Blockchain-based Payment for Carbon Trading

Oscar Golding (z5160173)
Supervised by: Dr. Sherry Xu, Dr. Qinghua Lu

Thesis B: UNSW

August 9, 2021

Outline

Problem

- Energy production can be certified on the blockchain.
- Blockchain solves an Environmental, Social and Corporate Governance (ESG) problem for energy certification.
- Carbon trading is a politically contentious field lacking trust.

Aim

- Can automated certification on the blockchain be used to deliver *trust* in the market for carbon?
- Can blockchain-based hydrogen certification be used as a motivating example for carbon trading?

Thesis B Aims

- Explore how *Hyperledger Fabric* can be used to develop a blockchain carbon market.
- Understand the performance trade-offs of putting a carbon trading platform on the blockchain.
- Identify how ESG hydrogen certificates can be used to automate a carbon market.

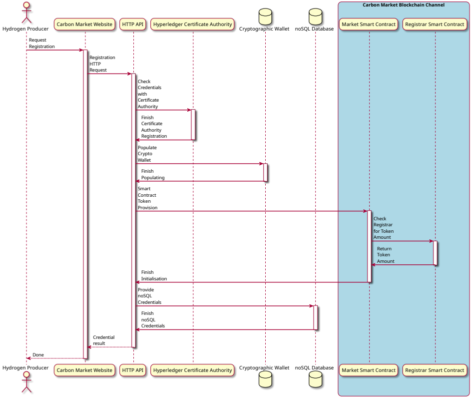
Quick Overview

- *Hyperledger Fabric*
- Full stack blockchain application.
- User roles tied to a blockchain certificate authority - *X.509* certificates.
- On-chain *CouchDB* for indexed blockchain queries.
- Distributed smart contracts.

User Roles

- Energy producers and certifiers are registered with the Hyperledger Fabric Certificate Authority (CA).
- Upon account registration, a producer is registered with the CA.
- Chaincode is called on behalf of a producer/certifier.
- Distributed smart contracts for account creation.

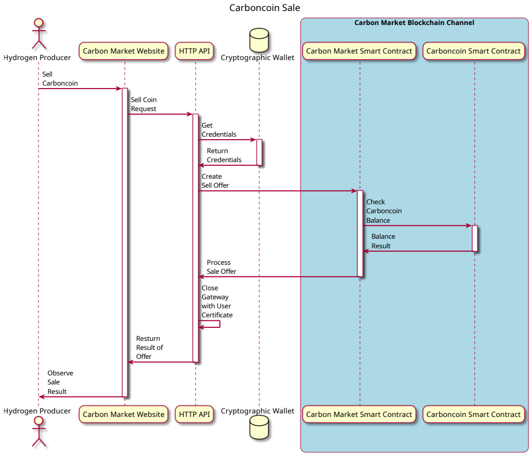
Producer Creation Example



Carbon Sales

- A producer is allowed to sell a fungible token called *Carboncoin*.
- Offer for sale of tokens is stored on the blockchain.
- Aim is to encourage distributed trading of carbon using the blockchain as an intermediary.
- The producer entirely drives the trading process.

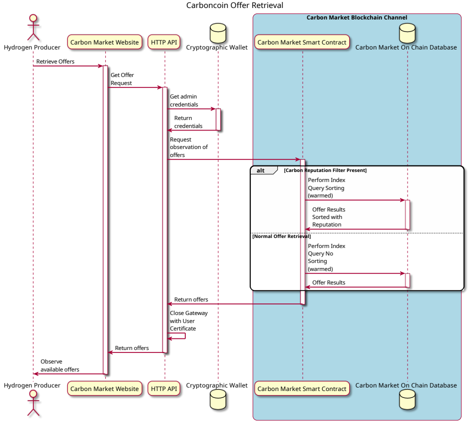
Carboncoin Sale Example



Viewing Offers

- An on-chain *CouchDB* index is warmed for retrieving offers.
  - Warming happens whenever a new block is cut.
- Optional *carbon reputation* is attached to an offer so producers can ethically purchase carbon.
- Carbon reputation assists with increasing market quality.

Retrieving Offers Example

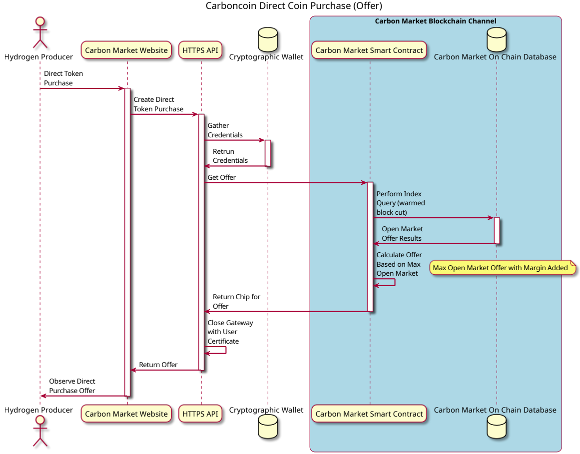


Direct Market Interaction

- A producer can directly purchase *Carboncoin* outside of the open market at an *extra cost*.
- The user is given an on-chain offer token to purchase *Carboncoin*.
- The price per token is calculated using the maximum offer on the open market.
- Each x_i in Equation 1 represents an active offer in the market.

$$\text{Direct Offer} = \max\left(\langle x_1, x_2, \ldots, x_n \rangle\right) + 50 \tag{1}$$

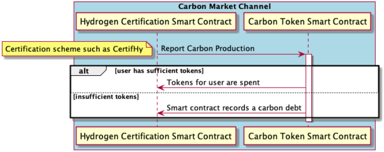
Direct Offer Creation Example



ESG Certificate Interaction

- Market activity triggered by an ESG certifier recording carbon production.
- As a step in certificate creation, the certifier invokes the carbon market smart contract.
- Both the certifier and the carbon market exist on the same *Hyperledger* channel.
- If the user does not have enough *Carboncoin* to pay for production, then a debt is recorded.

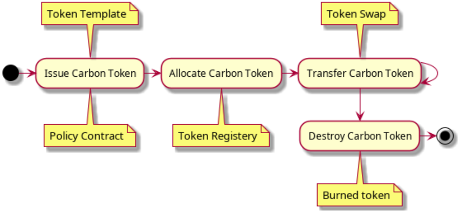
Figure: Channel Interaction



Patterns

- Token template
- Policy contract
- Token registery
- Token swap
- Burned token

Figure: Carboncoin Lifecycle



Policy Contract Pattern

- All blockchain operations are bounded by policies which provide rules on how *Carboncoin* can be used.
- Only producers with the *producer* role can buy or sell *Carboncoin*.
- A user can never sell more *Carboncoin* than the amount contained inside their account.
- A user's *X.509* certificate is required to perform write operations on the blockchain.

Token Swap Pattern

- *Carboncoin* can be swapped between users.
- Policies are attached when doing a swap:
  - Active offer is required.
  - Seller must have enough *Carboncoin*.
  - The buyer must meet their open offer obligations first before purchasing tokens.
- The swap happens for only the *Carboncoin* token.

Burned Token

- A *Carboncoin* is burned when a producer is required to pay for carbon production.
- *Digital Physical Parity* exists between real carbon production and the carbon reputation in the market.
    - Certifiers play a signficant role in maintaining the digital physical parity between carbon production and carbon reputation.
- Debts are recorded when a user does not have enough *Carboncoin* to pay for carbon production. Debts can be paid at later dates.

System Performance

- Although the aim of the thesis is not to produce the most high throughput carbon market - the performance of the system is still worth exploring.
- The performance of *Fabric* has a tendency to suffer in the *Validation Phase* of the transaction lifecycle.
- An observed tendency of Hyperledger is that as the transactions per second (TPS) increases, so do errors [2].

Common Bottlenecks

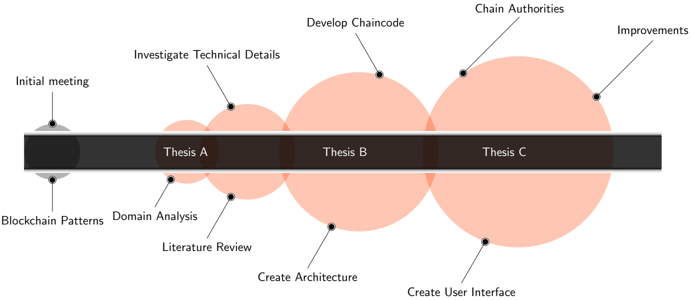
- Multi-Version Concurrency Control (MVCC) - transactions in the same block updating the same key (transaction dependency).
- Phantom Read Conflicts - performing a read on a key range which has been updated.
  - For some reading range i to j, if a key has recently been inserted then read a phantom read happens.

Enhancements to TPS

- Represent assets on the blockchain as a sum of deltas to avoid MVCC errors.
- Example: CarbonCoin is the sum of deltas in Equation 2.
  - Each δ_i contains a unique combination of owner, transaction identifier and sign.
  - Each x_i represents the asset value (for example 500).
- Localise the phantom read conflicts into 'low TPS' domains.

$$\text{Asset Value} = \delta_1 x_1 + \delta_2 x_2 + \cdots + \delta_n x_n \tag{2}$$

Original Research Timeline



Updated Research Timeline

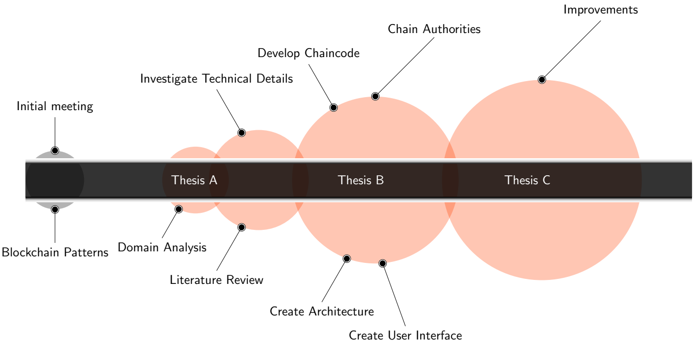


Table Representation

- Original plan for Thesis B. Green records the task being completed.

Table: Plan for Thesis B

Week	Plan
1	Hyperledger Documentation
2	Hyperledger Documentation
3	Hyperledger Documentation
4	Smart Contract Programming - Producer Register
5	Smart Contract Programming - Offer Lifecycle
6	Smart Contract Programming - Carbon Reputation
7	Smart Contract Programming - Direct Purchase
8	API Construction - Account Creation
9	API Construction - Wiring Requests to Offers
10	API Construction - UI Functionality

Plan Update

- Ahead of schedule - working prototype with chaincode, implemented architecture and a user interface.
- Plan for Thesis C:
  - Exploration of blockchain performance (TPS).
  - Generalisation of blockchain patterns to sources of energy outside of hydrogen - for example water.
  - The auctioning of *Carboncoin* to hydrogen producers.
  - Payment channel for recording off-chain transactions.

References I

Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed Cocco, and Jason Yellick.
Hyperledger fabric: A distributed operating system for permissioned blockchains.
In *Proceedings of the Thirteenth EuroSys Conference*, EuroSys '18, New York, NY, USA, 2018. Association for Computing Machinery.

Jeeta Ann Chacko, Ruben Mayer, and Hans-Arno Jacobsen.
Why do my blockchain transactions fail? a study of hyperledger fabric.
In *Proceedings of the 2021 International Conference on Management of Data*, SIGMOD/PODS '21, page 221–234, New York, NY, USA, 2021. Association for Computing Machinery.