ShaktiCoin

The Mathematics behind the *Proof of Effort* Project
Swiss Shakti Foundation

Two Guys from the Milky Way*

September 2017 to May 2019

Part III of IV.

Abstract

Proof of effort is the idea behind the Shakti Foundation's project to overcome poverty and illiteracy by providing every child on Earth with finances to access education.

The simplified description is as follows: Every child on Earth will be granted one Shakti Coin per day, provided that they improve their education by being enrolled in a school or other educational institution.

Proof of Effort is an algorithm implemented by the Shakti Foundation to provide schoolchildren with an easy way to prove their active participation in the project and hence deserve the reward.

This document presents the mathematical building blocks of the Proof of Effort algorithm.

*Swiss Shakti Foundation

Contents

1 Glossary

Throughout this document, the following terms are used with the indicated meanings:

1. **Confederation**: an agreement among a group of separate bodies to cooperate with one another for a common cause(s) while each member maintains sovereign governance and remains independent.

2. **Confederated**: the state of being combined into one.

3. **Miners** or **Node Operators**: individuals who participate in the verification of effort declarations, are licensed to access the Shakti Network, and have committed computing resources (node presence) to reach consensus on and maintain the Shakti blockchain ledger.

4. **Shakti Network**: the logical and physical infrastructure of the Shakti Foundation, which is distributed, decentralized, and public. Anyone can join the Shakti Network by submitting their complete know-your-client (KYC) information. Once they have enrolled, they can choose to become a Shakti wallet holder, a miner/node operator, or both. All participants in the Shakti Network form a confederation.

5. **Blockchain**: a *shared ledger technology* that allows people who do not know each other to trust a record of *events*. The events are stored deterministically with *consensus*, and are simultaneously time stamped and immutable. The ledger will be distributed to all participants in the Shakti Network who use its technology to verify the underlying governance, distribution, and transactions mathematically. The record of events is chained chronologically and is indefinitely verifiable by any miner/node operator in the Shakti Network, thereby eliminating the need for a third-party intermediary.

6. **Shakti Mining Application**: a software application used by miners/node operators to connect with the Shakti Network.

7. **Schools**: all the entities accredited by the respective governing body in their jurisdiction. This term includes public schools and universities, private schools and universities, and other trusted NGO-managed schools and universities.

8. **Independent Schools**: specially certified schools that voluntarily agree to assume an active role in the Shakti Network. These schools are distinct in that they also assume the important role of validators.

9. **Servers**: the distributed network of servers owned by miners/node operators, the Shakti Foundation, and independent schools around the world. Servers use *single sign-on* (SSO), which is a methodology that implements a unique access-authorization mechanism across heterogeneous and geographically distributed servers. Servers take on the integrity of their owners, hence they must not be programmed or otherwise used in any way that would be indicative of their owners having integrity of less than the highest caliber or being susceptible to pressure to commit misdeeds.

10. **Schoolchildren**: students from 0 to 21 years of age that are attending a school or educational institution within the Shakti Network. All children submit their own effort declarations to collect Shakti Coins. Parents, specifically the mother, will receive the Shakti Coins earned by children under the age of 16. In some circumstances the Shakti Coins will be granted to a legal guardian or the child themselves.

    It must be noted that newborn children and children under the age required for enrollment in school are to be included in this framework, as some of them are already enrolled in school and others will be enrolled in school in the future. In addition, from the point of view of the Shakti Foundation, the period of classes spans the entire calendar year.

11. **Service Providers**: all the other entities that are external to the schools but equally involved in the education of schoolchildren. This includes school maintenance services, meal and food services, school-related transport services, sport and health trainers, and many more.

12. **Declarations**: all the activities related to the certification of effort of schoolchildren, schools, service providers, and validators.

13. **Validators**: participants within the Shakti Network who have been verified by a number of peers as an entity that can be trusted with responsibility and due process.

14. **Independent Validators**: specially certified validators who have earned a reputation for being trusted by peers and the community as a whole, for conducting themselves in a manner that is of the highest caliber, and for not being susceptible to pressure to commit misdeeds.

    Upon certification as independent validators, such entities (schools, school teachers, service providers, validators, miners/node operators, and other trusted entities) are approved to verify the existence of schoolchildren, schools, service providers, validators, and miners/node operators and also to identify inconsistent declarations.

15. **Shakti Coin**: the Shakti Foundation's digital money used for rewarding schoolchildren. Also, micropayments are awarded to schools, service providers, validators, and miners/node operators.

16. **SXE** (**S**hakti e**X**changed for **E**ducation): the currency symbol for Shakti Coins.

17. **Shakti Wallet**: a secure digital wallet (i.e., a software application) used for storing, sending, and receiving Shakti Coins. The wallet simply holds the private and public keys used for receiving the Coins and transferring them.

18. **Asymmetric Key Encryption**, also known as **Private/Public-Key Encryption**: a form of cryptography where the *key* normally used to encrypt and decrypt documents comes in a pair. The *private key* must be kept secret, while the *public key* can be publicly distributed. What one key encrypts, the other can decrypt. The private key can generate the public key, but not vice versa.

19. **Byzantine Consortium Consensus Algorithm**: one of the algorithms utilized for reaching agreement in a distributed ledger. Basically, each participant in the consortium votes for or against the inclusion of a transaction in the distributed ledger. As soon as a "quorum" is reached, the transaction is either added or discarded, depending on the outcome of the vote.

20. **Distributed Ledger**: essentially a distributed and replicated database in which transactions such as the Proof of Effort declarations are stored in a cryptographically secure and unmodifiable way. The database is replicated across all participants, and some algorithms (such as the Byzantine Consortium Consensus algorithm) ensure that all replicas contain exactly the same data.

21. **Difficulty Levels**: the controls and verifications that have to be carried out for the effort declarations to be fully validated. The difficulty levels increase with the age of the schoolchild.

22. **Regional Validation Levels**: the controls that have to be carried out in order to fully validate schools and service providers during registrations and effort declarations. The regional validation levels vary geographically.

2 Sets, Functions, and Mathematical Notation Used

The following sets are used in this document:

Table 1: **Sets used in this document**

Set	**Definition**
C	set of all existing schoolchildren in the world
C_R	set of schoolchildren registered with the Shakti Network
C_V	set of schoolchildren validated by the Shakti Network
S	set of all existing schools in the world
S_R	set of schools registered with the Shakti Network
S_V	set of schools validated by the Shakti Network
S_T	set of trusted independent schools in the Shakti Network
P	set of all existing service providers in the world
P_R	set of service providers registered with the Shakti Network
P_V	set of service providers validated by the Shakti Network
P_B	set of all schools-bound service providers
V	set of all possible validators in the world
V_R	set of validators registered with the Shakti Network
V_V	set of validators validated by the Shakti Network
V_T	set of trusted independent validators in the Shakti Network
M	set of all possible miners/node operators in the world
M_R	set of miners/node operators registered with the Shakti Network
M_V	set of miners/node operators validated by the Shakti Network
M_T	set of trusted independent miners/node operators in the Shakti Network
W	set of wallet holders
D	set of schoolchildren's difficulty levels (see Table 5)
R_S	set of schools' regional validation levels
R_P	set of service providers' regional validation levels
E_D	set of all declared efforts
E_{DC}	set of schoolchildren's declared efforts
E_{DS}	set of schools' declared efforts
E_{DP}	set of service providers' declared efforts
E_{DV}	set of validators' declared efforts
E_G	set of granted efforts

Table 1: **Sets used in this document** (continued)

Set	**Definition**
B	the Boolean set, which has only two elements: true and false
$\mathbb{R}$	set of all real numbers
$\mathbb{R}_{\geq 0}$	set of all non-negative real numbers
$\mathbb{R}_{>0}$	set of all positive real numbers
$\mathbb{R}^n$	the set $\mathbb{R}^n = \overbrace{\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}}^{n \text{ factors}}$ for a fixed positive integer n (the set of all n-tuples $(x_1, x_2, x_3, \ldots, x_n)$ of real numbers $x_1, x_2, x_3, \ldots x_n$)
T	set that represents *periods of time* in terms of days, weeks, and months
U	set that contains the necessary *units* of measurement

The following functions are used in this document:

Table 2: **Functions used in this document**

Function	**Definition**
Reg_c: $\mathsf{C} \to \mathsf{C}_R$	schoolchildren's registration function
Val_c: $\mathsf{C}_R \times \mathsf{D} \to \mathsf{C}_V$	schoolchildren's validation function
Reg_s: $\mathsf{S} \to \mathsf{S}_R$	schools' registration function
Val_s: $\mathsf{S}_R \times \mathsf{R}_S \to \mathsf{S}_V$	schools' validation function
Fed_s: $\mathsf{S}_V \times \mathsf{R}_S \to \mathsf{S}_T$	schools' consortium enrollment function
Reg_p: $\mathsf{P} \to \mathsf{P}_R$	service providers' registration function
Val_p: $\mathsf{P}_R \times \mathsf{R}_P \to \mathsf{P}_V$	service providers' validation function
Bnd_{sp}: $\mathsf{P}_V \times \mathsf{R}_P \times \mathsf{S}_V \times \mathsf{R}_S \to \mathsf{P}_B$	schools/service-providers binding function
Reg_v: $\mathsf{V} \to \mathsf{V}_R$	validators' registration function
Val_v: $\mathsf{V}_R \to \mathsf{V}_V$	validators' validation function
Cert_v: $\mathsf{V}_V \to \mathsf{V}_T$	validators' certification function
Reg_m: $\mathsf{M} \to \mathsf{M}_R$	miners' registration function
Val_m: $\mathsf{M}_R \to \mathsf{M}_V$	miners' validation function
Eval_m: $\mathsf{M}_V \to \mathsf{M}_T$	miners' evaluation function
Dec_c: $\mathsf{C}_V \times \mathsf{D} \times \mathsf{T} \times \mathbb{R}_{>0} \times \mathbb{R}^n \to \mathsf{E}_{DC}$	schoolchildren's declaration function
Dec_s: $\mathsf{S}_V \times \mathsf{C}_V \times \mathsf{R}_S \times \mathsf{T} \times \mathbb{R}_{>0} \times \mathbb{R}^n \to \mathsf{E}_{DS}$	schools' declaration function
Dec_p: $\mathsf{P}_V \times \mathsf{C}_V \times \mathsf{R}_P \times \mathsf{T} \times \mathbb{R}_{>0} \times \mathbb{R}^n \to \mathsf{E}_{DP}$	service providers' declaration function
Dec_v: $\mathsf{V}_V \times \mathsf{C}_V \times \mathsf{T} \times \mathbb{R}_{>0} \times \mathbb{R}^n \to \mathsf{E}_{DV}$	validators' declaration function
Grant_E: $\mathsf{E}_D \to \mathsf{E}_G$	effort-granting function
$\mathcal{D}_R$: $\mathsf{E}_D \to \mathsf{B}$	declaration reliability function
$\mathcal{T}_{cs}$: $\mathsf{D} \times \mathsf{R}_S \times \mathsf{U} \to \mathbb{R}_{\geq 0}$	schoolchildren/schools threshold function
$\mathcal{T}_{cp}$: $\mathsf{D} \times \mathsf{R}_P \times \mathsf{U} \to \mathbb{R}_{\geq 0}$	schoolchildren/service-providers threshold function
$\mathcal{T}_{cv}$: $\mathsf{D} \times \mathsf{U} \to \mathbb{R}_{\geq 0}$	schoolchildren/validators threshold function
$\mathcal{T}_{sv}$: $\mathsf{R}_S \times \mathsf{U} \to \mathbb{R}_{\geq 0}$	schools/validators threshold function
$\mathcal{T}_{pv}$: $\mathsf{R}_P \times \mathsf{U} \to \mathbb{R}_{\geq 0}$	service-providers/validators threshold function
$\mathcal{C}_{cs}$: $\mathsf{D} \times \mathsf{R}_S \times \mathsf{U} \times \mathbb{R} \times \mathbb{R} \to \mathsf{B}$	schoolchildren/schools close enough function
$\mathcal{C}_{cp}$: $\mathsf{D} \times \mathsf{R}_P \times \mathsf{U} \times \mathbb{R} \times \mathbb{R} \to \mathsf{B}$	schoolchildren/service-providers close enough function
$\mathcal{C}_{cv}$: $\mathsf{D} \times \mathsf{U} \times \mathbb{R} \times \mathbb{R} \to \mathsf{B}$	schoolchildren/validators close enough function
$\mathcal{C}_{sv}$: $\mathsf{R}_S \times \mathsf{U} \times \mathbb{R} \times \mathbb{R} \to \mathsf{B}$	schools/validators close enough function
$\mathcal{C}_{pv}$: $\mathsf{R}_P \times \mathsf{U} \times \mathbb{R} \times \mathbb{R} \to \mathsf{B}$	service-providers/validators close enough function

The following notation is used in the definitions of sets:

Table 3: **Basic set notation**

Notation	**Definition**
$\mathsf{X} = \{x_1, x_2, ..., x_n\}$	This is the basic definition of a set, which is done by listing its elements. We say that the set X consists of the elements (and only the elements) x_1, x_2, x_3, ..., x_n.
$x \in \mathsf{X}$	This notation means that x is in the set X (equivalently, that x belongs to the set X or that x is an element of the set X). For example, $x_1 \in \mathsf{X}$, $x_2 \in \mathsf{X}$, ..., $x_n \in \mathsf{X}$.
$\mathsf{Y} = \{y\text{: } y = f(x)$ for some $x \in \mathsf{X}\}$	This notation defines a new set Y as the result of applying the transformation/function f to the elements of another set. In this case, we say that Y consists of the elements y obtained by applying the function f to the elements of X. More briefly, Y is the set of y for which $y = f(x)$ for some x in X.
$\mathsf{Z} = \{z\text{: } z = f(x, y)$ for some $x \in \mathsf{X}$ and some $y \in \mathsf{Y}\}$	This notation defines a new set Z as the result of applying the transformation/function f to the *ordered pairs* of elements of two distinct sets. In this case, we say that Z consists of the elements z obtained by applying the function f to the ordered pairs of elements (x, y) where $x \in \mathsf{X}$ and $y \in \mathsf{Y}$. More briefly, Z is the set of z for which $z = f(x, y)$ for some ordered pair (x, y) with x in X and y in Y.
$\mathsf{A} \times \mathsf{B}$	The symbol $\times$ is the *Cartesian product* operator and denotes the multiplication operation between sets. The output is a new set that has the ordered pairs (a, b) with $a \in \mathsf{A}$ and $b \in \mathsf{B}$ as elements. We can say that $\mathsf{A} \times \mathsf{B} = \{(a, b)\text{: } a \in \mathsf{A}$ and $b \in \mathsf{B}\}$. Similarly, $\mathsf{A} \times \mathsf{B} \times \mathsf{C} = \{(a, b, c)\text{: } a \in \mathsf{A},\ b \in \mathsf{B},$ and $c \in \mathsf{C}\}$.
$\mathsf{A} \subset \mathsf{B}$	Given two sets A and B, this notation means that A is a *proper subset* of B. That is, every element of A is also an element of B, and there is at least one element of B that is <u>not</u> an element of A, hence $\mathsf{A} \neq \mathsf{B}$.
$\mathsf{A} \subseteq \mathsf{B}$	Given two sets A and B, this notation means that A is a *subset* of B as shown above, but the equivalence $\mathsf{A} = \mathsf{B}$ can also be true. In other words, both relations are possible: $\mathsf{A} \subset \mathsf{B}$ and $\mathsf{A} = \mathsf{B}$.
$\mathsf{A} = \mathsf{X} \cup \mathsf{Y} \cup \mathsf{Z}$	This notation means that a new set A is the result of combining the sets X, Y, and Z. We say that A is the *union* of those sets, that is, A consists of everything that is an element of at least one of the sets X, Y, Z. If $\mathsf{X} = \{x_1, x_2\}$, $\mathsf{Y} = \{y_1, y_2, y_3\}$, and $\mathsf{Z} = \{z_1, z_2, ..., z_n\}$, we can also express it with the extended notation $\mathsf{A} = \{x_1, x_2, y_1, y_2, y_3, z_1, z_2, ..., z_n\}$.

The following notation is used in the definitions of functions:

Table 4: **Basic function notation**

Notation	**Definition**
$f\colon \mathsf{X} \to \mathsf{Y}$	This is the classic notation for defining a function. It says that the function f has the set X as *domain* and the set Y as *co-domain*. Thus f "maps" elements of the set X to elements of the set Y. This notation also says that f takes a single argument and returns a single value, which is often expressed as "$y = f(x)$" when $x \in \mathsf{X}$ and y is the element of Y which is returned when x is the input.
$f\colon \mathsf{X} \to \mathsf{X}$	This is the same definition as above. In this case, however, the *domain* and the *co-domain* coincide.
$f\colon \mathsf{X} \times \mathsf{Y} \to \mathsf{Z}$	This is a slightly more complex notation for the definition of a function. It says that the domain of the function f is the Cartesian product of the sets X and Y. In this case, f takes two arguments, one from set X and one from set Y, and outputs an element z of the set Z. More briefly, $z = f(x, y)$.
$\|x - y\|$	The symbol $\|...\|$ denotes the "norm" operator, which is used for expressing the *size* of the result of applying a linear operator, in our case the size of the difference between x and y. The *norm of the difference* is also used for expressing the *distance* between x and y.
$\bigwedge_{i=1}^{m} \beta_i$	The symbol $\wedge$ represents the logical "and" operator, which is applied to Boolean values, so $\alpha \wedge \beta$ is true if and only if both α and β are true. The operator $\bigwedge_{i=1}^{m}$ is shorthand for the repeated "and" operation over a set of Boolean values. Thus rather than writing $((((\beta_1 \wedge \beta_2) \wedge \beta_3) \cdots \beta_{m-1}) \wedge \beta_m)$, we simply write $\bigwedge_{i=1}^{m} \beta_i$. The global result is true if and only if all operands $\beta_1, \beta_2, \beta_3, \ldots, \beta_m$ are true.

3 Introduction

This document describes the mathematics behind what we call *proof of effort* (PoE), that is, *how* schoolchildren can prove they are actually focusing on their educational improvement, which is what the word *effort* refers to. Within this framework, the proxy measurement for effort is attendance at schools and educational institutions.

The basic idea behind PoE is the submission of multiple effort declarations and their verification. Specifically, this encompasses the following:

- Each of the following entities involved in the project will submit one or more effort declarations: each schoolchild, each school, each service provider, and each validator.
- Each miner/node operator will verify whether submitted declarations are formally correct and match with one another.
- For all matching declarations, the PoE Protocol will grant the expected number of Shakti Coins as codified.
- For each Shakti Coin granted to a schoolchild, micropayments are awarded to schools, service providers, validators, and miners/node operators.

4 Basic Sets

In this section, we present all the "actors" involved in the project, together with their characteristics, roles, and a suitable mathematical description.

For the PoE project of the Shakti Foundation, we have the following basic sets:

- C: the set of **schoolchildren** from age 0 to 21 years.
- S: the set of **schools** and **educational institutions** participating in the PoE project and therefore involved in the educational efforts of schoolchildren.
- P: the set of **service providers** involved in the educational efforts of schoolchildren. This is quite a large and diverse set, and includes school-meal services, school-transport services, other recreational services, physical education teachers, music teachers, trainers, and more.
- V: the set of **validators**, who take care of verifying and certifying the information submitted by all the aforementioned actors.
- M: the set of **miners/node operators**, which includes all the people involved in mining and verifying effort declarations.

To the basic sets listed thus far, we have to add two important sets that affect all the preceding ones:

- S_T: the set of **trusted independent schools**, which is the subset of schools that are trusted as an integral part of the Shakti Network and undertake the important role of validators.
- W: the set of all Shakti **wallet holders**, who, even if not directly involved in the education of schoolchildren, play a fundamental role in the success and stability of Shakti Coins and the Shakti Network.

There are also a few "technical" sets that are used throughout this document for tuning mathematical expressions and relationships.

- D: the set of **schoolchildren's difficulty levels** used for specifying the validation rules to be applied to schoolchildren according to their age.
- R_S: the set of **schools' regional validation levels** used for specifying the validation rules to be applied to schools according to their geographical location.
- R_P: the set of **service providers' regional validation levels** used for specifying the validation rules to be applied to service providers according to their geographical location.

The separation by geographical location is meant to provide the following advantages:

- Scalability and redundancy of the Shakti Network technical infrastructure.
- Avoiding the same kinds of issues observed in Bitcoin's mining infrastructure, where, according to the Buy Bitcoin Worldwide website,[1] 81% of the entire mining power at the time of publication of this document is managed by Chinese mining pools.

  We want to ensure that no nation, association, or consortium is in control of the PoE mining power. Therefore, miners/node operators will be able to mine only those transactions and declarations that are generated inside their own region, with a possible fail-over to surrounding regions in case of insufficient mining power or other technical issues.
- Improved fraud and scam detection. Using the regional validation levels (R_S and R_P), we are able to tune the required checks for validation of transactions and declarations region by region.

[1] Buy Bitcoin Worldwide: `https://www.buybitcoinworldwide.com/mining/pools/`

4.1 Technical sets

In this section, we will define the "technical" sets involved in this project.

4.1.1 Schoolchildren's difficulty levels

The basic framework used in the PoE (proof of the educational efforts) of schoolchildren is summarized in Table 5. The set of **schoolchildren's difficulty levels** is $\mathsf{D} = \{d_1, d_2, \ldots, d_8\}$, where d_i corresponds to level i in the table. A schoolchild's difficulty level is governed by their age, not the type of school they attend. The identification of school types with difficulty levels in the table should be considered as only a general guide.

Table 5: **Difficulty Levels**

i	**Age range**	**Review period**	**PoE is validated by**
Level 1: Pre-kindergarten, kindergarten, and Montessori school	0 to 4 years of age	4 years	A mix of: • parents • tutors • trusted NGOs • other trusted parties • miners/ node operators • schools • service providers • schoolchildren in levels 5–8
Level 2: Primary school, elementary school, and junior school	4+ to 7 years	3 years	
Level 3: Junior school and middle school	7+ to 10 years	3 years	
Level 4: Middle school, junior high school, and high school	10+ to 13 years	3 years	
Level 5: Junior high school, high school, and secondary school	13+ to 16 years	3 years	A mix of: • parents • tutors • trusted NGOs • other trusted parties • miners/ node operators • schools • service providers • schoolchildren in levels 7 and 8
Level 6: Secondary school and high school	16+ to 18 years	2 years	
Level 7: High school, college, vocational school, trade school, and institutions that fall into other categories	18+ to 20 years	2 years	
Level 8: Post-secondary school, college, vocational school, and graduate school	20+ to 21 years	1 year	

4.1.2 Schools' regional validation levels

To improve verification of effort, each geographical area will have its own set of controls and checks to be carried out during school validations and declarations. The set of **schools' regional validation levels** is $\mathsf{R}_S = \{r_{s_1}, r_{s_2}, ..., r_{s_n}\}$, where r_{s_i} is the list of mandatory controls for area i.

4.1.3 Service providers' regional validation levels

There is an analogous set of controls and checks for service providers: the set of **service providers' regional validation levels** $\mathsf{R}_P = \{r_{p_1}, r_{p_2}, ..., r_{p_n}\}$, where r_{p_i} is the list of mandatory controls for area i.

The difficulty levels within the sets R_S and R_P will be implemented based on controls appropriate for a given region.

4.2 Sets of schoolchildren

There are three sets used for schoolchildren:

- the set of all **schoolchildren** on Earth: C
- the set of **registered schoolchildren**, that is, the set of schoolchildren who have been registered with the Shakti Network: C_R
- the set of **validated schoolchildren**, that is, the set of registered schoolchildren who have been successfully validated (which means that they are actual schoolchildren who are living in the indicated countries and are of the declared age): C_V

The sets of schoolchildren are related as follows: $\mathsf{C}_V \subset \mathsf{C}_R \subset \mathsf{C}$, and hopefully one day $\mathsf{C}_V = \mathsf{C}_R = \mathsf{C}$.

There are two important functions needed for schoolchildren:

- The **schoolchildren's registration function**

$$\text{Reg}_c\colon \mathsf{C} \to \mathsf{C}_R$$

  will be used for registering schoolchildren with the Shakti Network. It will be implemented as a mobile and web application.

- The **schoolchildren's validation function**

$$\text{Val}_c\colon \mathsf{C}_R \times \mathsf{D} \to \mathsf{C}_V$$

  will be used for validating data on registered schoolchildren. It will be implemented via a mobile and web application.

Thus the sets of schoolchildren are defined as follows:

- $\mathsf{C} = \{c\colon\ c \text{ is a schoolchild on Earth who is of age 0 to 21 years}\}$
- $\mathsf{C}_R = \{c' \in \mathsf{C}\colon c' = \text{Reg}_c(c) \text{ for some } c \in \mathsf{C}\}$
- $\mathsf{C}_V = \{c'' \in \mathsf{C}_R\colon c'' = \text{Val}_c(c', d_j) \text{ for some } (c', d_j) \in \mathsf{C}_R \times \mathsf{D}\}$

It should be pointed out that all three sets of schoolchildren are "moving sets" in the sense that new schoolchildren keep entering the sets and other schoolchildren exit the sets. For this reason, we should have included a dependency on time, to take into account the current age of each schoolchild in the domains of the functions Reg_c and Val_c. This additional dependency, however, would have made the definitions of those functions too complicated, considering that their purpose is to define a process for allowing schoolchildren to be enrolled in the Shakti Foundation project.

4.3 Sets of schools

There are four sets used for schools:

- the set of all existing **schools** and **educational institutions** on Earth: S
- the set of **registered schools**, that is, the set of schools registered with the Shakti Network: S_R
- the set of **validated schools**, that is, the set of registered schools that have been successfully validated (which means that they are actual schools located in the specified countries and accredited by the respective governing body in their jurisdiction): S_V
- the set of **trusted independent schools**, that is, the set of validated schools that also play the role of validators: S_T

Just as with the sets of schoolchildren, the sets of schools are related as follows: $\mathsf{S}_T \subseteq \mathsf{S}_V \subset \mathsf{S}_R \subset \mathsf{S}$, and hopefully one day $\mathsf{S}_T \subseteq \mathsf{S}_V = \mathsf{S}_R = \mathsf{S}$.

Some additional functions are needed for schools:

- The **schools' registration function**
$$\mathrm{Reg}_s\colon \mathsf{S} \to \mathsf{S}_R$$
will be used for registering schools with the Shakti Network. It will be implemented as a mobile and web application.
- The **schools' validation function**
$$\mathrm{Val}_s\colon \mathsf{S}_R \times \mathsf{R}_S \to \mathsf{S}_V$$
will be used for validating registered schools. It will be implemented as a mobile and web application accessible by only trusted independent validators.
- The **schools' consortium enrollment function**
$$\mathrm{Fed}_s\colon \mathsf{S}_V \times \mathsf{R}_S \to \mathsf{S}_T$$
will be used for enrolling validated schools as trusted independent validators. It will be implemented as a mobile and web application accessible by only schools and validators. To become a trusted independent validator, more than a single validation will be required.

Thus the sets of schools are defined as follows:

- $\mathsf{S}_R = \{s' \in \mathsf{S}\colon s' = \mathrm{Reg}_s(s) \text{ for some } s \in \mathsf{S}\}$
- $\mathsf{S}_V = \{s'' \in \mathsf{S}_R\colon s'' = \mathrm{Val}_s(s', r_{s_k}) \text{ for some } (s', r_{s_k}) \in \mathsf{S}_R \times \mathsf{R}_S\}$
- $\mathsf{S}_T = \{s''' \in \mathsf{S}_V\colon s''' = \mathrm{Fed}_s(s'', r_{s_k}) \text{ for some } (s'', r_{s_k}) \in \mathsf{S}_V \times \mathsf{R}_S\}$

As already pointed out, the schools in the set S_T will be delegated to validate registered schoolchildren and other schools by using the schoolchildren's validation function and the schools' validation function, respectively.

4.4 Sets of service providers

There are four sets used for service providers:

- the set of all existing **service providers** on Earth: P
- the set of **registered service providers**: P_R
- the set of **validated service providers**: P_V

- the set of **schools-bound service providers**: P_B

  A given service provider can be bound to more than one school at a time.

Some functions are needed for service providers as well:

- The **service providers' registration function**

$$\text{Reg}_p\colon \mathsf{P} \to \mathsf{P}_R$$

  will be used for registering service providers with the Shakti Network. It will be implemented as a freely accessible mobile and web application.

- The **service providers' validation function**

$$\text{Val}_p\colon \mathsf{P}_R \times \mathsf{R}_P \to \mathsf{P}_V$$

  will be used for validating service providers. It will be implemented as a mobile and web application accessible by only trusted independent validators.

- The **schools/service-providers binding function**

$$\text{Bnd}_{sp}\colon \mathsf{P}_V \times \mathsf{R}_P \times \mathsf{S}_V \times \mathsf{R}_S \to \mathsf{P}_B$$

  will be used by schools and service providers for declaring their mutual involvement. It will be implemented as a mobile and web application accessible by only validated schools, validated service providers, and validated validators.

Thus the sets of service providers are defined as follows:

- $\mathsf{P}_R = \{p' \in \mathsf{P}\colon p' = \text{Reg}_p(p) \text{ for some } p \in \mathsf{P}\}$
- $\mathsf{P}_V = \{p'' \in \mathsf{P}_R\colon p'' = \text{Val}_p(p', r_{p_h}) \text{ for some } (p', r_{p_h}) \in \mathsf{P}_R \times \mathsf{R}_P\}$
- $\mathsf{P}_B = \{p''' \in \mathsf{P}_V\colon p''' = \text{Bnd}_{sp}(p'', r_{p_h}, s_j, r_{s_k}) \text{ for some } (p'', r_{p_h}, s_j, r_{s_k}) \in \mathsf{P}_V \times \mathsf{R}_P \times \mathsf{S}_V \times \mathsf{R}_S\}$. Of course, r_{p_h} and r_{s_k} must address the same geographical area.

4.5 Sets of validators

There are four sets used for validators:

- the abstract set of all possible **validators**: V
- the set of **registered validators**: V_R
- the set of **validated validators**: V_V
- the set of **trusted independent validators**: V_T

The functions needed for validators are as follows:

- The **validators' registration function**

$$\text{Reg}_v\colon \mathsf{V} \to \mathsf{V}_R$$

  will be used by aspiring validators to register with the Shakti Network. It will be implemented as a freely accessible mobile and web application.

- The **validators' validation function**

$$\mathrm{Val}_v\colon \mathsf{V}_R \to \mathsf{V}_V$$

  will be used by trusted independent validators for verifying the identity of new registered validators. It will be implemented as a restricted-access mobile and web application.

- The **validators' certification function**

$$\mathrm{Cert}_v\colon \mathsf{V}_V \to \mathsf{V}_T$$

  will be used by trusted independent validators for certifying that the status of trusted independent validator has been granted. It will be implemented as a mobile and web application accessible by only trusted independent validators.

Thus the sets of validators are defined as follows:

- $\mathsf{V}_R = \{\nu' \in \mathsf{V}\colon \nu' = \mathrm{Reg}_v(\nu) \text{ for some } \nu \in \mathsf{V}\}$
- $\mathsf{V}_V = \{\nu'' \in \mathsf{V}_R\colon \nu'' = \mathrm{Val}_v(\nu') \text{ for some } \nu' \in \mathsf{V}_R\}$
- $\mathsf{V}_T = \{\nu''' \in \mathsf{V}_V\colon \nu''' = \mathrm{Cert}_v(\nu'') \text{ for some } \nu'' \in \mathsf{V}_V\}$

Validators verify that schoolchildren exist and are actually attending school, that schools are accredited by the respective governing body in their jurisdiction, and that schools and service providers are actually providing the services that they claim. Trusted independent validators are special entities, such as trusted non-governmental organizations (NGOs), tutors, certified trusted parties, and miners/node operators with demonstrated administrative experience, that could contribute to the PoE process.

Schools, school teachers, and service providers will be allowed to register as validators and to seek certification as independent validators. However, to avoid collusion with key school personnel (principal, vice principal, and other administrative staff), they will not be permitted to validate the efforts of schoolchildren on two or more consecutive days. For example, a teacher who validates the efforts of schoolchildren on a Monday will not be permitted to do so on Tuesday of the same week. This rotation system will go even further toward hindering collusion as more and more teachers register as validators.

It is important to point out that there could be some overlap between the set S_T of trusted independent schools and the set V_T of trusted independent validators. Also, the reader should note that independent validators are the same as validated validators.

4.6 Sets of miners

Miners[2] are another fundamental entity of the entire Shakti Foundation project, as they mine and validate effort declarations submitted by schoolchildren, schools, service providers, and validators. As a reward for their work, they will be granted a micropayment of Shakti Coin correlated to the number of Shakti Coins granted to schoolchildren.

There are four sets used for miners:

- the abstract set of all possible **miners**: M
- the set of **registered miners**: M_R
- the set of **validated miners**: M_V
- the set of **trusted independent miners**: M_T

[2]For the sake of simplicity, the term *miner* is used here in lieu of *miner/node operator*.

The set of **registered miners** is

$$\mathsf{M}_R = \{m' \in \mathsf{M}\colon\ m' = \mathrm{Reg}_m(m) \text{ for some } m \in \mathsf{M}\},$$

where

$$\mathrm{Reg}_m\colon \mathsf{M} \to \mathsf{M}_R$$

is the **miners' registration function**, which will be implemented as a freely accessible mobile and web application.

Moreover, as we are adopting the Byzantine Consortium Consensus algorithm, which expects all miners to be known and trusted, all registered miners will have to undertake an identification phase and pass an evaluation phase before becoming *trusted independent* miners. Thus

$$\mathsf{M}_V = \{m'' \in \mathsf{M}_R\colon\ m'' = \mathrm{Val}_m(m') \text{ for some } m' \in \mathsf{M}_R\}$$

and

$$\mathsf{M}_T = \{m''' \in \mathsf{M}_V\colon\ m''' = \mathrm{Eval}_m(m'') \text{ for some } \ m'' \in \mathsf{M}_V\},$$

where

$$\mathrm{Val}_m\colon \mathsf{M}_R \to \mathsf{M}_V$$

and

$$\mathrm{Eval}_m\colon \mathsf{M}_V \to \mathsf{M}_T$$

are the **miners' validation function** and the **miners' evaluation function**, respectively.

After every aspiring miner has passed the evaluation phase (managed by the trusted independent validators), there will be a "voting" phase in which the other miners will be required to vote on the acceptance or denial of the new miner within the Shakti Network through the Byzantine Consortium Consensus algorithm. This voting is totally autonomous and based entirely on the verification that the necessary criteria are met. It is embedded in the *Shakti Mining Application* and requires no special action to be executed.

4.7 Set of wallet holders

Even if wallet holders are not directly involved in any phase of the PoE project, they are extremely important to the success of the project, because they ensure stability and a good reputation. The set of wallet holders is denoted by W.

5 Definition of *Effort*

We define effort as schoolchildren's actions toward furthering their education as measured through attendance. Attendance is an adequate measure, because a schoolchild's physical or virtual presence in a school is deterministic.

5.1 Effort management

In the Introduction (section 3), we briefly described how the PoE will be managed. In the following subsections, we describe in detail how the PoE Protocol will be achieved.

5.2 Sets of efforts

Given the generic definition of effort, we introduce the main sets of efforts:

- the set of **declared efforts**: E_D
- the set of **granted efforts**: E_G

The set of declared efforts (E_D) is the union of the following sets:

- the set of **schoolchildren's declared efforts**: E_{DC}
- the set of **schools' declared efforts**: E_{DS}
- the set of **service providers' declared efforts**: E_{DP}
- the set of **validators' declared efforts**: E_{DV}

There are some additional sets associated with the sets of efforts:

- One of these is T, the discrete set of *all finite time intervals* in terms of days, weeks, and months. It is important to consider that every declaration refers to a precise period of time, be it a day, a week, a month, or a specified period between two dates.
- Another important set is $\mathbb{R}_{>0}$, the set of all positive real numbers, which will be used for the instant in time at which every declaration is submitted.
- Last but not least, the set that we denote by $\mathbb{R}^n$ is the set of all n-tuples of real numbers, where n is a positive integer equal to the total number of items needed for every declaration of effort. This set is used for the generic data that represent the final goal of each declaration. Depending upon the difficulty level and the regional validation levels, those data could include geographical coordinates, age of the schoolchild, enrollment date, and many others.

The functions needed for declarations of effort are as follows:

- The **schoolchildren's declaration function**

$$\mathrm{Dec}_c\colon \mathsf{C}_V \times \mathsf{D} \times \mathsf{T} \times \mathbb{R}_{>0} \times \mathbb{R}^n \to \mathsf{E}_{DC}$$

  will be used by schoolchildren or their parents and tutors for submitting schoolchildren's educational effort declarations. This function will be implemented within a mobile and web application.

- The **schools' declaration function**

$$\mathrm{Dec}_s\colon \mathsf{S}_V \times \mathsf{C}_V \times \mathsf{R}_S \times \mathsf{T} \times \mathbb{R}_{>0} \times \mathbb{R}^n \to \mathsf{E}_{DS}$$

  will be used by schools for submitting educational effort declarations of their students. This function will be implemented within a mobile and web application accessible by only validated schools and educational institutions.

- The **service providers' declaration function**

$$\mathrm{Dec}_p\colon \mathsf{P}_V \times \mathsf{C}_V \times \mathsf{R}_P \times \mathsf{T} \times \mathbb{R}_{>0} \times \mathbb{R}^n \to \mathsf{E}_{DP}$$

  will be used by service providers for submitting their effort declarations. It will be implemented as a mobile and web application accessible by only validated service providers.

- The **validators' declaration function**

$$\mathrm{Dec}_v\colon \mathsf{V}_V \times \mathsf{C}_V \times \mathsf{T} \times \mathbb{R}_{>0} \times \mathbb{R}^n \to \mathsf{E}_{DV}$$

  will be used by validators for submitting schoolchildren's effort declarations. It will be implemented as a mobile and web application accessible by only validated validators.

Thus the sets of declared efforts are defined as follows:

- $\mathsf{E}_{DC} = \{\delta_{c_j t_k}\colon \delta_{c_j t_k} = \mathrm{Dec}_c(c_j, d_h, t_k, t, (x_1, \ldots, x_n))$
  for some $(c_j, d_h, t_k, t, (x_1, \ldots, x_n)) \in \mathsf{C}_V \times \mathsf{D} \times \mathsf{T} \times \mathbb{R}_{>0} \times \mathbb{R}^n\}$
- $\mathsf{E}_{DS} = \{\delta_{s_i c_j t_k}\colon \delta_{s_i c_j t_k} = \mathrm{Dec}_s(s_i, c_j, r_{s_h}, t_k, t, (x_1, \ldots, x_n))$
  for some $(s_i, c_j, r_{s_h}, t_k, t, (x_1, \ldots, x_n)) \in \mathsf{S}_V \times \mathsf{C}_V \times \mathsf{R}_S \times \mathsf{T} \times \mathbb{R}_{>0} \times \mathbb{R}^n\}$
- $\mathsf{E}_{DP} = \{\delta_{p_i c_j t_k}\colon \delta_{p_i c_j t_k} = \mathrm{Dec}_p(p_i, c_j, r_{p_h}, t_k, t, (x_1, \ldots, x_n))$
  for some $(p_i, c_j, r_{p_h}, t_k, t, (x_1, \ldots, x_n)) \in \mathsf{P}_V \times \mathsf{C}_V \times \mathsf{R}_P \times \mathsf{T} \times \mathbb{R}_{>0} \times \mathbb{R}^n\}$
- $\mathsf{E}_{DV} = \{\delta_{v_i c_j t_k}\colon \delta_{v_i c_j t_k} = \mathrm{Dec}_v(v_i, c_j, t_k, t, (x_1, \ldots, x_n))\}$
  for some $(v_i, c_j, t_k, t, (x_1, \ldots, x_n)) \in \mathsf{V}_V \times \mathsf{C}_V \times \mathsf{T} \times \mathbb{R}_{>0} \times \mathbb{R}^n\}$

The set of all declared efforts is

$$\begin{aligned} \mathsf{E}_D &= \mathsf{E}_{DC} \cup \mathsf{E}_{DS} \cup \mathsf{E}_{DP} \cup \mathsf{E}_{DV} \\ &= \{\Delta_{c_j t_k}\colon c_j \in \mathsf{C}_V, t_k \in \mathsf{T}\}, \end{aligned}$$

where $\Delta_{c_j t_k}$ is a declaration submitted for schoolchild c_j in reference to time period t_k. That is,

$$\begin{aligned} \Delta_{c_j t_k} \in\ & \{\delta_{c_j t_k} \in \mathsf{E}_{DC}\} \\ & \bigcup \big(\cup_i\ \{\delta_{s_i c_j t_k} \in \mathsf{E}_{DS}\colon s_i \in \mathsf{S}_V\}\big) \\ & \bigcup \big(\cup_i\ \{\delta_{p_i c_j t_k} \in \mathsf{E}_{DP}\colon p_i \in \mathsf{P}_V\}\big) \\ & \bigcup \big(\cup_i\ \{\delta_{v_i c_j t_k} \in \mathsf{E}_{DV}\colon v_i \in \mathsf{V}_V\}\big) \end{aligned}$$

This complicated definition simply says that the set of effort declarations for schoolchild c_j that are in reference to time period t_k includes the effort declarations submitted by the schoolchild, as well as all the declarations submitted by schools, service providers, and validators for that schoolchild in reference to that period.

Given the set of effort declarations, we have the **effort-granting function**

$$\mathrm{Grant}_E\colon \mathsf{E}_D \to \mathsf{E}_G$$

and the **set of granted efforts**,

$$\mathsf{E}_G = \{e_{c_j t_k}\colon e_{c_j t_k} = \mathrm{Grant}_E(\Delta_{c_j t_k}) \text{ for some } \Delta_{c_j t_k} \in \mathsf{E}_D\}$$

5.3 Effort declaration functions

The effort declaration functions are another important set of functions we need to consider carefully. These functions allow schoolchildren, schools, service providers, and validators to submit their declarations. Any entity can submit as many declarations as needed; for example, a school can submit a declaration for a particular schoolchild, and each teacher in the role of validator can submit declarations for that same schoolchild.

We have seen that there is a different function for each type of submitted declaration, mainly because each declaration type has different inputs and associated controls.

As an example, some of the data included are as follows:

- declaration type: schoolchild, school, service provider, or validator
- unique identifier: public address of the *issuer*
- period of time to which the declaration refers
- location, that is, the geographical region to which the declaration refers
- randomly generated data, such as a universally unique identifier (UUID), to make each declaration unique
- cryptographic data for privacy and identity protection (public keys and signatures)
- for validators, the *validator reliability level*, which is a Shakti-assigned numeric value (from -10 to $+10$) that's used to give more weight to effort declarations made by highly ranked validators (in the event of conflicting declarations, the validator reliability level will be used to resolve issues on a case-by-case basis)
- *timestamp* indicating the time at which the declaration is submitted

5.4 Validation of effort

Critical to the validation of effort is the concept of *difference*. What really matters is the *difference* between declarations issued by schoolchildren and the declarations issued by schools, service providers, and validators.

5.4.1 Declaration reliability function

The **declaration reliability function** is the *difference* function. Since a declaration is made up of several items, we can think of this function,

$$\mathcal{D}_R\colon \mathsf{E}_D \to \mathsf{B},$$

where $\mathsf{B} = \{\text{true},\ \text{false}\}$, in terms of the differences between related declarations. It basically tells us whether a specific declaration is reliable, that is, whether it can be trusted—and, as a result, the Shakti Foundation can assign the planned reward to the schoolchild, school, service providers, validators, and miners/node operators involved in the submission and validation of that declaration.

The complexity in defining *implementation* of the declaration reliability function is due to the multitude of items and different units each declaration is made up of. We could say that each declaration δ_x is a heterogeneous set of items. To compute the final result, we first need to solve the problem of normalizing the differences between heterogeneous entities.

To focus on this problem's boundaries, let's say that if δ_x and δ_y are two declarations, their difference or *distance*[3] is

$$\text{Diff}(\delta_x, \delta_y) = \|\delta_x - \delta_y\|$$

[3]Here, the term *distance* refers to the *mathematical* distance.

As each declaration is made up of heterogeneous items, we cannot simply apply the norm operator to their difference, even though what we ultimately need is a simple scalar value. Thus we will use a different approach.

Given two declarations, $\delta_x = \{\alpha_{x_1}, \alpha_{x_2}, ..., \alpha_{x_n}\}$ and $\delta_y = \{\alpha_{y_1}, \alpha_{y_2}, ..., \alpha_{y_n}\}$, we are perfectly able to compute the difference between homogeneous values (i.e., values expressed in the same unit). Thus if α_{x_1} and α_{y_1} are such values, their difference (distance) is $\|\alpha_{x_1} - \alpha_{y_1}\|$.

However, we cannot simply write

$$\|\delta_x - \delta_y\| = \{\, \|\alpha_{x_1} - \alpha_{y_1}\|,\ \|\alpha_{x_2} - \alpha_{y_2}\|, ...,\ \|\alpha_{x_n} - \alpha_{y_n}\| \,\},$$

for the following reasons:

- The norm operator returns a non-negative real number, not a set.
- Different "sub-distances" $\|\alpha_{x_i} - \alpha_{y_i}\|$, $\|\alpha_{x_j} - \alpha_{y_j}\|$ could be expressed in different units. For example, some of them could be expressed in units of spatial distance, while others could be expressed in units of time, and still others, such as geo-location data, names of schools and courses, or meal types, could be expressed in still other units. Quantities that are expressed in different units are incommensurate and cannot be combined.

We need *something* to make the set of heterogeneous differences homogeneous. The something we are looking for is the **close enough functions**.

The close enough functions tell us how close two declarations are to each other. For this computation, we are going to use the following items:

- the pertinent *units*:

  geo-location coordinates

  local time

  postal code (where available)

  any other unit able to improve the accuracy of fraud detection

- the *difficulty levels*
- the *regional area thresholds*

The advantage in using these items is the removal of all dependencies on heterogeneous data types embedded in declarations.

We will compare pairs of homogeneous data types to determine whether they are "close enough," and return a Boolean value (either true or false) as a result.

5.4.2 Threshold functions (purpose)

For the task of determining whether the values of a pair of homogeneous items are "close enough" (i.e., to determine the maximum amount by which they are allowed to differ), we introduce the **threshold functions**.

The threshold functions all have similar signatures and use the difficulty levels, regional validation levels, and units to return a value which will then be compared to the difference between the values of an actual pair of homogeneous items.

Moreover, the regional validation levels, which aim to provide protection against fraud and scams, constitute a fine-tuning mechanism for the consistency requirements.

Recall that the symbol U denotes the set of units: $\mathsf{U} = \{u_1, u_2, ..., u_n\}$. For example, u_1 could be a unit of distance, to express the distance between two cities; and u_2 could be a unit of time, such as hours, days, or weeks, to express the length of time between two events. The set U is needed because each threshold function returns a different value, depending on the unit to which it applies. Also, recall that the symbol $\mathbb{R}_{\geq 0}$ denotes the set of all non-negative real numbers.

A different threshold function is needed for each type of declaration comparison:

- the **schoolchildren/schools threshold function**

$$\mathcal{T}_{cs}\colon \mathsf{D} \times \mathsf{R}_S \times \mathsf{U} \to \mathbb{R}_{\geq 0}$$

- the **schoolchildren/service-providers threshold function**

$$\mathcal{T}_{cp}\colon \mathsf{D} \times \mathsf{R}_P \times \mathsf{U} \to \mathbb{R}_{\geq 0}$$

- the **schoolchildren/validators threshold function**

$$\mathcal{T}_{cv}\colon \mathsf{D} \times \mathsf{U} \to \mathbb{R}_{\geq 0}$$

We introduce two additional threshold functions—to monitor schools' and service providers' behavior, not just schoolchildren's behavior. For this purpose, validators' declarations are mandatory, as we use their declarations to compare and verify both schools and service providers.

These additional functions are as follows:

- the **schools/validators threshold function**

$$\mathcal{T}_{sv}\colon \mathsf{R}_S \times \mathsf{U} \to \mathbb{R}_{\geq 0}$$

- the **service-providers/validators threshold function**

$$\mathcal{T}_{pv}\colon \mathsf{R}_P \times \mathsf{U} \to \mathbb{R}_{\geq 0}$$

5.4.3 Threshold functions (implementation)

Considering the critical task that the threshold functions are going to be used for, we briefly discuss their implementation as well.

The most flexible implementation is based on the use of 2-dimensional arrays (matrices) and 3-dimensional arrays (cubes). We need to implement a separate *cube/matrix* for each threshold function:

- schoolchildren/schools threshold function cube:
  - dimension 1: *schoolchildren's difficulty levels*
  - dimension 2: *schools' regional validation levels*
  - dimension 3: *units*
- schoolchildren/service-providers threshold function cube:
  - dimension 1: *schoolchildren's difficulty levels*
  - dimension 2: *service providers' regional validation levels*
  - dimension 3: *units*
- schoolchildren/validators threshold function matrix:
  - dimension 1: *schoolchildren's difficulty levels*
  - dimension 2: *units*

- schools/validators threshold function matrix:

  dimension 1: *schools' regional validation levels*

  dimension 2: *units*

- service-providers/validators threshold function matrix:

  dimension 1: *service providers' regional validation levels*

  dimension 2: *units*

These data structures have several advantages:

- Each threshold function can easily be tuned by simply changing the entries in the *cube/matrix* for that function.
- New measures can easily be added by simply increasing the dimensions of the pertinent *cube/matrix*.
- The computational resources required and the processing costs are not unreasonable, as there is no need to pay for excess computing power.

5.5 Close enough functions

We now have everything we need for the close enough functions, as described in section 5.4.1:

- The **schoolchildren/schools close enough function**

  $$\mathcal{C}_{cs}\colon (\mathsf{D} \times \mathsf{R}_S \times \mathsf{U}) \times \mathbb{R} \times \mathbb{R} \to \mathsf{B}$$

  will be used for comparing schoolchildren's declarations to schools' declarations, that is, declarations that we previously denoted by $\delta_{c_j t_k}$ and $\delta_{s_i c_j t_k}$, respectively.

  This function receives the same parameters (from $\mathsf{D} \times \mathsf{R}_S \times \mathsf{U}$) for the two declarations, along with the values of a pair of homogeneous items (from $\mathbb{R} \times \mathbb{R}$) that are to be compared. It first passes the parameters (from $\mathsf{D} \times \mathsf{R}_S \times \mathsf{U}$) to the threshold function ($\mathcal{T}_{cs}$), which outputs a value that it compares to the difference between the values of the pair of homogeneous items. It then returns a Boolean value that indicates whether the values of that pair of items are "close enough."

  Of course, this function must be applied to each item that's to be compared in the two declarations. This means that if we are comparing the declarations $\delta_x = \{\alpha_{x_1}, \alpha_{x_2}, ..., \alpha_{x_n}\}$ and $\delta_y = \{\alpha_{y_1}, \alpha_{y_2}, ..., \alpha_{y_n}\}$, we need to call this function for all pairs of comparable items in the set $\{(\alpha_{x_1}, \alpha_{y_1}), (\alpha_{x_2}, \alpha_{y_2}), \ldots, (\alpha_{x_n}, \alpha_{y_n})\}$.

- The **schoolchildren/service-providers close enough function**

  $$\mathcal{C}_{cp}\colon (\mathsf{D} \times \mathsf{R}_P \times \mathsf{U}) \times \mathbb{R} \times \mathbb{R} \to \mathsf{B}$$

  will be used for comparing schoolchildren's declarations to service providers' declarations, that is, declarations that we previously denoted by $\delta_{c_j t_k}$ and $\delta_{p_i c_j t_k}$, respectively. The behavior of this function is analogous to that of the previous one.

- The **schoolchildren/validators close enough function**

  $$\mathcal{C}_{cv}\colon (\mathsf{D} \times \mathsf{U}) \times \mathbb{R} \times \mathbb{R} \to \mathsf{B}$$

  will be used for comparing schoolchildren's declarations to validators' declarations, that is, the declarations that we previously denoted by $\delta_{c_j t_k}$ and $\delta_{v_i c_j t_k}$, respectively. The behavior of this function is analogous to that of the previous ones. It will be implemented as a mobile and web application, and reserved for use by only trusted independent validators.

- The **schools/validators close enough function**

$$\mathcal{C}_{sv}\colon (\mathsf{R}_S \times \mathsf{U}) \times \mathbb{R} \times \mathbb{R} \to \mathsf{B}$$

  will be used by validators to certify that schools are operating correctly and honestly. The behavior of this function is analogous to that of the previous ones. It will be implemented as a mobile and web application, and reserved for use by only trusted independent validators.

- The **service-providers/validators close enough function**

$$\mathcal{C}_{pv}\colon (\mathsf{R}_P \times \mathsf{U}) \times \mathbb{R} \times \mathbb{R} \to \mathsf{B}$$

  will be used by validators to certify that service providers are operating correctly and honestly. The behavior of this function is analogous to that of the previous ones. It will be implemented as a mobile and web application, and reserved for use by only trusted independent validators.

The sets within parentheses correspond to the *cubes/matrices* that will be used in the implementation of the threshold functions.

The implementation of the schoolchildren/schools close enough function is straightforward, as it computes the absolute difference between the input values. For a pair of generic (but homogeneous) declaration items α_x, α_y,

$$\mathcal{C}_{cs}(d_i, r_{s_j}, u_h, \alpha_x, \alpha_y) = \text{true} \iff \|\alpha_x - \alpha_y\| \leq \varepsilon_{\mathcal{T}_{cs}},$$

where $\varepsilon_{\mathcal{T}_{cs}}$ is the value returned by the corresponding threshold function; that is,

$$\varepsilon_{\mathcal{T}_{cs}} = \mathcal{T}_{cs}(d_i, r_{s_j}, u_h)$$

Now the difference

$$\text{Diff}(\delta_x, \delta_y) = \|\delta_x - \delta_y\|$$

for comparison of a schoolchild's declaration to a school's declaration becomes

$$\begin{aligned}\text{Diff}(\delta_{c_j t_k}, \delta_{s_i c_j t_k}) \text{ is close enough} \iff \|\alpha_{(c_j t_k)1} - \alpha_{(s_i c_j t_k)1}\| \leq \mathcal{T}_{cs}(d_h, r_{s_l}, u_1), ..., \\ \|\alpha_{(c_j t_k)n} - \alpha_{(s_i c_j t_k)n}\| \leq \mathcal{T}_{cs}(d_h, r_{s_l}, u_n),\end{aligned}$$

that is, $\text{Diff}(\delta_{c_j t_k}, \delta_{s_i c_j t_k})$ is close enough if and only if

$$\mathcal{C}_{cs}(d_h, r_{s_l}, u_1, \alpha_{(c_j t_k)1}, \alpha_{(s_i c_j t_k)1}) = \text{true}, ..., \ \mathcal{C}_{cs}(d_h, r_{s_l}, u_n, \alpha_{(c_j t_k)n}, \alpha_{(s_i c_j t_k)n}) = \text{true}$$

Thus the value of the close enough function must be true for all items in the two declarations; in other words, all items in the two declarations must be close enough.

The above formula includes evaluation of only the schoolchildren/schools close enough function. However, depending on the difficulty level and the regional validation levels, evaluation of the schoolchildren/service-providers close enough function and/or the schoolchildren/validators close enough function may be required.

In the general case, therefore, for schoolchild c_j to be validated (i.e., for c_j to become an element of the set C_V) in reference to time period $t_k \in \mathsf{T}$, we need to evaluate all of the following:

- $\text{Diff}(\delta_{c_j t_k}, \delta_{s_i c_j t_k})$, where $s_i \in \mathsf{S}_V$ is the school in which the schoolchild is currently enrolled
- $\text{Diff}(\delta_{c_j t_k}, \delta_{p_i c_j t_k})$ for all service providers $p_i \in \mathsf{P}_V$ that are involved in the education of the schoolchild
- $\text{Diff}(\delta_{c_j t_k}, \delta_{v_i c_j t_k})$ for all validators $v_i \in \mathsf{V}_V$ that are involved in the education and control of the schoolchild

Given the "Diff" function, the exact implementation of the declaration reliability function (in 5.4.1) is trivial:

$$\mathcal{D}_R(\Delta_{c_j t_k}) = \text{Diff}(\delta_{c_j t_k}, \delta_{s_i c_j t_k}) \ \wedge \left(\bigwedge_{i=1}^{l} \text{Diff}(\delta_{c_j t_k}, \delta_{p_i c_j t_k}) \right) \ \wedge \left(\bigwedge_{i=1}^{m} \text{Diff}(\delta_{c_j t_k}, \delta_{\nu_i c_j t_k}) \right),$$

where l and m are the numbers of service provider declarations and validator declarations, respectively, for schoolchild c_j in reference to time period t_k.

What this formula says is: The value of the declaration reliability function for schoolchild c_j in reference to time period t_k is true if and only if all the *mandatory* declarations are close enough in the sense defined by the close enough functions.

The declarations that always need to be present for schoolchild $\boldsymbol{c_j}$ are the schoolchild's declaration ($\boldsymbol{\delta_{c_j t_k}}$) and the corresponding declaration submitted by school $\boldsymbol{s_i}$ for schoolchild $\boldsymbol{c_j}$ ($\boldsymbol{\delta_{s_i c_j t_k}}$).

Optionally and depending on the boundary conditions, there could be declarations submitted by the related service providers $\boldsymbol{p_i}$ ($\boldsymbol{\delta_{p_i c_j t_k}}$) and—depending on the regional validation levels—declarations submitted by the related validators $\boldsymbol{v_i}$ ($\boldsymbol{\delta_{v_i c_j t_k}}$).

What is also important to highlight is that $\boldsymbol{t_k}$ does not refer to an *instant in time*, but rather to a *period of time*, for example, a specific day or week or an interval between two dates. The length of $\boldsymbol{t_k}$ depends on the regional validation levels.

6 Conclusion

In this document, we have presented the mathematical principles upon which the PoE process is based. The PoE Protocol is the bedrock of the monetary framework of the Shakti Foundation, which aims to decimate the cycle of global poverty by empowering children through education.

Our decision to domicile the Shakti Foundation in Switzerland is not an arbitrary one. The reasons for this are threefold:

1. Given that the purpose of the Foundation is to empower children through education, the founders of the Shakti Foundation drew inspiration from the success of Switzerland's commitment to education. The Swiss' commitment to education, research, and innovation did not develop organically; it was enshrined in Switzerland's constitution in 1848.

2. The Shakti Foundation intends to highlight how the Swiss' strategy can succeed in other nations that, like Switzerland, have few natural resources and a small population—and also in nations that have only one of those two characteristics.

   The high-performing, knowledge-based Swiss people achieved prosperity by embracing academic freedom as the principle upon which to develop their education system. Another key innovation of the Swiss consisted of making both the provincial level and the federal level responsible for education, as well as making the federal level responsible for research and innovation. This has ensured accountability and investment at all levels, and fueled the growth of their knowledge-based society.

3. The progressive laws of Switzerland provide a strong legal basis for the Shakti Foundation and its Constitution as envisioned by the founders. Switzerland is currently a world leader in digital money and has embraced it as a legitimate medium of exchange within its society, economy, and legal framework. This means that the Shakti Foundation will have laws that will protect its infrastructure and an environment that will be conducive to promoting the aspirations of the Foundation to build and grow its network.

The Shakti Foundation's PoE Protocol is specifically engineered to address the shortcomings of the UN's Education for All (EFA) Initiative. The lack of primary education is keeping many generations within a cycle of poverty. The PoE Protocol is a unique self-propagating mechanism that aims to overcome the unsustainable first-generation digital-money protocols with the new generation of digital money. The PoE Protocol grants Shakti Coins only when evidenced by the efforts of schoolchildren within the Shakti Network.

By combining the Shakti Foundation's Constitution, Switzerland's laws, and the PoE Protocol, the Foundation aims to engage every child and their family, support their participation in sustainable development, and ultimately further the UN's Sustainable Development Goals.

Two Guys from the Milky Way

ShaktiCoin