CIVP: Cryptocurrency Internal Validation Process

Abstract

Cryptocurrency Internal Validation Process" or "CIVP" which uses internal-based features to achieve much faster, and orders of magnitudes less energy for transaction validations . This was accomplished through two primary means. First, the proposed CIVP process identifies the crypto dollars with individualized specific serial numbers and tracks just the initial issuance of each specific CIVPdollar by date and time. Second, the CIVP process relies upon mathematical algorithms embedded within each serial numbered crypto dollar to provide both an automatic validation of any proposed transaction and to prevent any counterfeiting, double spending, or the use of stolen cryptocurrency. The validation nodes themselves require little storage, processing time, or electric energy to validate or to keep track of the limited data necessary to support large numbers of CIVP-based transactions. Finally, the proposed CIVP process should have a validation process time orders of magnitude faster than the current cryptocurrencies, making the use of CIVP based crypto dollars much more scalable.

Keywords: blockchain, CIVP, internal, crypto

CIVP: Cryptocurrency Internal Validation Process

INTRODUCTION

As commerce and financial reliance on the internet continues to grow there has been a proliferation of cryptocurrencies introduced into the cyber market. By and large these cryptocurrencies, particularly those most traded at the current time, employ blockchain technology as a means to provide a peer-to-peer distributed ledger system to track and validate transactions or blocks (Geissler et al., 2019). The validation process, such as Proof of Work or Proof of Stake, is employed to both record transactions and to ensure against over-spending (Duong et al., 2018). This validation process generally relies upon a network of cryptocurrency peers who are usually paid a cryptocurrency validation fee.

Some of the major claimed benefits of cryptocurrency is that it (1) promotes transactions without an intermediary validation entity, like a bank, (2) lowers peer-to-peer transaction costs, (3) can provide autonomy between participants, and (4) it can make international monetary transactions less complicated and cumbersome as compared to wiring money overseas. Notwithstanding these claimed benefits, the validation process used in current cryptocurrencies is slow (Mukhopadhyay et al., 2016) as compared to what consumers experience with other payment mechanisms such as credit cards or bank cards. It requires large amounts of electricity (particularly proof-of-work, not so much proof of stake) to support the mining process (Li et al., 2019).

Consequently, what is needed for a cryptocurrency to be functionally equivalent to current fiat money or credit card type transactions is scalability which is defined as the ability of cryptocurrency to handle a large number of transactions at one time. This will require a much faster transaction validation process and preferably a much more energy efficient validation process. What is proposed herein is just such a blockchain-type distributed ledger

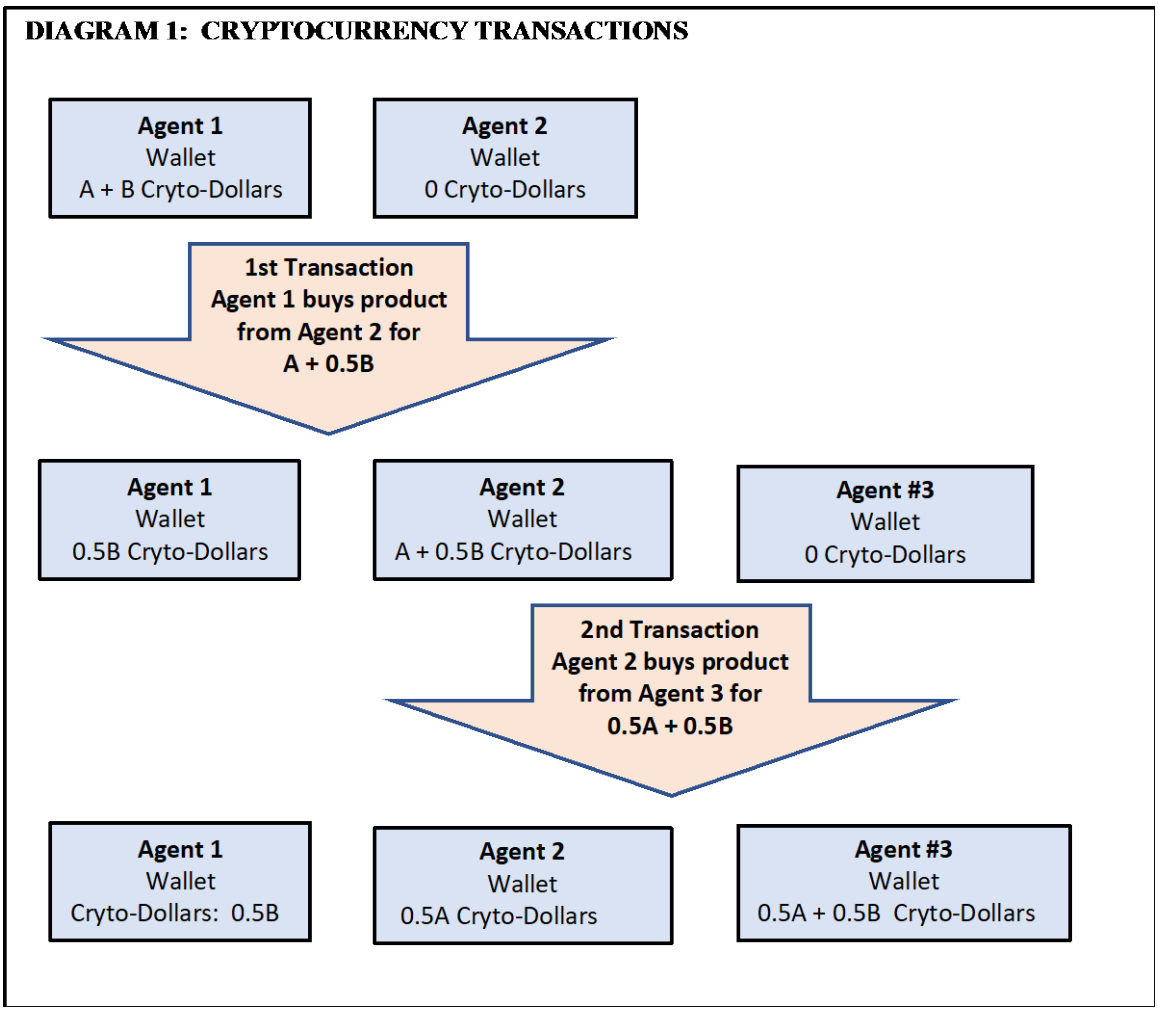
cryptocurrency validation procedure called the **"Cryptocurrency Internal Validation Process" or "CIVP."**

TRANSACTIONS

To understand the CIVP process it is first necessary to understand the basic cryptocurrency transactions and related tracking process. Heretofore, most if not all cryptocurrencies have relied upon a verification and tracking process that follows and records every transaction (date, amount, and other relevant data) of each particular cryptocurrency. Such a system requires large amounts of data storage and search capabilities which to date have been slow to verify and complete a transaction (as compared to Visa type bankcard systems). The proposed CIVP process operates from a different perspective in that it basically relies upon specific serial numbered cryptocurrency with "embedded" mathematical algorithms and logic statements. The serial numbers, along with a very limited amount of initial currency issuance data, is recorded in what will be a very small and easily searched time differentiated blockchain that, along with the embedded automatically functioning mathematical algorithms is the only information necessary to validate (or mine) a transaction. Tracking of the CIVP transactions only rely upon the initial serial number delineated issuance data, as opposed to following and storing all transactions. The serialized cryptocurrency uses embedded, unchangeable and un-hackable mathematical algorithms for validation of all future transactions which results in a cryptocurrency whose transactions' validation saves time, energy, data storage requirements, and ultimately money.

Diagram 1 below provides a simplified basic idea of the transactions that take place in any monetary system including cryptocurrency transactions. As Diagram1 illustrates, Agent 1 has some cryptocurrency and seeks to purchase something from Agent 2. Note that this transaction can be purchasing goods, services, or exchanging the cryptocurrency for other currencies (like US dollars). Assume that Agent 1 possesses two $1 cryptocurrency bills, and we can label them as A and B and that Agent 1 purchases an item from Agent 2 for a cost

of $A plus $0.5B. This leaves Agent 1 with $0.5B in cryptocurrency and Agent 2 with $A plus $0.5B cryptocurrency. Similarly, when Agent 2 makes a purchase from Agent 3 it changes the cryptocurrency dollars in both Agent 2's and Agent 3's wallets. The CIVP process, with a modification of the standard cryptocurrency minting and tracking procedures, provides a straightforward procedure for tracking and verifying these types of cryptocurrency transactions.



CIVP KEY FEATURES

CIVP Basic Process Requirements

The key to CIVP's increased scalability (transaction speed) and minimal energy usage is related to several key features contained in the CIVP's unique crypto currency creation. These key features are:

- CIVP crypto dollars (henceforth "CIVPdollars") are individually identified by a special, dated serial number.
- CIVP transactions have embedded what is called a "Transaction Key" which contain a set of mathematical algorithms embedded within each specific CIVPdollar to (1)validate the CIVPdollar has not been stolen or counterfeited, (2) prevent hacking, (3) prevent double spending, and (4) to validate transactions can occur (for example, does the purchaser actually own and have sufficient CIVPdollars to complete the purchase).
- The CIVP process uses cryptographic hashing and a tracking of hash numbers to ensure the embedded mathematical algorithms are not changed.
- A CIVP compliant cryptocurrency wallet that has the functionality necessary to provide access to and store the CIVPdollar electronic signature (includes serial number, transaction key, and other data shown in Diagram 2). A CIVP mini-wallet may also be used for transaction purposes which is a wallet created by the Buyer's CIVP wallet specifically for the proposed transaction. In a transaction, the information contained in this mini-wallet is observable and/or provided to the Seller.[1] Note that this mini-wallet is not required but such a device could make the CIVP process more efficient.

[1] To verify that the information in this wallet is correct, attached to the proposed transaction, and has not been stolen or compromised by a bad actor, the information in this mini-wallet may be hashed along with the Buyers Transaction Password and Buyer's public account number and then displayed in the mini-wallet as the mini-wallet Verification Hash Number. This mini-wallet Verification Hash Number will also be communicated from the Buyer to the Seller in a separate communication which is protected using the Public Key/Private Key format. If somehow the mini-wallet data is compromised, the mini-wallet Verification Hash Number, which references the original Buyer's Transaction Password, will change and not match the separately communicated mini-wallet Verification Hash Number. In this way the Buyer and Seller can have confidence that the information being provided in the mini-wallet has not been compromised so long as the mini-wallet Verification Hash Number has not changed.

- The CIVP blockchain transaction validation and tracking system only needs to keep the original initial record of the serial number of each CIVPdollar issued and some related data shown in Diagram 3. After the initial issuance of a specific CIVPdollar no other tracking of that serial number or any related transactions is necessary. Simply put, the CIVP blockchain blocks do not have to track transactions or keep any record of historical transactions for transaction validation purposes beyond the information contained in the initial issuance block for each specific serial number identified CIVPdollar.
- The CIVPdollar owner and any entity that accepts the CIVPdollars must each establish CIVP cryptocurrency functionality with the CIVPdollar issuer in order to make use of the CIVP validation process, which could be as simple as opening a CIVP user account (this account could theoretically require no monetary commitment but simply allow access to CIVP transaction functions). This CIVP functionality is necessary because the CIVP validation process has some two-way communication procedures used for transaction validation purposes so both parties must have CIVP process functionality.
- A CIVP transaction requires communication security and some way to ensure the identity of party's to a transaction. To achieve this goal the CIVP process uses the Public Key/Private Key encryption methodology.
- The buyer and seller in a CIVP transaction process must have and keep private what is termed a Transaction Password which is used in the CIVP validation procedures described in Section 4.0.

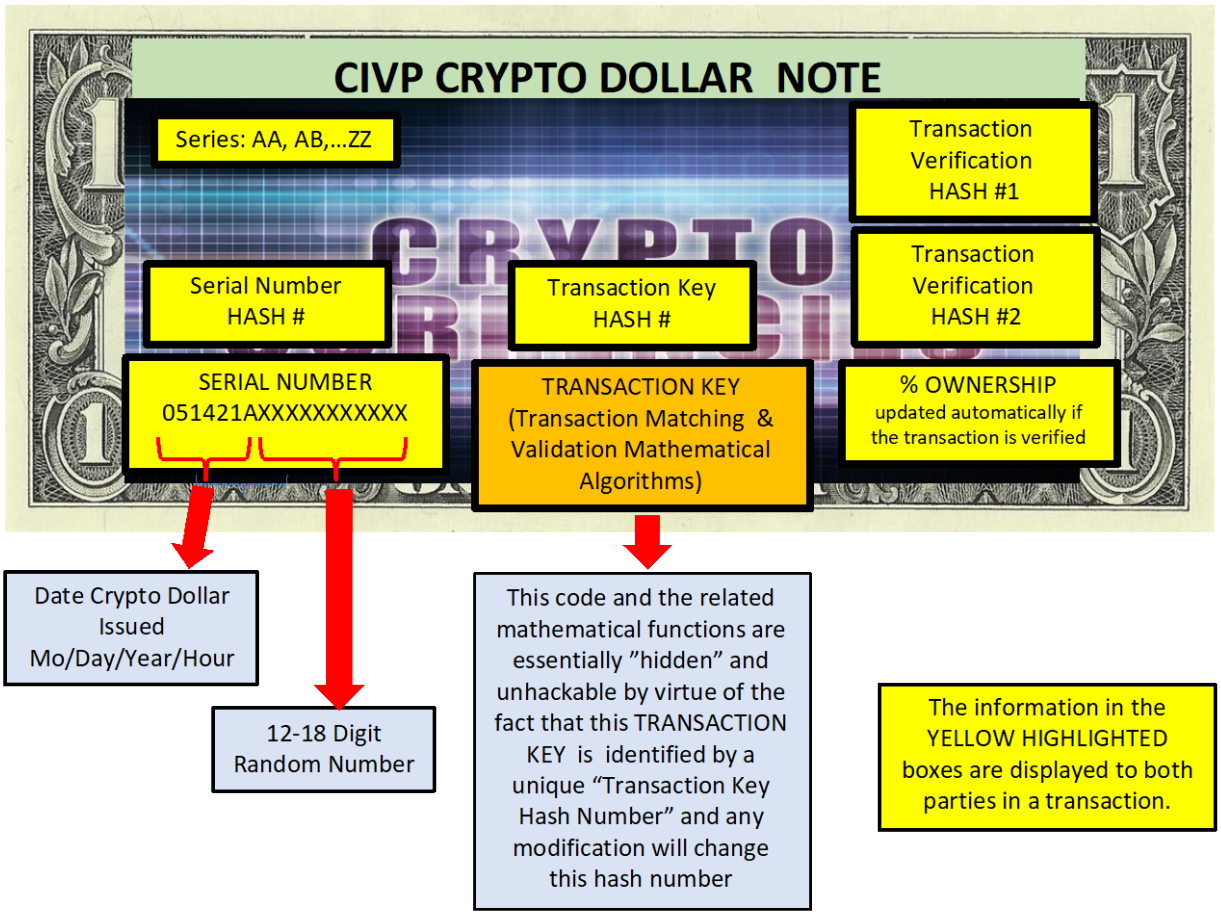
The CIVPdollar's Identification, Ownership and Transaction Validation Numbers

The CIVPdollar 's role in a transaction's validation process requires several identification numbers and some embedded mathematical formulas that follow every specific CIVPdollar serial number. These various identification numbers and formulas can best be explained by

visualizing a CIVPdollar (similar to looking at a US $1 bill in your wallet) which is shown in Diagram 2. These identifying factors, shown in Diagram 2, are "kept" in the CIVPdollar owner's wallet in a data file for each specific serial numbered CIVPdollar or percentage of that dollar. The identifying numbers highlighted in yellow on Diagram 2 are essentially shared with all parties to a particular transaction and used to validate that transaction (discussed in Section 4.0). The CIVP blockchain validation process system also relies upon a Public Key/Private Key encryption of all communications to ensure the parties are communicating with the expected transaction participants, otherwise the transaction information could not be seen.

Each of the CIVPdollar's identification numbers that are displayed in Diagram 2 are explained below.

DIAGRAM 2: A VISUAL DEPICTION OF A CIVP CRYPTO DOLLAR



- ***SERIAL NUMBER***
  Each individual CIVPdollar" issued[2] will be identified by a specific serial number which is displayed in the crypto wallet. The way a particular serial number is established is shown in shown in Table 1, and includes:

  - Timing related identifiers by date and the hour and minute issued (use a 24 hour clock from the Coordinated Universal Time UTC as found at: www.time.gov.
  - A multi digit random number (the length is determined by the security level one seeks).

[2] The issuance of the CIVPdollars could be from several sources such as someone purchasing a CIVPdollar or by a company using the CIVP process to distribute their CIVPdollars by awarding fees for services.

When a CIVPdollar is issued its serial number will be recorded in a block referred to as a "genesis" block for that serial number. Each genesis block will contain the serial number for every CIVPdollar issued over a particular time period, for example for one day. This blockchain tracking system is illustrated in Diagram 3. Once 100% of a serial number has been issued that information will be conveyed to and reflected in the genesis block, and any more information or tracking or data collection related to that serial number will not be necessary. Note that while one block must contain all of the information about a specific serial number, a block may actually contain several specific serial numbers and their related information.

It is possible that an entity could purchase a percentage of a CIVPdollar, therefore it is envisioned that once a CIVPdollar is "minted," that dollar will be issued to the next and the next and the next customer until that CIVPdollar is 100% issued. Note that in Diagram 3 it does allow for some small percentage of a "minted" CIVPdollar to be held back by the minting company to be used for fees or issued later. The reason for this feature is that there may be a need for CIVPdollars to be applied towards validation (mining) fees in which case the actual ownership of that portion of the minted dollar may be reserved for a future day or future block in the blockchain in which case some additional but rudimentary tracking for that small percentage may be required.[3]

[3] For example, assume in the genesis block on a particular date that 98.7896% of a particular serial number CIVPdollar has been issued and fees for validation services are yet to be paid. Assume those fees are paid three days later, in which case the genesis block may have been "closed out." In such a situation, to align the serial number of the paid fees with the date that serial number was initially established could be accomplished in two ways. One, the CIVPdollar issuer may simply take ownership of that small percentage and keep in a "company" wallet in which case the CIVP tracking process would be the same as with any CIVP dollar owner. A second option is to wait and as that specific serial number is fully subscribed simply add block "branches" to the genesis block that relates all minting of that particular serial number to the appropriate genesis block date.

TABLE 1: CIVP Currency Serial Numbering System					
	Date of Issuance			Time the CIVPdollar was Issued	This will be a 12-18 digit random number
	Month	Day	Year	Use 24 clock, e.g. 1624 is 4:24 PM EST	
Serial Number	XX	xx	xx	xxxx	xxxxxxxxxxxxxx

DIAGRAM 3: EXAMPLE OF CVIP PROCESS "BLOCKS"

BLOCK 1

Block 1 Date Code: 051421

SERIAL NUMBER	SERIES	Owner A % NUMBER	Owner B % Ownership	Owner C % Ownership	% Reserved Ownership For Fees	Transaction Key Hash Number
• 051421-0232-034297436222	AA	74.3459	20.2334	4.066	1.3547	xxxxxxxxxx
• 051421-0232-034297324402	AA	100.0000	0	0	0	xxxxxxxxxx
• 051421-1323-225042385009	AA	100.0000	0	0	0	xxxxxxxxxx
• 051421-1424-485896010203	AA	32.3033	61.6967	6.0900	0	xxxxxxxxxx
• 051421-1639-593000382993	AB	100.0000	0	0	0	xxxxxxxxxx

BLOCK 2

Block 1 Date Code: 051422

SERIAL NUMBER	SERIES	Owner A % NUMBER	Owner B % Ownership	Owner C % Ownership	% Reserved Ownership For Fees	Transaction Key Hash Number
• 051422-0432-034297436222	AB	94.0059	1.3938	3.779	0.8213	xxxxxxxxxx
• 051422-0952-034297324402	AB	100.0000	0	0	0	xxxxxxxxxx
• 051422-1129-225042385009	AB	100.0000	0	0	0	xxxxxxxxxx
• 051422-1244-485896010203	AB	35.7763	61.2237	1.0143	1.9857	xxxxxxxxxx
• 051422-1609-593000382993	AC	100.0000	0	0	0	xxxxxxxxxx

Note each block has a date code. Validating if a specific crypto dollar has been issued, the date and time shown in the crypto dollar serial number can be easily tracked to an individual block date, and than a proposed transaction's serial numbers can be compared to the serial numbers in that block – this will be a very fast process

- ***SERIAL NUMBER HASH #[4]***

  This Serial Number Hash # is generated using the serial number and the percentage of ownership of that specific CIVPdollar the buyer has at the time that specific serial # was issued. This Serial Number Hash # will change when a transaction is completed because the owner of that serial number has "spent" some of those crypto dollars

[4] Hash numbers can be developed using any one of a number of procedures, but the hashing procedure, once adopted, must remain the same for all serial numbers in a specific series. The reason is based on the fact that there is a need for both the buyer and sellers to know what hashing procedure is used for each particular serial number.

and this change in the percentage ownership will result in automatically changing this Serial Number Hash Number. The use of this Serial Number Hash Number and the mechanism for automatically changing this number is discussed in Section 4.0.

- ***SERIES NUMBER***

  A series number is provided that begins with AA and is changed to AB, AC, AD, …. ZZ. The reason for this Series Number is that over time there could be updates to the Transaction Key or the hashing protocols. When this happens this Series Number will change. Therefore, if there is a need to track or "replace" older series number CIVPdollars or the related hashing procedures this identification mechanism can be used to effectuate such a desire.

- ***TRANSACTION KEY***

  This transaction key is a set of mathematical formulas that, for the most part, are universal with every CIVPdollar issued for each specific Series Number. The formula and other data contained in this Transaction Key (discussed in Section 4.0) are part of each CIVPdollar's electronic signature and these formulas and any other data in the Transaction Key is locked and not accessible once a serial number has been issued. To ensure the formulas and any other information in a Transaction Key have not been tampered with each CIVPdollar also has a Transaction Key Hash Number which never changes and this Transaction Key Hash Number can be checked to ensure information in the Transaction key has not been changed.

- ***TRANSACTION KEY HASH NUMBER***

  This Transaction Key Hash Number is attached to each CIVPdollar on issuance. This hash number is created by compressing the Transaction Key's embedded formulas along with the Serial Number. The Transaction Key is used to compute the percentage ownership and some other values shown in Diagram 2. It is also used for validation of transactions (explained in Section 4.0). In a transaction process, the recipient of any CIVPdollar must be able to confirm this Transaction Key Hash Number

has not been changed from its original value (displayed in each CIVPdollar's genesis block).

- ***TRANSACTION VERIFICATION HASH # 1 and # 2***

  These hash numbers are attached to each CIVPdollar on issuance. The Transaction Verification Hash# is developed using the serial number and the buyer's Transaction Password. The basic function of these hash numbers is if they are the same, the transaction's CIVPdollars have not been stolen, counterfeited, or being double spent. This will be explained more fully in Section 4.0.

  These Transaction Verification Hash #s are created as follows:

  - Transaction Verification Hash #1 - Calculated internally by a mathematical formula in the Transaction key using a hash function that compresses the Serial Number and the CIVPdollar owner's Transaction Password.[5] This hash number is calculated on the initial issuance (or in a future transaction to a new owner of that CIVPdollar) of the serial numbered CIVPdollar. This Transaction Validation #1 will not change or have to be updated unless the CIVPdollar owner has changed or the owner has updated his Transaction Password - which should be infrequent and only be accepted with appropriate security procedures.
  - Transaction Verification Hash #2 - Calculated using a hash function that compresses the Serial Number and the CIVPdollar owner's Transaction Password. This hash number is calculated for every *proposed* transaction and requires that the buyer manually input their Transaction Password when a transaction (like spending) is undertaken. Note that if a bad actor has somehow stolen or tried to duplicate and then use this specific CIVPdollar,

[5] The Transaction Password is a password that the CIVP client establishes when they open their CIVP account and can be changed as necessary. It is recommended that it be different from the client's account password and different from their Private Key and that it be protected from display as much so as a client's Private Key and only be used in a proposed transaction.

that bad actor will have to enter a Transaction Password which, unless somehow the bad actor knows the original password, will result in this Transaction Verification Hash #2 not being equal to Transaction Verification Hash #1 and the proposed transaction will not be allowed.

- ***% OWNERSHIP***

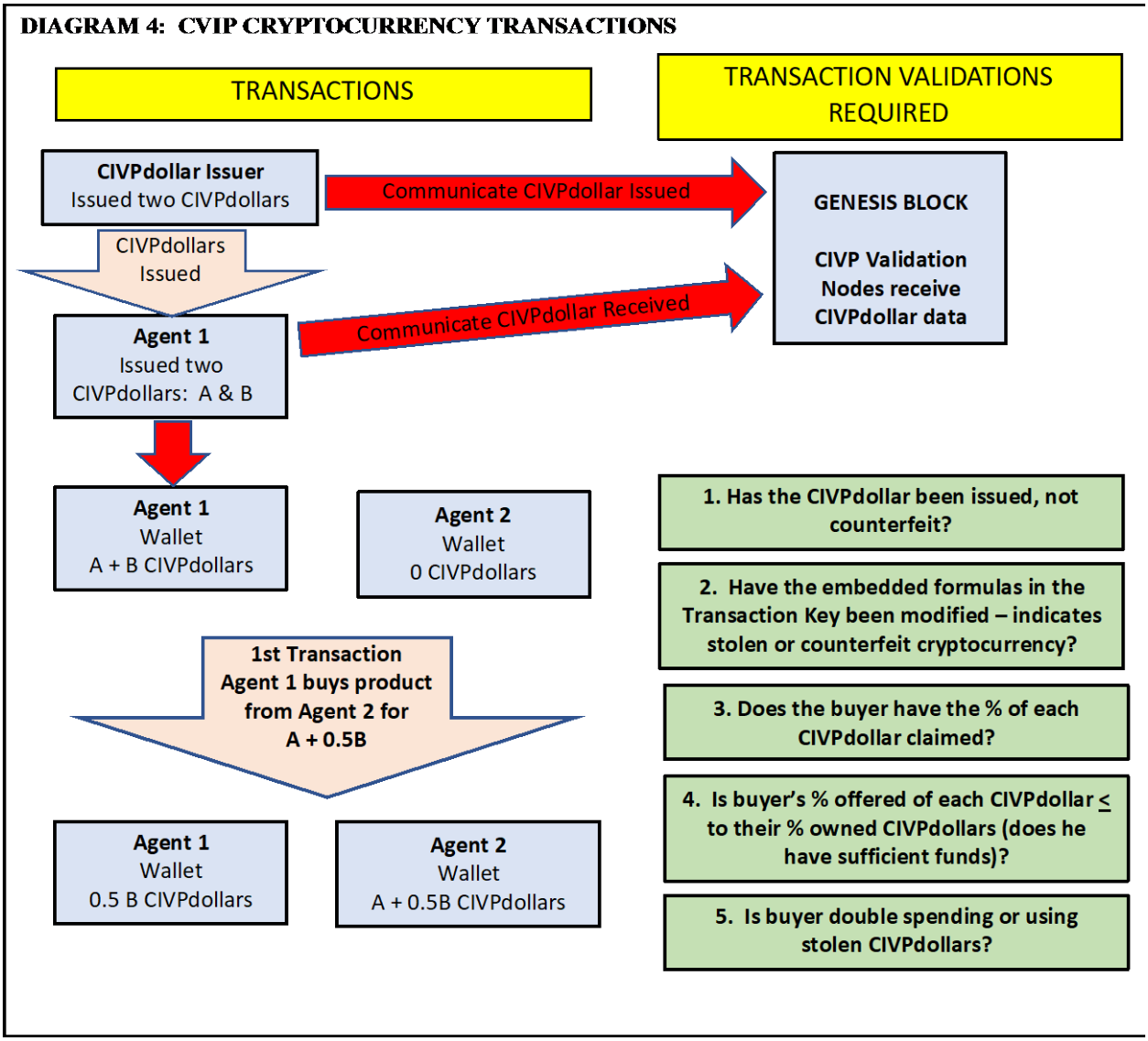
  This simply displays the percentage of a specific serial number CIVPdollar a person owns at that specific time. At the initial issuance of the CIVPdollar, this value is established and essentially "displayed" on the CIVPdollar. This percentage will change when a purchase is made and can only be changed by the formulas in the Transaction Key. If these Transaction Key formulas are tampered with the Transaction Key Hash Number will no longer be "correct" and this is easily verified by referring to a CIVPdollar's genesis block in the blockchain.

THE CIVP TRANSACTION, VALIDATION, AND TRACKING PROCEDURE

The most important aspect of the CIVP process is that the validation of transactions is largely automatic from formulas embedded in each CIVPdollar's Transaction Key. This process is further described below

The Basic CIVPdollar Transaction That Requires Validation (or mining)

Diagram 4 illustrates a basic cryptocurrency transaction where a buyer (Agent 1) is purchasing a product from a seller (Agent 2). This transaction could also reflect the sale of cryptocurrency through a cryptocurrency exchange site.



As Diagram 4 illustrates there are five essential validation requirements in the cryptocurrency transaction, and these are:

1. Is the CIVP cryptocurrency counterfeit?
2. Have the embedded formulas or other information in the Transaction Key been modified or tampered with?
3. Does the buyer have the % of CIVPdollars he claims?

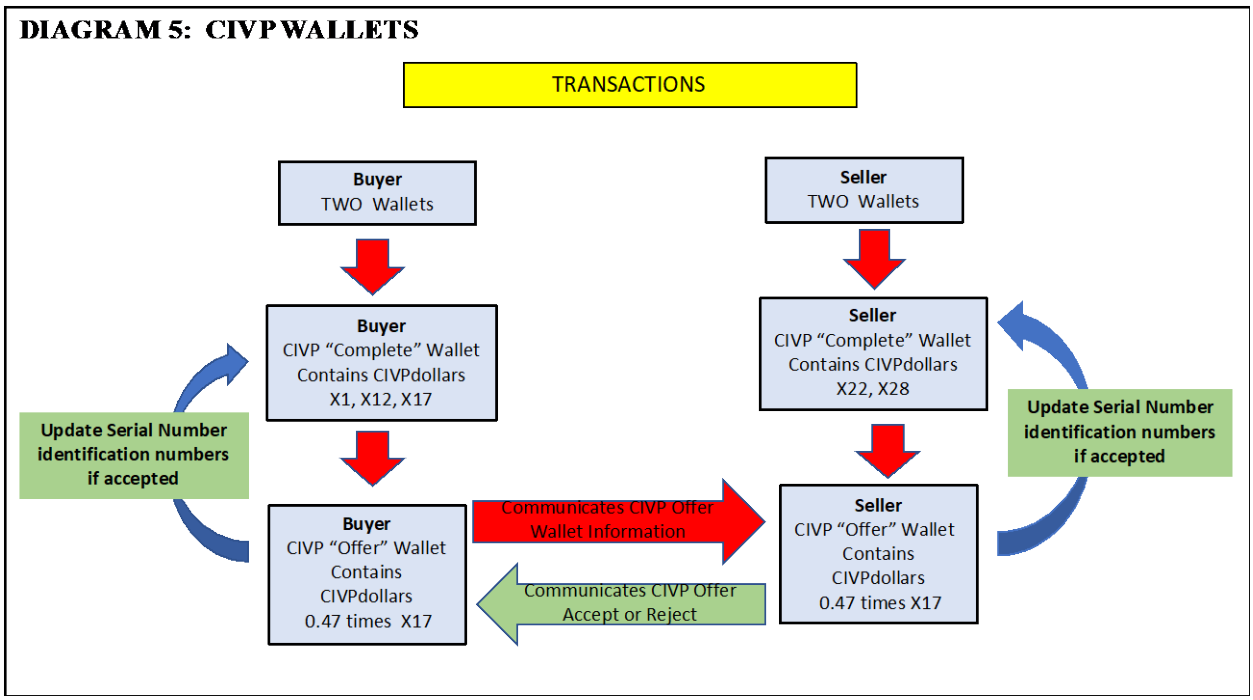
4. Has the buyer offered the seller "enough" cryptocurrency? In a normal monetary transaction using for example, US dollars, this is an easy verification because the buyer simply offers the seller sufficient cash to cover the proposed transaction's cost. With cryptocurrency this issue is more complicated because the seller must somehow confirm the buyer has actually offered a sufficient amount of the cryptocurrency.
5. Is the buyer double spending or has the cryptocurrency been stolen (said another way, confirm that the cryptocurrency actually belongs to the proposed buyer)?

In the CIVP process, the validation of these five criteria is sufficient to validate that a proposed transaction can proceed - and if it does proceed, in the CIVP process several of the serial number related identification numbers shown in Diagram 2 will be automatically updated to reflect what occurred in the transaction.

Finally, there are several ways an offer to purchase can be made and the related identification numbers provided to the seller - however, an automated process would be best. Therefore, the CIVP process recommends that CIVP compatible wallets be developed and any proposed transaction follow the process shown in Diagram 5. As Diagram 5 indicates, each buyer has a "complete-wallet" that contains information (shown on Diagram 2) for every one of his CIVPdollars. The buyer also has what is called an "offer-wallet" (or mini-wallet as referenced earlier) which only contains the information on the serial numbered CIVPdollars being offered in the transaction, plus the percentage of each dollar being offered in the transaction. Similarly, the seller has both a complete-wallet and an offer-wallet.

A CIVP complete wallet has the capability to take a proposed transaction and calculate the best combination of CIVPdollars, by serial number and percentage offered, necessary to complete a transaction. The CIVP complete-wallet, when given instructions to do so, will place this information in the buyer's offer-wallet. That offer-wallet and the identification

numbers shown on Diagram 2 along with the percentage of each serial number being offered will be shared with the prospective seller and essentially copied into the seller's offer-wallet. When instructed to proceed with validation, the information in the seller's offer-wallet will be triggered and a series of transaction validation procedures will begin (the mathematical formulas contained in the Transaction Key).



The Automated Transaction Verification and Updating Formulas In the Transaction Key

In a CIVP wallet (accessed by a private, secure passcode) there are essentially two types of transactions, "spending" and "receiving." When a buyer proposes a specific transaction, that proposed transaction is placed in the buyer's Offer-Wallet and communicated to the seller's Offer-Wallet. Next, a transaction verification signal from the seller to their Offer-Wallet will initiate a series of mathematical analysis contained in the Transaction Key. This analysis will either validate or reject the proposed transaction. If a transaction is validated, then other formulas contained in the transaction key will update the specific serial number

identification numbers (Diagram 2) as necessary in both the buyer's and the seller's Complete-Wallets.

The basic buyer/seller transaction process is shown stepwise in Table 2. As this table indicates the basic transaction has 11 distinct steps from the original communication of an offer to purchase to the validation of the purchase and subsequently to the updating of the data associated with each CIVPdollar serial number. Both the validation of the purchase and the updating of the serial number data use formulas embedded in each CIVPdollar's Transaction Key.

TABLE 2: CIVP TRANSACTION AND VALIDATION PROCESS (assume two parties involved, a "Buyer" offering to purchase a product for $X CIVPdollars and a "Seller" who accepts CIVPdollars)				
Step	**Communication Flow**	**Communication Purpose**	**Information Provided or Obtained**	**Security/Validation Protocol**
STEP 1	Buyer → Seller	Purchase Offer Initiated	A. Buyer offers Seller $XX CIVPdollars to purchase Product Y	Public Key/Private Key** - ensures the correct buyer made the offer
STEP 2	Buyer Offer-Wallet→ Seller Offer-Wallet	Purchase Offer Details Communicated to Seller (accomplished by allowing access to the Buyer's CIVP wallet or to a CIVP "mini-wallet*")	A. Information from CIVPdollar (see Diagram 2) • Serial number, % ownership, Serial # Hash Number, Transaction Key Hash #, Transaction Verification Hash #s 1 & 2 B. % of Serial Number offered in transaction	Public Key/Private Key **
STEP 3	Seller→ Buyer	Has Buyer offered "enough" cryptocurrency?	% of Serial Number offered in transaction - provided in the communication noted above	Public Key/Private Key** - this can be automatically calculated in Seller's Offer-Wallet
STEP 4	Block*→ Seller Offer-Wallet	Has serial number been issued - is serial # counterfeit?	Serial number from Genesis Block	Check if the buyer's cryptocurrency serial number has been issued and is recorded in the block chain - ***TRANSACTION KEY FORMULA S1***
STEP 5	Block*→ Seller Offer-Wallet	Has Transaction Key been modified?	Transaction Key Hash# calculated from Buyer's wallet & Transaction Key Hash # in the genesis block.	If the Transaction Key Hash # in buyer's wallet = Transaction Key Hash # in block chain the Transaction Key formulas have not been modified - ***TRANSACTION KEY FORMULA S2***
STEP 6	Block*→ Seller Offer-Wallet	Does Buyer have the % of Serial #X that buyer claims?	Serial #, % ownership, Serial # hash #	Seller HASHES the % ownership plus the serial number, compares to Buyer's reported Serial # Hash #, if these are the same the % ownership claimed by Buyer is correct - ***TRANSACTION KEY FORMULA S3***
STEP 7	Block*→ Seller Offer-Wallet	Does Buyer have sufficient funds?	Serial #, % ownership owned, % ownership offered	Check that the % offered by buyer is $\leq$ to the % owned by buyer - ***TRANSACTION KEY FORMULA S4***

STEP 8	Buyer → Seller	Has Serial # been double spent or stolen?	From wallet - Transaction Verification Hash #1 and Transaction Verification Hash #2	If Transaction Verification Hash # 1 = Transaction Verification Hash #2 cryptocurrency not likely been stolen or double spent - ***TRANSACTION KEY FORMULA S5***
STEP 9	Seller→ Buyer	Seller has validated and accepted the offer	Seller communicated to Buyer the purchase has been accepted	Public Key/Private Key** - Ensures the correct seller accepted the offer - ***TRANSACTION KEY FORMULA S6***
STEP 10	Buyer→ Seller	Buyer validates desire to make purchase	Buyer communicates to Seller the purchase has been accepted	***TRANSACTION KEY FORMULA B1***
STEP 11	Automatic if buyer & seller validates the purchase	Update all CIVPdollar data attached to the serial number(s)	Transaction Key automatically updates the data displayed on the Buyer's and Seller's specific serial number CIVPdollars - ***TRANSACTION KEY FORMULA S7, S8, S9, B2, B3***	

* Blocks and the information in each block are made public once validated.

** Public Key/Private Key cryptography format to ensure communication came from the intended parties.

The transaction process begins with basic communications between the prospective Buyer and Seller, Steps 1 and 2 in Table 1 whereby the Buyer indicates the desire to make a purchase and conveys the purchase offer to the Seller. In Step 3, the Seller communicates back to the Buyer whether the offer is "enough" and if so, once the transaction is validated the offer can be accepted.

At this point in time the Seller will "trigger" the CIVP automatic validation procedures which initiates a series of formulas contained in the Transaction Key - labeled as Steps 4 through 11 in Table 1. These formulas and what each one does is shown below.

Seller's Transaction Key Formulas

1. *Formula S1 - Has the Serial Number Been Issued (Table 1, Step 4)?*

   This is an IF/THEN statement and when triggered, automatically compares the offered serial number in the Offer-Wallet to the serial numbers listed in the block chain - the time stamp on the serial number enhances the speed of such an inquiry. IF the serial number has been issued, THEN the transaction assumes the serial number has been issued and has not been counterfeited and transaction can proceed, otherwise the transaction is terminated.

2. *Formula S2 - Have the Transaction Key Formulas Been Changed (Table 1, Step 5)?*

   This formula is an IF/THEN statement that does two things. First, it calculates a Transaction Key Hash # compressing the Transaction Key information along with the Serial number and using the same hashing procedure that was used to produce the

Transaction Key Hash # shown in the genesis block.[6] Next it compares this calculated Transaction Key Hash # to the Transaction Key Hash # for that serial number and found in the Genesis Block. IF these two has #s are equal, THEN the Transaction Key has not been modified and the transaction validation can proceed to the next step - otherwise, the transaction is canceled.

Why this Transaction Key Hash # is important is because this hash number should never change. Theoretically, a party could try and hack the embedded Transaction Key formulas but to do so would change the Transaction Key Hash #. A second potential hack would be for a bad actor to try and manually enter the Transaction Key Hash #. To ensure a party cannot manually make such a change this information is linked to a formula in the Transaction Key, therefore even if one could change this manually the Transaction Key hash key formula would simply change it back.

3. *Formula S3 -Does the Buyer Own the Claimed Percentage of Each Specific CIVPdollar Serial Number (Table 1, Step 6)?*

   This formula is an IF/THEN statement that checks the % ownership by taking the serial number and the % ownership of each serial number to develop a calculated Serial Number Hash# using the same hashing procedure that was used to produce the Serial Number Hash # shown in the Buyer's "offer wallet."[7] Next IF this calculated Serial Hash # is equal to the Serial Hash # in the Offer-Wallet, THEN the buyer does have the percentage of ownership claimed in the Offer-Wallet and the transaction

[6] This is accomplished by referencing the Series Number of each serial number and using the corresponding hash calculation algorithm.
[7] This is accomplished by referencing the Series Number of each serial number and using the corresponding hash calculation algorithm.

can proceed to the next step, otherwise the transaction is cancelled. Note that the % ownership is updated automatically by formulas in the Transaction Key (S7, B2) in both the Seller's and Buyer's wallets every time the Buyer "spends" some of a specific serial number's currency. This percentage ownership cannot be "tampered with" without also changing the Serial Number Hash #, which if tried, would invalidate the transaction.

4. *Formula S4 - Does the Buyer Own A Sufficient Percentage of Each Specific CIVP Serial Number To Complete the Transaction (Table 1, Step 7)?*

   This formula is an IF/THEN statement that checks the percentage owned in the Offer-Wallet to the percentage being offered in the transaction. Once Formula S3 has been validated, if the percentage offered for a specific serial number (this is displayed in the Offer-Wallet) is less than or equal to the percentage owned (this is displayed in the Offer-Wallet) and updated as the buyer "spends" each serial number CIVPdollar), the buyer has offered a sufficient percentage of that CIVPdollar, THEN the transaction can proceed, if not, the transaction is cancelled. This also helps to prevent double or over-spending. Also transactions are time differentiated, with the "first spent" transactions going first. This fact, coupled with the transaction validation and update procedure being largely automatic and very fast, also helps prevent double spending.

5. *Formula S5 - Has the CIVPdollar Serial Number Been Stolen or Double Spent (Table 1, Step 8)?*

   This is an IF/THEN statement based on information provided in the Buyer's Offer Wallet (see Formula B1). In the offer wallet there is the Transaction Verification Hash #1 (compressing the serial number and the Transaction Password the first time the Buyer

owns some portion of a specific serial number CIVPdollar) displayed in the Buyer's Offer Wallet. When the Buyer makes an offer to the Seller, a second formula calculates a Transaction Verification Hash #2 which requires the Buyer to input a Transaction Password for the proposed transaction (this is similar to entering a PIN code when using a bank card).

The IF/THEN statement that checks to determine IF the Transaction Verification Hash #1 is equal to the recently calculated Transaction Verification Hash #2.[8] IF these two values are the same it is assumed that the correct owner of the CIVPdollars being offered actually made the offer, THEN the transaction can proceed. Otherwise, the transaction is cancelled.

This check helps prevent a bad actor from stealing and using the CIVPdollars and attempting a purchase with those dollars as the purchase is prevented unless the bad actor somehow knows and can enter into the proposed purchase the true owners Transaction Password. For all intents and purposes this is the "blue ink" bomb placed in a would-be bank robbers money bag that explodes and renders the stolen currency useless. Another security used to prevent this type of counterfeit occurrence is the fact that the Public Key/Private Key communication format helps ensure the parties to a transaction are the true and only participants.

6. *Formula S6- The Transaction Key Communicates to the Buyer That the Transaction Can Proceed (Table 1, Step 9)?*

[8] Note that if a bad actor has somehow stolen or tried to duplicate and then use this specific CIVPdollar, it is likely that bad actor will enter an incorrect Transaction Password which will result in this Transaction Verification Hash #2 not being equal to Transaction Verification Hash #1 and the transaction will be invalidated.

This is an IF/THEN statement that communicates to the Buyer that IF all the preceding formulas are positively satisfied, THEN this transaction can proceed. IF not, this formula communicates to the Buyer and Seller that the transaction as proposed cannot go forward and provides information related to why the transaction failed.

7. *Formula S7 - Update the Percentage Ownership (Table 1, Step 11).*

This formula is an IF/THEN statement and only activated IF instructed to do so by the seller. It is assumed that if the transaction has been validated and this validation communicated to the Buyer, the Buyer will respond (*Formula B2*) to proceed with the transaction and the Seller will so designate to the Transaction Key. Once the transaction has been confirmed by both parties, this formula automatically updates and records the percentage of ownership of a particular serial number CIVPdollar in the Seller's Complete-Wallet. Obviously, if the transaction is not completed for any reason the percentage of ownership value is not updated.

It should be noted that this automatic update to the percentage ownership follows the serial number for every transaction - and it does so for both the Seller (in this *Formula S7*) and the Buyer (in the *Formula B3* below). It is this feature that by and large eliminates the need to track transactions.[9]

8. *Formula S8 - Update the Serial Number Hash # (Table 1, Step 11).*

This formula is an IF/THEN statement that states IF the transaction has been completed, THEN this formula updates the serial number hash # in the Seller's Complete-Wallet using the serial number and the new percentage ownership.

[9] From an account reporting standpoint, this means that the individual Buyers and Sellers are responsible for keeping whatever accounting books and records are required by their respective regulatory authorities.

9. *Formula S9 - Update the Seller's Transaction Verification Hash # (Table 1, Step 11).*

This formula is an IF/THEN statement that states IF the transaction has been completed, the Seller must calculate (automatically in the Transaction Key) for this specific serial number CIVP dollar their own Transaction Verification Hash #1 so that the Seller can use any percentage of that CIVPdollar in a future transaction.

Buyer's Transaction Key Formulas

1. *Formula B1 - Update the Serial Number Hash # (Table 1, Step 1).*

This formula is actually two different formulas. The first formula calculates Transaction Verification Hash #1 (compressing the serial number and the Transaction Password) the first time the Buyer owns some portion of a specific serial number CIVPdollar and this Transaction Verification Hash #1 is displayed in the buyer's Offer Wallet does not change until a percentage of ownership changes.

A second formula calculates a Transaction Verification Hash #2 which requires the Buyer to input a Transaction Password for every proposed transaction (this is similar to entering a PIN code when using a bank card). This second Transaction Verification Hash# is also displayed in the Buyers Offer Wallet.

2. *Formula B2- Communicate Whether the Transaction Can Proceed (Table 1, Step 10).*

After the Seller has communicated to the Buyer that the transaction has been validated, the Buyer must confirm that they wish to go ahead with the transaction. This is an IF/THEN statement that communicates to the Seller that IF the Buyer has confirmed that they want to complete the transaction THEN this transaction can

proceed. IF not, this formula communicates to the Seller that the transaction as proposed cannot go forward.

3. *Formula B3 - Update the Percentage Ownership (Table 1, Step 11).*

   This formula is an IF/THEN statement and only activated IF in Step 2 above that the Buyer has responded to proceed with the transaction. Once the transaction has been confirmed by both parties, THEN this formula automatically updates and (1) records the new percentage of ownership of a particular serial number CIVPdollar in the Buyer's Complete-Wallet and (2) cancels out all of the information in the Buyer's Offer-Wallet. Obviously, if the transaction is not completed for any reason the percentage of ownership value is not updated.

4. *Formula B4 - Update the Serial Number Hash # (Table 1, Step 11).*

   This formula uses and IF/THEN statement to create the serial number hash number using the serial number and the updated percentage ownership of the Buyer. IF a transaction is completed THEN the Serial Number Hash # will be recalculated and this information will be conveyed to the Buyer's Complete-Wallet (this is also conveyed to the blockchain validation nodes on initial issuance).

5. *Formula B5 - Update the Buyer's Transaction Verification Hash #1 (Table 1, Step 11).*

   This formula is an IF/THEN statement that states IF the transaction has been completed, the Buyer must recalculate (in the Transaction Key) for this specific serial number CIVP dollar a new Transaction Verification Hash #1 so that the Buyer can use any remaining percentage of that CIVPdollar in a future transaction.

It should be apparent that each of the Transaction Key embedded formulas can be computed, and subsequent transactions validated, very quickly - in fact, it is expected that the transaction validation process will be as fast as current credit card validations. Moreover, like current bank or credit card transactions the parties to the transaction will have much the same transaction validation requirements, e.g. the Buyer must (1) make an offer, (2) put in a Transaction Password, and (3) confirm that the Buyer wants to complete the transaction. Therefore, the CIVP process overcomes the scalability issue inherent in the cryptocurrency offerings to date.

Additional Discussion Regarding the CIVPdollar Security

There is always the potential for bad actors to try and compromise any electronic system thus it is appropriate to directly address CIVP's inherent security against some of the potentially more egregious forms of hacking or deceit that might be attempted.

- Stealing data from an entity's CIVP wallet - this might be possible but would require that the bad actor somehow knows the party being compromised wallet's password and their transaction password and any other security codes. To the extent parties use adequate caution to protect their wallets from such a security breach, this risk is no more prevalent for a CIVP system as it is with any cryptocurrency. In fact, it is likely that the CIVP spending validation procedures related to Transaction Verification Hash #s could actually diminish the possibility of this type of hack because it makes being able to actually "spend" any of the "stolen" cryptocurrency practically impossible (the bad actor would have to know the original owner's Transaction Password).
- Counterfeiting and/or duplication of serial numbers - This would be very unlikely because only the issuer of the CIVP currency can provide the required data to populate a genesis blocks. To the extent the issuer of the currency is verifiable, which can be protected a number of ways, it is unlikely that any bad actor would be able to originate counterfeit serial numbers that would be accepted by the validation nodes.

DISCUSSION REGARDING THE CIVP PROCESS VALIDATION NODES

A final consideration in the CIVP process is what type of blockchain validation nodes might be required. Based on the fact that there is limited data to be stored (only the original issuance serial number information) the number of validation nodes could be an unlimited number of participants or it could be restricted to a "trusted" few. Moreover, because the transaction validation mechanism is almost entirely automated, the time, energy, and computer requirements related to validation is miniscule as compared to cryptocurrencies using proof-of-work or even proof-of-stake type validation mechanisms. Based on these considerations it is likely that any CIVP-related cryptocurrency is likely to use some form of private or a limited number of validation nodes - it will simply be easier and faster.

Two final considerations related to CIVP's limited validation requirements are (1) what type of fees might be required to support the validating nodes and (2) how, if not through mining, might the CIVPdollars be issued. As to the first point, any validation fees will be left to the market participants to determine. As for the second question, there are several ways the CIVPdollars might get "issued." For example, the aforementioned validation fees could certainly be used to distribute a limited number of CIVPdollars. Other potential "issuance" mechanisms might be to offer the CIVPdollars through an auction or as a straight purchase option.

CONCLUSION

Proposed herein is an electronic transactions process, called the "Cryptocurrency Internal Validation Process" or "CIVP." The process and related cryptocurrency provides all of the positive attributes of today's cryptocurrencies but does so using a much faster transaction validation process with limited reliance on external validation procedures. This was accomplished through two primary means. First, where the standard cryptocurrency transactions validation procedures rely upon blockchains that track every transaction, the

proposed CIVP process identifies the crypto dollars with individualized specific serial numbers and tracks just the initial issuance of each specific CIVPdollar by date and time. Second, the CIVP process relies upon mathematical algorithms embedded within each serial numbered crypto dollar to provide both an automatic validation of any proposed transaction and to prevent any counterfeiting, double spending, or the use of stolen cryptocurrency. The validation nodes themselves require little storage, processing time, or energy to keep track of the limited data necessary to support large numbers of CIVP-based transactions and therefore should be much more acceptable for transaction purposes, especially as it relates to significantly reduced energy requirements. Finally, the proposed CIVP process should have a validation process time orders of magnitude faster than the current cryptocurrencies, making the use of CIVP based crypto dollars much more acceptable from a transaction scalability perspective.

CONFLICT OF INTEREST

The authors did not receive support from any organization for the submitted work.

REFERENCES

Duong, T., Chepurnoy, A., Fan, L., & Zhou, H.-S. (2018). Twinscoin: A cryptocurrency via proof-of-work and proof-of-stake. Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts,

Geissler, S., Prantl, T., Lange, S., Wamser, F., & Hossfeld, T. (2019). Discrete-time analysis of the blockchain distributed ledger technology. 2019 31st International Teletraffic Congress (ITC 31), Budapest, Hungary

Li, J., Li, N., Peng, J., Cui, H., & Wu, Z. (2019). Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies. *Energy, 168*, 160-168.

Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., & Brooks, R. (2016). A brief survey of cryptocurrency systems. 2016 14th annual conference on privacy, security and trust (PST),