# Certore

**Abstract**

The problem of ensuring system's individual parts successful communication and interaction, determination of criteria for quality measurement and constituents for its efficient functioning occurs with every defined area development and growth. Given task can be solved with help of standardization and certification implementation, where the process of standards development and acceptance is usually complicated, bureaucratic, and frequently yields human impact. Indeed, the absence of its produces users distrust, high volatility and other harmful impacts, causes in unpredictable consequences. We present an automatic system for standards and certificates development, based on events flow. We also describe common problems in considered area, which can be solved by using the proposed system.

## 1 Executive summary

### 1.1. Introduction

Technical progress brings us number of facilities; meanwhile standards are a prime part that stands behind. Standardization is a key element, which allows each part not only to communicate with other elements, but also to provide *quality* of the whole system. Once established standards provide a set of rules, definitions and criteria aimed at achievement of the system improvement by increasing efficiency and productivity.

Standardization itself is the activity of establishing with regard to actual or potential problems, provisions for common and repeated use. This process is aimed to achieve the optimum degree of order in the given context [1]. By definition, standardization contains the methods for quality criteria detection and control. These can be applied to existing or under development systems, which match the described guidelines, by introduction of certificates and standards. Generally, governances, companies or organizations control a process of establishing and handling. The most innovative way of standardization management is an open community – a group of subjects that has an expertise in a certain field. In addition, each member from open community should be interested in compliance and development of rules as crucial tool for experience, sharing, and communication.

Why are standards effective? The 1991 Annual Report of the American Society for Testing and Materials (ASTM) said: "Standards are the vehicle of communication for producers and users. They serve as a common language, defining quality and establishing safety criteria. Costs are lower if procedures are standardized; training is also simplified. And consumers accept products more readily when they can be judged on intrinsic merit [2]." Products designed in accordance with standards and guidelines conform required quality and enhance *confidence among users*. Certified products more satisfy users' needs and switch focus between brands in highly competitive markets.

Standards' preparation, acceptance and implementation in researched area must consist of such steps:

- determination of system levels and sublevels;
- finding of *value drivers* for every system level (including level of inputs and outputs);
- certification and standardization according to defined value drivers;
- selection operational indicators to measure impact of standards (optionally);

Standards are introduced and accepted by open community based on consensus. The main and efficient way for members' status quo reflection is voting. Voting is a process of making decisions or expressing opinions. It usually followed by discussions, debates or election campaigns [3]. Ability to provide every stage transparency is a base factor to ensure fair voting.

### 1.2. The area

Every technical system including cryptocurrencies requires standards to be organized as the complete system, which will allow being integrated and accepted by outer world. Another important part of a system is the economical component. Economical component defines *value* and social recognition, affecting value measurement and adding. A process of value creation is *procurement*, that should be accompanied by a unique activity, which belongs to economical part and includes (or could be presented as) technical process for producing characteristics of two areas. Blockchain procurement process (mining) stands by ideal unit having open separated system as primary and not existed solely in technical scope, but necessary physical resources (equipment, electricity, software development etc.) for successful functioning. A system missing any of described above parts can be detected as *interrupted-cycle* technology and can call for further actions to assure full cycle flow. Designated features determine digital currency as technical-economic system operating in two fields simultaneously with keeping features of each of them.

Economics is an area where digital currency face outer influences, interact with them and has an impact on each other resulting in integrated and non-isolated system. Undergo external impacts digital tokens particularly proceed under regulation and laws of existed elements; given object cannot be considered out of existed economical systems and its interaction with fiat declined, thus artificially increasing isolation and producing sufficient harm. The revers is also true, digital currency *impact on existed economical systems*, fiat by communicating via certain methods and channels.

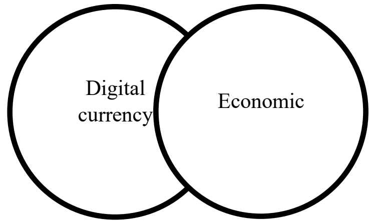



**Figure 1.** Cross-interaction of determined systems

For example, removing computer processing part causes significant shift of object from digital scope directly to traditional systems and deprive of key features being indispensable basis and crucial warranty for successful lifecycle. This also shows capability of technical area to develop and maintain currencies still with some limitations, like digital divide - a complex phenomenon that is concerned with the impact of information inequality due to lack of access to information and communication technology with three distinct aspects: global divide, social divide and democratic divide [4].

However, what are the rules for successful global procurement of crypto tokens? Can we define them? It's an attempt to determine vision of basic standards, criteria, definitions and bring required quality to newly created technical-economic system, known as digital currencies.

### 1.3. Applicability

Procurement process elimination as constituent part is a reason of system and cycle integrity violation and is prove of given statements correctness. It causes high volatility and breach of users' trust affected negatively on whole market. Non-coordinated community actions can bring a similar negative effect (like Segwit2x [5]) and is a direct consequence of standards absence. Standardization stands out in this case as method for system persistent improvement, adding necessary stability with improving so holders' confidence and achieving new dimension.

Standards should be implemented for each scope separately, establishing in conjunction a measurement unit for complex evaluation of considered object. Digital crypto currency as block-chain technology expected to meet next requirements, which also can be detected as basic criteria or value drivers:

- decentralization (as double-spending problem solution [6]);
- anonymity;
- security;
- reliability;
- convenience;

Every proposed standard therefore belongs to one of the defined areas and related to type, that is selected with a certain value driver. Consequently, standard's scope and value driver could be determined directly during a creation stage, making possible specified required conditions and resources for acceptance and implementation processes. Finally, selection of *operational indicators* to measure standards impact could be established, in considering market price of object as basic indicator, but not limiting number or permission to use. Thus, need for introduction and appliance of standardization for considered object is proven and described in scheme for further implementation by Certore.

# 2. Certore as platform

## 2.1. **Description**

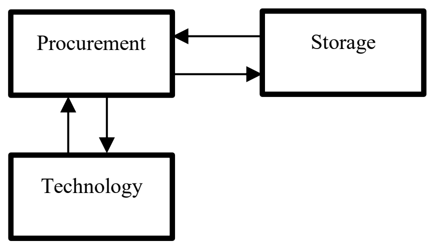



**Figure 2.** Complete cycle of digital currency

A process of digital currency functioning (**Figure 2**) with complete cycle consists of three stages where the base is digital technology (blockchain as example), which define common features and capabilities of object; obligatory further process of procurement, that is built upon preliminary determined technology and storage as technical implementation of human interface – wallet. Any disturbance, modification or feedback interruption between the stages leads to cycle interruption and shift of balance, having as result interrupted-cycle digital currency, which requires significant resources for tracing, eliciting and flaws eliminating with possible appearance of crucial consequences.

Common process of standard development can be represented by using *events chain*, where each next event could be triggered back in case of not matching conditions; respectively, event flow is finished if certain interaction occurs. For example, an event is triggered back twice, that marks event flow as excessive and causes standard acceptance termination despite the fact that standard is not implemented. Rules and description for standard development will be provided by Certore and open community and accepted using web-portal having Certore as intermediary, implementer and generator but not a decision-making institution. This will allow providing desirable process transparency, substantiality and capability to balance preservation during possible outer interruption cases or other types of impact on organized system. A key feature of Certore is standardization and certification event based on automatic system (*SCEBAS*) for standards and certificates development events flow control and acceptance, which ensures human impact isolation with further avoiding of undesirable consequences.

Each phase of the described process, including level inputs and outputs, can be standardized and described using the proposed practices, therefore incorporating efficient and transparent system, comprising external impact persistence, legitimacy and stability as key capabilities. Standards' introduction is based on relation determination to area, accentuation of proper value driver, and operational indicators as a method to measure implemented standards influence. **Table 1** shows primary value drivers that constitute framework for next development and improvement as a part of standards and certificates.

**Table 1.** Primary value drivers

| Value driver | Description |
|---|---|
| Decentralization | Ability to support and provide procurement and store stages separation both in technical and economical areas |
| Security | System characteristic for stability and integrity preservation under abnormal impacts |
| Reliability | Property to keep all system attributes and parameters during defined time period and limits required to its normal functioning |
| Efficiency | Relationship between the result achieved and the resources used [7] |
| Privacy | Capability to isolate and limit any technical systems' non-relevant information before conveyance |

Last step of standard introduction is applicability's efficiency measurement, where the determinative factor is operational indicators choice correctness, which is described by the formula:

$$E_t = \sum_{i=0}^{n} \frac{E_n \cdot k_n}{n},$$

where $E_t$ – total efficiency, $E_n$ – operational indicator efficiency, $k_n$ – weight coefficient, $n$ – number of operational indicators.

Certore must provide community portal, which has to satisfy such requirements:

- provide clear problems solutions, improvements implementation and further standards and certificates technology development;
- provide and protect community members voting process as key way of standards and certification rules acceptance;
- use described approaches for SCEBAS implementation and/or any related software development;

- assure each community member and currency holder access to portal;
- guarantee transparent system of voting area of members' acceptance and possible members' involvement;
- support community involvement and promote standards as only and proper way of digital currencies improvement and quality factor;
- provide sufficient load handling ability and uninterrupted work, including DDOS or any stress attacks type sustainability;
- prevent and detect any possible harmful or fraud activity, which can influence on SCEBAS or standards and certificates development process;

Certore obliges:

- use portal voting area as basic and only way of acceptance and development of standards and certification rules, software business logic etc. as SCEBAS implementation;
- develop required software, based on accepted standards or proposed by Certore as possible initial solution of existed problems (by software means developed from the ground, unit, functional and other types of tests, commits and pull-requests, automatic certificates and related systems, including automatic standards matching and determination);
- provide voting and acceptance process security and transparency by SCEBAS and other possible ways;
- ensure platform standardization and certification area access and usage for individual specialists, related hardware and software producing organizations, scientific and research units;
- propose necessary problems solutions, facilitate standardization and certification scope enhancement as required attribute and synonym of quality;
- guarantee secure data store and prevent 3-rd side access, having in mind cryptography as one of main methods for data protection;
- focus on usage and implementation automatized system and reduce human interaction and participation in any system level;
- promote digital currency technology and standardization as it's essential part, involving new members to community;

## 2.2. Portal

### 2.2.1. Features

Portal is a web-based application, which allows introducing, proposing, accepting and even implementing standards, certificates or other units. It accompanied by standardization and certification process, receiving users as key input value including voting process input parameter and as non-related objects. This application based on automatic system having SCEBAS as core and constituent parts separately, thereby minimizing direct human impact, but not eliminating human interaction as still indispensable on some levels. In any case, Certore portal focuses on automatization and reducing possible harmful human impact on SCEBAS or directly on standards development and implementation process. Thus, previously described SCEBAS is a primary portal and Certore part to provide all defined functions and match declared requirements, represented on **Figure 3**.

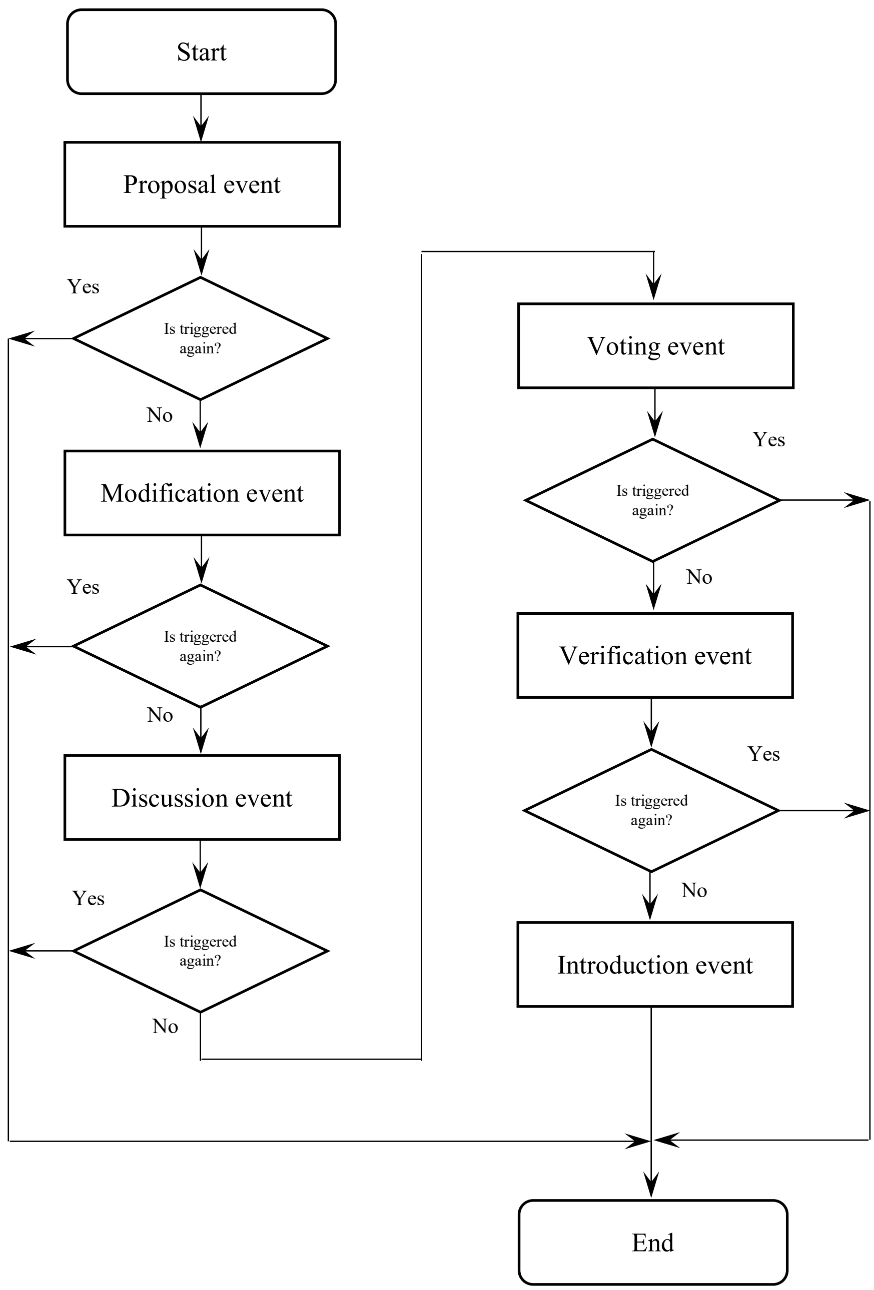



**Figure 3.** SCEBAS events chain

Reaching the main goals of the current system provides as significant community coverage as possible, that determine multilingualism as probably the main portal feature. Next languages are proposed to initial implementation and support:

- English en, ISO 639-1 code [8];
- Chinese zh;
- Spanish es;
- Russian ru;

In the same manner not to limit or decrease target audience amount portal access has to be ensured to all users' types including personal, considered or related business fields, scientific and research organizations access. In conjunction with multilingual content this composition is necessary functional for reaching sufficient part of community, but accepting the fact of given diversity to bring additional complexity for system and determining creation of well-defined organized system to access and areas control, that provide successful and efficient SCEBAS functioning as requirement. This should consider a strict separation of users' roles and areas, where selected role will be strictly limited, and it will be a subject to accepted rules.

Important part of obtaining and keeping trust and community recognition is the ability to keep process transparency and substantiality, which might be expressed by exposing voting results without limitation. It could also contain semiautomatic system, which prevents fraud, scam, vote rigging, bribery and other forms of voting manipulations detection.

### 2.2.2. Areas

Main portal space, where standards development and acceptance take place is *voting area,* consists of next subareas:

- *main* (economical) subarea – place for implementation development and acceptance part of standardization process, if standard can be detected as related to economical or/and has more features, which can be determined as economical characteristics, then technical;
- *technical* subarea – space for standards and certificates development and acceptance, if certificate or standard can be determined as technical or/and has more features and capabilities, which can be determined as technical characteristics, then economical;

Each voting subarea should consist of next sections (**Figure 4**):

- *technology* section;
- *procurement* section;
- *storage* section;
- *other* section;

Other areas are optional and not underlying SCEBAS, so they will be proposed by Certore or community and accepted by implementing voting area as an object for further discussion.

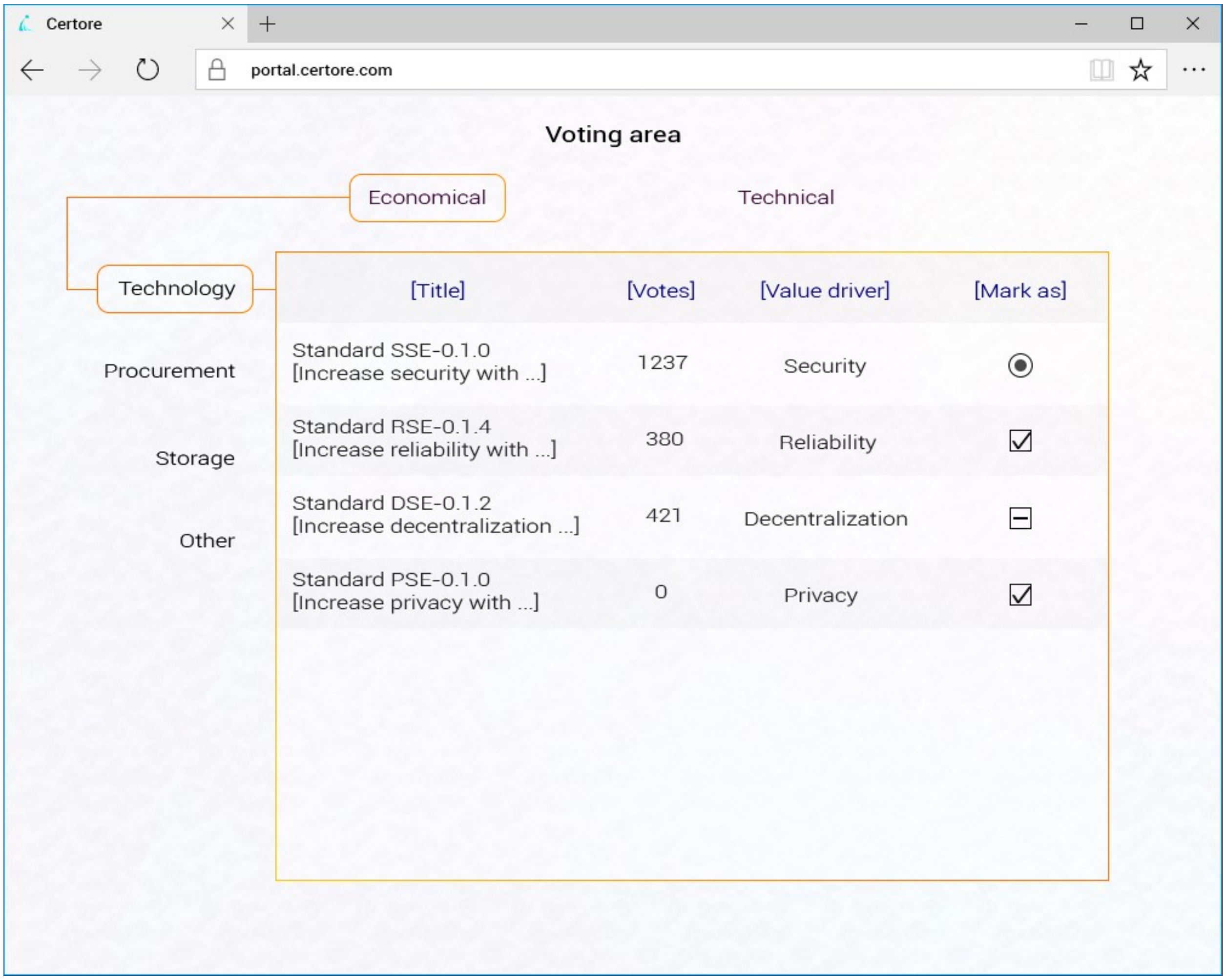



**Figure 4.** Prototype of voting area

### 2.2.3. User roles and access system

Portal access will be granted for users with next roles:

- *members* (registered users);
- *voters* (investors and approved by request) – subjects of any type, which are part of community and/or have experience in economical fields, that can be proven in number of ways, like public activity, commercial and scientific expertise, investment in Certore etc.;
- *technical voters* (approved by request) – persons or organizations with must expertise in defined area, that can be proven by certain methods, like published software, commercial experience, scientific activity, certain field company is operating etc.;

Obtaining user access to voting area will be provided by two-level system, where the first level is a part of SCEBAS and the second – administrator verification acceptance action, with ability to renew access request after prescribed changes and requirements are fulfilled.

### 2.3. Certification and standardization

#### 2.3.1. Technology

Technology in considered scope is a set of rules, methods and descriptions, typically implemented in a form of software with possible various equipment engagement. It matches criteria of digital currency, token or any possible recognizable form of value creation. It can be measured with usage of the defined value drivers, which will support existed standards. Classical example of technology is proof-of-work blockchain, which requires a certain amount of equipment to provide further deployment. However, the problem is that there are much more software production than equipment for its apply. This practice does not have any influence on technology type as one possible way of implementation, but it becomes a primary model.

Certification of technology can be performed as automatic or semi-automatic process. SCEBAS standards can be considered as basic and necessary condition, represented in related to object type that supports mutual communication and often is realized as *software.* Here and further by software we mean a developed functional unit and other types of tests, "commits" and "pull-requests", automatic certificates and related systems, including automatic standards matching, 3-rd parties open source software and libraries.

Procedure of standards and certificates development and acceptance for considered system level occur in allotted portal section with built-in SCEBAS. It should follow the rules described above and be a coherent reliable segment of higher-level system. Comprehensive range of technologies can be accepted as candidates without any factitious restrictions, rules and impossibility of standards introduction, which cause undesirable regulations and impacts.

#### 2.3.2. Procurement

Process of digital units' creation is established with obligatory technology usage as primary level of complete system. It is accompanied by use of resources, which ensure continuous technology deployment different in time range and their volume. Mentioned above is a procurement and it may contain next alternating values:

- time range required for unit creation;
- minimum volume of equipment for unit procurement;
- necessary client information accepted as technology input;
- client actions affected on information;

*Procurement index* is a value, which describes relation between equipment amount and the time range of a single unit creation for considered object. It cannot be used as part of SCEBAS, but it can be calculated and displayed by Certore as important characteristics of digital currencies. Economical component procurement index PI can be represented as:

$$PI = \frac{p}{T_c},$$

where $p$ – price for object in USD, $T_c$ – time for single unit generation.

Equipment as segment of procurement process has to be defined and verified with usage of standardization and certification technologies in sever ways:

- by installing provided software, including developed by Certore;
- by technology itself, if contains tools for measurement and information storaging and transfer;
- directly by authorized organization;

All procurement subjects, which can't be identified as process or equipment, but can be detected as its indispensable part, such as nodes, portals or any places for clients communication, cooperation and increasing process quality. They also may be certified as described above.

### 2.3.3. Storage and other

Human interface is used for displaying and processing of information, received directly from technology level as input. Its primary goal is information processing and transferring, possible storage and support. Storage cannot be used for saving units such as digital tokens, currencies preservation. It does not bring any methods, which may have an impact on previous levels by changing their inner structure. Technology and procurement process can affect storage by changing internal structure, which is an information input.

Direct communication between technology and client storage should contain such characteristics:

- security – critically important to ensure client data and information safe and reliable preservation and processing;
- reliability – ability to provide uninterrupted and unlimited storage functioning and communication between level during one or more levels state change and proper reflection of these changes;
- convenient – property to anticipate and fulfill client expectation about system and processes quality;

Storage may obtain certificates with help of installed software or any other types of software interaction. Any type of subjects, which cannot be determined, as levels described, must be detected as *other* and require further management and actions, including public discussion, SCEBAS processing etc.

## 3. Research and calculations

### 3.1. Research

According to absence of strict rules and guidelines for the current field, estimation of significant cryptocurrencies set stands out as off-gauge and hard task. Thus, a number of questions arises when users face a certain token:

- expectable term of life for considered currency;
- fairness of economical characteristics;
- novelty and uniqueness;
- quality of technical part;
- parameters to compare between cryptocurrencies;
- range of values to use;

Multiple mathematical apparatuses can be applied in this case. "Fuzzy logic" can be provided as the most suitable and convenient solution. It allows to formalize and easily create input-output rules. Value drivers are basic and irreplaceable part of SCEBAS, which represents the primary idea for calculations of cryptocurrency united estimation.

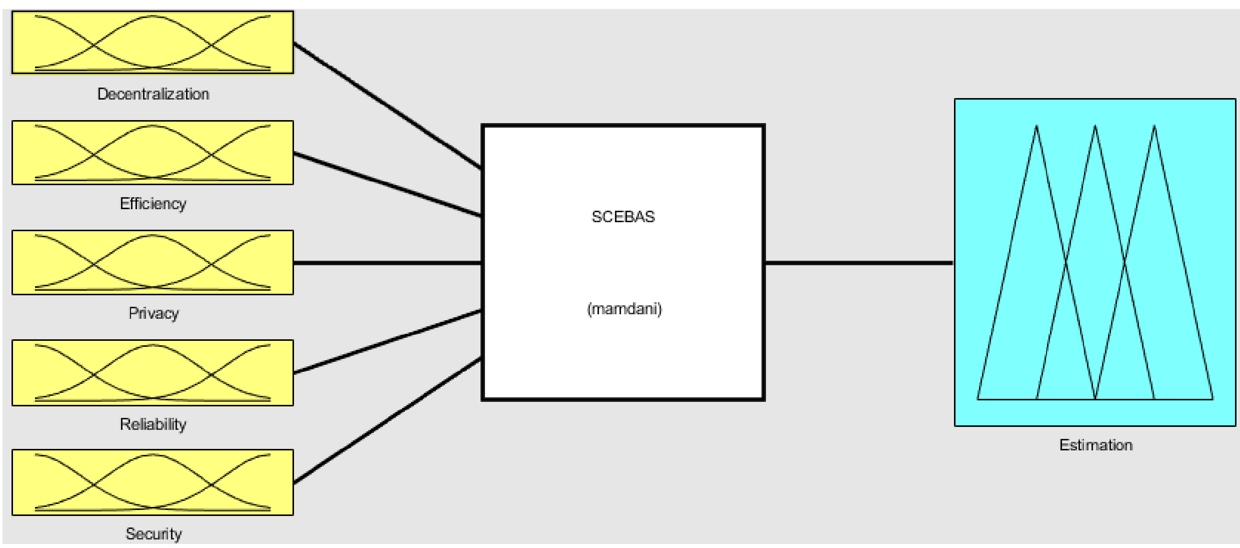



**Figure 5.** SCEBAS constituents using fuzzy logic

Every SCEBAS component has its own inputs and fuzzy rules for calculation of output efficiency values. Output of each component is presented as linguistic variable "Estimation" with values: "negative", "bad", "neutral", "good", and "excellent". Membership function has triangular type with range [0–100%].

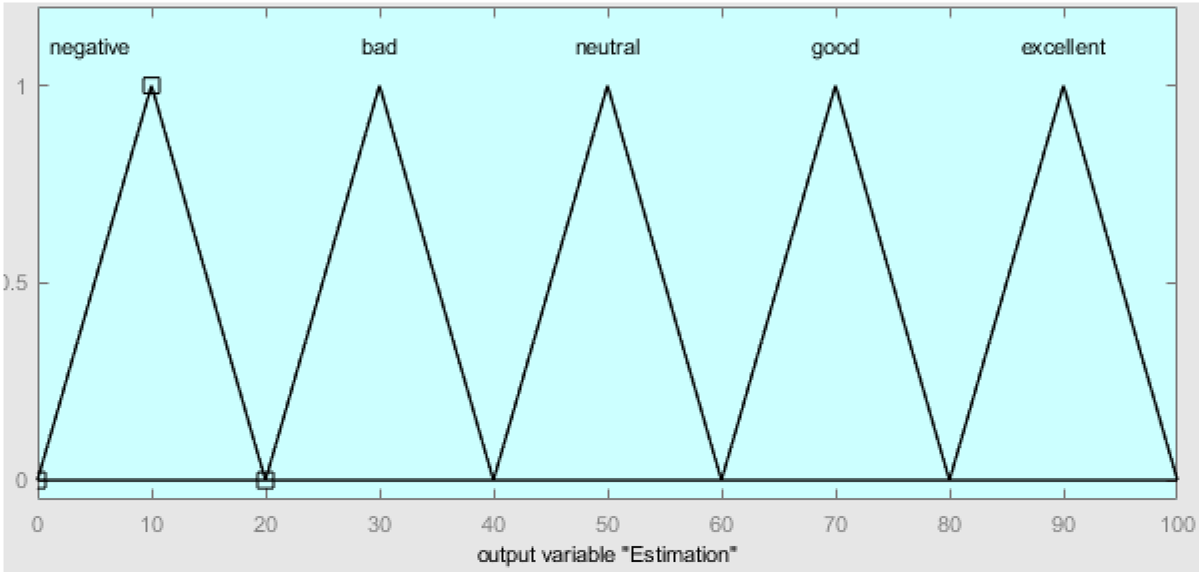



**Figure 6.** Estimation linguistic variable

Inputs for SCEBAS components presented as membership functions with triangular and Gaussian types (depending on parameter).

The triangular curve is a function of a vector, x, and depends on three scalar parameters a, b, and c, as given by

$$f(x,a,b,c) = \begin{cases} 0, & x \leq a \\ \dfrac{x-a}{b-a}, & a \leq x \leq b \\ \dfrac{c-x}{c-b}, & b \leq x \leq c \\ 0, & c \leq x \end{cases}$$

The symmetric Gaussian function depends on two parameters σ and c as given by

$$f(x,\sigma,c) = e^{\frac{-(x-c)^2}{2\sigma^2}} \quad [9]$$

*Decentralization* component has 3 inputs and 1 output scheme (**Figure 7**).

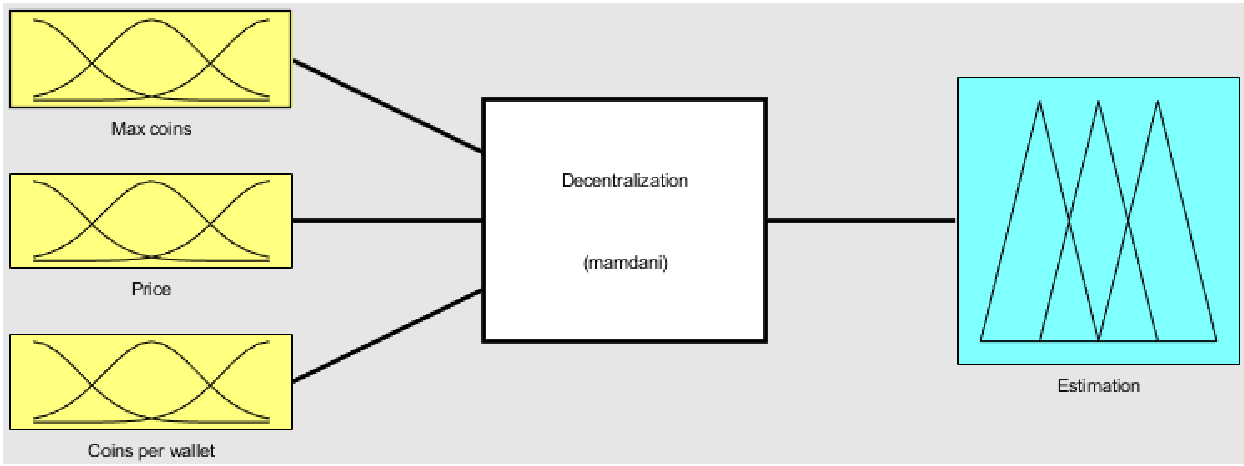



**Figure 7.** Decentralization value driver

Inputs presented as linguistic variables are next:

- “Max coins” – circulating coins supply at current time. Membership function has Gaussian type with range [0–$10^{12}$] and values: [“few”, “enough”, “a lot”, “to much”, “lost of”];

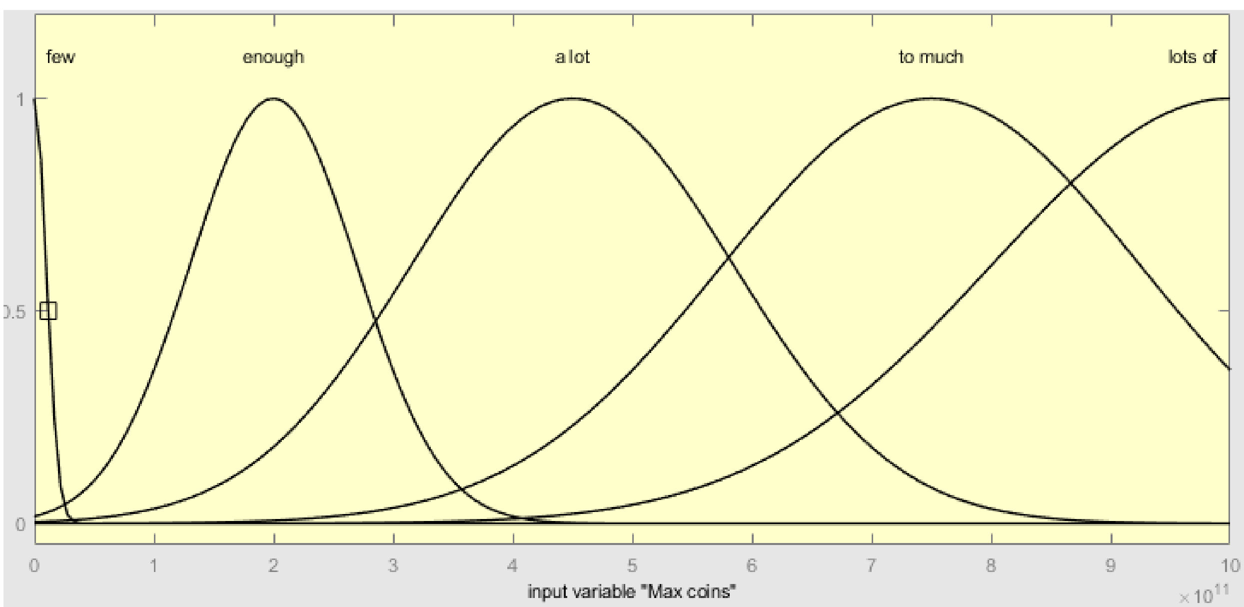



**Figure 8.** Decentralization max coin input

- “Price” – the average market price of cryptocurrency. Membership function has Gaussian type with range [0–5·$10^4$] and values: [“low”, “medium”, “high”];

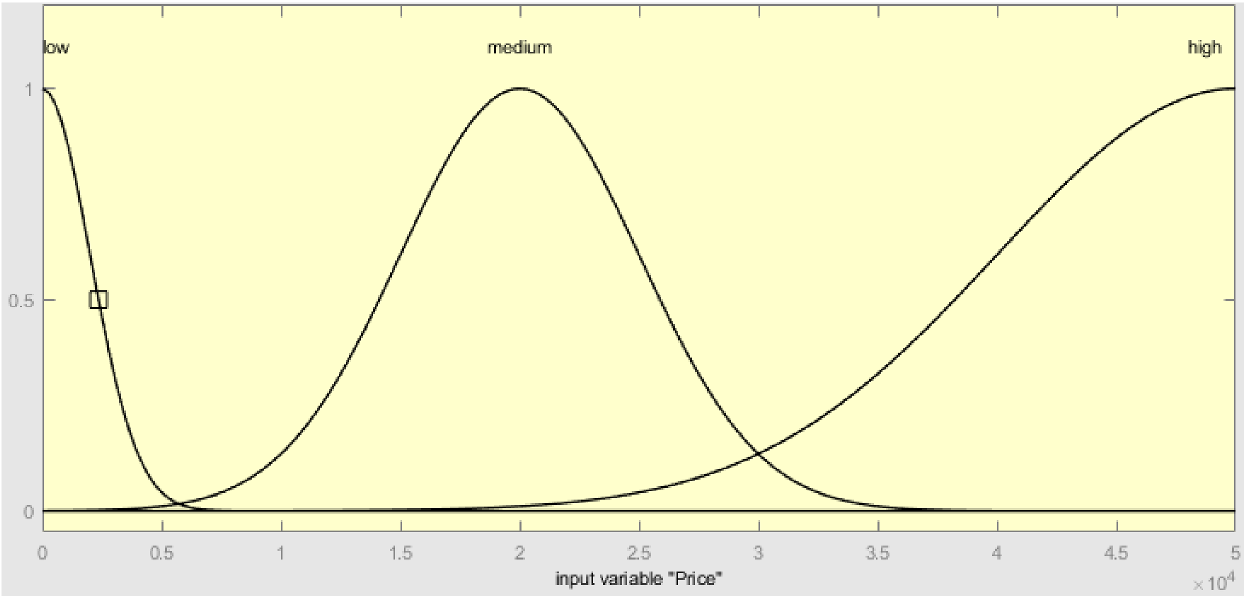



**Figure 9.** Decentralization price input

- "Coins in richest wallet" – amount of coins stored in top wallet from rich list. Membership function has Gaussian type with range [0–0.01% from circulating coins supply] and values: ["normal", "a lot"];

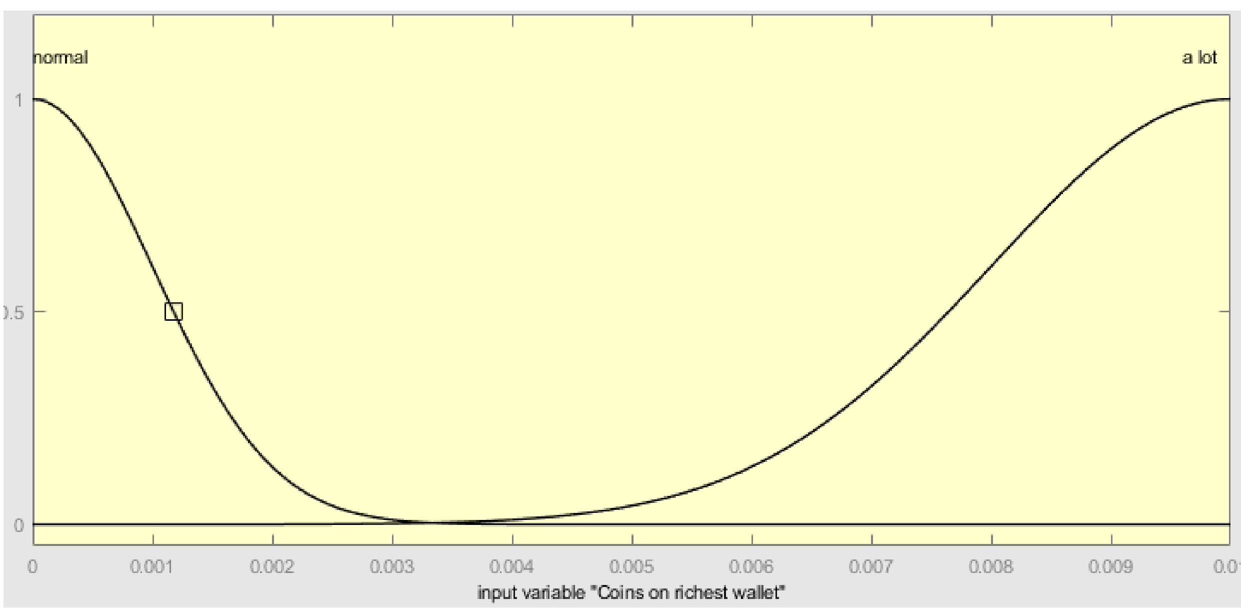



**Figure 10.** Decentralization coins in richest wallet input

*Security* component has 2 inputs and 1 output scheme (**Figure 11**).

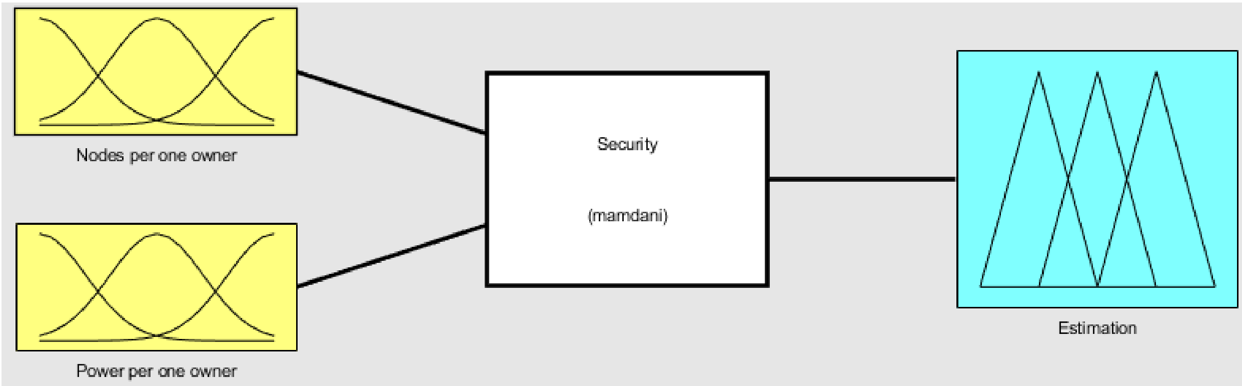



**Figure 11.** Security value driver

Inputs represented as linguistic variables are next:

- "Nodes per one owner" – how many nodes are controlled by one person or organization (less percentage means less influence on network functioning). Membership function has Gaussian type with range [0–100%] and values: ["normal", "risky", "critical"];

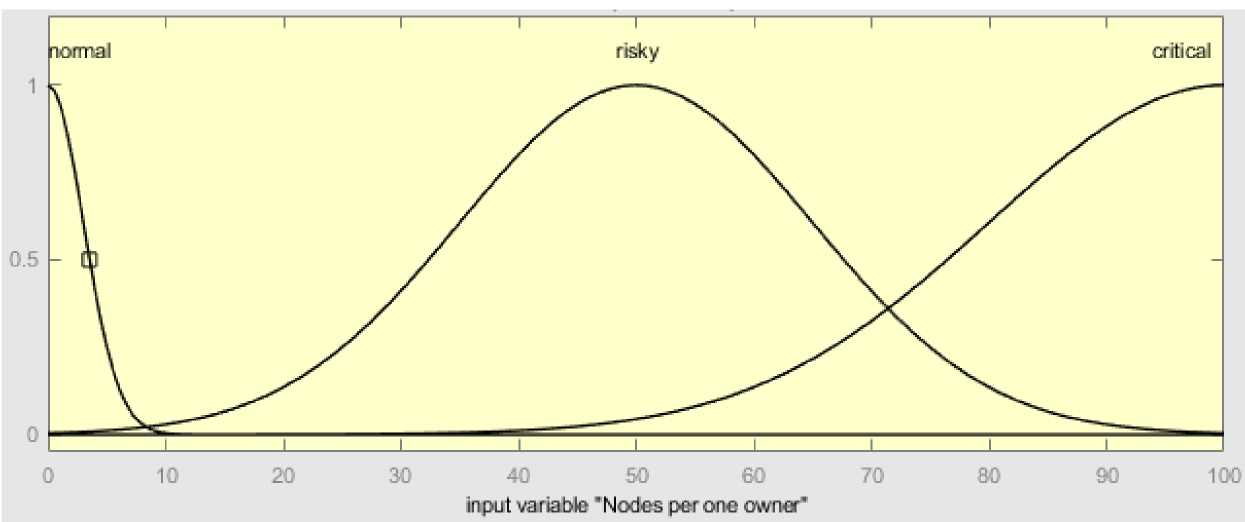



**Figure 12.** Security nodes per one owner input

- "Power per one owner" – relation of hardware power to one person or organization for blocks generated by POW/POS systems. Membership function has Gaussian type with range [0–100%] and values: ["low", "medium", "high", "critical"];

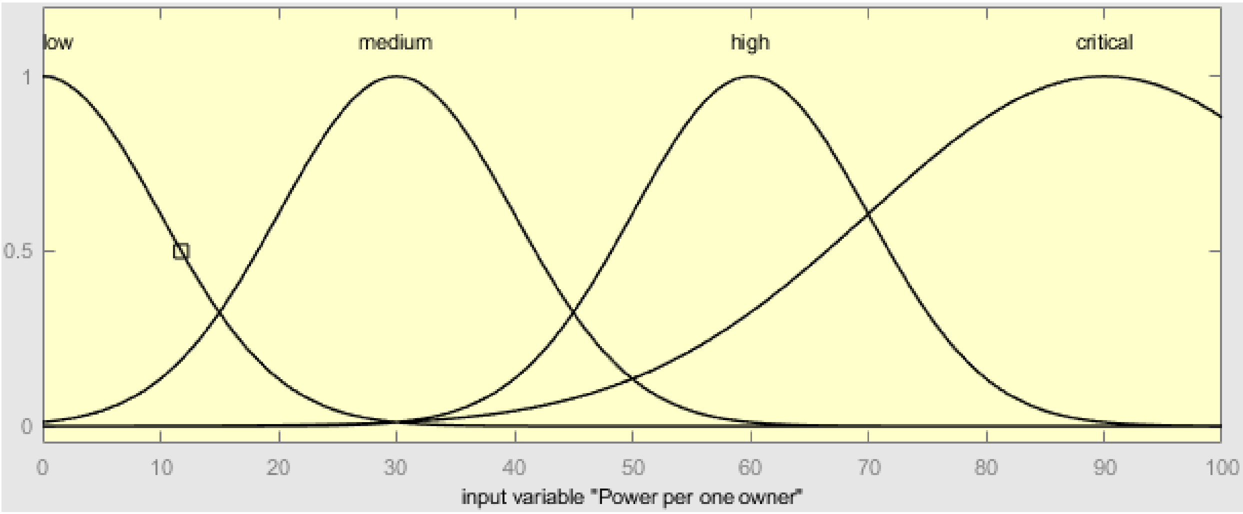



**Figure 13.** Security power per one owner input

*Reliability* component has 4 inputs and 1 output (**Figure 14**).

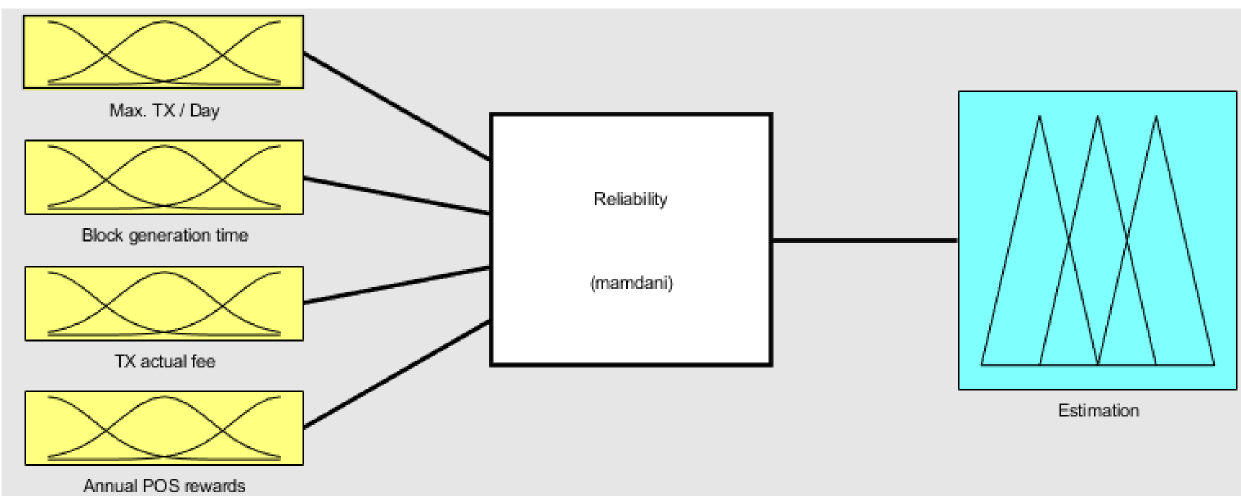



**Figure 14.** Reliability value driver

Inputs represented as linguistic variables are next:

- “Max. TX / Day” – average count of completed transactions per day. Membership function has Gaussian type with range [0–$10^8$] and values: [“low”, “medium”, “high”];

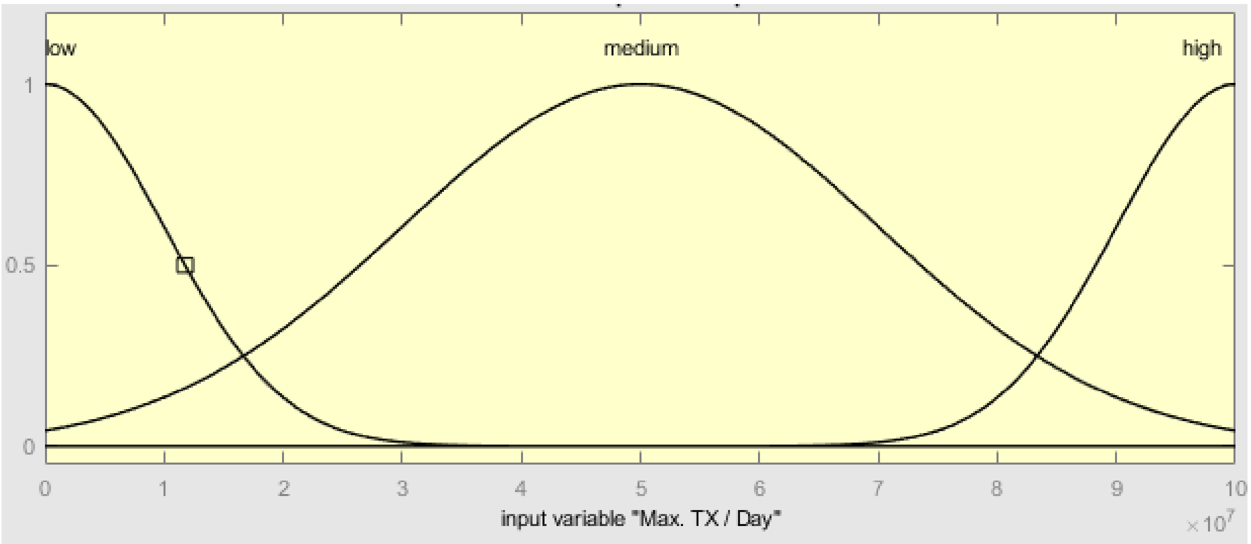



**Figure 15.** Reliability max. TX / Day input

- "Block generation time" – time needed for one block generation (depends on cryptocurrency algorithm). Membership function has Gaussian type with range [0–20 minutes] and values: ["super-fast", "fast", "normal" , "slow"];

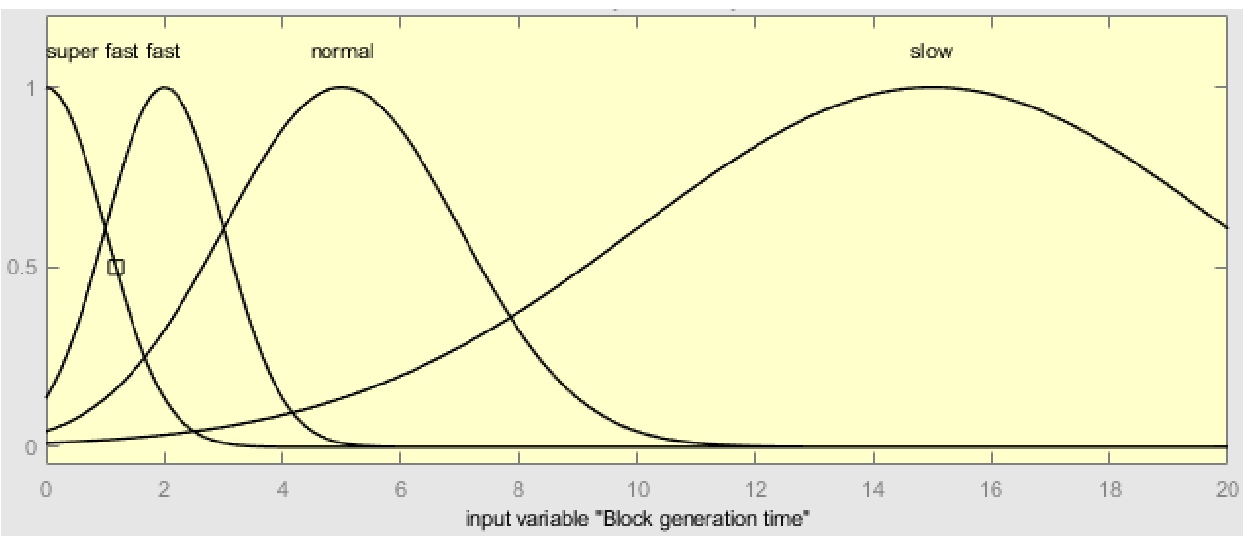



**Figure 16.** Reliability block generation time input

- "TX actual fee" – the lowest fee value needed to complete one transaction during the day. Membership function has Gaussian type with range [0–0.5% of average cryptocurrency price] and values: ["low", "medium", "high" , "critical"];

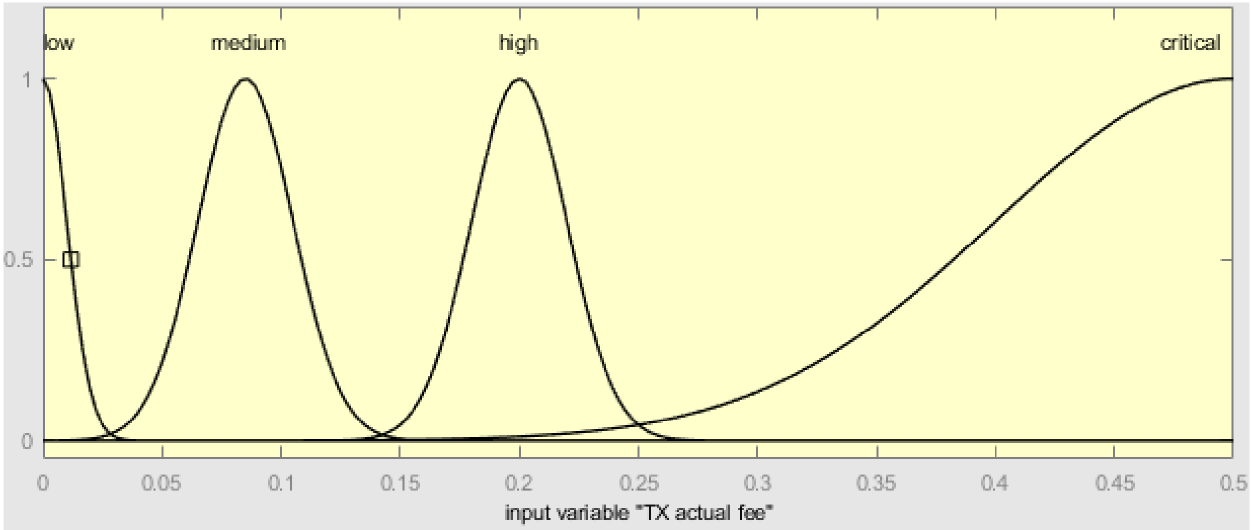



**Figure 17.** Reliability TX actual fee input

- “Annual POS rewards” – amount of coins that will be earned by cryptocurrency holders for certain period. Membership function has Gaussian type with range [0–500% of wallet deposit] and values: [“low”, “medium”, “high”];

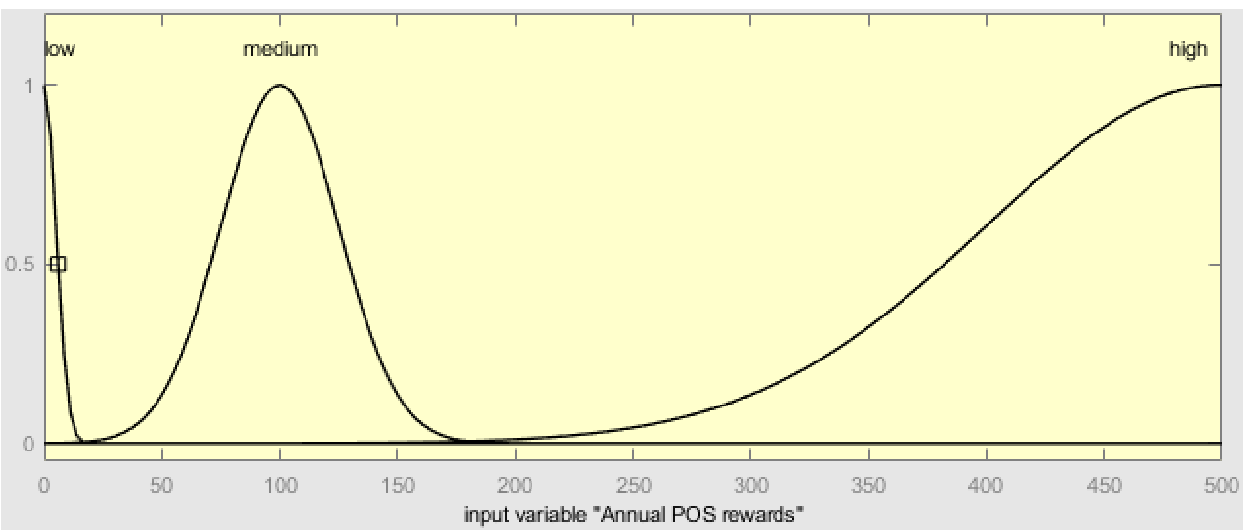



**Figure 18.** Reliability annual POS rewards input

*Efficiency* component has 2 inputs and 1 output (**Figure 19**).

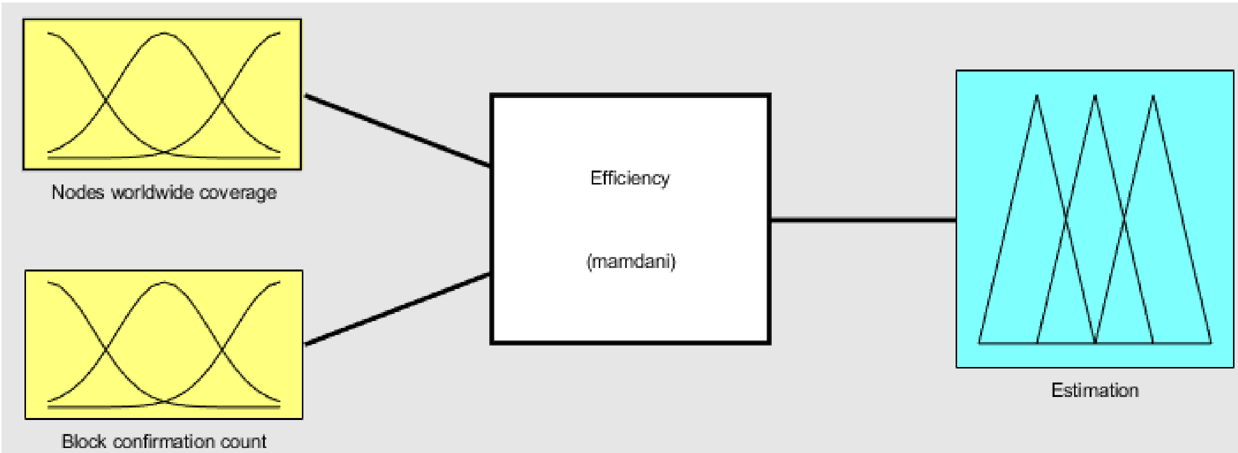



**Figure 19.** Efficiency value driver

Inputs represented as linguistic variables are next:

- "Nodes worldwide coverage" – a number of nodes available globally and separated by countries for support cryptocurrency network. Membership function has Gaussian type with range [0–100%] (where 100% means that each country has at least 100 independent active nodes) and values: ["low", "medium", "high"];

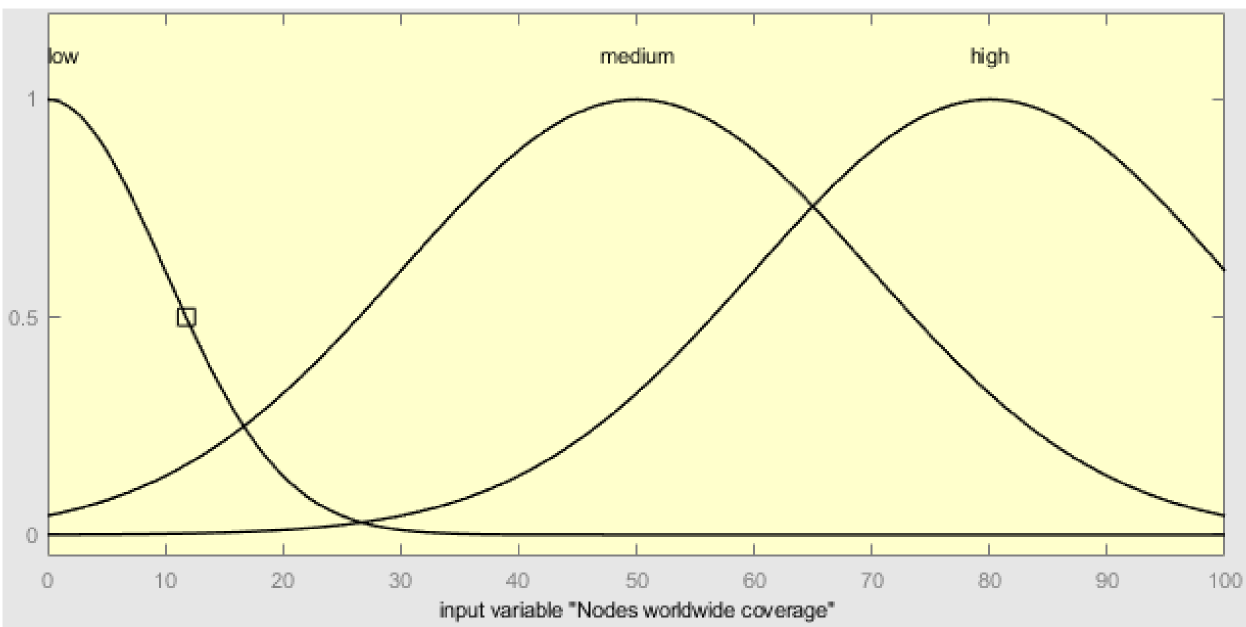



**Figure 20.** Efficiency nodes worldwide coverage input

- "Blocks confirmation count" – blocks volume to wait until transaction will be confirmed. Membership function has Gaussian type with range [0–100] and values: ["low", "medium", "high"];

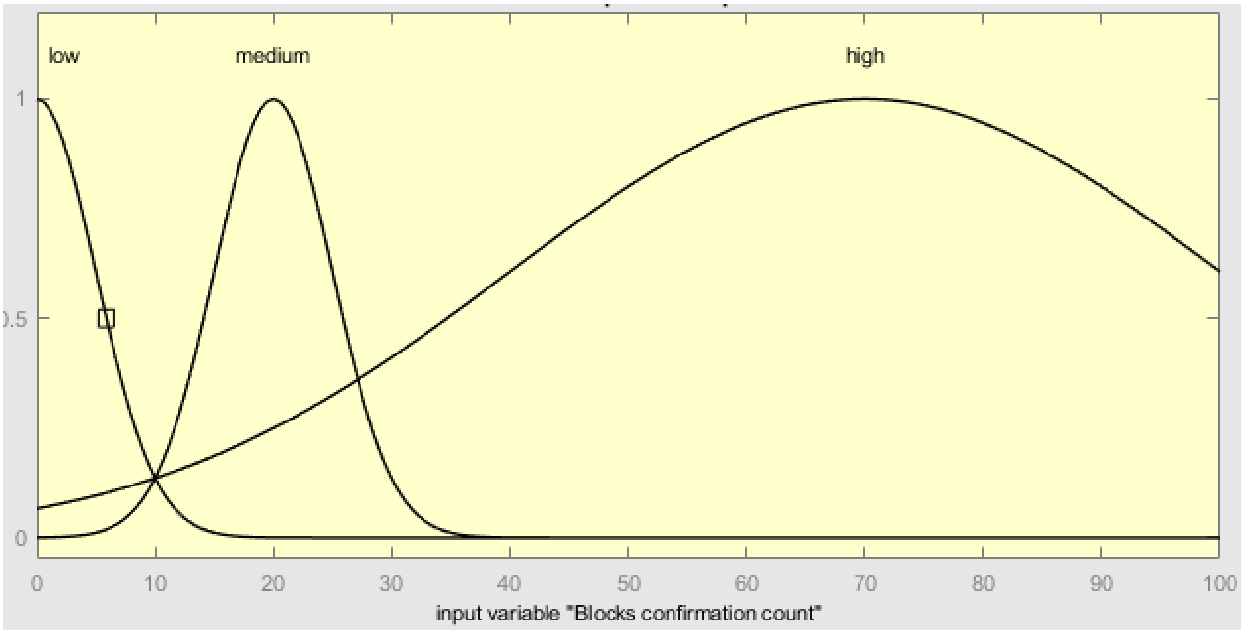



**Figure 21.** Efficiency blocks confirmation count input

*Privacy* component has 3 inputs and 1 output (**Figure 22**).

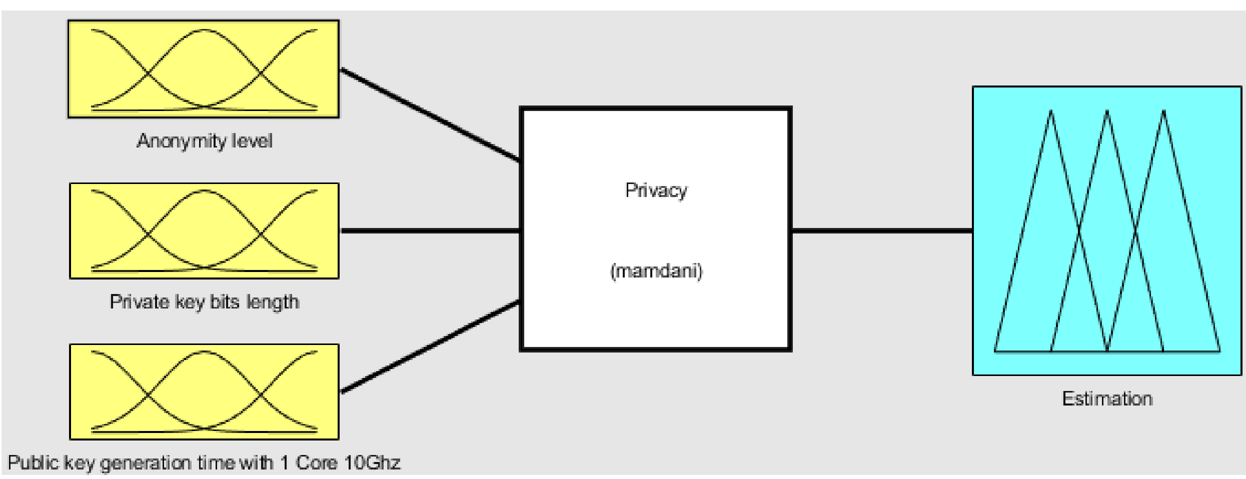



**Figure 22.** Privacy value driver

Inputs represented as linguistic variables are next:

- “Anonymity level” – relative value, which describes the difficulty level of transaction participant tracking. It depends on capabilities to obfuscate clients’ IP addresses, supporting anonymous transactions (with included mobile transactions), and a level of blockchain publicity. Membership function has Gaussian type with range [0–100%] and values: [“low”, “medium”, “high”];

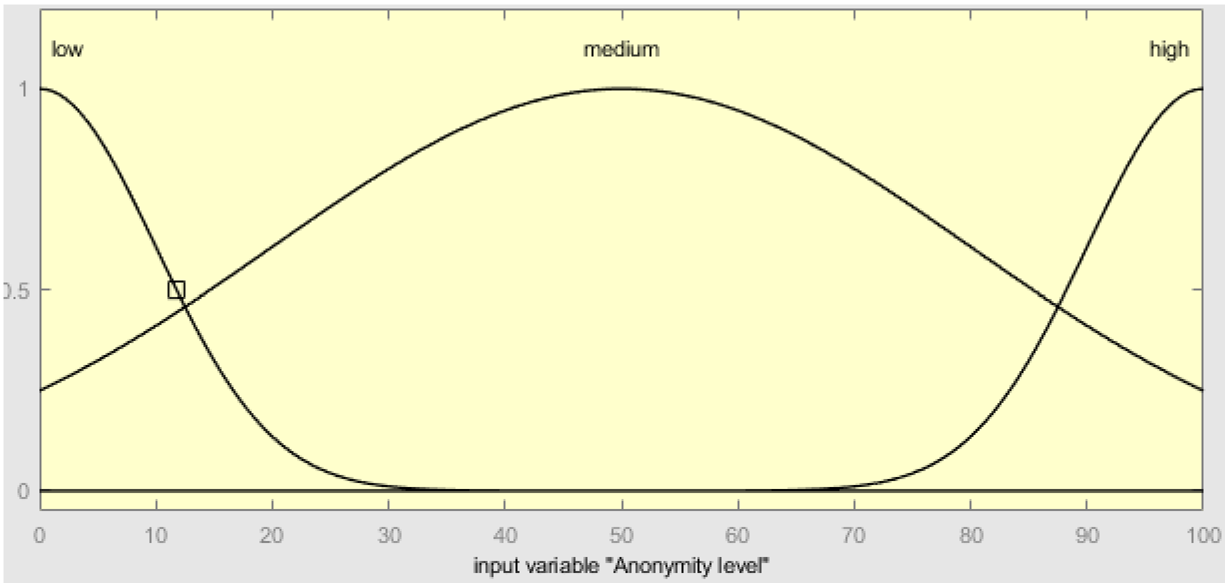



**Figure 23.** Privacy anonymity level input

- “Private key bits length” – the length of cryptocurrency wallet private key. Membership function has Gaussian type with range [0–16384 bits] and values: [“short”, “medium”, “long”];

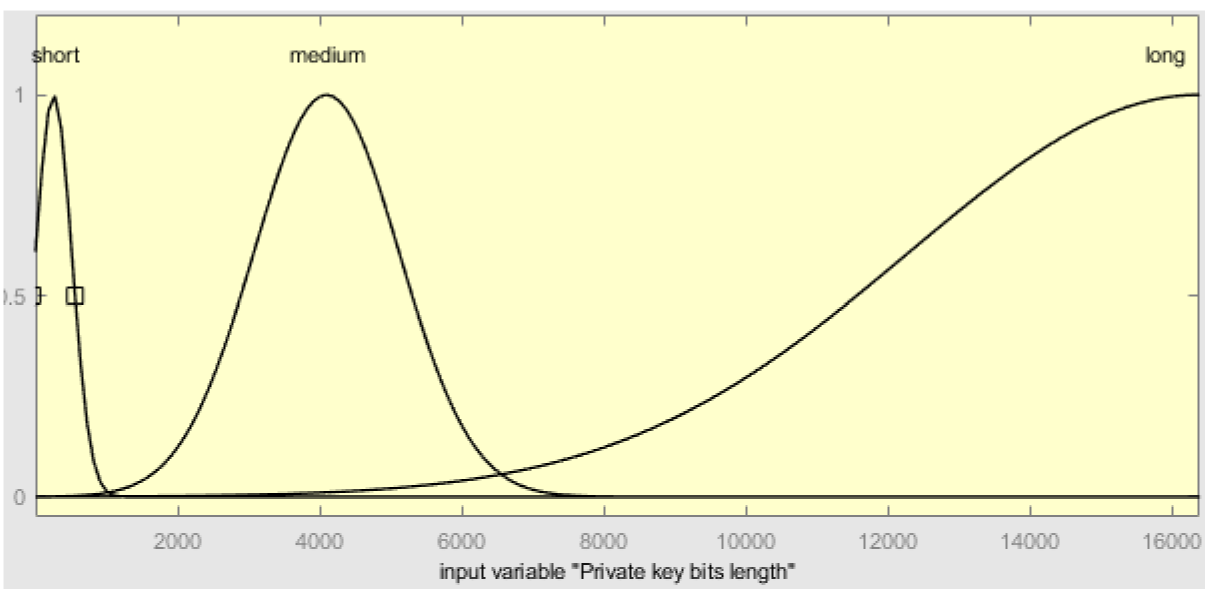



**Figure 24.** Privacy private key bits length vel input

- "PK gen. time with 1 Core 10GHz CPU" – average time for public key generated by private key with using 1 Core 10Ghz CPU. Membership function has Gaussian type with range [0–60000 ms] (where 1s = 1000ms) and values: ["fast", "medium", "slow"];

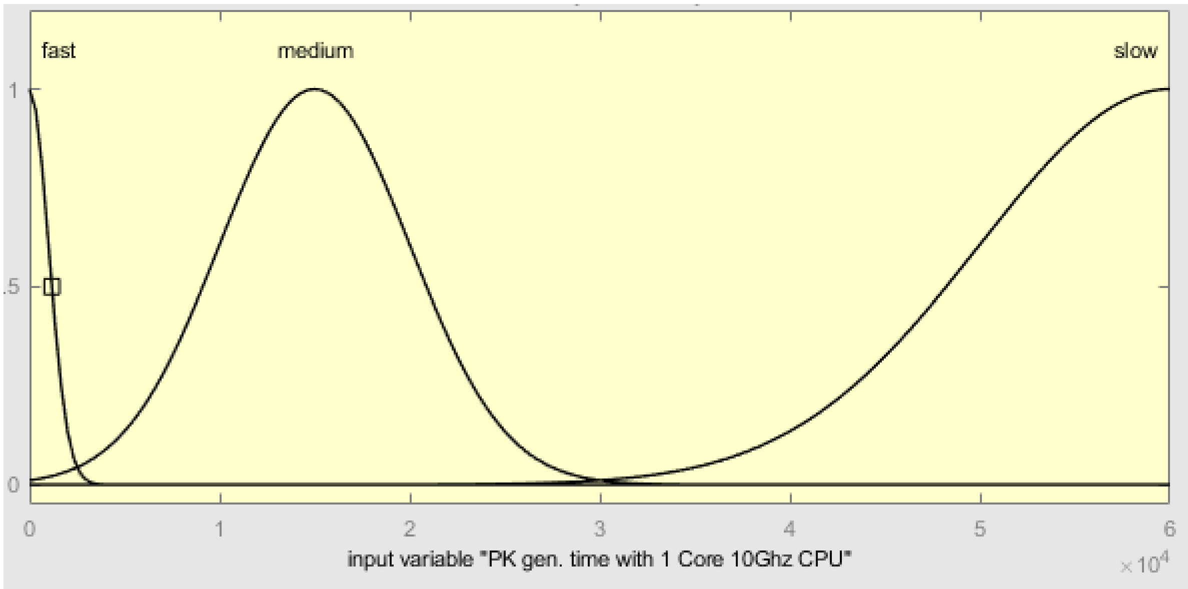



**Figure 25.** Privacy PK gen. time with 1 Core 10GHz CPU input

### 3.2. Results of estimation for Bitcoin cryptocurrency

*Decentralization*: input – [1.68e+11;1e+04;0.01], output – 14%;

Sources:

- https://coinmarketcap.com
- https://bitinfocharts.com/ru/top-100-richest-bitcoin-addresses.html

*Security*: input – [10;25.2], output – 50.5;

Sources:

- https://www.buybitcoinworldwide.com/mining/pools/
- https://bitnodes.earn.com

*Reliability*: input – [5e+05;10;0.1;0], output – 45.3

Sources:

- https://bitcoin.org
- https://bitcoinfees.earn.com

- https://blockchain.info/ru/charts/n-transactions?timespan=all

*Efficiency*: input – [15;6], output – 49.3

Sources:

- https://bitnodes.earn.com
- https://en.bitcoin.it/wiki/Confirmation

*Privacy*: input – [20;256;100], output – 28.6

Sources:

- https://en.bitcoin.it/wiki/Anonymity
- https://github.com/bitcoin/bitcoin

*SCEBAS Estimation*: input [14;50.5;45.3;49.3;28.6], output – 31.1% (**Figure 26**).

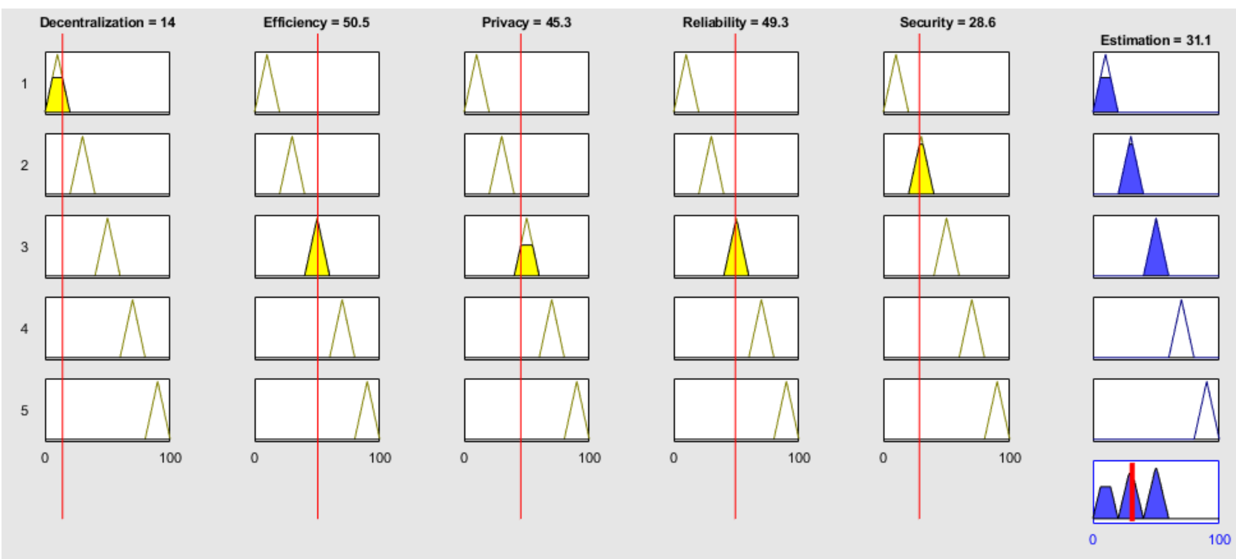



**Figure 26.** SCEBAS estimation

Estimation results indicate that weak points of bitcoin are decentralization (the reason is many ASICs, that are mostly placed in China), and security level (private key length is short, and speed of generation public addresses by private keys is relatively high).

Estimation result 31.1% is a strong "C".

# 4. Certore tokens

## 4.1. Certore

Currently used technology could be represented as an expendable model. Each next unit generation requires more equipment power and growing network could produces multiple undesirable consequences, such as the increase of transaction time, transaction fee etc. Equipment volume, which depends directly on expandable model, can be described as maximum value of possible usage:

$$V = \max(volume_e)$$

Therefore, additional costs appear due to increasing of equipment volume and network size, which result directly in reduction of procurement process profitability. Let $\lambda$ be an equilibrium or point at which cost equals profit of unit generation. We define a function of profit, which is related to procurement index at a certain moment of time to equilibrium procurement index:

$$f_{profit} = \frac{PI_t}{\lambda} > 1,$$

$$\lambda = \frac{p}{T_c}, when\ costs = profit$$

The technology that can be described as expandable model, which includes procurement process, is defined as such*: function of procurement profit is aimed to equilibrium with each generated unit, when amount of equipment is constant.* This vulnerability can be eliminated according to detected technology scopes in several ways:

- by increasing number of units and technology improving;
- by increasing amount of units keeping technology in current state, if such type of changes affects technology (analog is fiat emission);
- by improving of technology keeping number of units;

Certification of units, which invoke this process manually or automatically, should be implemented by using software or any other possible type of tools, provided by Certore and with mandatory SCEBAS involvement (**Figure 5**). Procurement process of Certore tokens will be implemented according to accepted standards and cannot be removed or replaced.

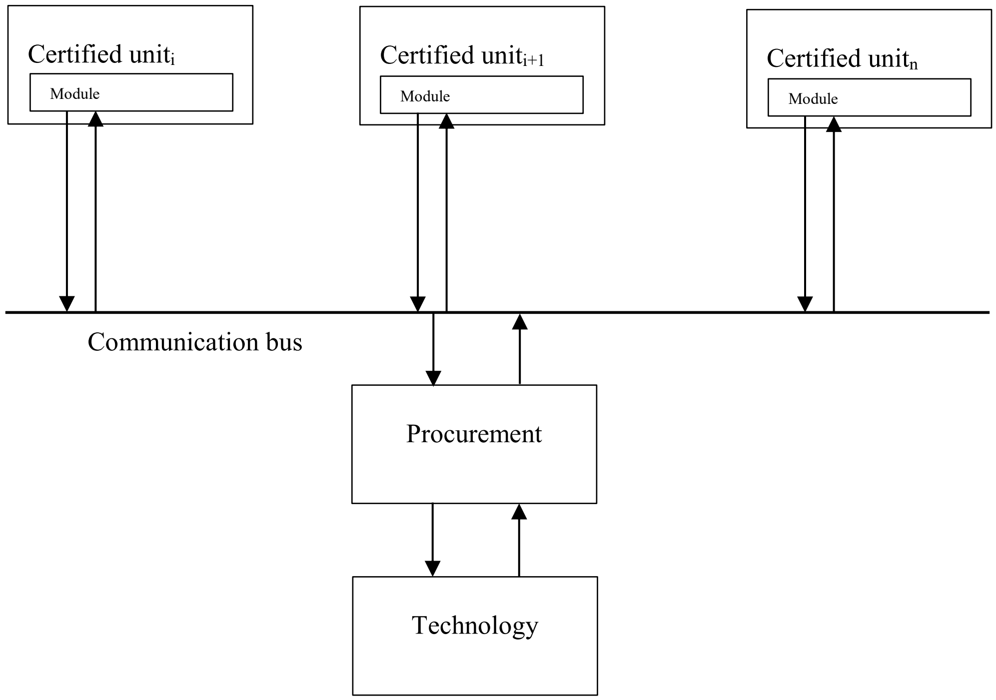



**Figure 27.** Possible certification process

The process of communication can be realized by a set of public API and/or any type of technical tools, which provide relations between certificating unit and Certore technology through procurement process as a method of standardization, certification, tokens production and distribution. This process can receive, pass and transform information according to required state depending on communication level without any distortion. Technology and procurement compile a united Certore system, which serves not only as a bridge between certificating units and process of standard and certificated development, including SCEBAS as required part and token producer and distributor.

## 4.2. Tokens

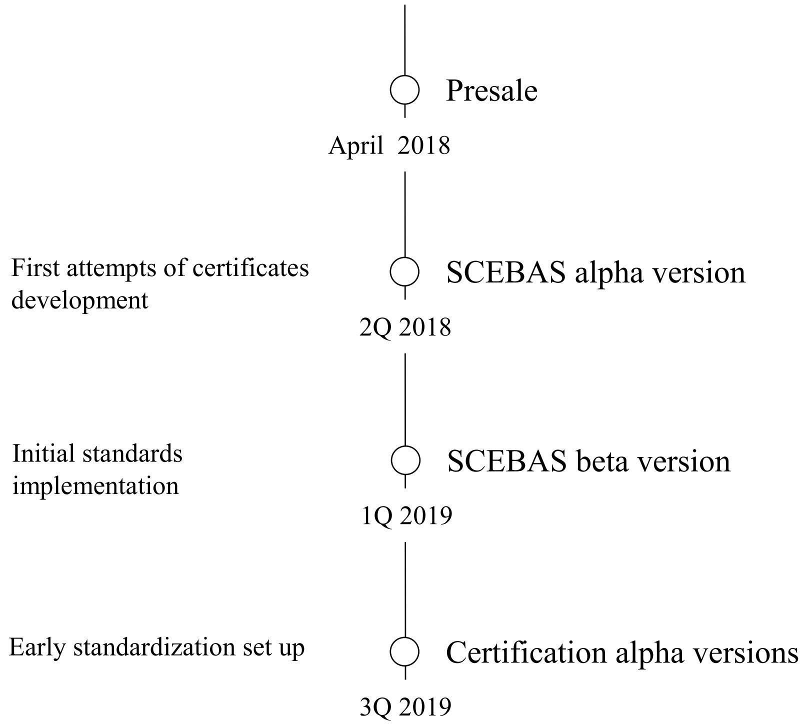
Total volume of available tokens is 75.000.000.

Maximum amount available for presale is 7.500.000 tokens, 67.500.000 are reserved and will be dispatched at ICO stage.

Technology and related items can be modified and changed during development process, standard and certificate introduction, including described and determined possible problems, which will be solved with help of SCEBAS.

Information about ICO and possible bonus stages will be provided by the rules of transparency, justice and publicity.

## 5. Roadmap


Presale
April 2018
First attempts of certificates development
SCEBAS alpha version
2Q 2018
Initial standards implementation
SCEBAS beta version
1Q 2019
Early standardization set up
Certification alpha versions
3Q 2019

## Reference


[1] International Organization for Standardization, 2011. *ISO in brief.*

[2] The American Society of Mechanical Engineers (ASME), 2017. *Examples of Use of Codes and Standards for Students in Mechanical Engineering and Other Fields.* ASME Srtandards & Certifications, 27

[3] Voting, 2017. https://en.wikipedia.org/wiki/Voting

[4] Norris, P., 2001. *Digital divide: Civic engagement, information poverty, and the Internet worldwide*. Cambridge, USA: Cambridge University Press.

[5] https://segwit2x.github.io

[6] Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf, 1

[7] International Organization for Standardization, 2015. *Quality management systems — Fundamentals and vocabulary.* ISO/FDIS 9000:2015(E), 22

[8] International Organization for Standardization, 2014. *Codes for the Representation of Names of Languages*.

[9] Zadeh, L.A., 1965. "Fuzzy sets". *Information and Control*. 8 (3): 338–353

# Appendix

## *SCEBAS.fis*

```
[System]
Name='SCEBAS'
Type='mamdani'
Version=2.0
NumInputs=5
NumOutputs=1
NumRules=5
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'

[Input1]
Name='Decentralization'
Range=[0 100]
NumMFs=5
MF1='negative':'trimf',[0 10 20]
MF2='bad':'trimf',[20 30 40]
MF3='neutral':'trimf',[40 50 60]
MF4='good':'trimf',[60 70 80]
MF5='excellent':'trimf',[80 90 100]

[Input2]
Name='Efficiency'
Range=[0 100]
NumMFs=5
MF1='negative':'trimf',[0 10 20]
MF2='bad':'trimf',[20 30 40]
MF3='neutral':'trimf',[40 50 60]
MF4='good':'trimf',[60 70 80]
MF5='excellent':'trimf',[80 90 100]

[Input3]
Name='Privacy'
Range=[0 100]
NumMFs=5
MF1='negative':'trimf',[0 10 20]
MF2='bad':'trimf',[20 30 40]
MF3='neutral':'trimf',[40 50 60]
MF4='good':'trimf',[60 70 80]
MF5='excellent':'trimf',[80 90 100]

[Input4]
Name='Reliability'
Range=[0 100]
NumMFs=5
MF1='negative':'trimf',[0 10 20]
MF2='bad':'trimf',[20 30 40]
MF3='neutral':'trimf',[40 50 60]
MF4='good':'trimf',[60 70 80]
MF5='excellent':'trimf',[80 90 100]

[Input5]
Name='Security'
Range=[0 100]
NumMFs=5
MF1='negative':'trimf',[0 10 20]
MF2='bad':'trimf',[20 30 40]
```

MF3='neutral':'trimf',[40 50 60]
MF4='good':'trimf',[60 70 80]
MF5='excellent':'trimf',[80 90 100]

[Output1]
Name='Estimation'
Range=[0 100]
NumMFs=5
MF1='negative':'trimf',[0 10 20]
MF2='bad':'trimf',[20 30 40]
MF3='neutral':'trimf',[40 50 60]
MF4='good':'trimf',[60 70 80]
MF5='excellent':'trimf',[80 90 100]

[Rules]
1 1 1 1 1, 1 (1) : 2
2 2 2 2 2, 2 (1) : 2
3 3 3 3 3, 3 (1) : 2
4 4 4 4 4, 4 (1) : 2
5 5 5 5 5, 5 (1) : 2

## *Decentralization.fis*

```
[System]
Name='Decentralization'
Type='mamdani'
Version=2.0
NumInputs=3
NumOutputs=1
NumRules=5
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'

[Input1]
Name='Max coins'
Range=[0 1000000000000]
NumMFs=5
MF1='few':'gaussmf',[10000000000 0]
MF2='enough':'gaussmf',[70000000000 200000000000]
MF3='a lot':'gaussmf',[135000000000 450000000000]
MF4='to much':'gaussmf',[175000000000 750000000000]
MF5='lots of':'gaussmf',[200000000000 1000000000000]

[Input2]
Name='Price'
Range=[0 50000]
NumMFs=3
MF1='low':'gaussmf',[2000 0]
MF2='medium':'gaussmf',[5000 20000]
MF3='high':'gaussmf',[10000 50000]

[Input3]
Name='Coins on richest wallet'
Range=[0 0.01]
NumMFs=2
MF1='normal':'gaussmf',[0.001 0]
MF2='a lot':'gaussmf',[0.002 0.01]

[Output1]
Name='Estimation'
Range=[0 100]
NumMFs=5
MF1='negative':'trimf',[0 10 20]
MF2='bad':'trimf',[20 30 40]
MF3='neutral':'trimf',[40 50 60]
MF4='good':'trimf',[60 70 80]
MF5='excellent':'trimf',[80 90 100]

[Rules]
0 3 2, 1 (1) : 2
2 2 2, 2 (1) : 1
3 2 1, 3 (1) : 1
4 1 1, 4 (1) : 1
5 2 1, 5 (1) : 1
```

## *Security.fis*

```
[System]
Name='Security'
Type='mamdani'
Version=2.0
NumInputs=2
NumOutputs=1
NumRules=5
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'

[Input1]
Name='Nodes per one owner'
Range=[0 100]
NumMFs=3
MF1='normal':'gaussmf',[3 0]
MF2='risky':'gaussmf',[15 50]
MF3='critical':'gaussmf',[20 100]

[Input2]
Name='Power per one owner'
Range=[0 100]
NumMFs=4
MF1='low':'gaussmf',[10 0]
MF2='medium':'gaussmf',[10 30]
MF3='high':'gaussmf',[10 60]
MF4='critical':'gaussmf',[20 90]

[Output1]
Name='Estimation'
Range=[0 100]
NumMFs=5
MF1='negative':'trimf',[0 10 20]
MF2='bad':'trimf',[20 30 40]
MF3='neutral':'trimf',[40 50 60]
MF4='good':'trimf',[60 70 80]
MF5='excellent':'trimf',[80 90 100]

[Rules]
1 1, 5 (1) : 1
1 2, 4 (1) : 1
2 3, 3 (1) : 2
3 3, 2 (1) : 1
3 4, 1 (1) : 2
```

## *Reliability.fis*

```
[System]
Name='Reliability'
Type='mamdani'
Version=2.0
NumInputs=4
NumOutputs=1
NumRules=5
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'

[Input1]
Name='Max. TX / Day'
Range=[0 100000000]
NumMFs=3
MF1='low':'gaussmf',[10000000 0]
MF2='medium':'gaussmf',[20000000 50000000]
MF3='high':'gaussmf',[10000000 100000000]

[Input2]
Name='Block generation time'
Range=[0 20]
NumMFs=4
MF1='super fast':'gaussmf',[1 0]
MF2='fast':'gaussmf',[1 2]
MF3='normal':'gaussmf',[2 5]
MF4='slow':'gaussmf',[5 15]

[Input3]
Name='TX actual fee'
Range=[0 0.5]
NumMFs=4
MF1='low':'gaussmf',[0.01 0]
MF2='medium':'gaussmf',[0.02 0.085]
MF3='high':'gaussmf',[0.02 0.2]
MF4='critical':'gaussmf',[0.1 0.5]

[Input4]
Name='Annual POS rewards'
Range=[0 500]
NumMFs=3
MF1='low':'gaussmf',[5 0]
MF2='medium':'gaussmf',[25 100]
MF3='high':'gaussmf',[100 500]

[Output1]
Name='Estimation'
Range=[0 100]
NumMFs=5
MF1='negative':'trimf',[0 10 20]
MF2='bad':'trimf',[20 30 40]
MF3='neutral':'trimf',[40 50 60]
MF4='good':'trimf',[60 70 80]
MF5='excellent':'trimf',[80 90 100]

[Rules]
0 4 4 3, 1 (1) : 2
1 0 0 2, 2 (1) : 2
0 3 3 0, 3 (1) : 2
2 2 2 1, 4 (1) : 1
3 1 1 1, 5 (1) : 2
```

## *Efficiency.fis*

```
[System]
Name='Efficiency'
Type='mamdani'
Version=2.0
NumInputs=2
NumOutputs=1
NumRules=5
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'

[Input1]
Name='Nodes worldwide coverage'
Range=[0 100]
NumMFs=3
MF1='low':'gaussmf',[10 0]
MF2='medium':'gaussmf',[20 50]
MF3='high':'gaussmf',[20 80]

[Input2]
Name='Blocks confirmation count'
Range=[0 100]
NumMFs=3
MF1='low':'gaussmf',[5 0]
MF2='medium':'gaussmf',[5 20]
MF3='high':'gaussmf',[30 70]

[Output1]
Name='Estimation'
Range=[0 100]
NumMFs=5
MF1='negative':'trimf',[0 10 20]
MF2='bad':'trimf',[20 30 40]
MF3='neutral':'trimf',[40 50 60]
MF4='good':'trimf',[60 70 80]
MF5='excellent':'trimf',[80 90 100]

[Rules]
3 1, 5 (1) : 1
2 1, 4 (1) : 1
2 2, 3 (1) : 1
1 2, 2 (1) : 1
1 3, 1 (1) : 1
```

## *Privacy.fis*

```
[System]
Name='Privacy'
Type='mamdani'
Version=2.0
NumInputs=3
NumOutputs=1
NumRules=5
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'

[Input1]
Name='Anonymity level'
Range=[0 100]
NumMFs=3
MF1='low':'gaussmf',[10 0]
MF2='medium':'gaussmf',[30 50]
MF3='high':'gaussmf',[10 100]

[Input2]
Name='Private key bits length'
Range=[1 16384]
NumMFs=3
MF1='short':'gaussmf',[256 256]
MF2='medium':'gaussmf',[1024 4096]
MF3='long':'gaussmf',[4096 16380]

[Input3]
Name='PK gen. time with 1 Core 10Ghz CPU'
Range=[0 60000]
NumMFs=3
MF1='fast':'gaussmf',[1000 0]
MF2='medium':'gaussmf',[5000 15000]
MF3='slow':'gaussmf',[10000 60000]

[Output1]
Name='Estimation'
Range=[0 100]
NumMFs=5
MF1='negative':'trimf',[0 10 20]
MF2='bad':'trimf',[20 30 40]
MF3='neutral':'trimf',[40 50 60]
MF4='good':'trimf',[60 70 80]
MF5='excellent':'trimf',[80 90 100]

[Rules]
1 0 1, 1 (1) : 2
1 1 1, 2 (1) : 1
2 0 2, 3 (1) : 2
2 2 2, 4 (1) : 1
```