



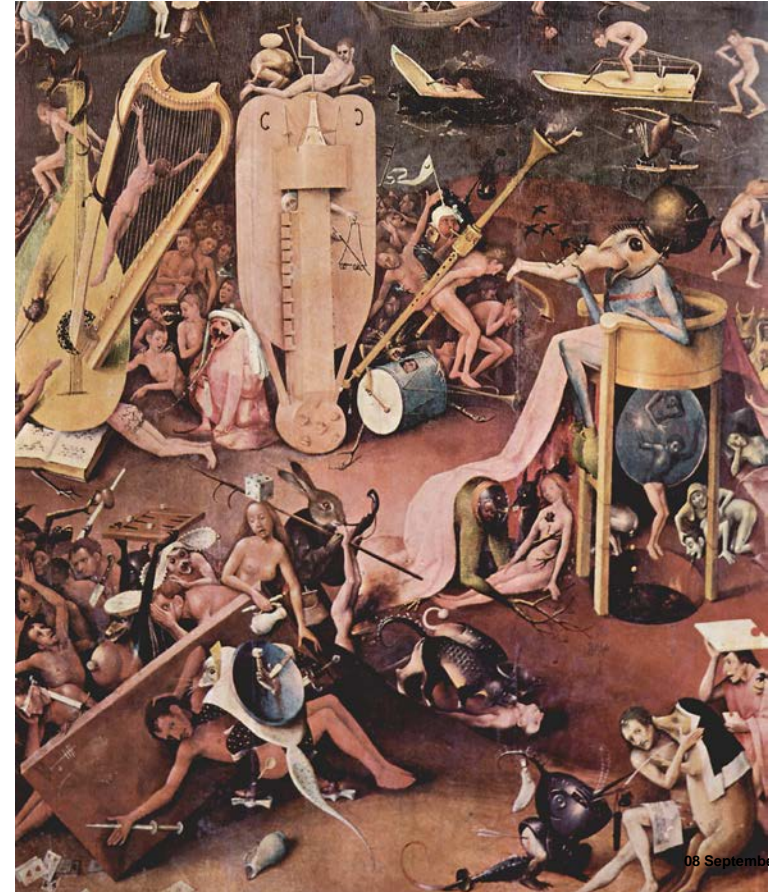
› BLOCKCHAIN TECHNOLOGY AND FRAUD IN THE AGRIFOOD SECTOR

Opportunities and challenges | Dr. C.A.W. Brewster

TNO innovation for life

OUTLINE

- › The promise of blockchain technology
- › The political origins and assumptions
- › Current interest in agrifood
- › The challenge of the physical to digital interface – and abuses of CAP
- › Cautionary conclusions



BLOCKCHAIN AND DISTRIBUTED LEDGERS

- › A distributed, decentralised, shared database (ledger)
 - › Distributed across the network – every participant has a complete copy
 - › Every copy is the same almost instantly
 - › No transaction can be deleted
 - › Usually open and public – everyone can add transactions
- › Strong political dimension to blockchain technology
 - › Smart contracts and distributed autonomous organisations
 - › Desire to remain outside government control
 - › Hugely optimistic about automation of all human activity and “tokenisation



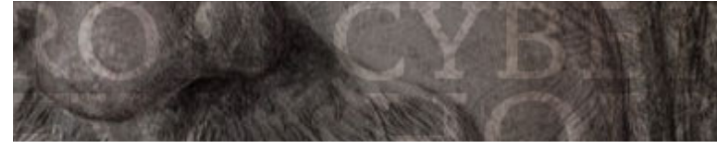
CORE DESIGN CHOICES IN BLOCKCHAINS

- › **Permission design** – open, unpermisioned vs. closed, permissioned
- › **Choice of consensus algorithm** – proof or work vs. proof of stake vs. other options
- › **Smart contracts** – very sexy but cause a lot of problems
- › **Use of a cryptocurrency** – depends on the choice of consensus algorithm mostly
- › **Governance** – who has the final say, who unplugs the blockchain or forces a hard fork.



THE POLITICS OF BLOCKCHAIN

- › Origins of Bitcoin and blockchains lie in libertarian and cypherpunk movement
 - › Eric Hughes - *A Cypherpunk's Manifesto*
 - › Barlow's *A declaration of independence of Cyberspace*
 - › The Crypto Wars of 1990s – attempts by US/UK government to prevent widespread use of cryptography
- › Principles
 - › Privacy of communications
 - › Anonymity
 - › Opposition to censorship
 - › Strongly anti-government



A Declaration of the Independence of Cyberspace

by John Perry Barlow

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

<https://www.eff.org/cyberspace-independence>

MONETARY INDEPENDENCE

- › Cypherpunk closely related to US libertarian tradition
 - › Anti-government in any form *except to protect private property!*
 - › Best known modern cypherpunk is Julian Assange
- › Monetary independence
 - › Early example was E-gold (<https://www.wired.com/2009/06/e-gold/>)
 - › Major argument for Bitcoin was independence from government - wanting to be the “bank of the internet”
 - › Bitcoin was design so that there could be no “printing of money”
 - › No inflation considered as a key benefit.
- › Julian Assange’s Wikileaks problems were major driver for Bitcoin uptake – when Visa/Mastercard/Paypal stopped transactions 2011

<http://www.cs.ru.nl/~jhh/pub/secsem/chaum1985bigbrother.pdf>

ARTICLES

SECURITY WITHOUT IDENTIFICATION: TRANSACTION SYSTEMS TO MAKE BIG BROTHER OBSOLETE

The large-scale automated transaction systems of the near future can be designed to protect the privacy and maintain the security of both individuals and organizations.

DAVID CHAUM

Computerization is robbing individuals of the ability to monitor and control the ways information about them is used. As organizations in both the private and the public sectors routinely exchange such information, individuals have no way of knowing if the information is inaccurate, obsolete, or otherwise inappropriate. The foundation is being laid for a dossier society, in which computers could be used to infer individuals' life styles, habits, whereabouts, and preferences.

for machine-readable national identity documents gaining momentum. But organizations already use essentially identifying data as name, date, and place of birth or name and address to match or link their records on individuals with those maintained by other organizations.

With the new approach, an individual uses a different account number or “digital pseudonym” with each organization. Individuals will create all such pseudonyms. Information fur



POLITICAL INDEPENDENCE

- › Major argument for blockchain is to create systems outside government control
- › Closely related to focus on removing “third party”
- › In libertarian universe, government and government actors are always bad
- › Smart contracts eliminate third parties e.g. lawyers, notaries, banks, insurance companies
- › Concept of “self sovereign identity” (blockchain based identity management) again seeks to remove government as prover of identity

<https://goo.gl/gcyAuN>



<https://goo.gl/kJyK8G>

NONETHELESS

BLOCKCHAIN EXPLOSION 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.
- › Agriledger (<http://www.agriledger.com/>) “Blockchain for the greater good” → blockchain + network + “framework of trust” + cheap smartphones
- › Origin Trail (<http://origin-trail.com/>) “genuine transparency to stand out in the marketplace and increase trust in your brand” → “A global platform for building transparency in supply chains.”
- › Arc-Net (<http://arc-net.io/>) “a secure, immutable, trusted chain of custody for a product or asset” → “Enhancing Brand Protection and Consumer Loyalty”
- ›and many more



THE PROMISE: WHY BLOCKCHAINS IN AGRIFOOD?

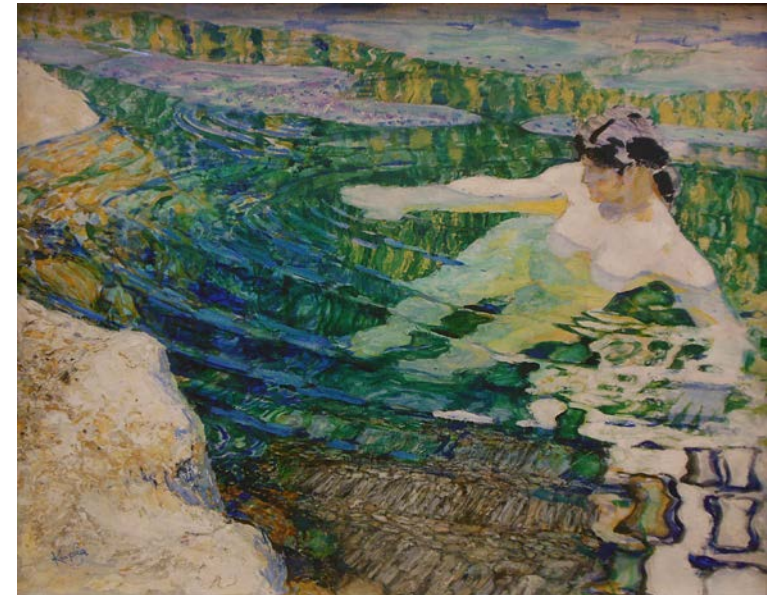
- › Partly due to general hype that Blockchain is a solution to everything
- › Partly due to the perception that Blockchain is a “universal database that all actors can transparently read and write to”.
- › Partly due to ignorance - e.g. belief that it would be easy to put lots of data on the blockchain and control access (neither are true)



BENEFITS: TRANSPARENCY

- › All transactions on a blockchain are visible (to everyone ... or to selected parties)
- › Immediate visibility (replication) of transactions means no third party is needed (... considered a virtue)
- › Transparency of ledger eliminates fraud (it is claimed)
- › Transparency = trust (or elimination of need for trust)

- › **Claims in the agrifood context:** transparency of the food supply chain, tracking and tracing, transparency of inputs and outputs
 - › **And here fraud and corruption in state funding**



BENEFIT: IMMUTABILITY

- › All transactions written to the blockchain are immutable/cannot be changed
- › Immutability also guarantees avoidance of fraud or tampering
- › **Claims in the agrifood context:** food fraud can be eliminated, environmental reporting can be made more effective (Dutch manure case)
 - › Usually food fraud is understood to concern the supply chain not government subsidies.
 - › The question is where is “mutability” the key problem in fraud.



BENEFITS: ROBUSTNESS & DECENTRALISATION

- › Because the database is distributed, it cannot fail
 - › No single point of failure
 - › No single point of control
- › Helpful when competitive/enemy parties need to work together
- › **Claims in the agrifood context:** Supposed to lower costs, increase independence of the sector, increase efficiency
 - › **In my experience no evidence that this is true!**
 - › **BUT WEF have published a white paper saying for logistics potential major cost reduction:**
http://www3.weforum.org/docs/WEF_White_Paper_Trade_Tech_.pdf



BENEFIT: SMART CONTRACTS

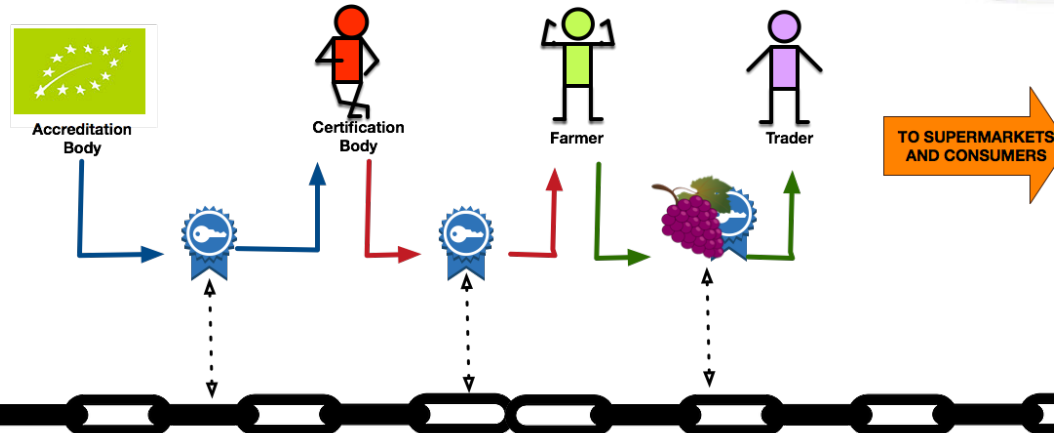
- › A smart contract is a software implementation of legal contract. Originally developed by Nick Szabo in early '90s
- › Idea is to transfer contractual obligation onto an impersonal software system
- › Much excitement now that one can “run” smart contracts on the blockchain
- › Ethereum first to provide an infrastructure to run a VM for smart contracts. Many other frameworks have followed.
- › Huge technical problems – errors and software failures
 - › **HOWEVER somewhat attractive for CAP disbursements for example**



EXAMPLE USE CASE: CERTIFICATION OF TABLE GRAPES

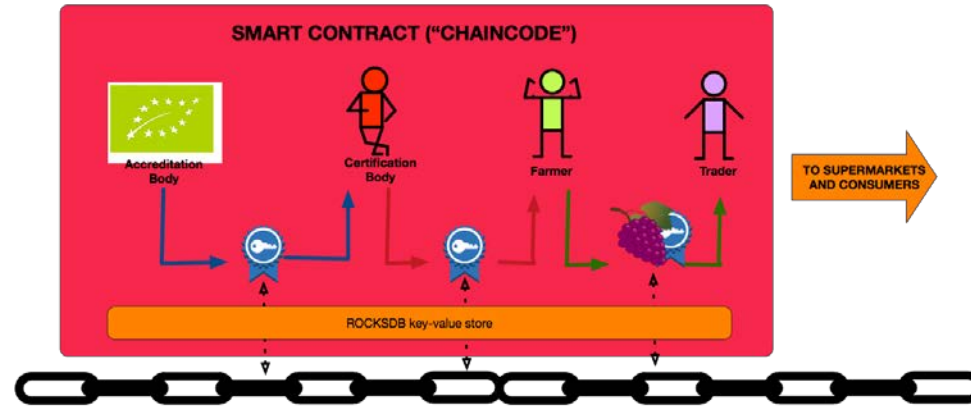
WUR/TNO TABLE GRAPE POC

- › Small project in collaboration with WUR, funded by Dutch EZ Ministry (2017)
- › Based on previous work on the table grape supply chain from South Africa to the Netherlands.
- › Objective to demonstrate that grape certifications (organic, Fairtrade) can be managed on a blockchain



TECHNICAL DESIGN

- › Built with Hyperledger 0.6 on a permissioned blockchain.
- › Using a smart contract (“chaincode”) written in GO lang. Each SC in its own docker container.
- › Business relationships encapsulated in the smart contract.
- › Allows update and query of data (e.g. using identifier of box of grapes)
- › Data is stored in a key-value store (RocksDB for v0.6)
- › Code is open sourced (<https://github.com/JaccoSpek/agrifood-blockchain>)



LIMITATIONS

- › Scalability
 - › Technology in constant development, but we do not know how this will perform with very large numbers of transactions.
 - › Similarly, we do not know, yet, how this will perform with many participants/nodes.
 - › Millions of agrifood transactions per day, all recorded on a blockchain may cause cumulative disk space issues
- › Visibility
 - › We can control data access to these participants within a smart contract. This means a different set of partners needs a different smart contract.
 - › Current versions of Hyperledger Fabric have similar problem
- › Digital to physical interface
 - › Does not prevent GIGO (Garbage in, garbage out)

BO AGRO: CURRENT PROJECT: ADDING SEMANTICS TO MANAGE BUSINESS LOGIC

- › Richer more complex set of data points
- › Using semantics (OWL, SHACL) to manage the business logic (e.g. enforce specific rules on the data)
- › Removes need for “smart contracts”, while retaining immutability of data.
- › Data is annotated with metadata concerning the ontology and rule set (in SHACL) used – all written on the blockchain
- › Uses BigchainDB, more scalable, more flexible.
- › **Governance remains key!**



BIGCHAIN 



FUNDAMENTAL FRAUD PROBLEM: DIGITAL TO PHYSICAL INTERFACE

TYPICAL ABUSES OF CAP (ANECDOTAL)

- › Group buys equipment it previously owned, carries on using it as before.
- › Group buys second hand equipment, subsidized for new equipment.
- › Abuse of three quotation rule for private procurement.
- › Subsidy claimed for building barn used to build personal home, subsidy for “agritourism” used to build own home.
- › Company A buys digger with subsidy, then asks for subsidy for lorry. Upon refusal, own founds company B to request subsidy for truck. Upon agreement, truck is used exclusively for Company A.
- › Company A gets subsidy for modernising winery. Then asks for subsidy for bottling plant. Upon refusal, company splits into A + B, and company B applies successfully for bottling plant subsidy.
- › Farmer seeks subsidy for tourism houses but to avoid subsidy limit, splits request into 5 (Famer, wife, 3 X sons)



Personal communication from ex-OPEKEPE employee
(Greece)

PHYSICAL TO DIGITAL INTERFACE

- › If fraudulent activity occurs before registering in the digital domain, very hard to identify or control.
- › For example, if non-organic grapes are bought by farmer and sold as his, hard to spot. It is claimed that 30-50% of “organic” food is not!
- › In CAP, if a family has 2-3 companies is that intentional fraud, or tradition/habit, or just good “tax planning”?



https://www.washingtonpost.com/business/economy/the-labels-said-organic-but-these-massive-imports-of-corn-and-soybeans-werent/2017/05/12/6d165984-2b76-11e7-a616-d7c8a68c1a66_story.html

WHAT IS NEEDED TO SPOT FRAUD?

- › Complete transparency ideally! But in reality
- › For organic grapes: we need to know the size of farm, to calculate probable crop quantity. Can only be an approximation due to crop variety, weather and soil variability! **Approximately doable!**
- › For a farmer asking for multiple subsidies: We need a complete profile of family member, social network, relations of **patronage** and back-scratching, etc., etc. **Very very hard to do accurately.**
 - › **Impossible without a significant level of surveillance on a major part of our society.**
 - › **Blockchain technology is largely irrelevant here.**



A RECENT EXAMPLE: SLOVAK AGRICULTURE PAYING AGENCY (ACCUSATIONS)

- › **Babindol:** Many grants and subsidies when to a small group of people from one village.
 - › They all had strong connections to the party in power.
 - › Subsidies used in some cases for agribusiness, in some cases not.
- › **Kuciak:** Entry of Italian mafia to abuse of rural funds in Slovakia.
 - › Major demand for transparency – “ensure that the Agricultural Payment Agency pays farm subsidies only to an entity that has a valid legal relationship to the subsidized land”

Home News Politics Justice & Home Affairs Slovak farmers drive tractors into car

Slovak farmers drive tractors into car subsidy fraud

By George Geroni | EUNACTV.com with AFP



Suspicious "rural entrepreneurs" involved with Smer emerge in Nitra

Successful businesspeople from the village of Babindol who have received subsidies from EU funds worth millions have connections to the ruling Smer party.

Workers harvest grapes at Jaroslav Ostorozovic's vineyard in the Slovakian part of the Tokaj wine-growing region near Mala Trna, Slovakia | Attila Balazs/EPA

OLAF examines alleged abuse of EU funds in Slovakia

Irregularities were raised by murdered journalist Ján Kuciak and Green MEPs.

By GIULIA PARAVICINI | 3/27/18, 2:47 PM CET | Updated 3/27/18, 3:42 PM CET

EU anti-fraud office OLAF confirmed today it has opened “a selection” into alleged fraud and mismanagement of EU funds and agriculture subsidies in Slovakia.

A selection is the preliminary assessment to see if there are grounds to open a full

ALSO BULGARIA

- › **BUT** the technology question here is how could Blockchain technology help?



HOME ABOUT NEWS OPINION CURIO DIASPORA MEDIA FREEDOM

Mafia rules in Bulgarian agriculture with the help of EU subsidies

January 12, 2018 By Editors – 2 Comments



Agricultural land in Bulgaria [Capital weekly]

For more than 10 years since Bulgaria has joined the EU, European agricultural funds are distributed mainly to a small number of big producers through large scale corruption, while the small land owners are deprived from their property with the complicity of the authorities, writes Georgi Kerelov.

TWO KEY FEATURES: 1 - IMMUTABILITY

- › Recording of land ownership, payments, recipients etc.
- › Providing a permanent, ideally transparent record
- › Potentially avoids possibility of post hoc tampering.
- › **Good Idea. Many difficulties.**
 - › Immutability is only good if transparent.
 - › If transparent, what data is available and to whom?
 - › GDPR?
 - › Privacy?
- › No solution to nepotism and family connections!



2. SMART CONTRACTS

- › Seemingly brilliant idea – encode business logic and contractual obligations onto an immutable infrastructure. **BUT**
 1. Who establishes the rules/contract to start with? (Governance)
 2. How can we be sure there are no errors (in code or rules)? (Quality control and social agreement)
 3. What happens when the world changes? (knowledge representation/semantics)
- › So far incredibly error prone (most famously TheDAO)



PLATONIC IDEALS VS. ARISTOTELIAN REALITY

- › Smart contracts (and blockchain technology in general) are a Platonic ideal – they indicate a belief in perfect idealised reality.
 - › We imagine business and other processes as abstract ideals with perfect features and performance.
- › Aristotle believed in observation of reality, rather than inferring from abstract principles.
 - › In reality, real life interactions are complex with lots of variations and exceptions.
- › We can systematise and automate processes – this seems to be a passion of our culture – but to avert disaster we need to **keep humans in the loop**.



CONCLUSIONS

- › Blockchain technology is no silver bullet to solve corruption and fraud (neither in food integrity, not in CAP)
- › It can have a limited role in providing an **immutable record** and potentially automating some business processes (using smart contracts or similar)
- › **Governance needs to be carefully thought through – who has the final say?**
- › For CAP: Avoid techno-utopian fantasies
- › For Blockchain: Beware the political implications inherent in the technology.



A nighttime photograph of a city street. On the left is a brick building with lit windows. On the right is a modern building with a curved facade and lit windows. A long-exposure light trail of a green car is visible, curving across the street. A white horizontal line runs across the bottom of the image.

› THANK YOU FOR YOUR
ATTENTION

Take a look:
[BLOCKCHAIN.TNO.NL](https://blockchain.tno.nl)

TNO innovation
for life