# Applying blockchain

## In the public sector

*August Botsford*

*Technical Director ChromaWay*

# Hypothesis

*Blockchain is a route to a new kind of generalised software infrastructure that can address systemic issues with IT infrastructure in the public sector*

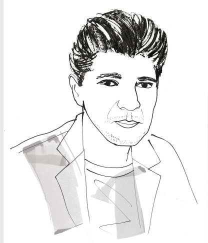
# Summary

- ChromaWay background & technology
- Brief discussion of what blockchain is and why one might use it
- Blockchain relevance to the public sector
- Cases working in the public sector (Swedish Land Registry, Colombia Chambers of Commerce, e-Krona)
- Crossover cases: private sector approach (Land Registration, ID)
- A new kind of cloud?

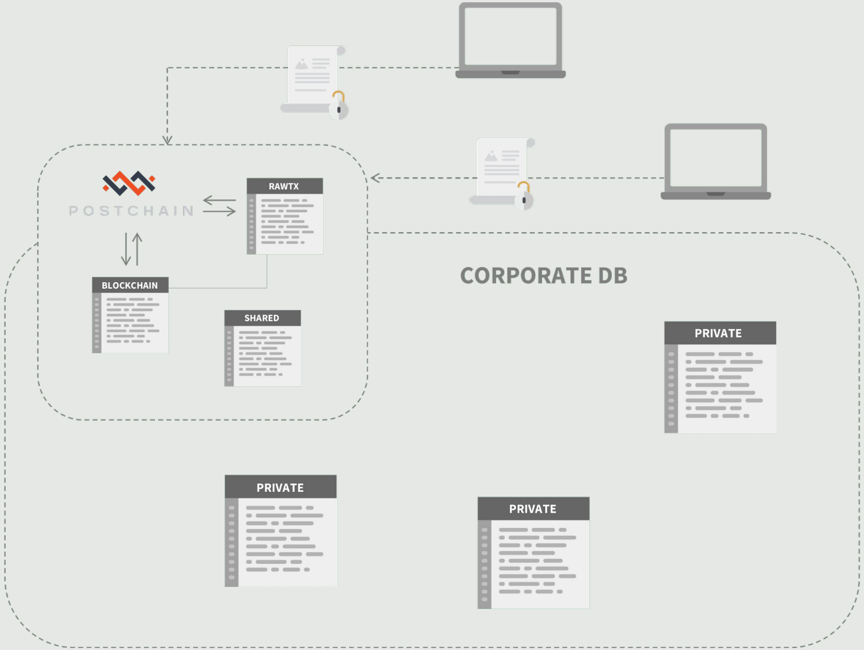
# ChromaWay background & technology

# Company

- ChromaWay, founded in 2014, currently ~40 employees spread around the world
- We make core platform technologies, as well as undertaking project and consultancy work
- Our most notable projects include the Swedish land registry, Andhra Pradesh land registry, and the Green Assets Wallet

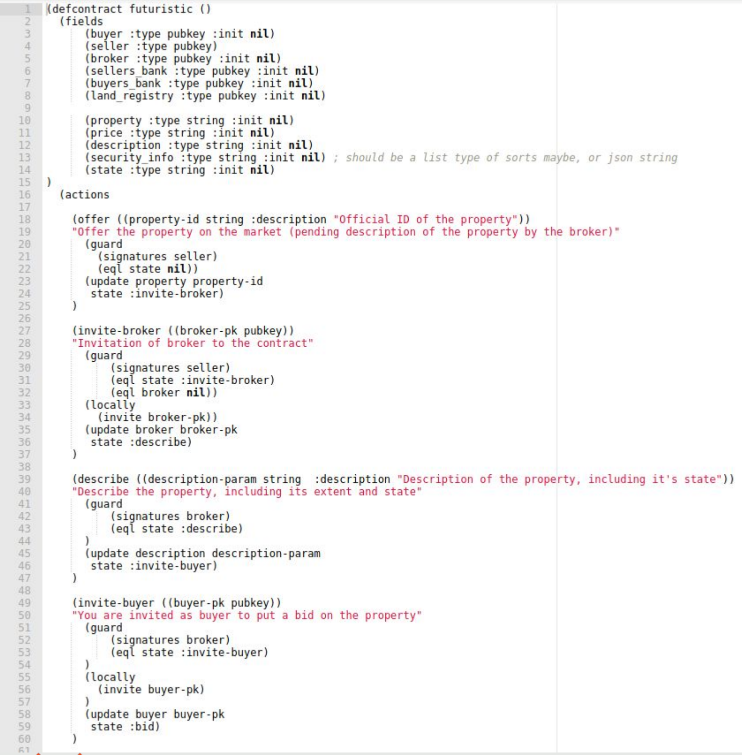


# Postchain: “relational blockchain”



- **A blockchain is a** (distributed) **database**, so it should manage data in the best way possible
- ACID properties of **relational database management system** provide most features a blockchain requires
- **Relational model is the gold standard**. Mature, tested, powerful, and ubiquitous
- Blockchain + relational model = *usable blockchain*

# Esplix: client-side smart contracts



```
(defcontract futuristic ()
  (fields
      (buyer :type pubkey :init nil)
      (seller :type pubkey)
      (broker :type pubkey :init nil)
      (sellers_bank :type pubkey :init nil)
      (buyers_bank :type pubkey :init nil)
      (land_registry :type pubkey :init nil)

      (property :type string :init nil)
      (price :type string :init nil)
      (description :type string :init nil)
      (security_info :type string :init nil) ; should be a list type of sorts maybe, or json string
      (state :type string :init nil)
)
  (actions

    (offer ((property-id string :description "Official ID of the property"))
    "Offer the property on the market (pending description of the property by the broker)"
      (guard
        (signatures seller)
        (eql state nil))
      (update property property-id
       state :invite-broker)
    )

    (invite-broker ((broker-pk pubkey))
    "Invitation of broker to the contract"
      (guard
          (signatures seller)
          (eql state :invite-broker)
          (eql broker nil))
      (locally
        (invite broker-pk))
      (update broker broker-pk
       state :describe)
    )

    (describe ((description-param string  :description "Description of the property, including it's state"))
    "Describe the property, including its extent and state"
      (guard
          (signatures broker)
          (eql state :describe)
      )
      (update description description-param
       state :invite-buyer)
    )

    (invite-buyer ((buyer-pk pubkey))
    "You are invited as buyer to put a bid on the property"
      (guard
          (signatures broker)
          (eql state :invite-buyer)
      )
      (locally
        (invite buyer-pk)
      )
      (update buyer buyer-pk
       state :bid)
    )
```

- Secure scripting language with client side validation
- Non-Turing complete, fully parenthesised, and very safe language for writing contracts
- All contract code is executed on the client side with assertions recorded on the blockchain
- High performance, low risk, and private form of smart contracts

# What is blockchain and why would one use it?

# What is blockchain all about?

*"The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority. Simply put, it is a machine for creating trust."*

**The Economist - 2015**

Commonly expressed as the properties of **decentralisation** and the process of **disintermediation**

# Benefits of decentralisation

- Fault tolerance— decentralized systems are less likely to fail accidentally because they rely on many separate components
- Attack resistance— decentralized systems are more expensive to attack and destroy or manipulate because they lack sensitive central points
- Collusion resistance—it is much harder for participants in decentralized systems to collude to act in ways that benefit them at the expense of other participants

https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

# Disintermediation

- Our interactions are mediated because we cannot trust each other
- In highly reductive terms, the institutions of society derive from this fact
- Mediation can create *inefficiency, insecurity,* and *inequality* because the interests of the mediator are not perfectly aligned with those of the mediated
- Providing alternatives to certain forms of mediation can improve *efficiency*, *security*, and *equality*
- Technology mediates, often in a very complex and abstract way

# Blockchain in the public sector

# Potential

- Public organisations operate digital services just as the private sector does
- The public sector has a greater responsibility to provide services which are secure, accessible, equitable, and transparent
- The public sector often also has a mandate for opening its data, supporting integrations, and fostering ecosystems
- Security, transparency, cooperation. These are things that blockchain should be able to help with

# Problems

- Blockchain implementations are usually quite unproven technology
- Blockchain introduces a new kind of complexity, in that the vendor/client relationship is not as straightforward
- Building a blockchain solution requires a significant change in approach
- Blockchains are generally not well suited to applications which require privacy
- Participating in a blockchain network entails a higher degree of responsibility for writing/auditing/maintaining code

# Value proposition

For us, one of the most interesting key value propositions of blockchain in the public sector is that it can provide an alternative to private sector information monopolies, and can enable public institutions to share work more effectively. It can do so by:

- Introducing a concept of collective ownership of IT infrastructure
- Providing a generalised decentralised programming environment
- Stimulating competition in the cloud

# Some cases in the public sector

# Blockchain title transfer with Lantmäteriet

- Among the first government blockchain projects in the world
- Consortium of project owners led by Lantmäteriet, coordinated by Kairos future, and with ChromaWay as the primary technology provider
- The project has now concluded its third phase

Telia Company

EVRY

LANTMÄTERIET

Landshypotek Bank

KAIROS FUTURE

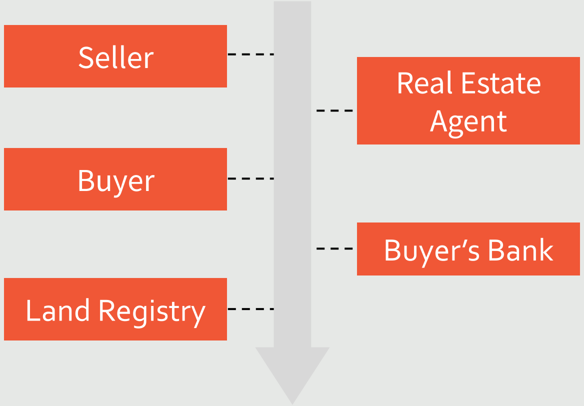
SBAB!

UNDER NDA

# Why blockchain for land registration?

- In Sweden and other advanced economies,  land registration is often a cumbersome and slow process with lots of paper involved
- In developing economies, land registration is often unreliable and associated with a lot of fraud and corruption
- Reliable land registration can have many economic knock on effects
- Blockchain is well suited: many non-aligned actors can be involved, perfect transparency is not problematic

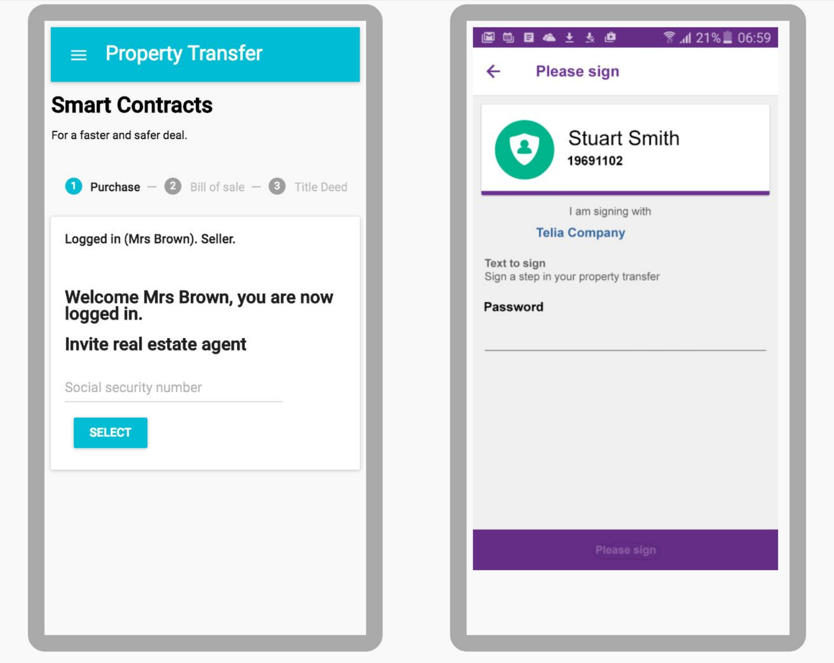
# Blockchain title transfer with Lantmäteriet



- Esplix smart contract orchestrates the process of transferring property ownership
- A process that, in Sweden, usually takes three months could be completed in hours
- The system can reduce the incidence of property fraud in Sweden, and in areas where the problem is much more severe

# Blockchain title transfer with Lantmäteriet

- Participants initiate, approve, and monitor contract events using a cross-platform app
- e-ID was provided by Telia, a large telecom in Sweden, but the system could work with other ID providers
- Signature driven workflow, contract participants are ‘invited’ to sign when it is their turn



Property Transfer

Smart Contracts

For a faster and safer deal.

1 Purchase — 2 Bill of sale — 3 Title Deed

Logged in (Mrs Brown). Seller.

Welcome Mrs Brown, you are now logged in.

Invite real estate agent

Social security number

SELECT

21% 06:59

Please sign

Stuart Smith
19691102

I am signing with
Telia Company

Text to sign
Sign a step in your property transfer

Password

Please sign

# Riksbanken e-krona

- Sweden's central bank is investigating the possibility of issuing an "e-krona"
- A direct claim on the central bank, available in real time to the general public
- Chromaway has proposed a solution based on Postchain

# Why?

- Central bank fears losing control of national currency
- Citizens have limited access to a vehicle free of credit risk
- Swedish citizen data is too accessible to foreign actors
- Insufficient money supply in the event of a national crisis or disaster
- Vulnerability of digital infrastructure to attack or subversion
- Insufficient efficiency and resilience in payment services

# Next phase

- Tender process has begun
- Likely that Riksbanken will opt for a non-blockchain solution
- Tender requirements too stringent for ChromaWay, although we will offer our advice and support

# Colombia Chambers of Commerce

- Concerned the Registro Único de Proponentes (RUP) which registers businesses so they qualify as vendors for government tenders.
- The RUP is a core process of all Chambers, it is highly valued by the business community
- It requires interaction with numerous external participants and is time consuming for Chamber staff and businesses as data must be collected manually from numerous external sources
- The Chambers are limited in their ability to validate the data.

# Solution

- ChromaWay modelled the RUP process, and implemented a smart contract using Esplix to facilitate the collection and validation of data
- The application was implemented as a blockchain, contract, and web front-end
- The pilot was successful, negotiations are ongoing for taking the solution to production

# Crossover cases

# Private sector solutions to public sector problems

- It is a common claim that private, for-profit companies are better and faster innovators than publicly financed institutions
- In many areas, we are witnessing a hybrid approach where public institutions privatise parts of their operations, emulate private sector practices, or rely more heavily on the private sector
- ChromaWay's experience with this has been in the areas of land registration and e-ID

# e-ID

- BankID is a notable private initiative which has achieved massive adoption in Sweden and in Norway and is used to access government services
- Together with a partner, we recently launched a private initiative to provide privacy-preserving e-ID in Taiwan.
- Blockchain is useful because it allows for greater sovereignty of the user over their data
- In this case, it means that the ID application can selectively reveal personal information, without that information leaving the user’s device

# Land registration

- Land registries around the world are hiving off parts or all of their operations to the private sector
- We have worked with land registries in Australia, Canada, and the UK
- Mostly they are interested in process orchestration using smart contracts
- Increased efficiencies mean better and more profitable services

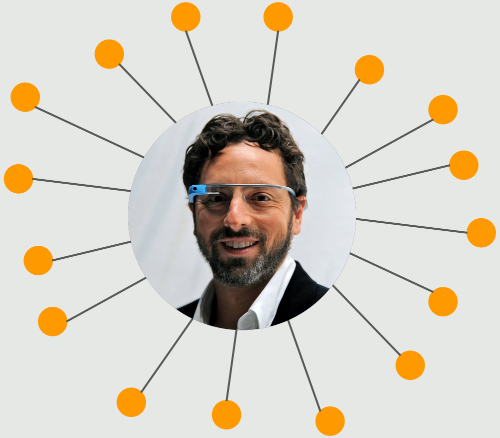
# A new kind of cloud?

# Cloud, SaaS, managed hosting

Managing physical servers is an operational challenge. Especially if high security is required. It is increasingly popular to use cloud hosted software, or to deploy applications to cloud hosting infrastructure like AWS or Google Cloud.

Potential problems:

- **Vendor lock-in**
- **Single point of failure**
- **Privacy concerns**
- **Lack of control**



● User

# Vendor lock-in

- In house IT systems and custom solutions were once the norm
- Increasing complexity means it is increasingly common to “externalise” IT services
- Cloud services are dominated by a few big names
- Risk of excessive dependence on a private company
- It is possible to mitigate, but maybe there’s a better way?

# Properties of blockchain implementations

- In all the previous examples, the blockchain implementation is run across a range of hardware and software. Cryptography mitigates this asymmetry and makes sure everything stays in consensus
- Installation and development are highly customised
- There is a lack of understanding and best practice about setting up, owning, and maintaining a blockchain application
- Ideally there would be a generalised infrastructure upon which to deploy and operate applications, like AWS but decentralised

# Public/Private blockchains

- Blockchains are “traditionally” divided into public or private categories
- All of the projects which we have worked on have employed private blockchains
- Public blockchains allow anyone to join, and maintain consensus through economic means
- Private blockchains implement access control, and maintain consensus using some kind of fault tolerant consensus algorithm
- In general, we can say that existing public blockchains are *too public,* and private ones *too private*

# Problems with public blockchain platforms

- There are many competing blockchain platforms which target generalised standard for operating applications which are decentralised
- There are three main issues with the approaches which we have evaluated:
    - Very poor user experience for application developers and for users
    - Crude economic model which is impractical for real applications
    - Lack of granularity

# Poor UX

- Unsafe languages lead to costly bugs
- Lack of effective tooling means that deployment is a crude affair
- Applications are usually more like loose bundles of “smart contracts” -- they don’t exist in a strict sense
- Data management and storage is cumbersome

# Crude economic model

- Blockchains are usually economically secured
- Inherent costs deter spam, disincentivise bad behaviour, and prevent front running
- Generally this is expressed as some kind of “cost per operation” or transaction fee
- Coupled with volatile cryptocurrencies this leads to wildly unpredictable (and often quite expensive) operation costs
- Subscription, one time fee, freemium models are impossible

# Lack of granularity

- There is usually basically only one “tier” of entity in a blockchain system
- There is no differentiation between a high security finance application and one that involves trading pictures of cats
- Both kinds of application are catered for equally inadequately

# An alternative?

Hypothesis: *Blockchain is a route to a new kind of generalised software infrastructure that can address systemic issues with IT infrastructure in the public sector*

It is our hope that our new platform to bridge the gap between public and private blockchains, allowing the public sector to divest themselves of bearing full responsibility for their IT infrastructure, without surrendering it wholly to a third party.

We believe it can achieve this by virtue of the following features

# An alternative?

- Type safe and easy to use programming language
- “Relational blockchain” for a rich programming model with many mod cons
- Sidechains for “horizontal scalability”
- Network segregation for a diverse and heterogeneous ecosystem
- Fee model abstraction
- Tiered “provider” system

# Thanks for listening!