Journal of Libertarian Studies
Volume 25, No. 1 (2021): XXX–XXX

New Directions in Crypto-Politics

Vicente Jara-Vera

ABSTRACT: With the emergence of modern secure digital systems, various technologies are being used in polling and government procedures. However, they have been proposed and applied in a way that is conventional and not innovative. This article proposes a change of perspective that favors a political framework in line with human dignity, consisting of individual freedom and equality before the law. Through various schemes, cryptographic protocols, and based on some elements of monero cryptocurrency (one of the most secure in existence)—such as double pairs of private and public keys, subaddresses, one-time ring signatures, and elliptic curve cryptography—this article presents a responsible voting scheme with profit and loss criteria for voters that is able to further the base political framework. In addition, multiple problems are addressed, including ballot counting, double voting, electoral fraud, and politicians', political parties' and voters' responsibilities.

I. INTRODUCTION

The development and progress of information and communication sciences have changed multiple aspects of society since the mid-twentieth century. One of the basic characteristics of communication processes is security, where cryptology, as an applied mathematical science, provides consistency and replies to many of its inherent challenges. In particular, information and communication technologies have provided automation,

Vicente Jara-Vera (vicente.jara@upm.es) has a PhD Telecommunications Engineering and is a cryptologist at Polytechnical University of Madrid, Spain, with scientific research in the area of mathematics, especially number theory and cryptography. He is a university professor and lectures on different subjects related to mathematics, cryptography and cybersecurity.

digitization, and integration across many social areas of interest, including politics.

The recent emergence of blockchain technology has generated not only expectations and revolutions in the areas where it has emerged, cryptocurrencies, banking, and financing processes, but also in social-political processes and decision-making, based upon its unique cryptographic and network characteristics. It is the so-called blockchain government (Swan 2015), where various services are decentralized and personalized, and political-social processes are both oriented toward citizenship, improving methods, using compromise (or consensus) structures, and smart contracts (McCorry, Shahandashti, and Hao 2017).

However, already before the use of blockchain, voting systems joining elective aspects with those of the market, such as decentralized, delegative democracy; liquid (or revocable delegative) democracy; random-sample elections; and even futarchy, or two-layer democracy, have been proposed as interesting options to improve present democratic systems, which are so inadequate in many aspects (Hoppe 2001; Brennan 2016).

Nevertheless, all those options are too aligned with the existing status quo, providing only modifications of the democratic system that improve some aspects, and many times putting on a pedestal, even sacralizing, the democratic process. These changes create a patchwork, unaware that it is the system itself that has to be replaced, as this paper proposes. These items are expounded, developed, and discussed in this article.

To pay a tribute to the paper that changed cryptography's panorama, "New Directions in Cryptography," by Whitfield Diffie and Martin Hellman (1976), which established the distinction between classic and modern cryptography and between symmetric and asymmetric cryptography, this article makes a proposal in the area of politics but because of its use of cryptographic technologies suggests new directions in "crypto-politics."

Timothy C. May, founder of the crypto-anarchist movement, of libertarian persuasion, and author of "The Crypto Anarchist Manifesto" (May 1988), perceived many of the political and social changes that cryptography would foster in the near future (May 1994). A few years later, Wei Dai (1998) stated: "I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally

associated with the word 'anarchy', in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary."

Although David Chaum (1983) is considered the inventor of digital currency, it was Dai ([1998]) who wrote the first paper about what cryptocurrencies would be, which a decade later would receive a reply in the bitcoin article by Satoshi Nakamoto (2008, [2008]). Bitcoin was structurally similar to the bit gold of Nick Szabo (2005) and also made use of the ideas of Adam Back (2003), the developer of hashcash as an algorithm of cryptographic proof of work based on hash functions. The rest is history. As is evident, these investigations from the start not only dealt with cryptographic coins but also with cryptographic contracts, as well as with the basics and structure of a proposal against government intromission and in favor of liberties in a world of equal users (May 1994).

II. THE CRYPTO-POLITICAL STRUCTURE OF THE ELECTORAL PROCESS

The basic and common methodology of voting election processes is that the voters choose what they consider the best among different options or candidates. The count of votes follows, and a winning candidate or party is expected to emerge.

After the period of office, no matter how it went, the decisions taken, the extent of compliance with the program, the successes and failures attained, or the conditions in which what was governed are left, the "res publica", the voters that voted the candidate or party in this procedure, being usually anonymous, cannot be rewarded nor sanctioned for the results of their choice. Neither voters that chose the non winning options are taken into account.

Next, it is developed and specified how this can be changed, making voters responsible for their decisions.

Deposit for Participating

To vote, it is necessary to be a member of the electoral census. This list is managed by the census authority. This authority is not necessarily a governmental bureaucratic authority, and as will be specified later it could be a decentralized structure based on blockchain technology. This set of members of the electoral census is called *M*. However, it is also necessary to make a deposit prior

to voting, which creates a new set, *N*. This aspect helps create responsibility for voting.

As implied above, it is important that citizens be held accountable for their decisions based on the candidates they put into office. Although leaders' decisions fall on all citizens, the pros and cons of decisions that have been made in social and economic areas must especially fall on those that have voted for them. Thus, citizens who succeeded with their vote have to be rewarded (later it will be clear what success means), all the more if these decisions helped all voters, including those who voted for another option. For the same reason, citizens whose vote was a failure must be penalized.

This raises the question of the optimal deposit amount required to participate in set *N*. The solution is complex, and only some conditions for bounding the limits can be provided. The deposit must be low enough not to prevent any potential voter (the poorest) from voting but sufficient to encourage responsibility (including among the wealthiest), the loss of this amount being a relative reduction and damage, and at the same time a desirable reward for voting with the right criteria, which will be expounded later. One or two months' average wages for the population could be a good benchmark. This amount will certainly be more valued by the less well-off, which will lead them to vote with greater conscience, as they can earn more by selecting a good government. By contrast, for the wealthiest, the loss of this amount will be less important, although if the government did not make the right decisions it would be the rich who would have more to lose. Another option is that the amount would differ for each voter, perhaps derived from an average of the individual's wages or rent. In this case there could also be a minimum value, such as 75 percent of the average wage in the country, for all who have never had a salary, such as the young population. This last option (different deposit depending on the voter) seems to be a better distribution, but if the vote is not the same price for all citizens eliminates its egalitarian aspect, which is essential.

Next are the more technical aspects, based on cryptography, that are necessary for the design and implementation of the structure of the electoral process.

Elliptic Curves

Asymmetric key cryptography in the elliptic curves schemes has excellent properties and security advantages over other methods.

Such schemes are the basis of this paper's voting proposal (Cohen et al. 2005; ENISA 2014; Barker 2020).

Generating an Elliptic Curve for the Electoral Process

Although there are diverse curves designed for public use, because the voting process is very sensitive it is more appropriate to generate an elliptic curve randomly, checking its adequacy and security (Bernstein and Lange 2017).

M is, as previously defined, the set of potential voters in the census. They appear on a list generated by the census authority that is publicly accessible. All members must have a public key (*KPub*) and a private key (*KPriv*)—for asymmetric cryptography, not necessarily elliptic curve cryptography now—to enable them to interact in a secure manner with the census authority.

Members of set *M* will be offered the opportunity to participate in the generation of the elliptic curve parameters that will be used during the election, with the expectation that the volunteers' data will be sufficient to generate the curve. Using their private keys ($KPriv_i$), volunteer participants will send the census authority a binary or text stream (c_i) of a length of their choosing. The streams will be considered binary streams, and the set of streams received will be arranged from small to large, $\{c_1,c_2,...,c_g\}$.

After a given period, the data received will be made public without disclosing origins or personal links with the concrete citizen. Participating citizens can then verify their own values (c_i). To guarantee that the central census authority does not alter the compound with additional values (c_x), in a public live broadcast a new value (c_k) will be generated from a pseudorandom natural source and added as a binary number to the set of streams in its corresponding place ordinally to create an orderly final stream which is then expressed in a sequential continuous manner, $C = c_1 \,||\, c_2 \,||\, ... \,||\, c_{g+1}$.

The quantity of "1" bits in *C* is then calculated. If the total is even, function composition h( ) ≡ SHA-3-512(SHA-2-512( )) is applied, otherwise h( ) ≡ SHA-2-512(SHA-3-512( )). But to what will it be applied? The different values c_i are circular shifted to the left for as many "1" bits as the value of the ordinal they had in *C*, resulting in $h(CLS_j\ (c_i))$ for each of them. These new values are rearranged again from lowest to highest by applying a circular shift to the left for as many bits as the value of the ordinal they now have. Finally,

the hash function $h(\ )$ obtained before is applied to obtain the final value, H, which is 512 bits long:

$$H = h(CLS_1(h(CLS_i(c_j)))||CLS_2(h(CLS_d(c_r)))||...||CLS_{g+1}(h(CLS_b(c_v)))).$$

Security-wise, the process is oriented so that the obtained value H cannot be known in advance nor can be forced into a determined value range. In this process, the hash functions, which are secure cryptographic primitives, are the key element. Here are used two types of hash functions, both structurally different from one another: SHA-2 and SHA-3. Versions with 512 output bits are applied (SHA-2-512, SHA-3-512).

With regard to SHA-2, there are no practical attacks, although the weaknesses of SHA-0 and SHA-1, SHA-2 being so related to them, motivated the desire for a different way to carry out hash functions. This was the reason for the construction of SHA-3.

In this voting process, if one or more voters sent to the census authority their previously prepared streams for which they have calculated the SHA-2 and SHA-3 hash values, nobody could know all the values. Moreover, even if only one voter does not participate in this plot, it is not possible to know the final value (H), much less c_k or the number of ones. Hence the SHA-3-512(SHA-2-512( )) and SHA-2-512(SHA-3-512( )) values obtained cannot be foreseen without knowing the precise input values due to the properties inherent to these functions. Furthermore, the corresponding ordinal in stream C and in the hash value stream, and therefore the value of the circular shift to the left applied to each in every case, cannot be known, making it impossible to estimate the final H value.

The system's value is thus unpredictable, facing odds of 2^{-512}, unless all voters conspire. Even if they did, c_k would persist. But in the end, the conspiracy would work against them, as they are competing among themselves to choose the best candidate in the elections.

The elliptic curve generation process and the values obtained remain public, and no one, not even the census authority, can alter H. Thus, maximum and total transparency is given to its generation.

The H value can then be taken as the seed of a pseudorandom generator to obtain a prime number (p) of the order of 512 bits, an appropriate length for secure encryption. Through this random value a secure elliptic curve is generated, for which there are solvent proposals (Baignères et al. 2016). Alternatively, departing from H, the next-highest prime value p can be sought, which will define the field $\mathbf{F}_p$ of the elliptic curve.

In addition, users will also provide a different c_i value to generate the rest of the parameters of the elliptic curve via a similar procedure.

Naturally, a series of mathematical security requirements must be adhered to during this cryptographic process, and the values finally obtained must be expressed and exhibited (Flori et al. 2015; Bernstein and Lange 2017).

With the elliptic curve finally defined, each voter will then randomly generate a private and a public key for the electoral process.

Cryptographic Keys

Most cryptocurrencies, such as bitcoin, use a single private key and its respective public key (Nakamoto 2008, [2008]). However, this results in a certain loss of anonymity and the knowledge of the transactions of an address.

With the monero cryptocurrency the procedure is more complex, but it solves the previous problem by using pairs of private and public keys, and thus new public and private keys that are not linked to the original ones can be created anonymously. The voting system proposed here follows monero's addresses model (Saberhagen 2013).

Each user has a double set of keys (i.e., two private [a_1 and a_2] and two public [A_1 and A_2]). Here, a_1 is the original private key and a_2 is the cryptographically derived private key from a_1. If user B wishes to make a payment to user A, he generates a random value, r, to obtain a new point on the curve, R. Using the public values of user A, [A_1 and A_2], user B generates the so-called public one-time key, P, that is linked to user B. User A, having received R, calculates a value, x, which is the private one-time key, known only to A. Both one-time keys are related to each other and are used only in this transaction and not in any other. Thus, the recipient's anonymity is preserved. However, the verification allows user A to know that the transaction is destined for him, he is taking part in the correct transaction.

Anyone who sees the use of P only knows that a certain transaction has occurred and cannot relate it to user A. Moreover, this address may possibly never be used again, as it was generated for that particular transaction.

If it were necessary for B to verify that he sent the payment, it would suffice to show the r value or to use a zero-knowledge protocol to prove that he knows it without disclosing it. On the

other hand, if A were forced to prove that he was the recipient, it would suffice to disclose only the so-called tracking key, (a_2, A_1), keeping at the same time the security of his data and values by not revealing the original private key, a_1.

User B can always either generate a new address (public key) or use subaddresses without anyone knowing that they are linked to him. He can even send money from his original account to this new address without anyone knowing who owns the account. The remittance from B to A is obtained from this new account or address.

Regarding the electoral process, each member of set *M* will now have their own public key, $(A_1, A_2)_i$, and private key, $(a_1, a_2)_i$.

As described, this scheme allows the generation of subaddresses (Noether and Goodell 2017). From values (A_1, A_2) and (a_1, a_2) one can generate as many related subaddresses as desired (1,2,3...,*y*,...).

The method of applying this scheme of addresses and subaddresses is to annex a subaddress generated by the voter when the ballot is cast, as he will receive the monetary amount of the electoral process at that subaddress, if applicable (the procedure will be explained later), by generating a one-time public subaddress (A_1^y, A_2^y) by means of his address $[(a_1,a_2),(A_1,A_2)]$ and a random number, *y*.

Nobody can identify to whom the money was sent. The one-time address will not be used again. Moreover, it is not possible to link the subaddress to any of the original public keys when sending ballots or to know the set of final voters (*N*), which is protected by the strength and computational intractability of solving the elliptic curve discrete logarithm problem (ECDLP). Hence, complete anonymity of the electoral process and of the winning or losing voters is ensured.

Generation of an Effective Voters' Group

Given a set of recorded voters, *M*, and *N*, the subset of those who made the deposit, $N \subseteq M$. Apart from the census authority, it is not publicly known who is in set *N* because the payments are made using *KPub* and *KPriv* keys. These are keys that link each citizen with a determined *KPub*, and in this way when a citizen on the census makes the deposit he also sends the census authority the public keys he has himself created in relation to the elliptic curve generated for voting, $(A_1, A_2)_i$. Thus, the census authority can verify that the deposit was made by a recorded citizen in *M* and consider him within the new set *N*.

To each member of set N the census authority sends an original ballot, m_0 (that after being filled becomes m) as well as the whole set's group of public keys, $\{(A_1, A_2)_1,...,(A_1, A_2)_N\}$. Via a ring signature, the census authority will accept a maximum of N votes, one from each member of N.

One-Time Ring Signatures

The concept of a digital signature first appeared in the work of Whitfield Diffie and Martin Hellman (1976). Since then, several types of signatures have emerged that seek anonymity, particularly with regard to e-money contexts.

Bitcoin, the first cryptocurrency, only offers false anonymity, because although the person making a given transaction is not known, only his public asymmetric key, transactions are still linkable. Other cryptocurrencies have since been developed that seek to attain true anonymity via blind signature (Chaum 1983), DC-nets (Chaum 1988), group signature (Chaum and Van Heyst 1991), or ring signature.

The model presented in this article uses ring signature, developed by Rivest, Shamir, and Tauman (2001). Through ring signature a message can be signed, leaving proof that it has been signed by a member of a given group (without having to request authorization from anyone in the originating group), though without disclosing who specifically has signed it. This scheme has the qualities of being anonymous, unforgeable, untraceable, and unlinkable. Hence, the signatory cannot be identified, nor can it be known whether two different signatures were made by the same person or entity.

There are different variants of ring signature, such as the linkable spontaneous anonymous group signature scheme and traceable ring signature. Using traceable ring signature variant, a modification of Nicolas van Saberhagen's (2013) CryptoNote/monero, called one-time ring signature, was made, emphasizing that one can only securely sign once. If the ring signature were used twice, the link between both would be known, although the identity of the signatory would still not be disclosed. These aspects (anonymous, unforgeable, untraceable, unlinkable, and one-time-sign) are sufficient for the voting scenario. Thus, it will not be necessary to use other ring signature variants which are more oriented to the number of transactions, such as Confidential

Transaction, RingCT, Ring CT2.0; interlocking rings versions such as Borromean ring signature or multisignatures; or even quick variants such as Ring CT3.0 or CLSAG.

The one-time ring signature's phases are described next.

Generation

As has been mentioned, after the elliptic curve has been generated, each voter generates his private and public keys related to the elliptic curve of the election process. It is to be noted that this first phase has already been made, as mentioned above (see Cryptographic Keys section), although with a pair of keys, private and public. This pair of keys corresponds to $(a_2, A_2)_i$, which will be generically named (x_i, P_i) for each member of set N.

Moreover, each voter generates the so-called key image, $I = x_i \cdot H_P(P_i)$, H_P being a hash function on points of the curve.

Signature

The signatory creates a one-time ring signature with noninteractive zero-knowledge. Let (x_s, P_s) be his pair of keys. From the set N of other possible voters the signatory selects a subset, S', of n elements, with the condition that he is not in said subset, and together with his own value, P_s, he builds $S = S' \cup \{P_s\}$.

With other random values he calculates a series of parameters (points on the elliptic curve), L_i and R_i, with the range of i being 0 to n. Then a noninteractive challenge is built:

$$c = H_S\,(m, L_0, L_1, \ldots, L_n, R_0, R_1, \ldots, R_n),$$

where m is the message being signed and H_S is a hash function.

The signatory then generates a response to the challenge from the previous data to obtain c_i and r_i, with the range of i being from 0 to n. Thus, the signature becomes

$$\sigma = (I, c_0, c_1, \ldots, c_n, r_0, r_1, \ldots, r_n).$$

Verification

Through m, S, and σ it is verified that the signature comes from someone in the group of possible signatories (in our case, voters of set N).

Link

The verifier checks whether value I has been previously used, which is forbidden. To do this, the set of values already received, $\{I_i\}$, is checked for $I \in \{I_i\}$ or $I \notin \{I_i\}$.

For the security analysis of the one-time ring signature protocol, please see Saberhagen (2013).

As mentioned above, the properties of the one-time ring signature protocol that make it suitable for an election process are anonymity (more specifically, set anonymity), by which it is considered equiprobable that any member of the group has performed the signing operation; untraceableness, because all possible senders are equiprobable parties to each incoming transaction; and unlinkableness, because it is not possible to know who voted and what their vote was. Simultaneously, the transaction remains linked to its sender, who is able to prove if necessary that he is the signatory, and the protocol also detects the case of two or more outgoing transactions sent by the same person.

The set N of final voters forms the ring. Its quantity (assumed to be a large numeric set) makes it computationally complex to determine the origin of a filled-in ballot, that is, the message m in the protocol. There can only be one transaction (vote delivery). At the time of voting, the number of voters will be either the maximum, N, or less (it may be that some would finally not vote for reasons whatsoever). Only ring members can vote, anyone foreign to the ring of members being detected and barred, and their ballots discarded. It is only possible to vote once; a double vote is detected, which prevents this new value from being recorded, only the first vote collected being considered. Neither can it be known who has voted for what, as only untraceable ballots of the different voters of set N are collected. On each ballot there is a subaddress to which the reward will be sent if the vote is considered a winning one (in terms of the gain and loss experienced under the elected government), but it is not possible to know which of the voters lost money and which gained it.

III. GAIN AND LOSS CRITERION

The government and the different political parties must be confronted with a series of variables considered of fundamental political importance. These variables will consist of a set of

principles (see next section), a framework, or a normative criterion by which the government during the term of office—and during the campaign and elections process—will be analyzed and evaluated.

If an elected party, the ruling party, increases the variables of the framework of principles after the term of office, this means that its voters win the money put down by all other voters. However, this is not that simple. What value is considered an increase? Can it be positive or negative? Is it some determined positive percentage? Where should the boundary be placed? The way to solve this problem is to find a reference point.

So that a party that often wins, with many habitual voters, will be content with very low positive percentage values in its program, which it could obtain very comfortably, cyclically obtaining for its voters the money of the other voters and continually taking power, even increasing the voters' quota. Therefore, all the parties' political programs must be taken into account. These programs will allow to calculate the appropriate value with which to compare a government's performance.

Parties must be judged for what they have actually accomplished, but also for what they promised they would do, as they gained many voters through their political platforms. However, due to the inherent asymmetry between the two, much more weight must be given to what was done than to what was promised. Hence, each political platform has a certain percentage value, p_i%, relative to the variables of the framework of axioms, the normative criteria.

These percentages (p_i%) must be considered in relation to the mass of voters that the party obtained in the last election, v_i, in order that no parties with no electoral base can skew the calculus with big promises. In this way, the average value of the proposals presented, μ, may be calculated:

(1) $\mu = \sum_{i=1}^{n} \frac{(v_i p_i)}{100}\%$

If there are many new parties (perhaps over 40 percent) or parties with new acronyms or names but similar politicians running under a new party, the previous rule can be altered such that value μ is not limited to previously existing parties, and a variant of equation (1) that does not take the v_i value into account can be utilized:

$\mu = \sum_{i=1}^{n} \frac{p_i}{n}\%$.

Suppose that political party X wins an election, and that its political proposal is p_X. With mean μ, the different electoral proposals, p_i, and the value finally obtained after X's term, f_X, an orderly partition of gains and losses can be made. Hence, is provided the following gain and loss valuation scheme:

- $\forall\, i, p_i > 0$: Although political programs can be presented that lower the characteristics that are evaluated, giving negative percentages, the normal thing will be that $p_i > 0$. A political program that does not increase the variables related to the principles' framework can never be given.

  Two possible situations are considered:

  1. $f_X < \mu$

     (a) For each party for whom $f_X < p_i$, X's voters lose the money they contributed, which pass to the voters of p_i in an equitable manner.

     (b) Voters of the parties for whom $p_i \leq f_X$ lose their contributed funds, and they pass both to X and to parties with $f_X < p_i$.

     (c) Voters of the parties for whom $f_X < p_i$ recover their contributions.

  2. $\mu \leq f_X$

     (a) For each party where $f_X \geq p_i$, X's voters gain the money contributed and a percentage of that of the parties for whom $f_X < p_i$. The value of this is $100 \cdot \sum_{j=1}^{n} (\frac{1}{2})^j$, j being the number of political proposals (p_i) in the range $\mu \leq p_i \leq p_X$. The rest of the money contributed by the voters of these parties is returned to them. If $f_X < p_X$ and there is a p_i higher than f_X, all its voters receive their own money and half of what X's voters contributed.

- As an extreme case, if all voters vote for the same party, all participants would recover their money.

To better appreciate the system, table (1) contains all the possible options for an election involving six political parties.

Methodology of Losses and Gains

It is desirable that the requirements and procedures of this scheme be clear, simple, and minimal in number. And they are.

This procedure encourages citizens to vote for parties having p_i higher or equal to the mean μ, which will lead to an improvement in the exercise of the principles of the political framework.

The elected party's promises, p_X, has great weight in the procedure, but the party's results, f_X, are crucial. Also, the appraisal cannot be only between p_X and f_X, which will always offer, as previously noted, very low percentages of improvement. Hence, it is also necessary to compare f_X with μ. And the v_i values must also be taken into account to avoid distortions of the average value by emergent parties that make strong promises but are unlikely to be elected.

Political parties that offer very low program values will probably not be elected. Moreover, their voters will be fewer every time, even stagnating with very low values population-wise. These would be voters that lose money time and again and would end up being very marginal or disappearing.

Additionally, excessively low-value political proposals will lead to the emergence of more competitive parties with better proposals. Even though they will be starting without an established electorate, voters will be very tempted to support them if their proposals have high values.

Notably, a party that makes unattainable promises may inspire many people to vote for it but with the risk of not achieving what it promised, which will result in a considerable monetary loss for its voters. If the results are lower than μ and the government has been disastrous, the party will severely suffer the punishment of those that voted for it, and this will lower its prestige and the number of future voters.

Table 1: Example of the operation of the system for six political parties

	p_A		p_B
	← ⋯)	[…]	[…]
Candidate A wins	* V_A lose their deposits, to be divided between $\{V_B,V_C,V_D,V_E,V_F\}$. * $\{V_B,V_C,V_D,V_E,V_F\}$ recover their deposits.	* V_A lose their deposits, to be divided between $\{V_B,V_C,V_D,V_E,V_F\}$. * $\{V_B,V_C,V_D,V_E,V_F\}$ recover their deposits.	* V_A lose their deposits, to be divided between $\{V_C,V_D,V_E,V_F\}$. * $\{V_C,V_D,V_E,V_F\}$ recover their deposits. * V_B lose their deposits, to be divided between $\{V_A,V_C,V_D,V_E,V_F\}$.
Candidate B wins	* V_B lose their deposits, to be divided between $\{V_A,V_C,V_D,V_E,V_F\}$. * $\{V_A,V_C,V_D,V_E,V_F\}$ recover their deposits.	* V_B lose their deposits, to be divided between $\{V_C,V_D,V_E,V_F\}$. * $\{V_C,V_D,V_E,V_F\}$ recover their deposits. * V_A lose their deposits, to be divided between $\{V_B,V_C,V_D,V_E,V_F\}$.	* V_B lose their deposits, to be divided between $\{V_C,V_D,V_E,V_F\}$. * $\{V_C,V_D,V_E,V_F\}$ recover their deposits. * V_A lose their deposits, to be divided between $\{V_B,V_C,V_D,V_E,V_F\}$.
Candidate C wins	* V_C lose their deposits, to be divided between $\{V_A,V_B,V_D,V_E,V_F\}$. * $\{V_A,V_B,V_D,V_E,V_F\}$ recover their deposits.	* V_C lose their deposits, to be divided between $\{V_B,V_D,V_E,V_F\}$. * $\{V_B,V_D,V_E,V_F\}$ recover their deposits. * V_A lose their deposits, to be divided between $\{V_B,V_C,V_D,V_E,V_F\}$.	* V_C lose their deposits, to be divided between $\{V_D,V_E,V_F\}$. * $\{V_D,V_E,V_F\}$ recover their deposits. * $\{V_A,V_B\}$ lose their deposits, to be divided between $\{V_C,V_D,V_E,V_F\}$.
Candidate D wins	* V_D lose their deposits, to be divided between $\{V_A,V_B,V_C,V_E,V_F\}$. * $\{V_A,V_B,V_C,V_E,V_F\}$ recover their deposits.	* V_D lose their deposits, to be divided between $\{V_B,V_C,V_E,V_F\}$. * $\{V_B,V_C,V_E,V_F\}$ recover their deposits. * V_A lose their deposits, to be divided between $\{V_B,V_C,V_D,V_E,V_F\}$.	* V_D lose their deposits, to be divided between $\{V_C,V_E,V_F\}$. * $\{V_C,V_E,V_F\}$ recover their deposits. * $\{V_A,V_B\}$ lose their deposits, to be divided between $\{V_C,V_D,V_E,V_F\}$.
Candidate E wins	* V_E lose their deposits, to be divided between $\{V_A,V_B,V_C,V_D,V_F\}$. * $\{V_A,V_B,V_C,V_D,V_F\}$ recover their deposits.	* V_E lose their deposits, to be divided between $\{V_B,V_C,V_D,V_F\}$. * $\{V_B,V_C,V_D,V_F\}$ recover their deposits. * V_A lose their deposits, to be divided between $\{V_B,V_C,V_D,V_E,V_F\}$.	* V_E lose their deposits, to be divided between $\{V_C,V_D,V_F\}$. * $\{V_C,V_D,V_F\}$ recover their deposits. * $\{V_A,V_B\}$ lose their deposits, to be divided between $\{V_C,V_D,V_E,V_F\}$.
Candidate F wins	* V_F lose their deposits, to be divided between $\{V_A,V_B,V_C,V_D,V_E\}$. * $\{V_A,V_B,V_C,V_D,V_E\}$ recover their deposits.	* V_F lose their deposits, to be divided between $\{V_B,V_C,V_D,V_E\}$. * $\{V_B,V_C,V_D,V_E\}$ recover their deposits. * V_A lose their deposits, to be divided between $\{V_B,V_C,V_D,V_E,V_F\}$.	* V_F lose their deposits, to be divided between $\{V_C,V_D,V_E\}$. * $\{V_C,V_D,V_E\}$ recover their deposits. * $\{V_A,V_B\}$ lose their deposits, to be divided between $\{V_C,V_D,V_E,V_F\}$.

p_C	μ	p_D
[…]	[…]	[…]
* V_A lose their deposits, to be divided between $\{V_D,V_E,V_F\}$. * $\{V_D,V_E,V_F\}$ recover their deposits. * $\{V_B,V_C\}$ lose their deposits, to be divided between $\{V_A,V_D,V_E,V_F\}$.	* V_A win what $\{V_A,V_B,V_C\}$ deposited, 50% of $\{V_D\}$'s deposits, 25% of $\{V_E\}$'s deposits, and 12.5% of $\{V_F\}$'s deposits. * $\{V_D,V_E,V_F\}$ recover the remaining percentage of their deposits.	* V_A win what $\{V_A,V_B,V_C,V_D\}$ deposited, 50% of $\{V_E\}$'s deposits, and 25% of $\{V_F\}$'s deposits. * $\{V_E,V_F\}$ recover the remaining percentage of their deposits.
* V_B lose their deposits, to be divided between $\{V_D,V_E,V_F\}$. * $\{V_D,V_E,V_F\}$ recover their deposits. * $\{V_A,V_C\}$ lose their deposits, to be divided between $\{V_B,V_D,V_E,V_F\}$.	* V_B win what $\{V_A,V_B,V_C\}$ deposited, 50% of $\{V_D\}$'s deposits, 25% of $\{V_E\}$'s deposits, and 12.5% of $\{V_F\}$'s deposits. * $\{V_D,V_E,V_F\}$ recover the remaining percentage of their deposits.	* V_B win what $\{V_A,V_B,V_C,V_D\}$ deposited, 50% of $\{V_E\}$'s deposits, and 25% of $\{V_F\}$'s deposits. * $\{V_E,V_F\}$ recover the remaining percentage of their deposits.
* V_C lose their deposits, to be divided between $\{V_D,V_E,V_F\}$. * $\{V_D,V_E,V_F\}$ recover their deposits. * $\{V_A,V_B\}$ lose their deposits, to be divided between $\{V_C,V_D,V_E,V_F\}$.	* V_C win what $\{V_A,V_B,V_C\}$ deposited, 50% of $\{V_D\}$'s deposits, 25% of $\{V_E\}$'s deposits, and 12.5% of $\{V_F\}$'s deposits. * $\{V_D,V_E,V_F\}$ recover the remaining percentage of their deposits.	* V_C win what $\{V_A,V_B,V_C,V_D\}$ deposited, 50% of $\{V_E\}$'s deposits, and 25% of $\{V_F\}$'s deposits. * $\{V_E,V_F\}$ recover the remaining percentage of their deposits.
* V_D lose their deposits, to be divided between $\{V_E,V_F\}$. * $\{V_E,V_F\}$ recover their deposits. * $\{V_A,V_B,V_C\}$ lose their deposits, to be divided between $\{V_D,V_E,V_F\}$.	* V_D win what $\{V_A,V_B,V_C\}$ deposited, 50% of $\{V_D\}$'s deposits, 25% of $\{V_E\}$'s deposits, and 12.5% of $\{V_F\}$'s deposits. * $\{V_D,V_E,V_F\}$ recover the remaining percentage of their deposits. * $\{V_E,V_F\}$ win 50% of $\{V_D\}$'s deposits.	* V_D win what $\{V_A,V_B,V_C,V_D\}$ deposited, 50% of $\{V_E\}$'s deposits, and 25% of $\{V_F\}$'s deposits. * $\{V_E,V_F\}$ recover the remaining percentage of their deposits.
* V_E lose their deposits, to be divided between $\{V_D,V_F\}$. * $\{V_D,V_F\}$ recover their deposits. * $\{V_A,V_B,V_C\}$ lose their deposits, to be divided between $\{V_D,V_E,V_F\}$.	* V_E win what $\{V_A,V_B,V_C\}$ deposited, 50% of $\{V_D\}$'s deposits, 25% of $\{V_E\}$'s deposits, and 12.5% of $\{V_F\}$'s deposits. * $\{V_D,V_E,V_F\}$ recover the remaining percentage of their deposits. * $\{V_D,V_F\}$ win 50% of $\{V_E\}$'s deposits.	* V_E win what $\{V_A,V_B,V_C,V_D\}$ deposited, 50% of $\{V_E\}$'s deposits, and 25% of $\{V_F\}$'s deposits. * $\{V_E,V_F\}$ recover the remaining percentage of their deposits. * $\{V_F\}$ win 50% of $\{V_E\}$'s deposits.
* V_F lose their deposits, to be divided between $\{V_D,V_E\}$. * $\{V_D,V_E\}$ recover their deposits. * $\{V_A,V_B,V_C\}$ lose their deposits, to be divided between $\{V_D,V_E,V_F\}$.	* V_F win what $\{V_A,V_B,V_C\}$ deposited, 50% of $\{V_D\}$'s deposits, 25% of $\{V_E\}$'s deposits, and 12.5% of $\{V_F\}$'s deposits. * $\{V_D,V_E,V_F\}$ recover the remaining percentage of their deposits. * $\{V_D,V_E\}$ win 50% of $\{V_F\}$'s deposits.	* V_F win what $\{V_A,V_B,V_C,V_D\}$ deposited, 50% of $\{V_E\}$'s deposits, and 25% of $\{V_F\}$'s deposits. * $\{V_E,V_F\}$ recover the remaining percentage of their deposits. * $\{V_E\}$ win 50% of $\{V_F\}$'s deposits.

p_E	p_F
[…)	[…→
* V_A win what $\{V_A,V_B,V_C,V_D,V_E\}$ deposited and 50% of $\{V_F\}$'s deposits. * $\{V_F\}$ recover the other 50% of their deposits.	* V_A win what $\{V_A,V_B,V_C,V_D,V_E,V_F\}$ deposited.
* V_B win what $\{V_A,V_B,V_C,V_D,V_E\}$ deposited and 50% of $\{V_F\}$'s deposits. * $\{V_F\}$ recover the other 50% of their deposits.	* V_B win what $\{V_A,V_B,V_C,V_D,V_E,V_F\}$ deposited.
* V_C win what $\{V_A,V_B,V_C,V_D,V_E\}$ deposited and 50% of $\{V_F\}$'s deposits. * $\{V_F\}$ recover the other 50% of their deposits.	* V_C win what $\{V_A,V_B,V_C,V_D,V_E,V_F\}$ deposited.
* V_D win what $\{V_A,V_B,V_C,V_D,V_E\}$ deposited and 50% of $\{V_F\}$'s deposits. * $\{V_F\}$ recover the other 50% of their deposits.	* V_D win what $\{V_A,V_B,V_C,V_D,V_E,V_F\}$ deposited.
* V_E win what $\{V_A,V_B,V_C,V_D,V_E\}$ deposited and 50% of $\{V_F\}$'s deposits. * $\{V_F\}$ recover the other 50% of their deposits.	* V_E win what $\{V_A,V_B,V_C,V_D,V_E,V_F\}$ deposited.
* V_F win what $\{V_A,V_B,V_C,V_D,V_E\}$ deposited and 50% of $\{V_F\}$'s deposits. * $\{V_F\}$ recover the other 50% of their deposit.	* V_F win what $\{V_A,V_B,V_C,V_D,V_E,V_F\}$ deposited.

Note: V_i means party i voters.

By definition, there will always be political programs on both sides of μ, unless they coincide among themselves. Also, and as said before, $p_i > 0$ has been considered.

In their percentages all parties' p_i values can be expected to lie within a very close range (although the usual thing will be that said percentage, which is the total of the political program, comes from different values in the different sectors in which said political program is applied), so they will not have great diffusion (i.e., variance σ^2 will be small).

During an electoral campaign, debates and presentations of ideas will take place, which will lead to their further development and modification. This will lead a tendency for the political programs to resemble one another, because there is an incentive to vote for parties having a higher p_i, because voters stand to gain more money. Forty-eight hours before an election can be considered the cutoff by which parties will finalize their programs, which will then be configuration locked. Once the political programs have been finalized, the p_i values can be used to officially calculate μ.

A party that promises too much, with a very high p_i percentage, will be confronted, should it win, with a very high μ (if it had a high v_i of previous voters), which would make it difficult to carry out its proposals, for which the voters would be penalized: offering the party a high p_X and not fulfilling its promises, the voters are penalized, and with a loss of half the money contributed if there are p_i values higher than f_X.

On election day, voters will tend to vote for parties having a high p_i owing to the potential monetary gains. But this does not mean necessarily that they must elect the one with a higher p_i value. This is so because if the variance is not large, and if it is not easy to overcome p_X, the voters of losing parties with a high p_i value would gain a lot of money. The reason is that if most of the voters put their money on the candidate having the highest p_i and few voters on the second candidate (and fewer voters on the rest, descending linearly or exponentially, suppose), then in the case that the elected party had the highest p_i but ultimately a poor f_X, a small number of voters will win the monetary mass of a high number of voters. Therefore, irrespective of better models, it is likely that the votes would be balanced among the best p_i proposals.

To prevent impossible or impracticable program proposals offering very high p_i values, a limit can be set, perhaps of 100 or even 300 percent. This is important because such agendas would take the mean (μ) to unreachable values, and voters of the winning party would always be penalized relative to the supporters of losing parties with high p_i percentage.

Finally, if coalitions among parties surface, the p_i and v_i percentages would both change according to the average values calculated, it making clear to the citizens which is the final program proposed. Should a coalition occur during the term of office or during a given period, the percentages would be prorated.

These gain and loss rules increase both voter and politician responsibility. Leaders are driven to improve their government teams. Lying in political programs is penalized. On the other hand, the rules dilute the bigotry and the fanaticism of many voters, leading them to demand more from those for whom they vote. In addition, no voter will be proud of losing his money, and thus it will not be a merit to vote for certain negligent parties. All these aspects are discussed in more detail in the last section.

A variant, which is not considered in detail here, but which is suggested at this moment, is one in which each voter can not only put the entire deposit in the same political party, but in different parties, until completing the monetary total of the deposit. Consequently, the gains and losses will be applied in a corresponding and proportional manner.

Electoral Fraud

One of the major problems in electoral processes has always been fraud, still existing today despite and also due to the use of digital telematic procedures (Campbell 2005; Saltman 2006; Schaffer 2008).

This proposal minimizes fraud risk. After voting, it is known how many voters voted for the different options and thus the total amount of money deposited. Moreover, from the moment the term of office finishes (and also throughout it) f_X is calculated and compared with p_i values of the proposed political programs and with μ, allowing each voter to know immediately, based on his vote, which he cannot change, whether he will receive money and how much.

These data, which can be made public, showing the voters' subaddresses and votes without disclosing (as it is unknown) the concrete persons to whom they correspond, allow the particular composition of the vote to be known. And the evolution of gain and loss can be tracked in real time as the f_X value is realized during the term. This realization or fulfilment has to be precise and detailed, making it possible to establish when a given milestone has been achieved, to measure it, and to determine the percentage attained.

Each voter, if confronted with fraud whereby he would not receive the due money, can prove to the census authority or the pertinent legal body what his vote was, as well as his link with the cryptographic addresses and subaddresses he used in the electoral process.

Even if a pressure group who wanted to carry out an agenda could buy votes (something that can also happen today and with greater ease of purchase), it would have to pay huge amounts to influence the outcome in this system (since participating in the election is expensive enough). Furthermore, lobbyists stand to lose all their money owing to the nature of the loss and gain criteria. But there is still a doubt because not all countries have the same distribution of income in terms of monetary amount and number of citizens. In poor countries, very few have large incomes, many have low incomes, and there are hardly any middle classes. Here the lobbyists (rich) could influence the vote by buying the votes of many citizens (poor). But even though these poor countries are more fragile in the face of such an attack than other countries, it is still extremely expensive to influence the vote in this way. In any case, the possibility remains open of offering a more comprehensive, detailed, and argued response to this type of attack.

What's more, the census authority has a decentralized structure to avoid the risk of centralized control. It must also be transparent, and externally audited. Its decentralization can be achieved under blockchain technologies: secure and traceable P2P networks. To avoid fraudulent votes being cast for nonexistent, deceased, or illegal voters, crypto-biometrics can be added to the asymmetric key structures (Jara-Vera 2013). Additionally, other proposals such as proof of identity and proof of humanity can also be considered.

IV. POLITICAL FOUNDATIONS

Principles Framework

What are the regulating principles, the elements according to which the government will be assessed and that will serve as a basis in electoral processes? Without entering into a discussion of the debates around these qualities, which can be found in other authors, specialized therein, some of whom will be cited here, the following specifications must be made:

(1) The principles must be few, the minimum possible, as they are the framework of principles or axioms from which the rest of the rules and political programs are derived.

(2) They will have to be accepted by all citizens, by all individuals, because the different governments and political parties will be valued according to them.

(3) The principles must be inherent to human dignity. This does not disregard the ethical and philosophical difficulty of expressing and specifying the concepts of inherence and dignity.

Without going into the details, there are several hypothetical frameworks of principles that can be adopted:

- Hypothesis A: Happiness is the main aim of the individual, and he delegates its attainment to governments, which make it available to citizens.
- Hypothesis B: Since their emergence of governments, one of their main and at-hand aims has been to preserve the peace (internal and external), order, and welfare of community members.
- Hypothesis C: There are two human qualities that governments and political systems have, to a greater or lesser degree, defended and advocated, often considered antagonistic and conflicting qualities: liberty and equality (Dalberg 2016; Hayek [1960] 2020; Buchanan 1975; Rothbard 1998, [1995] 2006; Sandel 1984; Kuehnelt-Leddihn [1952] 2007; Frankfurt 2015). These elements are clearly inherent to people. Therefore, they can be considered universal. In general, parties of the Right and the Left, or, more accurately, less or more statist, respectively, have leaned more toward one side or another. Hence, liberty and equality can be considered as the founding elements and principles. Freedom is always individual, there not existing a collective freedom, because the individual is in himself worthwhile, irreplaceable,

> and never a means but an end. He is his own sovereign and so responsible for himself. On the other hand, equality means equal treatment before the law, juridical equality, because people are all morally equal, even though diverse and different by nature in their abilities, talents, and desires, which makes them individual, which is a great fortune.

Here hypothesis C—equality before the law, juridical equality, or isonomy, "isonomia" ("*ισονομία*"), and individual freedom or "atomo-eleutheria" ("*άτομο-ελευθερία*")—will be adopted as the framework of principles. These principles will be the only ones. They are in no way opposed but in combination work well together, as juridical equality is among individuals and freedom is the same, equal, for all.

Another Framework?

Equality before the law and individual freedom are possibly the only two principles that respect every individual. Adding any other principles to the framework or downgrading those two would reduce those properties in their essence.

The two selected principles lead to each person's respect for the ways of life of the rest (provided they respect the said framework of principles) in his own life's work. Nobody can impose his criteria and opinions on others but can suggest them in respectful and free interactions even though a person might regard certain ideas as the highest ways of life. That is why it is up to the individual to make the decisions he believes adequate for himself, as clearly expressed by Friedrich A. von Hayek ([1960] 2020; [1973] 2011). Only the individual has dominion and sovereignty over himself; he is responsible for his individual freedom, rejecting the imposition of authority over himself by any other person (Huemer 2012; Lomasky 1987).

Only through these principles can one reach, as Alberto Benegas Lynch (2015) said, an "unconditional respect for others' projects of life." Any other option is overpowering, overwhelming, disrespectful, and implies an intrusion in people's lives with abuse of power and imposition, and is thus dismissed as unethical and immoral. These two principles allow compliance with the justice precept, to give to each one his own, already stated by jurist Domitius Annius Ulpianus between the second or third century AD, "Suum cuique tribuere." There is nothing more proper and

universal than these two principles, which allow everyone to live his own life.

That is why juridical equality and individual freedom meet the prior requirements for the principle framework: (1) being minimal, (2) universally accepted, and (3) inherent to the dignity of the human being. Next, these two principles will be argued in relation to the three previously mentioned requirements.

- Regarding point (1), there are only two principles, no need for any others. On the basis of these any other organizational model can be carried out. Both principles can by themselves and with human creativity generate free relations among individuals such as contracts and allow the attainment of well-being, not only material but moral and spiritual.
- Regarding point (2), perhaps not everybody may desire this framework, as have been expounded it here, whether they wish to change it, add other elements, or even reduce equality before the law and individual liberty. However, any other option can indeed be considered as interfering in others' lives. That is why this framework, though it may not be radically and enthusiastically desirable to everybody, because many people wish to tell others imposingly how to live their lives, does allow everyone to do what they consider best with their lives.

  The properties of these two principles, isonomia and atomo-eleutheria, call for their moral imposition: impose on others that they do not meddle in another's life if they do not want this and, if they do, only as far as and for as long as they wish. This imposition emerges from the moral imposition of the human being's dignity as free and equal to all the rest before the law. A different thing, although additional, is that the person who wishes to live with lower degrees of freedom and equality, can always seek people with whom to live in an organizational regime with these modalities (even modalities of very little freedom and equality), although without losing his capability to leave an association that he entered freely, being able to leave in accordance with the contract subscribed to, always without losing his human dignity as a free individual and an equal before the law, as expressed by Juan Ramón Rallo (2019).

  At this time, an annotation on contracts is going to be made: blockchain technology is the best structure to protect contracts

under the expressed conditions. After the use of blockchain for cryptocurrencies, contracts may be the most immediate application, creating smart contracts (Szabo 1995) and with them smart property. By this means the decentralization of markets and relations among participating members can be attained. This affects all matters, be it raw materials or processed products, stock, services, capitals, funds, credits, loans, derivatives, options, futures, pensions, debt, trade agreements, patents, legal rights, bonds, licenses, registries, certificates, DAOs (decentralized autonomous organizations), DACs (decentralized autonomous corporations), DAS (decentralized autonomous societies)—in short, any of the existing varieties of relation among individuals or entities. Ethereum is a platform pioneer in this area; it is not predominantly a crypto coin, but a distributed general purpose computing platform on which other protocols and blockchains can be executed and where smart contracts can be subscribed to, permitting the display of decentralized applications (DApps). Other structures of smart contracts are Hyperledger Fabric, Corda, NEM, Stellar, and Waves (Hewa 2020).

- Regarding point (3), the selection of principles not including isonomy and atomo-eleutheria would be immoral, as it places some persons above the rest, thus restricting the others. Such principles can only be selected in the case, mentioned above, of organizations that individuals freely opt into, in a personal and contractual manner, and can always exit. These two principles that serve as the axiomatic framework for human beings -based on reason and will- are therefore the ones who lead to achieve their own ends, making clear their high dignity. However, on occasions, and always under contracts, for the reasons they consider, individuals can live with different degrees of freedom and equality levels among themselves, under consent, and always being able to get out of this situation with the contractual clauses.

Departing from the accepted hypothesis, C, the answer to the two discarded hypotheses is the following:

- Response to hypothesis A: There is no doubt that happiness is the desire of humans, but because of human diversity itself, not everybody pursues the same happiness, not even the same individual in different periods of his life. This human quest is

personal. And governments' attempts to reach happiness have only resulted in hell on earth, rather than a joyous and blessed paradise. The framework offered here is the one that can best help each individual, even with others' assistance, never imposition, reach said happy and blessed ending.

- Response to hypothesis B: Regarding peace, order, and welfare, these elements being noble, there could be a society of citizens under orderly regulations, a peaceful society, both inside and outside, and where there is sufficient economic well-being, but where citizens do not have much more than this, almost like a human farm where citizens are watched and controlled so that order and peace are maintained and are provided with food and rewarding sensorial activities. There may be or be conceived more thriving societies, but at the cost of sacrificing individual freedom and equality before the law. However, this is not a human ideal, but a dystopia to avoid.

  Going a little deeper into the wealth aspect, because of wealth's normal importance for any person, should it not be included as a principle? That is, should it be taken into account whether the government has created economic growth during its term or improved the working conditions, employment, monetary stability, etc.? As indicated before, there exists a problem that leads to the exclusion of economic success from the framework of principles: that there could be a government that boosted economic development at a maximum, while curtailing aspects of equality before the law and citizens' individual liberty. Thus, ironically, and knowing that it is contrary to intuition, economic success cannot be a valuative principle for governments.

  The two selected principles, equality before the law and individual liberty, are those that will, creatively, lead to people's material welfare, as expressed by Jesús Huerta de Soto (2010) and compiled by Deirdre Nansen McCloskey (2006).

  The individuals themselves, in general fostering free and never coercive relationships among themselves, will organize themselves in the best manner and ways according to their desires. This will include even arrangements which limit, sometimes considerably, aspects of freedom and equality, as these relations, which will be a sort of contract among individuals, will be created and generated by them to reach certain ends. Individuals will be able to cancel such contracts

> as desired. They will never be foisted on others, as they are personal contracts. The two axioms considered lead directly to the reduction of the state and the even greater reduction of any coercive government, since it is the individual people who govern themselves in the way they want, even though some individuals in a free and noncoercive way could group and choose, for themselves alone and for as long as they want, highly statist and bureaucratized government structures. This organization among individuals will allow them to achieve order, welfare, and internal and external peace through their own actions and decisions. In short, the other aspects of "human action" (Mises [1949] 1998) will be developed over this framework. This framework is thus the best response to human diversity in its defense of the institutions that permit the peaceful coexistence of different ideas, beliefs, and ways of life, as said by Chandran Kukathas (2003).

There is another aspect that, due to its importance, is necessary to mention. The two principles proposed as a political framework dignify human beings, but they do not solve all at once the host of human needs, not even material ones. Although there are people who wish to renounce their freedom and their human dignity, at least at some moments of their lives, just to have material things, this must be their own decision, not to be enforced on others. These two principles, individual freedom and juridical equality, as seen, in dignifying individuals make them responsible, which further enhances that dignity.

There is no doubt that life in a society led by these principles is not simpler than life under a paternalistic state, which would treat people as farm animals, but the former is more human because of those guiding principles. In such a society humans are responsible for themselves, each one able to choose and pursue his individual wishes, through trial and error, with training, with effort, and with the other individuals' free cooperation and help. The proposed framework will be the most moral and worthy for the human being, optimal and appropriate for the development of relations among individuals, business transactions, contracts, entrepreneurship, welfare, and well-being. It is the framework under which there would emerge a diversity of options for life, the framework of utopias of Robert Nozick (1974).

Comparison with Other Forms of Government

This political framework addresses the classic questions of who is to govern, how will they govern, and how much power will they have (Popper [1945] 2011). The answer is simple: each person will govern himself under the two principles of equality before the law and individual freedom.

Democracy defines a participatory citizenship and seeks to eliminate class and sectoral privileges but retains too many elements opposed to isonomy and atomo-eleutheria. Democracy must never be seen as an end in itself but as a means that will be modified as needed to best reach the ends of equality before the law and the recognition of each person's inherent freedom, under which everyone is able to seek his own personal ends.

Democracy soon leads to varying degrees of manipulation of the mass media and education by rulers, as well as manipulation of the voters, who are often irresponsible voters, and not capable of assuming their decisions in the electoral process. Even if there is no manipulation, it will always be immoral that a political program considered appropriate by some citizens, even if the majority, is imposed on the others using legal coercion and police force. The correct thing is that each person be left free to seek his desires, ends, and happiness (freedom that is always individual, atomo-eleutheria) where he considers best (and even not to seek it, if decided), all being considered equal before the law (isonomy). Nobody is to impose on another a predetermined way of life.

The voting system's framework of isonomy and atomo-eleutheria increases the responsibility of all agents and leads to greater individual freedom and equality before the law.

In addition, it also solves many other conflicts. The greatest is the so-called paradox of democracy (or of the majority), wherein the majority elects a tyranny, which is solved because in a society of individual freedom and equality before the law, based on contractual relations among individuals, only the established relations affect only those citizens who desire them and only for the period established in the contract; they cannot affect those who do not want that type of relationship.

This ideological framework also prevents the debasement to which politics, because it is based on coercion and interfering in others' lives, leads.

The voting system even eliminates the present issues of democratic populism and the fraud of broken political promises, as the government's political program becomes the means of judging its performance. The monetary ante and potential compensation should strongly mitigate voter bias and careless involvement. The voting system also provides a wholly public regulatory process with complete accountability and simultaneously anonymity.

Thus, it eliminates politicians' short-term vision and vote buying using budgets, as with these the rulers would reduce the levels of individual freedom and equality before the law. Voters will make demands of their rulers, have the capacity to express their demands, and the political parties themselves will make demands on their candidates and government structures, relegating the unfit and promoting the competent ones.

Confirmation and reconfirmation bias toward ideas supported and the effects of spellbinding or very charismatic, persuasive, and manipulative leaders are also eliminated or mitigated. Even though voters will always have rational biases or assumptions, even rational irrationality (Caplan 2007), this model tends to debug and minimize them.

One issue is the safeguarding and defense of the two principles of the regulatory framework. Only citizens united under these principles can guarantee their defense if confronted with those wanting to violate them. An institution that protects this framework from assault, and watches over it, is needed, perhaps being the only necessary nucleus of what could be called government, a minimum government. These government structures may be multiple and very decentralized.

How can this voting system be implemented? The only way is to show that any coercive political system is morally unacceptable, unworthy, and indecent, since it intrudes on people's personal lives in a coercive way. This highlights the strength of the proposal presented here, a system that promotes and enhances the values of individual freedom and equality before the law. In propounding these values, the system reveals the weakness of the other political proposals that rely on coercive force. An isonomy and atomo-eleutheria program requires intellectual acceptance and a volitional desire that accepts it. The imposition by force of the political framework presented to put it in effect as soon as possible could be desirable, but it would be counterproductive, for because

of its bad implementation it would become unacceptable despite the goodness of its ends. The process must be gradual, and it must be supported by an ethic, and a philosophy, because it must also overcome the inertia of the other political systems, in place and assumed for so many centuries and millennia. The model must from the beginning show the indecency and immorality of systems that are imposed on the individual, even if they are endorsed by the majority or by the ruler clothed in power.

This system allows anyone to live according to his ideology or beliefs, but only with those who wish to live by them as well, not with the rest who do not want it. And nobody prevents it from doing so. It should be possible, if desired, and when desired, to get out of that system of ideas to which someone has linked with other people, being able to go to another model of life. Live without coercion towards anyone and from anyone towards oneself. This voting system employing a monetary deposit, the gain and loss model, cryptographic technology, and a structure of two axioms (individual freedom and equality before the law), allow the implementation of a fair and worthy system of political relations.

Measuring Levels of Isonomy and Atomo-eleutheria

As expounded, the only political institutions that should exist are those that watch over the two principles, leaving all other institutions under the will of those who elect to belong to them through contract.

Since Kenneth J. Arrow ([1951] 1963), it has been known with evidence, that there is no universally valid decision criterion. The most apparently harmless criterion is contradictory and is not rational when an attempt is made to apply it to making social-political decisions. This is why political systems should only be based on axiomatic principles, which are less harmful and intruding, specifically individual freedom and equality under the law, leaving everything else to the free and egalitarian decision-making of individuals by means of voluntary, revocable, and modifiable contracts.

How to perform a percentage comparison of the framework's principles? In short, how can freedom and equality be compared? These concepts cannot be quantified or compared in a simple way, but ample and diverse uses of them in the different spheres and sectors of human activity can be generated. To account for this variety, it is necessary to isolate the spheres of the human environment, subdividing the subdivisions so as to have a diversity

of areas in which to intervene and propose government programs that increase the percentage of isonomy and atomo-eleutheria. It is necessary to diversify, quantify, divide, and subdivide them, although with much caution, and, even though it is not easy to ponder, subdivide, and catalog them qualitatively and quantitatively, it is possible to reach a certain granularity and measure.

All sociopolitical sectors would be analyzed; for example, territorial administration, from the most local level to the broadest, infrastructure, energy, the communications sector, labor markets, companies and their regulation, monetary and financial structures, pensions, health, education, culture, the environment, etc.

To deepen the explanation, considering pensions, for example, milestones and achievements would be established to move from the public pension system to the private one, eliminating the control exercised by politicians. As well as inequalities before the law of pensions for political or governing positions.

In the case of health, a diversity of milestones would be established to expand the freedom and legal equality of the sector and prevent a state monopoly or semimonopoly. All hospitals, distributors, intermediaries, health personnel, etc. would be considered here. As well as the diversity of specialties. And with all this, also health legislation. Ranks and values would be established that would mark the degree of freedom and equality before the law that is achieved by reaching the various milestones.

The process would be similar for education, with a diversity of values at each milestone. For example, the degree of individual freedom and equality before the law in each of its aspects should be measured, from the teaching staff to the curricular content. Freedom and deregulation should be encouraged, and without totalitarian control by the political structure. It is the development throughout the life of that person and his own interests, together with the supply and demand of the labor market itself, that marks the degree of education and training that he has and needs to face life and its challenges.

These aspects of divisions and subdivisions of the different socio-political areas, only mentioned, must be developed in greater depth (perhaps using simulations or experimental data), refining minor aspects of quantification. However, it is a complete and developed model that is offered here.

A question emerges now: Could progress take place in certain aspects of individual freedom and equality before the law and not in others? The answer is negative, as progress in some sectors will lead in the end to progress in the rest. This is so because progress will encourage governments to work on the most backward areas, because doing so would improve percentages more easily, so that the quest to increase the percentage of both principles will lead to an advance in all, no application being left behind forever, but just the contrary.

Several proposals and classifications have been made since the middle of the last century (Gwartney 1996), such the Heritage Foundation's worldwide Index of Economic Freedom (conducted since 1995), the Fraser and Cato Institutes's Economic Freedom of the World index (since 1996), and the Cato Institute's Human-Progress index. This work should be built upon so as to establish an index of the principles of individual freedom and equality before the law, which serve as the ideal government framework. Detailed road maps already exist that show how to proceed in different political and social spheres (Rallo 2014).

CONCLUSION

This article has proposed a political and electoral framework for anonymous and fully accountable voting based on cryptography.

After analyzing the different options and proposals, as well as their advantages and disadvantages, it has been shown that this framework, of minimum universal elements linked to the human being, in every place and time consists of individual freedom and equality before the law. Only these adhere to what is fair, allowing everyone to pursue their own ends without any coercion whatsoever. It is the only set that preserves political morality, any other possibility being a forceful and imposed meddling in others' lives.

With this framework as a foundation and through diverse division and subdivision procedures, a way of constructing diverse political programs in electoral processes was outlined. With these, a valuation process (with a deposit, and a losses and gains criterion, reflecting voluntary, free, and responsible actions) for parties' political programs and the policies ultimately carried out by the winning party in office were articulated.

By means of cryptography, as well by the use of the tools developed for the monero cryptocurrency, namely pairs of public and private keys and the one-time ring signatures, a technological structure has been constructed that is able to encourage, on the one hand, the progress of the two principles of the base political framework and, on the other hand, responsibility among voters and politicians for their own actions through monetary rewards and sanctions.

In addition, other significant problems have been solved such as those related to the census (who is entitled to vote and how to know if one's vote has been counted); double voting (similar to double spending in cryptocurrency, it is not possible to vote more than once); leadership and governance (who is to govern and how the government); and electoral fraud.

REFERENCES

Arrow, Kenneth J. (1951) 1963. *Social Choice and Individual Values*. New Haven, Conn.: Yale University Press.

Back, Adam. 2002. "Hashcash . A Denial of Service Counter-Measure." Cypherspace.org. http://www.cypherspace.org/hashcash.

Baignères, Thomas, Cécile Delerablée, Matthieu Finiasz, Louis Goubin, Tancrède Lepoint, and Matthieu Rivain. 2016. "Trap Me If You Can—Million Dollar Curve." IACR Cryptology ePrint Archive, report 2015/1249. https://eprint.iacr.org/2015/1249.pdf.

Barker, Elaine. 2020. *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*. NIST Special Publication 800-175B, Revision 1. Gaithersburg, Md.: NIST.

Benegas Lynch, Alberto. 2015. *La libertad es respeto recíproco*. Washington, D.C.: Cato Institute.

Bernstein, Daniel J., and Tanja Lange. 2017. "SafeCurves: Choosing Safe Curves for Elliptic Curve Cryptography." SafeCurves. Last modified Jan. 22, 2017. http://safecurves.cr.yp.to.

Brennan, Jason. 2016. *Against Democracy*. Princeton, N.J.: Princeton University Press.

Buchanan, James M. 1975. *The Limits of Liberty: Between Anarchy and Leviathan*. Chicago: University of Chicago Press.

Campbell, Tracy. 2005. *Deliver the Vote: A History of Election Fraud, an American Political Tradition, 1742–2004*. New York: Basic Books.

Caplan, Bryan. 2007. *The Myth of the Rational Voter: Why Democracies Choose Bad Policies*. Princeton, N.J.: Princeton University Press.

Chaum, David. 1983. "Blind Signatures for Untraceable Payments." In *Advances in Cryptology: Proceedings of Crypto 82*, edited by David Chaum, Ronald L. Rivest, and Alan T. Sherman, 199–203. New York: Springer Science+Business Media.

———. 1988. "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability." *Journal of Cryptology* 1, no. 1: 65–75.

Chaum, David, and Eugène van Heyst. 1991. "Group Signatures." *Advances in Cryptology—EUROCRYPT '91*, edited by D. W. Davies, 257–65. Berlin: Springer-Verlag.

Cohen, Henri, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. 2005. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Boca Raton, Fla.: Chapman and Hall/CRC.

Dai, Wei. (1998). *B-Money*. Weidai.com. http://www.weidai.com/bmoney.txt.

Dalberg, John Emerich Edward [Lord Acton]. 2016. *The History of Freedom (and Other Essays)*. Loschberg: Jazzybee Verlag Jürgen Beck.

Diffie, Whitfield, and Martin Hellman. 1976. "New Directions in Cryptography." *IEEE Transactions on Information Theory* 22: 644–54.

ENISA (European Union Agency for Network and Information Security). 2014. *Algorithms, Key Size and Parameters Report—2014*. Heraklion, Greece: ENISA.

Flori, Jean-Pierre, Jerôme Plût, Jean-René Reinhard, and Martin Ekera. 2015. "Diversity and Transparency for ECC." Paper presented at the NIST Workshop on Elliptic Curve Cryptography Standards, Gaithersburg, Md., June 11, 2015.

Frankfurt, Harry G. 2015. *On Inequality*. Princeton, N.J.: Princeton University Press.

Gwartney, James, Robert Lawson, and Walter Block. 1996. *Economic Freedom of the World: 1975–1995*. Vancouver: Fraser Institute.

Hayek, Friedrich A. von. (1960) 2020. *The Constitution of Liberty*. Reprint, London: Routledge.

———. (1973) 2011. *Law, Legislation and Liberty*. Reprint, London: Routledge.

Hewa, Tharaka, Mika Ylianttila, and Madhusanka Liyanage. 2020. "Survey on Blockchain Based Smart Contracts: Applications, Opportunities and Challenges." *Journal of Network and Computer Applications* 177: 1–55.

Hoppe, Hans-Hermann. 2001. *Democracy: The God That Failed: The Economics and Politics of Monarchy, Democracy, and Natural Order*. New Brunswick, N.J.: Transaction Publishers.

Huemer, Michael. 2012. *The Problem of Political Authority*. Basingstoke, Hampshire: Palgrave Macmillan.

Huerta de Soto, Jesús. 2010. *Socialism, Economic Calculation and Entrepreneurship*. Translated by Melinda Stroup. Cheltenham, U.K.: Edward Elgar.

Jara-Vera, Vicente, and Carmen Sánchez Ávila. 2013. "La criptobiometría y la redefinición de los conceptos de persona e identidad como claves para la seguridad." *DESEi+d* 2013: 583–90.

Kuehnelt-Leddihn, Erik von. 1952. *Liberty or Equality: The Challenge of Our Time*. Edited by John P. Hughes. Caldwell, Idaho: Caxton Printers.

Kukathas, Chandran. 2003. *The Liberal Archipelago: A Theory of Diversity and Freedom*. Oxford: Oxford University Press.

Lomasky, Loren E. 1987. *Persons, Rights, and the Moral Community*. New York: Oxford University Press.

May, Timothy C. 1992. "The Crypto Anarchist Manifesto." Cypherpunk mailing list archives, Activism: Cypherpunks (website). Nov. 22, 1992. https://www.activism.net/cypherpunk/crypto-anarchy.html.

———. 1994. "The Cybernomicon." Accessed June 18, 2021. http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ.

McCloskey, Deirdre Nansen. 2006. *The Bourgeois Virtues: Ethics for an Age of Commerce*. Chicago: University of Chicago Press.

McCorry, Patrick, Siamak F. Shahandashti, and Feng Hao. 2017. "A Smart Contract for Boardroom Voting with Maximum Voter Privacy." In *Financial Cryptography and Data Security*, edited by Aggelos Kiayias, 357–75. Cham, Switzerland: Springer.

Mises, Ludwig von. (1949) 1998. *Human Action: A Treatise on Economics*. scholar's ed. Auburn, Ala.: Ludwig von Mises Institute.

Nakamoto, Satoshi. 2008. "Bitcoin P2P e-Cash Paper." Cryptography mailing list archive, Nov. 1, 2008. https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html.

———. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin.org. https://bitcoin.org/bitcoin.pdf.

Noether, Sarang, and Brandon Goodell. 2017. *An Efficient Implementation of Monero Subaddresses*. Research bulletin MRL-0006, Monero Research Lab, October 3. https://web.getmonero.org/it/resources/research-lab/pubs/MRL-0006.pdf.

Nozick, Robert. 1974. *Anarchy, State, and Utopia*. New York: Basic Books.

Popper, Karl R. (1945) 2011. *The Open Society and Its Enemies*. Reprint, London: Routledge.

Rallo, Juan Ramón. 2014. *Una revolución liberal para España*. Bilbao, Spain: Deusto.

———. 2019. *Liberalismo: Los 10 principios básicos del orden político liberal*. Bilbao, Spain: Deusto.

Rivest, Ronald L., Adi Shamir, and Yael Tauman. 2001. "How to Leak a Secret." In *Advances in Cryptology—ASIACRYPT 2001*, edited by Colin Boyd, 552–65. Berlin: Springer.

Rothbard, Murray N. 1998. *The Ethics of Liberty*. New York: New York University Press.

———. (1995) 2006. *An Austrian Perspective on the History of Economic Thought*. 2 vols. Reprint, Auburn, Ala.: Ludwig von Mises Institute.

Saberhagen, Nicolas van. 2013. *CryptoNote v 2.0*. Cryptonote.org. https://cryptonote.org/whitepaper.pdf.

Saltman, Roy G. 2006. *The History and Politics of Voting Technology: In Quest of Integrity and Public Confidence*. London: Palgrave Macmillan.

Sandel, Michael. 1984. *Liberalism and Its Critics*. New York: New York University Press.

Schaffer, Frederic Charles. 2008. *The Hidden Costs of Clean Election Reform*. Ithaca, N.Y.: Cornell University Press.

Swan, Melanie. 2015. *Blockchain: Blueprint for a New Economy*. Sebastopol, Calif.: O'Reilly.

Szabo, Nick. 1995. "Smart Contracts Glossary." Satoshi Nakamoto Institute. 1995. https://nakamotoinstitute.org/smart-contracts-glossary.

———. 2005. "Bit Gold." Satoshi Nakamoto Institute. Dec. 29, 2005. https://nakamotoinstitute.org/bit-gold.