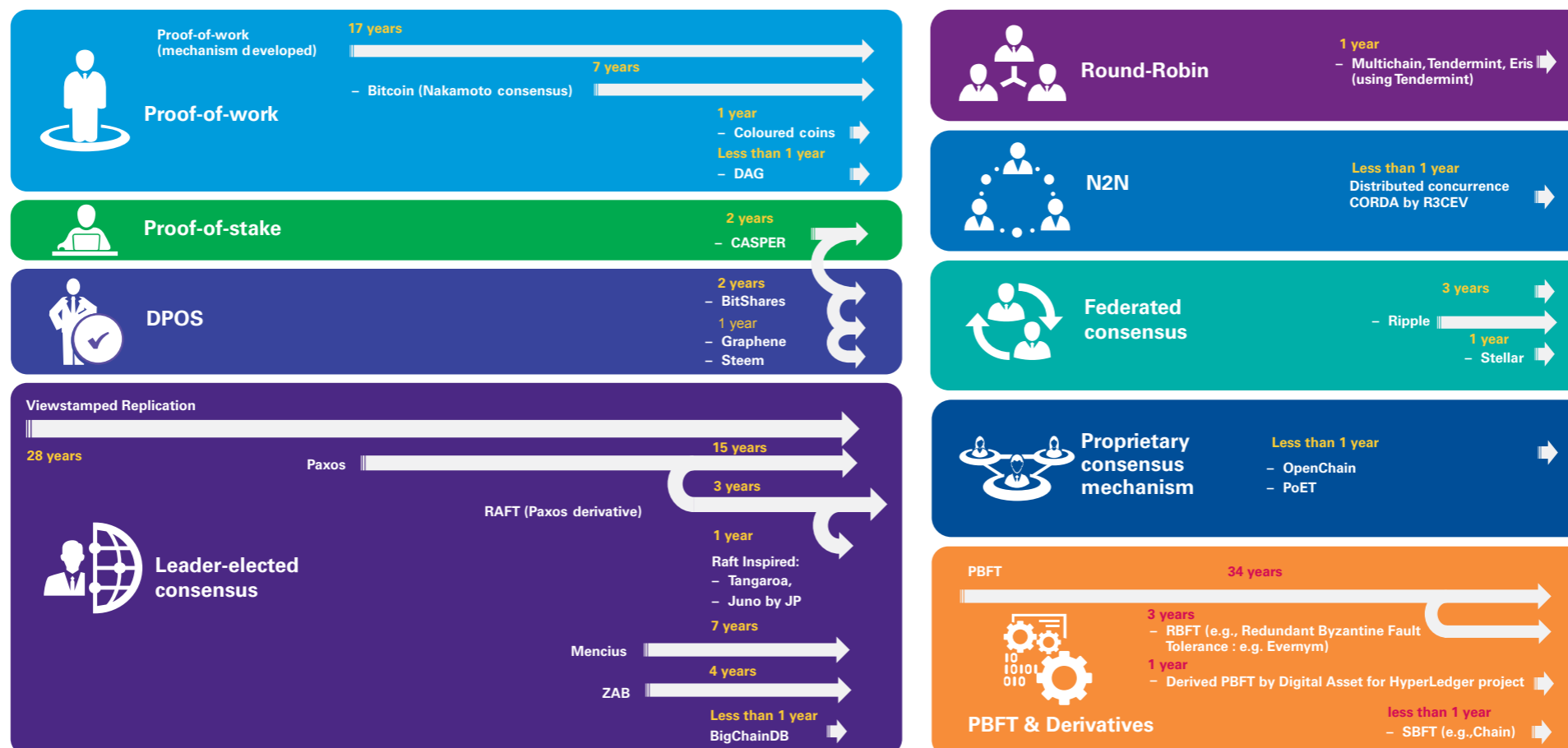
## Distributed Ledger Taxonomy





# Consensus and Governance

- ▶ Part of the intention with blockchain technology is to write the governance into the code
- ▶ The consensus algorithm is a key aspect of the governance of any blockchain - and there are several different kinds



# Key Feature: Permanent Ledger

- ▶ “Nothing can be deleted ....”
- ▶ The blockchain as a distributed write only ledger is an ideal repository for certain types of data
- ▶ Ideal for reducing some kinds insurance fraud
  - ▶ Record auto accidents so only one claim can be made
  - ▶ Record valuables so that no fraudulent claims are possible
  - ▶ Tracking art works across chains of custody

# Key Feature: Transparency and Trust

- ▶ All transactions on a blockchain can be visible (to everyone or to the selected parties)
- ▶ Immediate visibility (replication) of all transactions means no third party is needed
- ▶ “The transparency of this distributed ledger virtually eliminates fraud, which further reduces the costs of doing business for all parties involved.” — Jason Leibowitz

# Example technology: Ethereum

- ▶ Etheruem (<https://www.ethereum.org>) is a programmable smart contract platform, using *ether* as its unit of currency.
  - ▶ Also very slow, guaranteed uptime computer!
- ▶ Example of Blockchain 2.0 - creating platforms
- ▶ Started by Vitalik Buterin and Gavin Wood
- ▶ Presold \$15M worth of *ether* which has funded its development.
- ▶ Major visibility and public backing, e.g. now available on Microsoft Azure.



# Key feature: Smart Contracts

- ▶ A smart contract is a software implementation of legal contract. Originally developed by Nick Szabo in early '90s
- ▶ Idea is to transfer contractual obligation onto an impersonal software system
- ▶ Much excitement now that one can “run” smart contracts on the blockchain
- ▶ Bitcoin includes a form of smart contacts. **Etheruem** is an infrastructure to run a VM for smart contracts

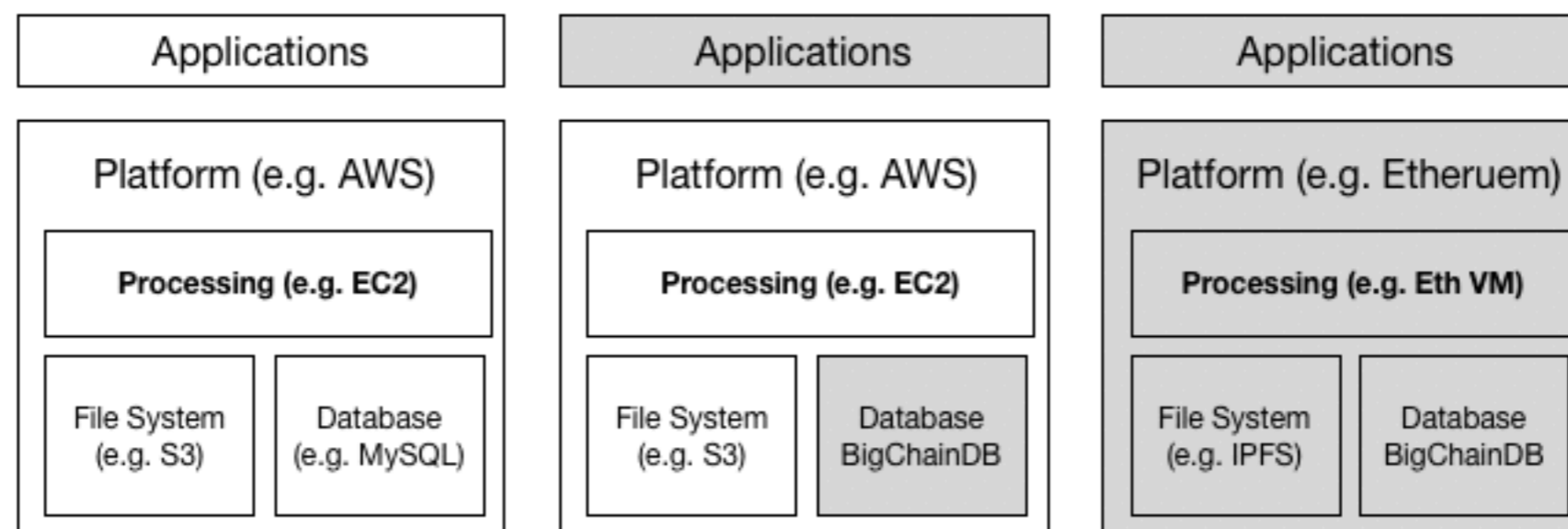
```

note: *** An Ethereum smart contract to sell a website for "5000 by March"
note: First, store buyer's ethereum address:
put 6af26739b9ffef8aa2985252e5357fde in storage slot BUYER
note: Then, store seller's ethereum address:
put feab802c014588f08bfee2741086c375 in storage slot SELLER
note: April 1, 2014 is 1396310400 in "computer time"
put 1396310400 in storage slot DEADLINE
note: If the agreed amount is received on time...
when transaction value ≥ 5000 ether
  and block timestamp ≤ storage slot DEADLINE
then
  note: ... then designate the buyer as the new website admin and pay the
  put storage slot BUYER in storage slot WEBSITE_
  spend contract balance to storage slot SELLER
  
```



# Example Technology: BigChainDB

- ▶ BigChainDB (<https://www.bigchaindb.com/>) is an attempt to solve the throughput challenge.
- ▶ BigChainDB provides a “blockchain” layer over a conventional DB (currently RethinkDB, soon MongoDB).
- ▶ Claims to handle 1m transactions per second
- ▶ Open source, under active development



# Real Examples (1)

- ▶ Everledger (<http://www.everledger.io/>)  
- Eris based permanent record of all **diamonds** to ensure authenticity and provide a record against fraudulent insurance claims.
- ▶ Dynamis (<http://www.dynamisapp.com/>) - Ethereum based, uses LinkedIn as social network and oracle to provide **unemployment insurance**



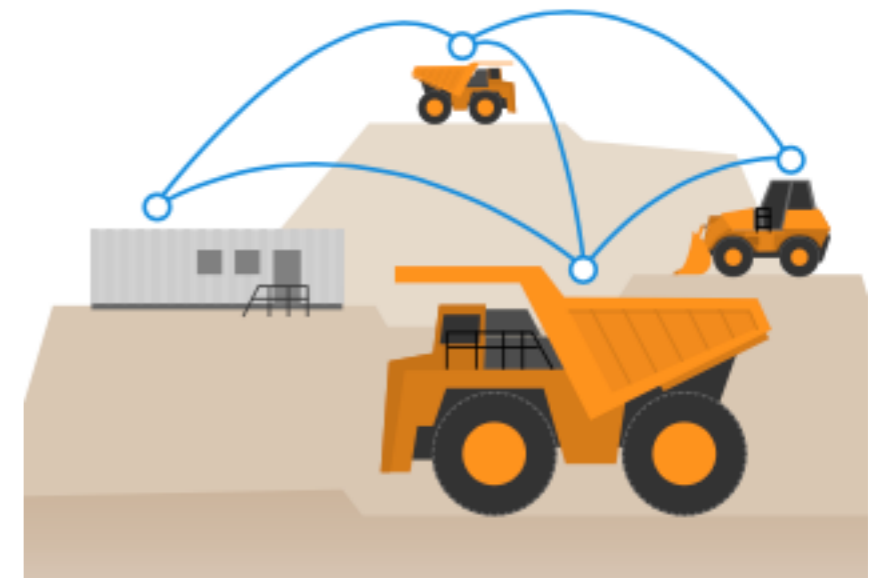
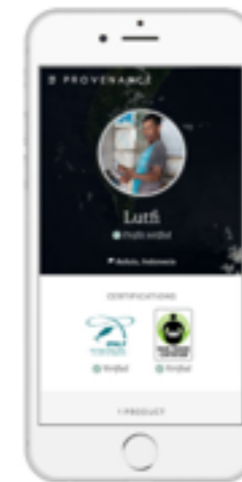
# Real examples (2)

- ▶ InsurEth (<http://insureth.mkvd.net/>) - Ethereum based flight insurance - contract runs on the Ethereum blockchain
- ▶ Augur (<http://www.augur.net/>) - Ethereum based prediction market



# Examples in agrifood

- ▶ Provenance.org (<https://www.provenance.org>) Ethereum based, focus on traceability and transparency, wants to “tell the story” of food, uses blockchains to guarantee trust.
- ▶ Filament (<https://filament.com>) wants to use blockchain for agricultural asset tracking.

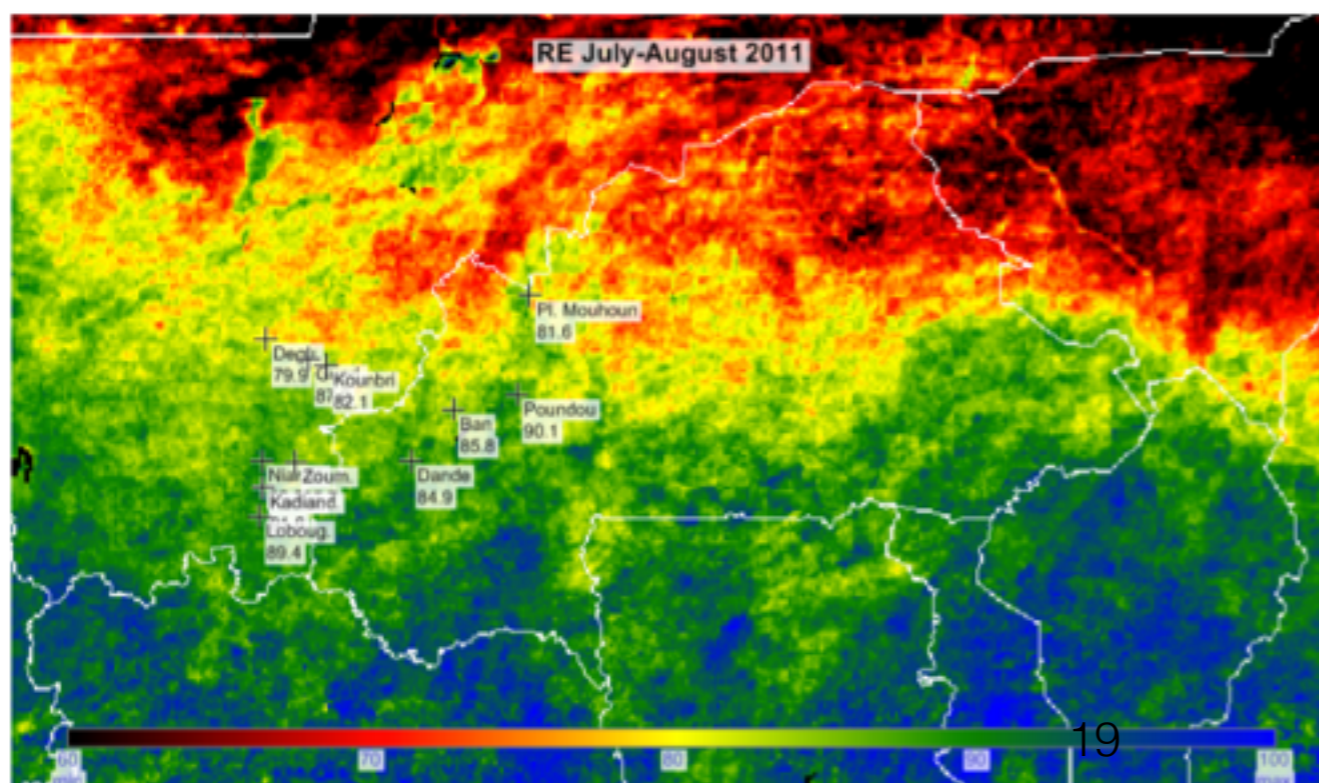
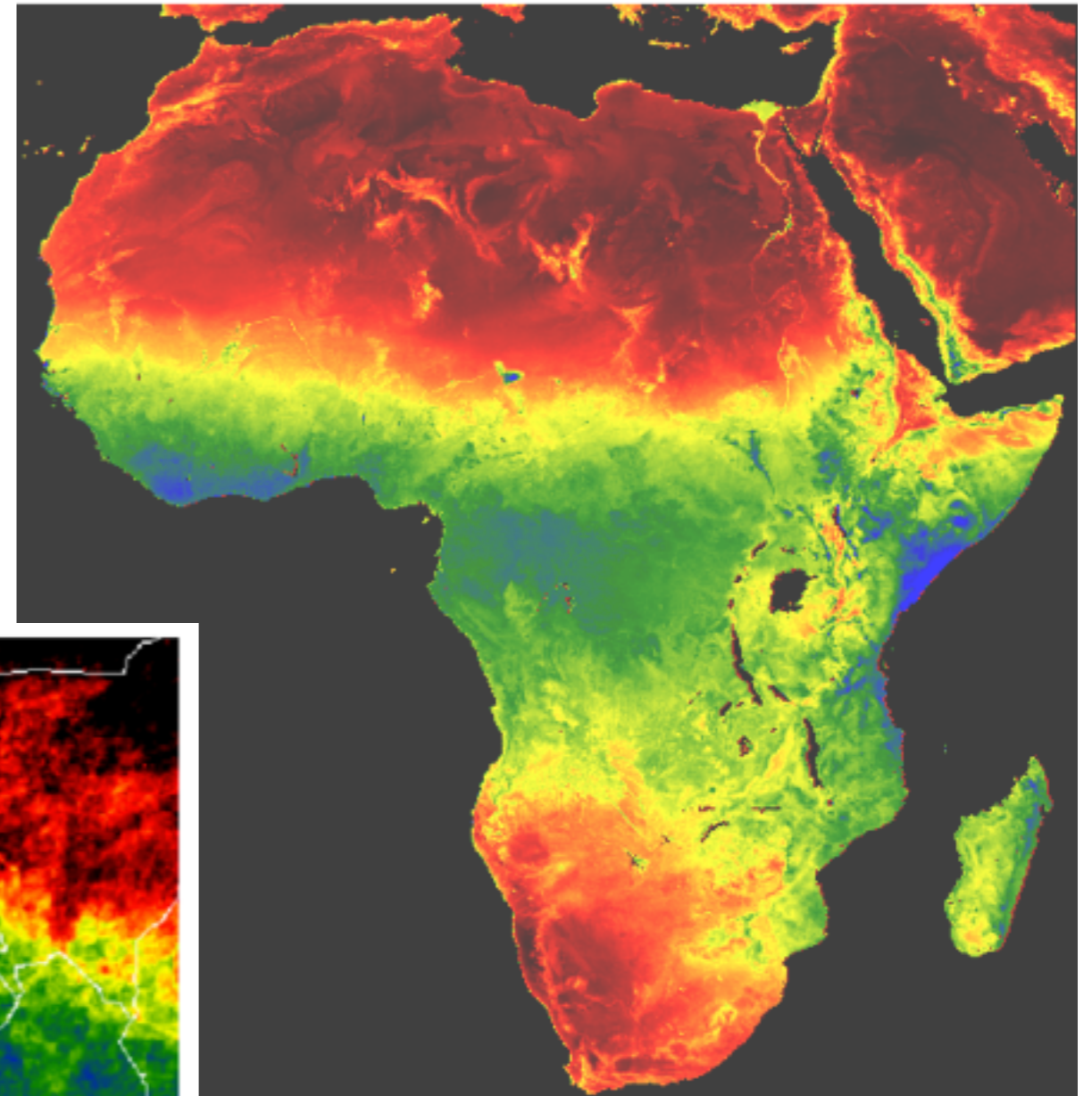


- ▶ SkuChain (<https://www.skuchain.com>) want to track containers and transport shipments using blockchains
- ▶ FarmShare (<http://farmshare.us>) want to build decentralised community support agriculture





# Crop Insurance: A hypothetical example



- EARS <http://www.ears.nl/>

# Conclusions: Blockchain Benefits

- ▶ **Decentralized / shared control** - situations where enemies need to work together for their mutual benefit, e.g. banks, perhaps in agrifood supply chains
- ▶ **Immutability / audit trail** - situations where it is of prime importance to have an immutable audit trail, where users cannot change data post hoc, e.g. Everledger for diamonds, perhaps for certification in agrifood
- ▶ **Assets / exchanges** - situations where the assets can live on the blockchain e.g. stock exchanges, currency or energy exchanges, perhaps for local agrifood marketplaces.

# Thank You

# QUESTIONS

# Further Reading/Links

- ▶ Walport, M. (2016) Distributed Ledger Technology: Beyond Blockchain Government Office for Science, URL: <https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review>
- ▶ The Future of Financial Services, World Economic Forum - [http://www3.weforum.org/docs/WEF\\_The\\_future\\_of\\_financial\\_services.pdf](http://www3.weforum.org/docs/WEF_The_future_of_financial_services.pdf)
- ▶ Huckstep, R. (2016) What's in Store for Blockchain? URL: <http://insurancethoughtleadership.com/whats-store-blockchain/>
- ▶ Rafiee, A. (2015) The Art of Forecasting: Augur's Decentralized Prediction Market URL: <http://bitcoinist.net/art-forecasting-augur-decentralized-prediction-market/>
- ▶ Redman, J. (2016) Six Ethereum Projects and its Five Competitors URL: <http://bitcoinist.net/six-ethereum-projects-and-its-five-competitors/>
- ▶ Gilbert, S. (2016) Innovation Blog: The Hype Cycle of Insurance Disruption URL: <http://www.insurancetimes.co.uk/innovation-blog-the-hype-cycle-of-insurance-disruption/1417196.article>
- ▶ Grewal-Carr, V. & Marshall, S. (2016) Blockchain, Enigma, Paradox, Opportunity Deloitte, URL: <http://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf>
- ▶ Vaughan, W. (2015) Improving Insurance with the Blockchain URL: <https://tierion.com/blog/improving-insurance-with-the-blockchain/>
- ▶ <http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable>
- ▶ <http://www.disledger.com/kpmg-blockchain-consensus-mechanism.pdf>

# Acknowledgements

- ▶ Thanks are due to Vinay Gupta, Oskar van Deventer, Trent McConaghy, Lan Ge, among others
  
- ▶ Image credits:
  - ▶ <https://commons.wikimedia.org/wiki/File:Bitcoin.png>
  
  - ▶ <https://www.flickr.com/photos/fdecomite/11464052775/in/gallery-gamingfloor-72157638888166706/>
  
  - ▶ <https://commons.wikimedia.org/wiki/File:CumaeenSibylByMichelangelo.jpg>
  
  - ▶ <http://nicolasrapp.com/portfolio/211/>
  
  - ▶ <http://avant.org/project/history-of-databases/>