PETROS STATHAS

stathasp@gmail.com

BOL: The Bonus of Life

Value is created from life.

Human population on Earth is well over 7,6 billion and rising. And a very large fraction of all those people are daily struggling for the means necessary to survive.

Through this struggle, people confer value to the things perceived as necessary. The more necessary something becomes, the more value it acquires – be it a commodity, an immaterial asset, an energy resource, a service offered, or anything else.

In the absence of life, the value of all these things would be meaningless. Human life, precious, inalienable, distinctly unique, is what begets value to all things; thus, it is only natural for this cumulative value to be offered back, as a bonus, to every human life.

To capitalize this value and use it for the betterment of every human life, we establish a new online community, whose sole purpose is to offer to every person an opportunity to acquire and harness her own Bonus Of Life (BOL).

RULES

1. One bonus of life (BOL) belongs rightfully, since the establishment of the community, to every living human being, without any distinction on age, gender, religion, nationality or otherwise, and irrespectively of participation to the community.
2. Every human individual has the right to participate to the community as a primary member. Entrance to the community is done via a registration procedure, using the individual's real identity. For children up to the age of 16 years, registration is done by their parents or guardians.
3. In order to claim and use her rightfully allotted bonus of life (BOL), every individual must create her own digital identity and link it with the account through which she will manage her BOL amount.
4. Participation to the community is voluntary. No one should be forced to participate unwillingly.
5. All participating members accept the community's rules of operation and seek to safeguard the community's prestige and extend its reach throughout humanity.
6. Every individual can claim her rightfully allotted BOL only once. If an individual does not claim her BOL during her lifetime, this BOL is equally distributed to all primary members of the community. The same also applies to BOL amounts of members that pass away without having spent them, and without having bequeathed them to any inheritors. These amounts, called share-outs or dividends, are distributed by the system, in equal terms, to all primary members of the community.

7. The rightfully allotted one BOL, as well as any share-outs, become possession of an individual from the moment she becomes member of the community. Once the amount is in her possession, she can use, manage and bequeath it, at will.
8. Individuals that are not capable of managing their accounts by themselves , can authorize a representative to do so. Also, accounts of children up to the age of 16 years are managed by their parents or guardians.
9. Companies, organizations, and other legally recognized entities can participate to the community as collective members, via the same registration procedure and using their real identification data (name, VAT number, etc.), in the internationally recognized form. Collective members can offer products or services, on payment with BOL.

   Collective members are not entitled to the initial 1 BOL or share-out amounts, as these are reserved only for living human beings. However, they can acquire BOLs in exchange for products or services offered to individual members.
10. All transactions inside the community will be done using as currency the BOL and its subdivisions: mili BOL (mBOL),micro BOL (μBOL), and dekanano BOL (dnBOL).

PROCEDURES AND RULES OF OPERATION

1. For the people to be able to utilize the Bonus Of Life, the BOL is introduced to the community as a digital cryptocurrency. Transactions using this currency will be made via the blockchain system, using a Byzantine Fault Tolerance (BFT) consensus protocol for the validation of the blocks in the chain.

2. The basis for the commencement of the blockchain is the present contract, detailing the terms and conditions for the operation of the community and the new currency. The participation of an individual in the community constitutes proof of acceptance of the contract's terms and conditions. The hash of this contract is the input hash to the genesis block.

3. The entrance of all members (individual and collective) to the community is done using the real and true identification data of the individual, company, or organization. Forging identity data by any member constitutes "cause" for termination the community's transactions with this member and deactivation of her account.

4. In order to ensure the uniqueness of participation for every individual, organization, or company, a set of rules, naming conventions and symbols is put into effect, uniformly and on world-wide basis. To this end, a unique CODENAME for every member of the community is established. Furthermore, to discriminate between individual and collective members (the latter being companies and organizations), the CODENAME for individuals will begin with the letter P, while for companies and organizations with the letter C.

5. Registration and authentication of individuals

Registration to the community and authentication of individual members are being done using procedures that ensure security of an individual's personal data and her right to participation/membership – that is, no one can prevent an individual to participate in the community. Everyone can participate in the community by her own free will, using personal data and documents that identify her as an individual-citizen, but without any dependencies from states, government agencies, organizations or companies that own, issue, or sell identification documents, personal data or online personal profiles. To this end, every individual is given the possibility to create, store and manage all documentation that identify her as a unique member of the community.

Using encryption algorithms and hash functions to ensure security, every individual can generate an encrypted identity profile with which she will be known to the community, while keeping private and confidential all her personal data.

5.1 Creation of the CODENAME

The CODENAME is the identifier with which every member is known to the community. It is generated in a way that uniquely identifies every person on world-wide basis, by using her real identification data and applying encryption techniques and hash functions, in order to ensure confidentiality.

Every prospective member creates her own CODENAME using her real name, in the internationally recognized "passport form" – that is, LATIN, ALL CAPITAL characters. If a passport is not available, the real name must be formed according the rules and conventions that apply to passports, regarding the mapping of characters to Latin alphabet, the capitalization and the ordering of names (in cases of more than one names).

The encoding of a real name into a CODENAME is done as follows:

P<COUNTRY CODE<SURNAME<1st GIVEN NAME<2nd GIVEN NAME<3rd NAME<BirthYear Gender<BdtNIN

The COUNTRY CODE is the three-letter country designation as defined in ISO 3166-1, part of the ISO 3166 standard.

In order to ensure the generation of a unique identifier for every individual on world-wide basis, and provide for adequate differentiation between individuals having identical names, additional pieces of information are placed after the full name:

- Year of birth, in 4-digit form (YYYY).
- Gender designation: M for male, F for female, and U for unspecified.
- NIN (national identification number) – an identifier assigned to every citizen of a state from the moment of birth, such as social security number, or national insurance number.

Finally, an alphanumeric character is added at the end (the default is 1, but users can choose any other alphabetic character or numeral).

In order to increase the level of protection and to better ensure the confidentiality of personal data, the following permutations are applied:

- Only the first character of the name is written in the field 1stGIVEN NAME (1ChN); the complete first given name, together with the birth date and the NIN

are appended after the gender designation.

- In the birth date, the 2 digits representing month are replaced by * symbols.
- In the NIN, the checksum digit and one more number are replaced by asterisk (*) symbols.

The resultant string of alphanumeric characters is being hashed twice, using the SHA256 algorithm. Then, from the doubly hashed string, the first 8 bytes (16 digits in base16) are taken and converted to base58. This result is placed directly after BirthYear&Gender. At the end of the whole string, the number 1 (or a user-selected number or letter) and 4additional checksum (in base16) digits are appended.

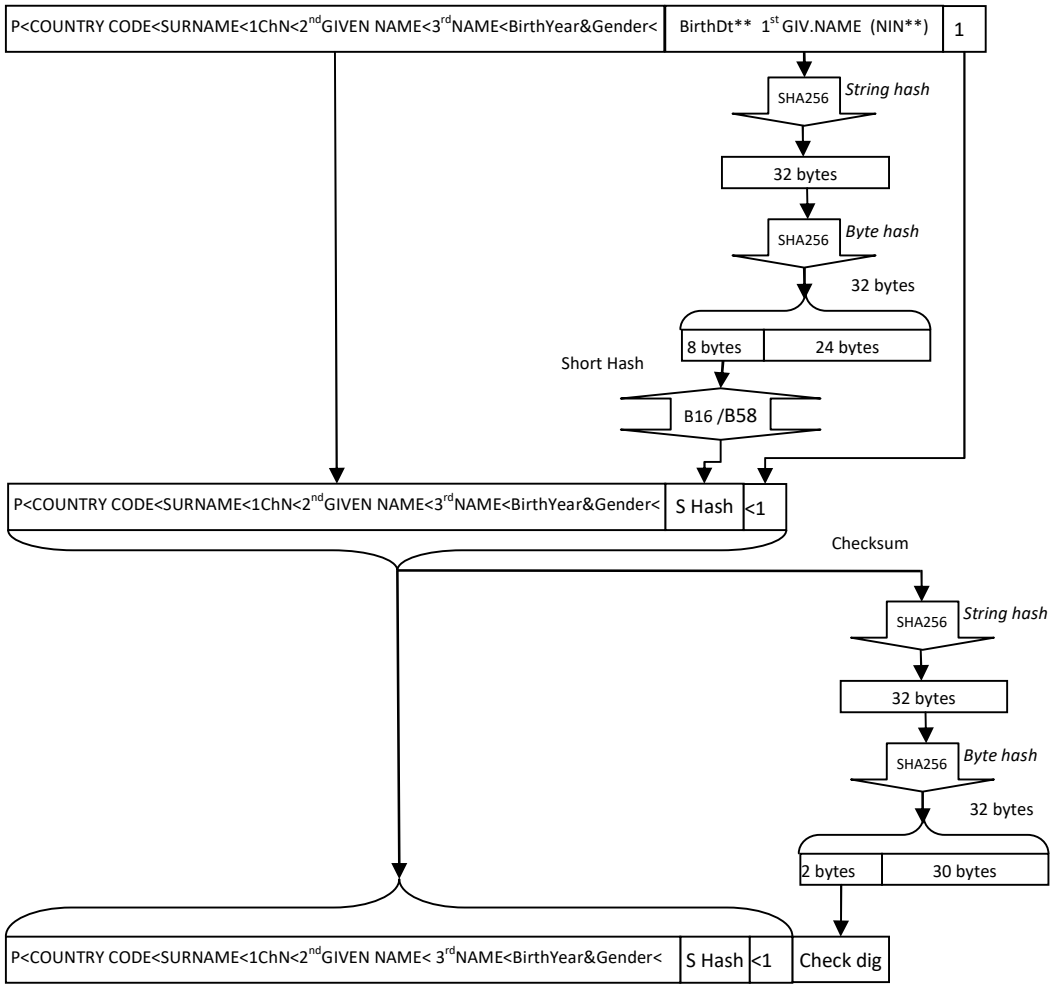

Fig.1 Creation of CODE NAME

As an example, consider the creation of a codename for a male Greek citizen named PAPADOPOULOS GIANNIS, born in 1963. The initially formed string
P<GRC<PAPADOPOULOS<GIANNIS<<<1963M<BirthDateNIN
is transformed according to the above-mentioned rules (see also Fig. 1 for details)
P<GRC<PAPADOPOULOS<G<<<1963M<Base58{Sha256[Sha256(1963**23GIANNIS23**63015**)]}<1Checkdigit
and the end result will have the form
P<GRC<PAPADOPOULOS<G<<<1963M<9BNWLsAgbjL<1F1BB

This is the CODENAME for the specific individual, as it will be displayed during her interactions with the community.
This encoding scheme results in a single CODENAME that can be used to uniquely identify every individual, on world-wide basis. To this end, there must be set the proper NIN (National Identification Number), for each country, in accordance to its standards, so that in can be used consistently by all its citizens. In the case of countries that do not use some form of National Identification Number as a unique identifier for every citizen from the moment of her birth, the Birth Identification Number (BIN, see Annex 1) will be encrypted in the short hash.

5.2 – Creation of Encrypted Digital Identity

The Encrypted Digital Identity (EDI) accompanies the CODENAME and is created by the prospective member. In order to generate the EDI, an individual can use personal and/or confidential identification data that are hashed (encrypted) by the SHA256 algorithm, so that no one else can access them.
EDI is the MAINHASH that is generated from a matrix including the CODENAME, NIN (see Fig. 2),as well as hashes for any number of other identification tokens, including passports, identity cards, driver's licenses, or various other documents such as phone/power bills, Family Status Certificates, etc. These tokens are selected by the prospective member, and must be in electronic format, specifically PDF or image files (paper documents can be converted to these formats via photographing or scanning). In addition, identification tokens such as voice (recorded in a sound file), photographic images, or other text documents can be included in the matrix. All these digital tokens must be encrypted via SHA256 algorithm and placed into the matrix by the prospective member. Furthermore, they must be stored, along with the matrix of hashes, in a safe medium such as USB stick, CD, SD card, etc., kept in a safe place. The set of these files comprise the prospective member's Digital Identity (DI) and are accessible solely by her. Visible to the community is only the Encrypted Digital Identity (EDI)that accompanies the CODENAME.
Prospective members having more than one citizenship can be registered only once to the community, as any other individual. One of the citizenships is used during registration, while the rest are encrypted, with all relevant documents, in the matrix of hashes (so as to be checked by the Authenticators, during the authentication procedure).
The following data elements are included as "required" in the matrix of hashes: CODENAME, NIN, Birth Date, Birth Country Code, nCT (CC1-CCN). nCT is the number of citizenships for the prospective member and CC1-CCN are the country codes of the respective states.
In this way, every individual can create an encrypted digital identity (EDI) which is a 32-byte hashed string that gets recorded to the blockchain and constitutes her unique and "official" identifier as a member of the community. The EDI is also used for authentication purposes, in order to verify/validate each member's identity. All files and documents that were used for EDI generation remain with their rightful owner

and are managed solely by her; no one else can acquire or reproduce them by using the EDI. By including more encrypted identification documents in the matrix, the user is given correspondingly more options during the authentication procedure (authenticator selection).

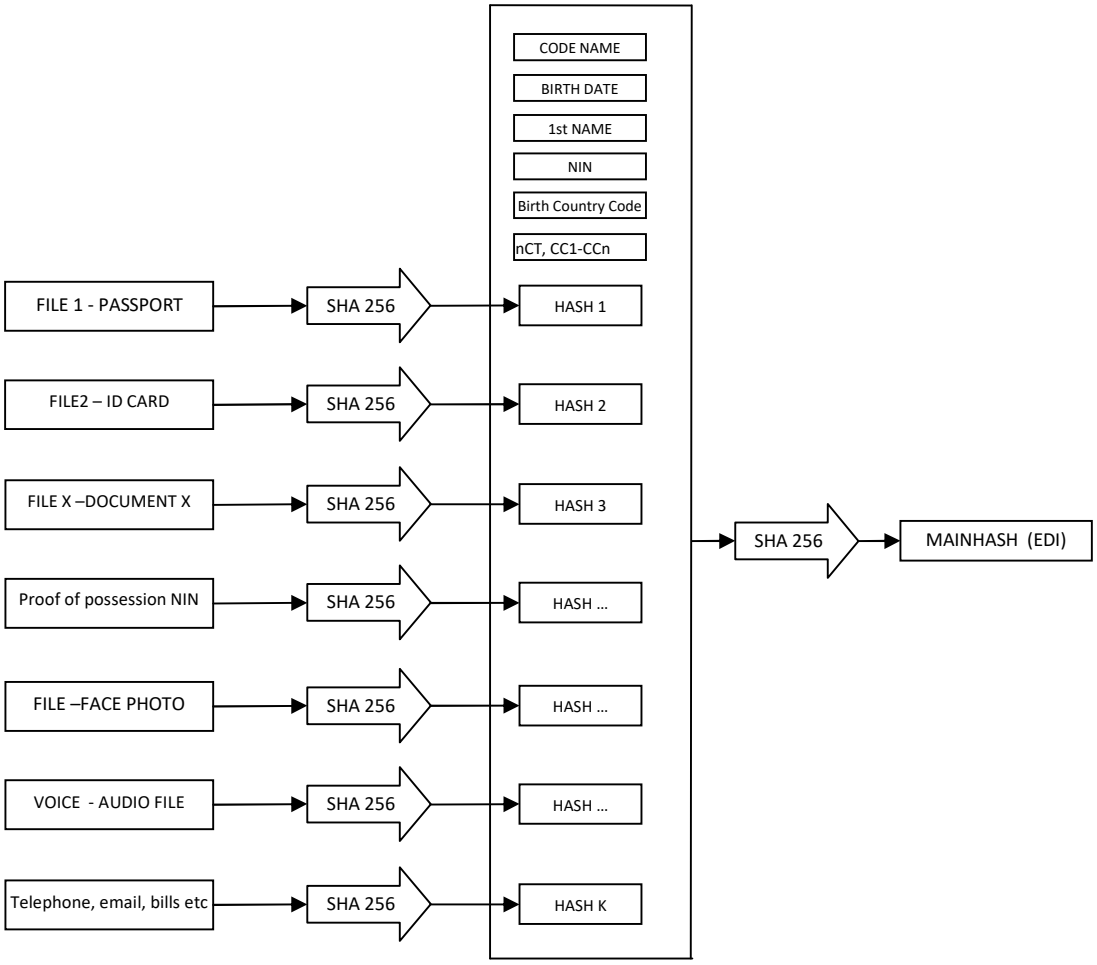

Fig.2 Creation of Encrypted Digital Identity (EDI)

5.3 – Creation of wallet and account

Every member can create her wallet and accounts in an independent and secure manner. The wallet includes the CODENAME, the EDI and the addresses of the member's accounts. The addresses are generated by combining the CODENAME and the public keys, after a special hashing procedure that guarantees the security of the public keys. In essence, the public keys become "hidden" inside the address and are revealed only when a spend transaction takes place.

Every account is a multi-sing address with two (2) public keys: one generated through the CODENAME, and one generated through the (secret) private key that has been selected by the member.

The address assigned to the wallet of every member is that person's Main Address. The Main Address is permanent (that is, it cannot be erased from the wallet) and it is used for collecting the initial BOL and share-out amounts. Every member's Main Address is recorded to the blockchain along with the CODENAME and EDI.

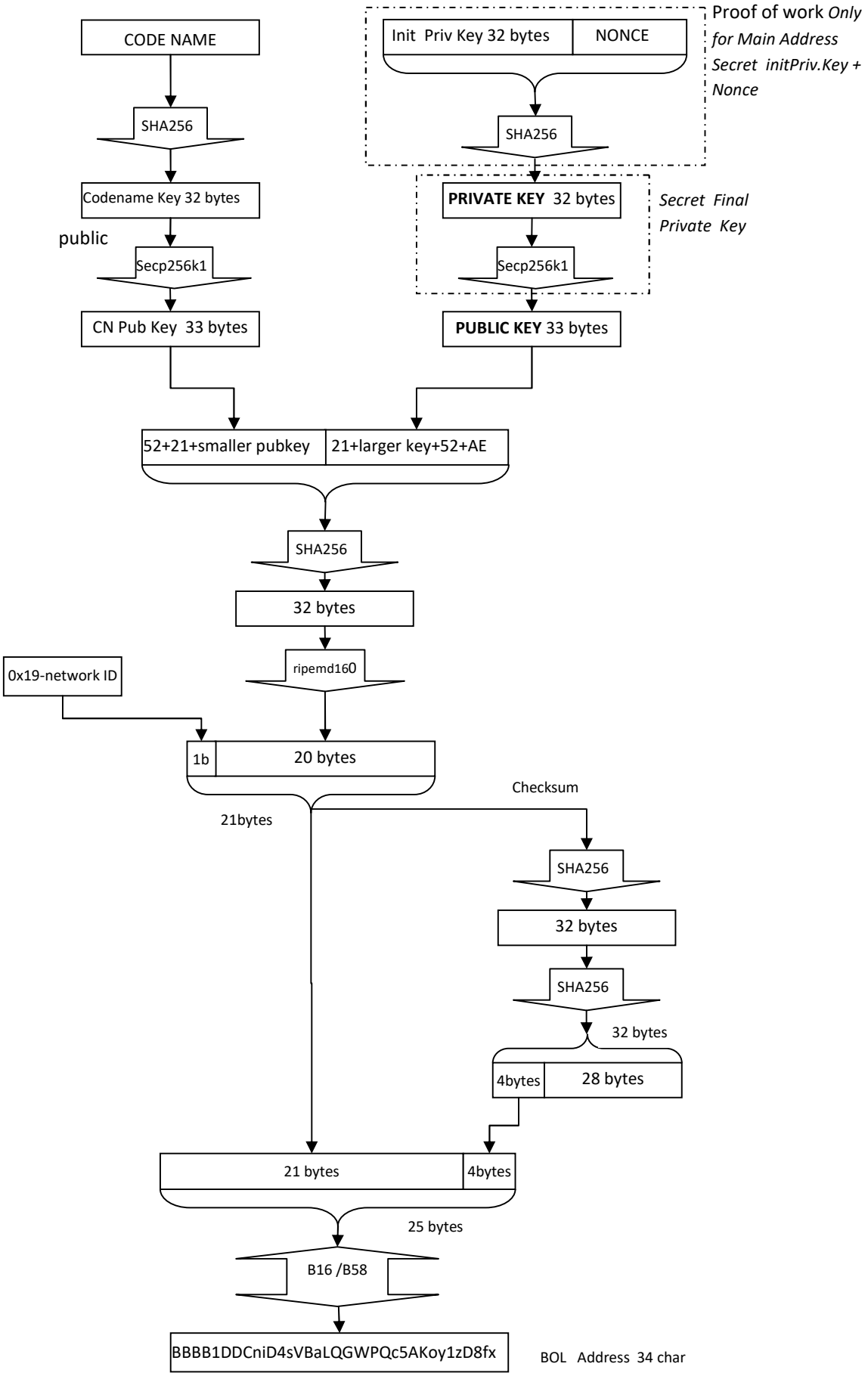

Fig.3 Creation of BOL 2-keys Address

Every member can have only one Main Address and an unlimited number of Commercial Addresses that are generated in the same manner. The formation of the Main Address is done using a proof-of-work protocol, in such a way that the first four characters of the address in base 58 (the network id and the three next ones) will correspond to the letter B (BBBB). For collective members, the formation of the Main Address is done in the same way, but the coding (network id and the three next characters) results to BCCC. This result is obtained with the addition of an arbitrary (nonce) number after the initial private key.
The data elements that are recorded/displayed in the blockchain for every member are:
CODE NAME --- EDI --- MAIN ADDRESS
P<GRC<PAPADOPOULOS<G<<<1963M<9BNWLsAgbjL<1F1BB
2CCAB0C334E585195B4F8A928DCE19FF637DD02ABD948BC52B6C9085A8800AF9
BBBB1DDCniD4sVBaLQGWPQc5AKoy1zD8fx

These data are used by the members for entrance in the community and for identification purposes.

In order to get registered in the community, every prospective member makes an initial transaction using the keys embedded in the Main Address. During this registration transaction the member enters its CODENAME and EDI. The blockchain validators check whether the entered CODENAME is unique (i.e., first occurrence) and if so, approve the registration transaction, which is recorded into the blockchain. From this point on, the individual is considered a primary member of the community and her rightfully allotted 1 BOL appears in the very next block of her account. This initial 1 BOL amount is augmented with the distribution dividends(share-outs) that are equally allotted to all primary members.The amountaccumulated to each account, at any moment,is permanently transferred to the accountafter a claim request, that is recorded into the blockchain as a claim transaction.

The CODENAME, EDI, and Main Address for companies and organizations are generated in the same manner, but with the following differentiations:

- In the CODENAME, the first letter is C
- In Main Address, the three characters after B is the letter C
- No initial BOLs are transferred in accounts belonging to companies and organizations

5.4 Authentication of members

In order to claim the BOL amount (initial 1 BOL and any shares) accumulated to its account, and use it for transactions, a member must be first authenticated. The authentication procedure ensures that

- the member has been registered, with its real personal data only once,
- the CODENAME shown by the system belongs indeed to the specific member.

Using the EDI that accompanies their CODENAME, members can choose the desired method of authentication, so that no personal data are revealed during the procedure, other than those included in the CODENAME.

Citizens that have an authentication certificate and/or digital signature issued from official government agencies or internationally recognized universities/institutions, can use it to sign, visibly (in a stamp-like form) some of the PDF files that are included in their EDI. This facilitates and expedites the authentication procedure.

Authentication must be done within one year since registration to the community; otherwise, the account will be considered fake, and hence will be deactivated. The amount corresponding to an unauthenticated account (shown to the system as an unclaimed amount) becomes available for sharing to the community. The time span for authentication is initially set to one year, but may change in the future, in order to improve the functionality of the system.

In order to safeguard the blockchain system against fraud attempts and other malicious intents, a proof-of-work protocol is employed during the Main Address generation procedure. This method computes the proper nonce number that is placed after the initial private key; by hashing this combination, another secret private key is computed, such that the first four characters of the generated address are Bs. This proof-of-work method can prevent malevolent attempts to introduce millions of fake addresses to the system in order to undermine the function of the distribution system by creating an unrealistic image for the community's population.

In addition, proof-of-work serves as a defense against targeted attacks to congest the system. Specifically, if the proof-of-work duration is set to 3minutes –a time interval that is barely noticeable by a normal member making a legitimate account–, an intruder will be able to generate, at maximum, 20 addresses per hour, or 175,200 addresses per year. However, because of the provisions of the validation procedure, these addresses cannot be authenticated and thus will be deactivated in one year's time. Furthermore, in a worst-case scenario of 1,000 [concurrent] intruders, the maximum number of 175,200,000 fake addresses that they can generate in one year is not enough to disrupt the function of the system.

By properly setting the time interval for the proof-of-work method and the authentication requirement, the robustness of the system against such attacks is secured.

In addition, the proof-of-work method serves to prevent attempts to generate fake accounts in the name of another member, aiming to intercept its CODENAME for any reason (such as to exclude the legitimate owner from the community). This is because the Short Hash included in the CODENAME produces such a large number of CODENAME combinations, that is impossible for any one person to hijack all of them.

Even in the case that the intruder knows the NIN and all the personal data required to obtain the right Short Hash, the inclusion of the P character after Gender produces 36more combinations to be tried. However, the system is constructed in such a way that after 10 attempts of registration with the same CODENAME, for every next attempt the system requires the authentication to take place concurrently with registration, and this can only be done by the real owner of the CODENAME.

The authentication of primary and collective members will be carried out by existing members of the community, known as authenticators, using as a safeguard the proof-of-stake protocol. The first members that are registered to the community undertake the task of authenticating the upcoming ones. In order to do so, the authenticators must possess, in advance, some form of official authentication certificate and digital signature, issued from official government agencies or internationally recognized universities/institutions. Furthermore, the authenticators undertake the obligation to employ all provisioned means of security for the protections of members' personal/confidential data. Authenticators receive from each authenticated member a small amount in BOL, as recompense for their service.

The authentication procedure can also be carried out by statutory organizations, banks, telecommunication and other utility companies, internet providers, etc., that are already authenticated members of the community and fulfill all the provisioned security requirements that guarantee the confidentiality of the members' personal data.

Thus, every individual that wishes to be authenticated has in her disposal many options for the selection of an authenticator, according to the identification data that has encrypted into her EDI, during her registration. The only elements communicated to the selected authenticator are the matrix of hashes and the source file corresponding to one or more of the hashes.

For example, referring to Fig. 2, if a member chooses a bank known to her as authenticator, she can communicate the file for hash2 (identity), so that the bank need only to compare this file with its own records. If a member chooses her telecommunications provider as authenticator, she can communicate the file for hash1 or hash2, and the file for hash7 with data that are already known to the authenticator, in order to expedite the authentication. Finally, in the case of authenticators that have no data about the member to be authenticated, she can communicate the file for hash2 (identity), the sound file, the mobile phone number, etc., so that the authenticator can make a video call (e.g., via Facetime, Viber, WhatsApp, Skype, etc.) in order to ascertain the identity and approve the authentication.

Authentication of every member will be done by two different authenticators. The first authenticator is selected by the member, from the pool of certified

authenticators. Upon approval of the authentication, the authenticator signs with his digital signature the member's CODENAME and this is recorded to the blockchain as an authentication transaction.

The selection of the second authenticator proceeds as follows: Based on the combination of the authentication transaction hash and the hash of the block in which the transaction has been recorded, an algorithm selects two different authenticators, so that the member can use anyone of them in order to obtain the second validation/digital signature and activate her account. In case that none of these two authenticators grants the authentication, the member's account is not activated. The member will have one more opportunity to repeat the authentication procedure, this time with different authenticators. If the authentication procedure fails again, the respective CODENAME and EDI are considered invalid.
In the case that an authentication procedure fails because of errors made by an otherwise legitimate member in the CODENAME, NIN, or EDI, the member can generate a new, valid CODENAME by changing the choice character P and, subsequently, new EDI and Main Address.

In the case of members with more than one citizenship, the authentication procedure will include the additional step of ensuring that only one registration exists for every such member, using the identification data for all citizenships that have been encrypted in the matrix of hashes.

A member's authentication status and real identity data can be verified by any other members doing transactions with the former one; the latter should check these for their own security.

Authenticators will not be able to use the recompense amounts collected from the authentications for a prescribed period of time. During this period, the recompense amounts will remain deposited in the authenticators' accounts as a collateral for the authentications**.**

In order to acquire the right to operate as a authenticator and to participate to blockchain validator committees, a higher-order authentication will be required, mandating more signatures as well as ownership of a prescribed quantity of BOL.

In case of loss or interception of a wallet's keys, it will be possible for its owner to set new keys, by creating a new Main Address and registering it, along with the respective CODENAME, to the blockchain, after a new, second-tier authentication procedure, based on the files already included in the EDI matrix. In the event of loss of the files whose hashes have been included in the EDI matrix, authentication via physical presence to second-tier authenticators will be required, for the creation of new EDI and Main Address that will be registered to the blockchain with the same CODENAME, which is uniqueand unchangeable for every individual. Transferring

amounts from old addresses to a new type C address will be done only upon signature of at least 4different authenticators, selected by the aforementioned authenticator-selection algorithm. Only distribution amounts from subsequent blocks will be deposited to the new Main Address, since the specific individual's right to the initial1 BOL has been already fulfilled with the old Main Address.

6. Registration and authentication for companies and organizations.
   The digital identity for a company or organization that wishes to participate to the community must include its international name and VAT number, as well as the digital signature of its legal representative. The representative must already be a member in order to register the company/organization. The headquarters address and the VAT number are included in the Short Hash. The legal documents representing the company, along with other identification data and the representative's personal data are placed, in encrypted form, in the matrix of hashes.

   The procedures for the generation of addresses and authentication of a company or organization is done in the same way as for the individuals. The general form of the CODENAME for a company or organization has the following form

   C<COUNTRYCODE<NAMEOFCOMPANY<TYPE< SH PC Cs

   For example, for a company named ELLINIKI DINAMI, the CODENAME, EDI,MAIN ADDRESS will have the following form:

   C<USA<IFESTOS_CONSTRUCTIONS <<2009C< MjN4Lc3hheS<15EB9
   2CCAB0C334E585195B4F8A928DCE19FF637DD02ABD948BC52B6C9085A8800AF9
   BCCCzvAT2UfrtzQVVYV8on4Y3kt4dsetT9

7. The members of the committees responsible for validating, through the consensus mechanism, the chain of blocks (blockchain validators) will be selected via an algorithm that is based on proof of stake and proof of contribution protocols. The algorithm gives priority to (a) members that own a considerable amount of BOL and (b) members that contribute knowledge and work for running the system, improving the algorithms and strengthen the security of the transactions.

8. Quantity, acquisition and distribution of BOLs
   The starting BOL amount will be equal to Earth's population at the time of constitution of the community and opening the blockchain , as derived from UN data. This reserve of BOLs will be augmented daily by an amount corresponding to the daily rate of births, such that the condition "1 BOL for every human being" is always satisfied. Thus, the production of new BOLs will be held constant at the global annual birth rate – that is, in the order of 1,80 - 1,9%, which is quite lower than the global inflation rate. Due to this fact, BOL can be considered as a reliable digital currency.

Referring to Fig. 4 , 5 , the working of the distribution system is as follows.

WORLD AMOUNT represents the amount of BOLs available to the distribution system at any time. On commencement of the blockchain, that is on block 0, the WORLD AMOUNT (designated as A_0) is equal to the global population (designated as P_0). Every individual can claim her rightfully allotted 1 BOL at any time; this amount remains reserved for her in the WORLD AMOUNT throughout her lifetime. In order to acquire the 1 BOL, the individual must become a member of the community and create her account. From this point on, all her transactions are recorded in the blockchain.

Based on UN statistical data –that is the birth rate (designated as rate B) and the death rate (designated as rate D)–, the births and deaths (B and D numbers) per day are calculated. Next, using the average block time, these numbers are reduced to the time span of one block (B_i and D_i, respectively). As a function of time, numbers B and D are adjusted using updated values of rate B and rate D; whenever deviations are found, the respective rate is suitably adjusted for the upcoming years.

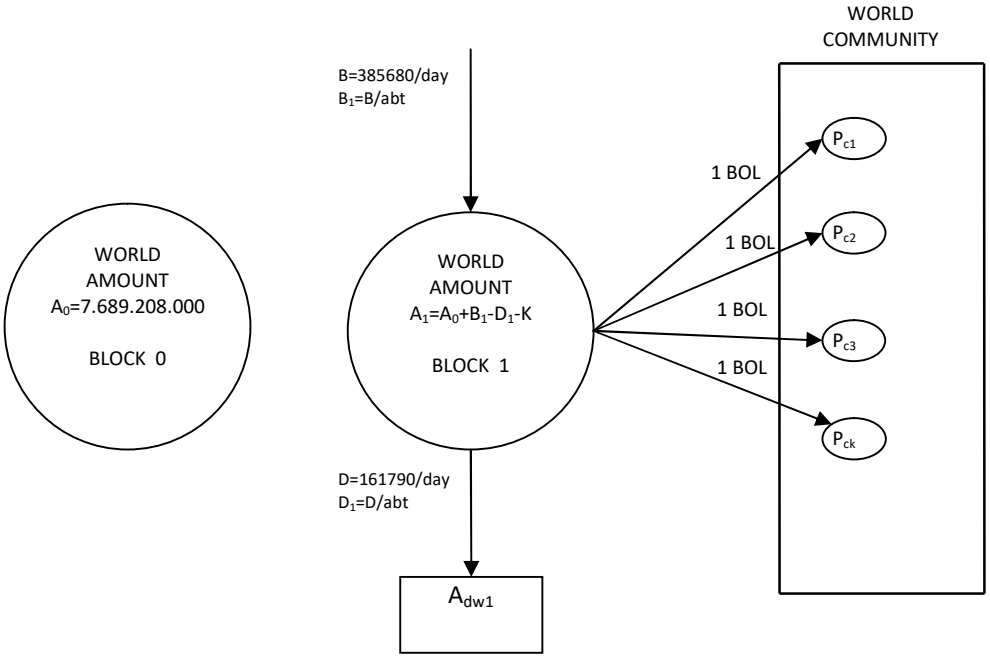

Fig.4 Distribution of BOLs at the block 1

The world population that corresponds to a block n(designated as P_n) is computed as

$$Pn = \left(P0 + \sum_{i=1}^{n} (Bi - Di) \right)$$

The P_n is composed of two components

$$Pn = Pcn + Pon$$

P_{cn} represents the total number of community's primary members in block n that have already acquired their rightfully allotted1 BOL. P_{on} represents the population that remains out of community.

The BOL amount that is available to the distribution system as WORLD AMOUNT at the closing of each block *n* (designated as A_n) is computed as

$$An = \left(A0 + \sum_{i=1}^{n} (Bi - Di) \right) - Pcn$$

The unused BOLs are equally shared to all primary members. "Unused" are considered the BOLs belonging (a) to individuals that pass away without having being members of the community, and (b) to community members that pass away without having specified inheritors.

The D_i amount corresponding to deaths is obtained as the sum of two components, $d_i = d_{ci} + d_{oi}$, where d_{ci} represents the community's members and d_{oi} represents the population out of community. Each component is computed in proportion to the respective population, as follows

$$dci = Di * \frac{Poi}{Pi} \qquad \text{and} \qquad doi = Di * \frac{Poi}{Pi}$$

The distribution amount corresponding to population P_{on} at block *n* is computed as

$$don = Dn * \frac{Pon}{Pn} = Dn * \frac{Pn - Pcn}{Pn} = Dn * (1 - \frac{Pcn}{Pn})$$

The distribution amount corresponding to population P_{cn} (d_{chn}) is the total sum of the amounts of the non-inherited accounts, as computed by the blockchain mechanism.

The distribution amount per person, A_{dwn}/P_{cn} is computed at the closing of each block, based on the population of valid members at that block. This amount is shown to the Main Address of a wallet as available, until a claim request from the respective member. The claim transaction that fulfills the request transfers to the member's Main Address the total amount that corresponds to the blocks created since the previous claim request. In order to reduce both the computational burden of the claiming process and the decimal rounding errors, the distribution amount per person may, in the future, be computed on daily basis rather than on block basis.

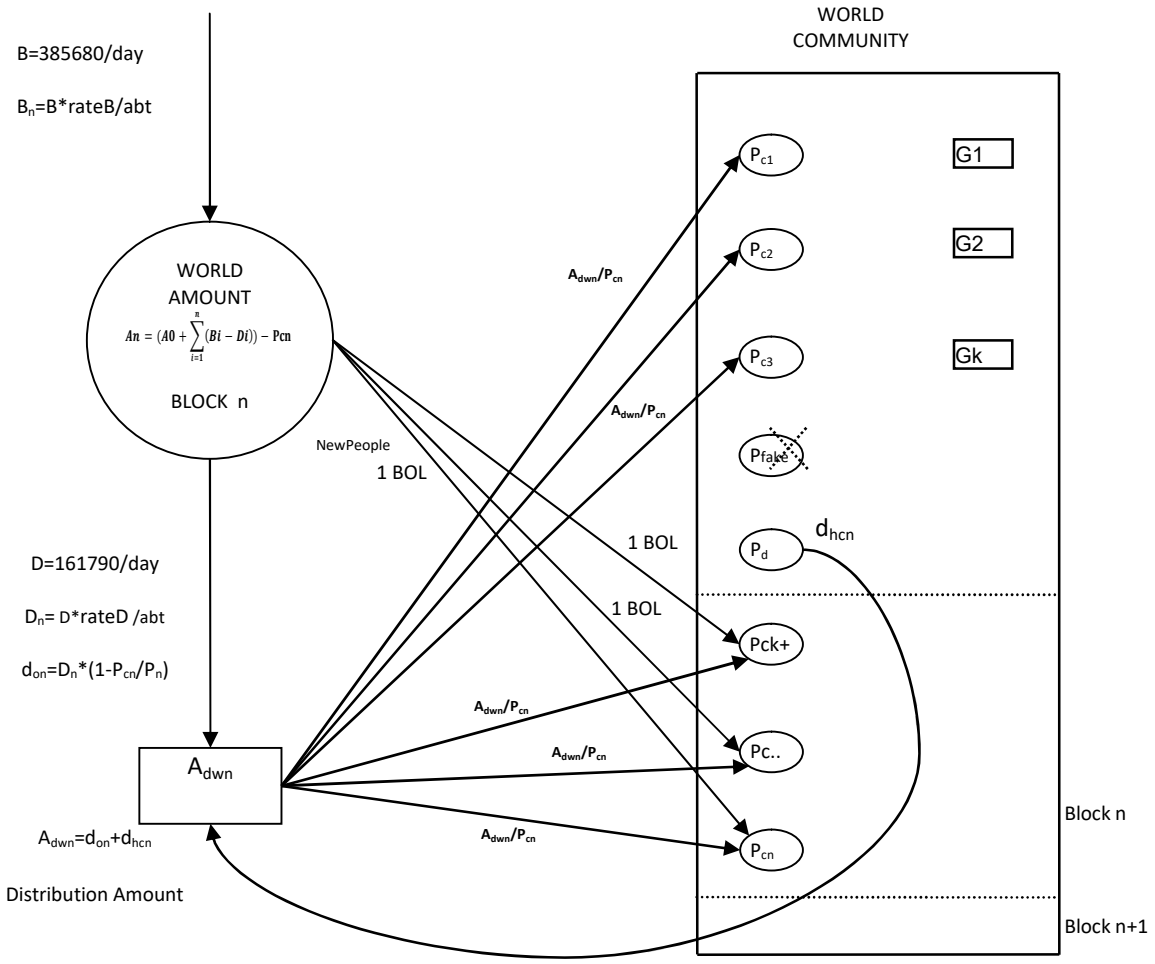

Fig.5 Distribution of BOLs at the closing of block n

9. Bequeathing BOLs is done by registering future inheritance transactions. These transactions are issued by the giver and are executed at the time of her choosing (corresponding to a certain block in the chain). At the time of execution, the amount available in the giver's wallet will be transferred to the inheritors, according with the giver's specifications (allocation percentages).Upon completion of the bequeathing process, the giver's wallet is deactivated and excluded from the distribution system. The future inheritance transaction can be cancelled or amended by the giver at any time, up to the block preceding the chosen "block of execution".
   When a member reaches the age of 99 years, as derived by the year of birth registered in the CODENAME, it is mandatory to repeat the authentication procedure, in order for its date of birth to be valid for the next 10-year time span. If the member is no longer in life and has not registered a future inheritance transaction, the BOLs accumulated to its account will be transferred to the WORLD AMOUNT and will be available to the distribution system for the next share-out. The same procedure is followed for the accounts of individual members or companies that remain inactive (no-transactions status) for 99 consecutive years.

10. Newborns and underage individuals can be introduced to the community by their

parents or guardians, in the same manner as adults. The management of their accounts is done by the parents or guardians up to the age of 16 years; upon reaching this age, they can invoke the second-tier authentication procedure that allows them to place new keys of their choosing in their account (by generating a new Main Address and including additional identification data) and create a new EDI, without changing the initial CODENAME. For as long as they manage their children accounts, parents can spend, for the benefit of the children, amounts coming from distributions, but not the initial 1BOL which will remain to the account, together with any accumulated distribution amounts, until a child reaches the age of 16 and be able to undertake the control and management of her account.

11. By large-scale participation in the New Global Community, the BOL will be able to unleash the value created by life, thus making human life a better proposition for the upcoming generations.

IN LIFE WE TRUST