PEN

Table of Contents

Introduction

Pen is a peer-to-peer implementation of some of the main parts of a participatory economy.
It is still under development. The *Parecon* economy invented by Michael Albert and Robin Hahnel is used as a model.

This document focuses on the technical solutions that is unique to Pen, and does not try to provide a general description of participatory economics.

The implementation is only one of many possible implementations, other implementations would probably emphasize other aspects and do other design decisions.

Pen main areas of intrest:

- Participatory planning
- Information publishing
- Council voting
- Participatory Credits
- Messaging
- Authentication and security

Overview

Two types of entities exists in the economy, individuals and councils. A council can be a council of individuals, or a council of councils(a federation). An individual or council can have several and different roles in the economy. All roles exists in the context of a council.

Councils

The councils mentioned here are those directly involved in the planning process. They are councils taking part in the consumption and production. Other types of councils can of course also exist in an economy but they are not covered here.

Councils have voting right in matters concerning other councils, such as the accepting of new councils or dismembering others.

Consumption

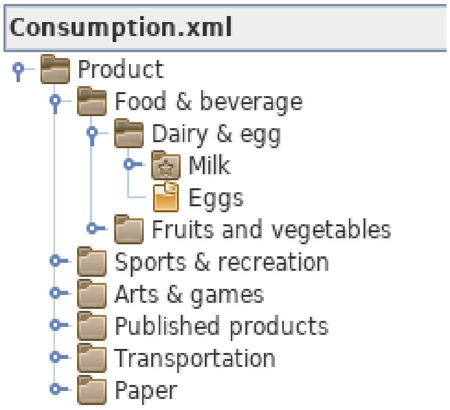
The categorization of consumption is mainly based on locality. In some cases there would be a sub categorization based on other factors.

For example, a federation of councils working for equal rights might be subcategorized based on equality for different genders, ethnic groups, different sexual orientations etc. The federation in turn would be a member of the national consumption council.

Products

In Pen the definition of a product is everything a council or individual can have as inputs. That means that everything produced by production councils as well as use rights for equipment, natural resources, skilled labor etc. are products.

A very special type of product is the work one does. It is measured in time and effort recalculated into medium effort hours.



The products of the Pen economy are structured by generalization in a tree structure. The leafs represents specific products from specific production councils. The root of the tree represents products in their most generalized form “Product”.

Most often a consumer would not be required to specify specific products in the proposal, but rather some generalized category. When a category is defined as “analogue”, it means that it is the most general form a consumer is able to choose.

Something like the eight digit UNSPSC product categorization system could be used as a basis when creating product id:s, just adding numbers to the end to get unique id:s.

Accounting

In Pen, product id:s also serves as account numbers, significantly simplifying accounting. This means that in the same way products can be generalized to product categories. So can accounts, when more general accounting information is required.

Network

The Pen project builds it´s functionalities on a peer-to-peer network of nodes. Nodes are applications running on a device. To join the network one has to be authenticated. Authentication is attained by becoming a member of a consumption council. All production/consumption councils should to the extent possible actively run a node.

Friendly organizations and people living outside the economy who wants to support the availability and resilience of the economy by running nodes could do so by being accepted as a supporter in a supporters council.

A p2p network implies internet access, but in many places there is none, or only to a varying degree. Since a functioning economy is so central to a society, the Pen project will provide as much functionality as possible even in a situation without internet.

Participatory planning

Orinary databases are used to handle the planning data. Proposals are signed by the member, and since the council has the members public key they can be verified.

Publishing of information

In a participatory economy there are many types of information that needs to be published or shared. Like prices and limits, information about products or councils, accounts from different part of the economy etc. Peer-to-peer networking was designed for sharing information and sould be well suited for the purpose.

Council voting

When a change is to be done to the current state of the economy, the change must first gain approval with a majority of the councils. It could be the accepting of a new council, accepting economic proposals etc.

One council starts the voting and owns the votation. When a council casts it´s vote, it does so by creating a vote object, signing it and adding it to the votation blockchain. Only one vote per council is accepted. If a majority of the councils voted for a certain change, the blockchain provides the evidence for that.

Participatory Credits

A Participatory Credit is an abstraction with the monetary value of 1, and might for example be defined as one thousandth of a hour of work at a medium effort.

A Credit Token is a digital representation of one or several Participatory Credits. They have a credit value, for example 1PC or 1000PC.

Credit Tokens are “personal” and might only be used once. They would be virtually impossible to counterfeit but can be copied. Their existence and current state is declared in the Credit Token Blockchain.

The tokens have three main states: issued, usable and accounted. A fourth state “used” exists to enable buying detached from the CTB when there is no access to the internet.

	Operation	State	Delegate	Can be used
1	The credit is issued	ISSUED	Issuing council	No
2	The user is defined	USABLE	The user	Yes
3	It is used	USED	Receiving council	No
4	It is accounted(and used)	ACCOUNTED	The common	No

Minting

Most ordinary crypto currencies are issued through by what is called POW(Proof Of Work) by someone solving a mathematical challenge. The outcome proves that the challenge was in fact solved, and all nodes could agree on the fact.

The Credit Tokens on the other hand would be issued through what could be called POM(Proof Of Majority) by a production council putting it´s proposal up for voting. The outcome of the voting proves if the proposal gained a majority of approvals. All nodes could then agree on the fact.

If the proposal got accepted, the council would gain the right to issue the number of tokens that is needed to cover the expenses as stated in the consumption proposal. The issuance is done by creating the tokens and adding them to the CTB.

Excess tokens at the end of the year would be accounted in special accounts. In the case when a council runs out of credits before the year has ended, it would have do a complementary proposal, applying for more through voting.

Since individuals are not allowed to issue tokens, councils who “sell” directly to individuals like shops, would need to have change credits. These “shop councils” could be allowed to do special votings, enabling them to issue tokens outside of the normal economic plan. However, when these exchange tokens are introduced into the economy, the same amount of normal tokens must be taken out. In order not to skew the plan.

Using

Before tokens can be used for consumption, the issuer has to define the user of the credits by setting the user public key and signing the key. This operation is only allowed if the tokens already exists in the CTB. The updated token is added to the CTB. In most cases the council self would be the user. In a workers council though, some of the credits would go to salaries.

When tokens are received as payment for a product, their validity should be checked. The existence and status of the tokens could be checked in the CTB if internet is available.

If internet is not available their existence could be checked in the latest copy of the CTB. In this case the definite state of the tokens would be indeterminable. The correctness of the user could however be verified by the issuers signature and consequentially the users signature.

When validity has been checked, the purchased product id and the user signature thereof is set in the token. The updated token is then added to the CTB as soon as possible to avoid double spending.

Since the token at this stage has been used, attributed to a product and added to the CTB it is accounted.

Payment examples

Example 1:
Formosa Plumbing Coop receives an invoice from a supply hub detailing 30,000 credits for 200 valves and 25,000 credits for 500m copper pipes. To pay for the products, the coop issues two tokens of the said amounts.

In the user signature fields the coop puts it´s own consumption public key and signs that. In the product fields the coop puts the product id of the valves and pipes respectively and signs that. The updated tokens are then added to the CTB.

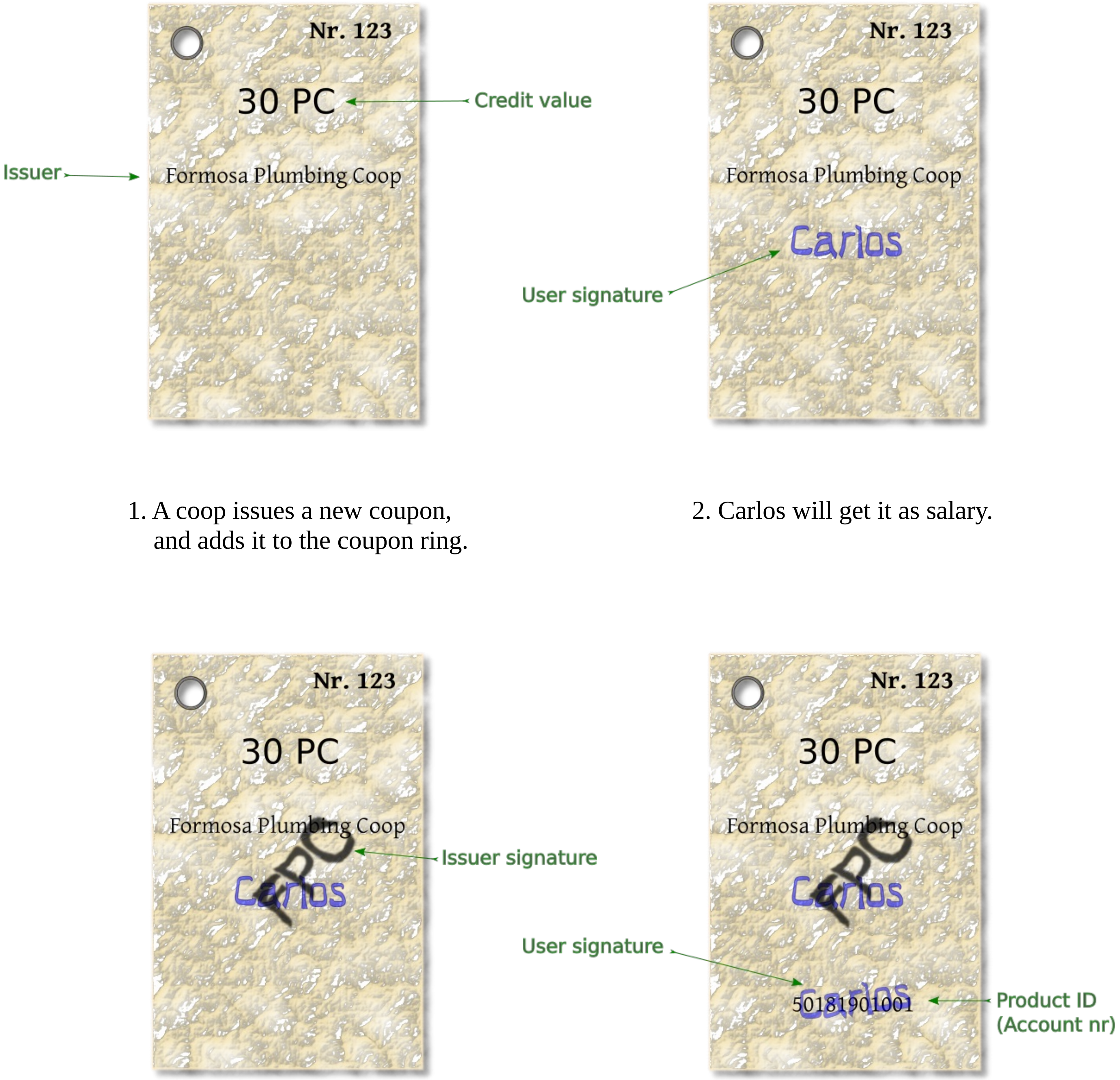
Example 2:
Carlos who is a worker at Formosa Plumbing Coop wants to buy some food items in a village store. The store lacks internet access but has a smartphone that is used as a register. Once a day the phone gets synchronized to the CTB.

Carlos does not own any devices that could be used to pay with, but he have a credit book. He shows the shop attendant what tokens he wants to use. He chooses a 10,000 credit token. To pay for the goods, it first needs to get exchanged into smaller tokens.

The attendant checks the token with the latest copy of the blockchain. Then sets the account nr to that of the stores exchange account, which Carlos signs by entering his password. The token is then added to the local blockchain copy for later synchronization. In exchange for the token the store uses some of it´s preissued change tokens of smaller values. Carlos is set as the user of these. With these tokens the food items can be payed and Carlos get his change back.

A simplified analogy

Sometimes it might be useful with a analogy to get the general idéa. This simplified analogy uses coupons and stamps instead of tokens and signatures, and a metal ring instead of the CTB.



1. A coop issues a new coupon, and adds it to the coupon ring.

2. Carlos will get it as salary.

3. The coop signs on that.

4. Carlos then uses the coupon to buy a loaf of bread.

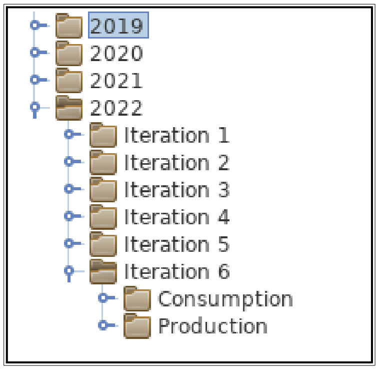
Administration

Forming a Pen economy

A Pen economy would formally be started by creating a Root node. The Root node have no role in the economy and exists in no context.

It does however provide the context for the national consumption and production councils to have roles in, and might thereby be said representing the economy itself. If compromised or stolen, it could be replaced by a new one.

Other benefits of having a root node is that it provides a clear and consistent authentication path connecting the consumption and production trees. It is also good for administrative purposes making iterations easily achievable and browsable.



Joining

For someone to join the economy he/she/it has to apply for membership in a council. In the case when the applicant itself is a council, the council where it seeks membership must hold a voting where a majority of the existing councils approves.

If an applicant is accepted, it would have to exchange public keys and other credentials with the council. The exchange must be done in a secure way, it could for example be meeting and snapping each others QR codes, transfer via a NFC link or USB.

Security

Economics are about peoples livelihood and at the core of a functioning society, security is therefore of absolutely essential. Evidence shows that security should be designed in from the start, and not added in as an after thought.

The Pen project has a rather high technical complexity, incorporating some innovative and untested solutions. Technical complexity generally means a large attack surface, and untested solutions could mean unexpected vulnerabilities. Segmenting the nodes into independently working functionalities is probably a good idea, as well as extensive testing and simulation.

The distributed nature of a peer-to-peer network means it has no center to attack or take down. On the other hand malware could potentially spread like wildfire. Special care needs to be taken when designing/implementing protocols and in the deserialization and parsing of data.

Authentication

Encryption

Using good cryptography in communication and storage is necessary to stop adversaries from interfering, and to protect the privacy of the users. The Sodium library has been chosen for the task because it is a highly regarded and mature open source project.