Title: SYSTEMS AND METHODS FOR MANAGING ALTERNATIVE CURRENCY TRANSACTIONS AND OPTIMIZING FINANCIAL REWARDS

Abstract: Alternative currency systems and methods that overcome virtual currency growth hurdles to maintain a decentralized network and individual miner reward are disclosed, including but not limited to the steps of providing a proof of knowledge platform criteria so that miners are incentivized to mine blocks they have knowledge about, and managing unspent and spent user transactions in block chains, with the goal of maintaining decentralized networks for alternative currency transactions and managing block chain size.

FIGURE 1
before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))
Systems and Methods for Managing Alternative Currency Transactions and Optimizing Financial Rewards

CROSS REFERENCE TO RELATED APPLICATIONS
This application claims priority to U.S. provisional application No. 62/039,975, filed on August 21, 2014, entitled Systems and Methods of Updating, Exchanging and Managing Alternative Currencies, and contains the entire contents thereof, herein by reference.

FIELD OF THE INVENTION
Systems and methods of managing alternative currency block chain transactions, and managing block chain size to maintain decentralized networks of alternative currencies and optimize financial rewards, using a computer and an alternative currency platform, are described herein. In particular, alternative currency systems and methods that overcome virtual currency growth hurdles to maintain decentralized networks and individual miner reward, including but not limited to the steps of providing a proof of knowledge platform criteria so that miners are incentivized to mine blocks they have knowledge about, and managing unspent and spent user transactions in block chains, with the goal of maintaining decentralized networks for alternative currency transactions and managing block chain size, as disclosed herein.

BACKGROUND
Use of cash and credit cards as a means for conducting financial transactions has a number of drawbacks for users. Cash, for example, is prone to being lost or stolen, with often little recourse. Similarly, in today's Internet based marketplace, credit card numbers may be readily stolen or accessed and used, leaving users with a need to find more reliable products for conducting financial transactions.

Alternative currencies are steadfastly growing as a computer-implemented medium of exchange that may help prevent theft and inflation, and that results in ease of transactions between customers and merchants in a virtual community. Today, a variety of alternative currencies have been created which can be used in exchange for
goods and services. Examples of alternative currencies that currently exist include but are not limited to Litecoin, Bitcoin, Dogecoin, Mastercoin and regional currencies such as tradebank credits.

Alternative currencies, often referred to as digital currencies or cryptocurrencies, work by having virtual alternative currency payments made in a peer-to-peer based system, as opposed to a banking or single central repository system. The virtual alternative currency payments are created as a reward when users offer their computing power to verify and record payment processing work in a public ledger in order to obtain more virtual alternative currencies, commonly referred to as mining. Virtual alternative currencies can also be exchanged for fiat money, and in exchange for products and services.

The most important part of many alternative currency systems is the public ledger that records financial transactions. Instead of having a centralized banking authority, computer servers run alternative currency software, which may be accessed over the Internet for anyone who joins. The software validates the transactions and records the transactions in block chains, commonly referred to as ledgers. The block chains thus carry the DNA code of transactions, to follow the chain-of-ownership of alternative currencies. However, problems arise when one mining pool obtains too much mining power, moving mining away from being decentralized, as further discussed in the example below.

In a recent incident, one of the largest mining pools had more than 50% of the mining power available for a sustained period of time. This same mining pool also had a history of double spend attacks, spending the alternative currency available more than once, making this mining pool's dominance even more threatening. Whenever a single entity has control over the majority of the mining power, it threatens decentralization and opens transactions up to many attacks. A concentration of miners into pools even further threatens decentralization when pool operators have control over which transactions are mined and which block is built upon. The inventors have thus developed systems and methods, implemented on a computer, in
accordance with embodiments of the present invention, where miners can optionally prove knowledge of the transaction data they are mining to earn a larger reward than miners who blindly do work given from a pool.

It is thus an object of the invention to provide financial reward to miners who mine on block chain transactions with proof of knowledge.

It is further an object of the present invention to provide methods to manage unspent and spent transactions as a tie-breaker technology implemented over a network.

It is further an object of the present invention to provide virtual currency methods and systems that are easily upgraded as use of the virtual currency grows.

It is further an object of the invention to provide systems that are easy to quickly certify transactions of alternative currencies.

It is further an object of the invention to provide trusted systems and social sites for users to make transactions with the potential of more frequent rewards.

It is further an object of the invention to provide parameters to prevent large mining companies from excessive mining and to maintaining a decentralized mining network.

In developing these features, the inventors have discovered unique virtual currency systems and methods, which are disclosed in detail herein.

**SUMMARY OF THE INVENTION**

Methods and systems of managing alternative currency block chain size and transactions and maintaining decentralized networks by implementing a tie-breaking technology and a proof of knowledge technology as disclosed in detail herein. The embodiments require a machine-readable alternative currency platform, and a machine, such as a computer to read the alternative currency platform.
BRIEF DESCRIPTION OF THE FIGURES

Figure 1 shows a flowchart with the steps for managing a tie in solving a block in an alternative currency transaction, in accordance with one embodiment of the present invention.

Figure 2 shows a flowchart with the steps for maintaining decentralized networks using proof of knowledge of alternative currency transactions in accordance with one embodiment of the present invention.

Figure 3 shows a flowchart with the steps for verifying proof of knowledge of alternative currency transactions in accordance with one embodiment of the present invention.

Figure 4 shows an example of a dynamic mining pool for maintaining decentralized networks in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Each of the embodiments herein can be conducted over a network, on a machine-readable alternative currency platform using, for instance, a computer processor to read the alternative currency platform, as further discussed in the exemplary embodiments.

Tie-Breaking: Managing Block Chain Size and Age

Blocks are generated at different frequencies in various virtual currencies. Selecting a target block generation time involves a tradeoff between quickly confirming transactions and the ability of the network to come to a consensus. If the target block generation time is too long, then blocks are generated infrequently and it takes an
inconvenient length of time before transactions are considered mature. Conversely, if the target block generation time is too short, then it is more likely that blocks will be solved nearly simultaneously. This causes networks to split their time mining on both chains, on which more simultaneous blocks may be solved, and the effect can sometimes be a tree of blocks rather than the desired linear chain of blocks.

A tree of blocks is undesirable because nodes can be working on different branches with different transaction sets, and thus a consensus is not achieved. Furthermore, nodes will not accept transactions that reference Unspent Transaction Outputs (UTXOs), which exist on other branches, causing the system to be incompatible between some parties. When this happens the system is essentially rendered useless as no consensus is ever achieved.

Many existing virtual alternative currency systems use a ten-minute target block generation rate likely because obtaining a consensus has been valued in the past over convenience. Current methods have made systems that are very robust and transactions that can be trusted not to be reversed after 1-2 confirmations (inclusions within a block). However, for many places that currency is used, it is not feasible to wait 10+ minutes before accepting a transaction. The inventors have thus developed systems and methods that will allow transactions to become confirmed more quickly and stymie the creation of many branches through the use of a tie-breaking procedure comparing the amount of alternative currency age destroyed, described in detail below.

**Tie-Breaking: Managing Unspent Transaction Outputs**

Alternative currency age destroyed is simply the product of the amount and the age of an Unspent Transaction Output (UTXO), typically measured in alternative currency-days. When UTXOs are used in a new transaction, any alternative currency age that had accumulated may be destroyed as an unspent transaction in order to manage block chain size, however the inventors have developed unique systems and methods of using alternative currency age as a tie-breaker as a proof of work (PoW/PoS) hybrid alternative currency to encourage the network and nodes attached to a network, for
sending, receiving, or forwarding information over a network, and come to a consensus quickly in the event of a tie, in accordance with one embodiment of the present invention.

Alternative currency age destroyed as a tie-breaker is used in accordance with one embodiment of the present invention in the event that two blocks are solved at roughly the same time. In accordance with this embodiment, the nodes with more stake in the system are the ones that win in the event of a tie. When nodes hear of a new solved block, the nodes essentially start a 5-second timer. If, before the timer ends, the nodes are made aware of a new block and the new block contains more destroyed alternative currency age than the previous block contained, then the node will choose it as the new correct chain because the block with more destroyed coin age is more likely to have a greater investment in the alternative currency methods and systems of the present invention. In accordance with this embodiment, when nodes hear about two (or more) new blocks within a short time period, they will all pick the same new block and broadcast it to their peers. In accordance with this embodiment, the network quickly decides which is the correct block in the event of a tie and comes to a consensus more quickly.

In accordance with the present embodiment, it may be the case that multiple new solved blocks have the same amount of destroyed alternative currency age and, thus, nodes have no way of breaking the tie between the two solved blocks. If this were to happen, then nodes would choose the block they received first as their correct block. However, this will not be very likely to happen because miners can destroy alternative currency age in their alternative currency base transactions in order to make their block more likely to be chosen in the event of a tie. The present embodiment will use a low target block generation frequency (on the order of one new block per 15 seconds, compared to new block generation every 10 minutes) in accordance with current technologies, which will result in more frequent ties in solved blocks. Thus, in accordance with the present invention, miners will compete for alternative currency age regularly as their block reward will depend on it, and it will be advantageous for a miner to maintain unspent transactions to accumulate alternative currency age, increase the chances that their block will be accepted in the case of a tie, and to
destroy their unspent transaction in the event of a tie to be chosen as the block with the most alternative currency age destroyed. By implementing the present embodiment, miners must compete to accumulate both hashing power and alternative currency age, where hashing power allows them to solve blocks and managing alternative currency age lets them win in the case of a tie.

Accordingly, in one embodiment of the present invention as shown in Figure 1, a method of managing alternative currency block chain transactions on a machine-readable alternative currency platform, the method comprising the steps of: providing an alternative currency with a high new block chain generation rate on a machine-readable alternative currency platform, step 100, determining, at one or more nodes on a network, a tie in solving two or more block chains, step 102, analyzing on the machine-readable platform said two or more block chains to determine the chain with the most destroyed alternative currency age, step 104, based on the analysis, choosing with a machine implemented platform, the block chain with the most destroyed alternative currency age, step 106, and, displaying for networks the block chain with the most destroyed alternative currency age, wherein the method results in an incentive for users to maintain unspent transactions based on amount and age in block chains and to increase destroyed alternative currency age in the event of a tie in solving two or more block chains on a network, step 108.

Yet another benefit of the present embodiment of using destroyed alternative currency age as a tie-breaking measure is that fees may be partially eliminated for miners of the new alternative currency described herein. Miners may include transactions into their block if they have a fee and/or if the transactions contribute to the destroyed alternative currency age for their block. Both provide the miner some benefit, the fee being a monetary gain and the destroyed alternative currency age causing the miner’s block to be chosen in the event of a tie. Since there is only a finite amount of alternative currency age in an alternative currency at any one time and it becomes used up once it is used in a transaction, destroyed alternative currency age can stand as a viable replacement for fees. As such, yet another step in accordance with the present embodiment includes removal of fees from transaction based on destroyed alternative currency age. The present embodiment allows a miner to obtain additional
financial incentives to include transactions from a block chain, thereby contributing to more efficient alternative currency systems and methods.

**Maintaining Decentralized Networks with Miners' Proof of Knowledge**

In accordance with one embodiment of the present invention, alternative currency transactions are managed to incentivize miners to control the set of transactions they mine by providing a proof of knowledge program implemented on a machine-readable alternative currency platform that rewards miners for proving knowledge of the transactions in their block. In accordance with this embodiment, verifying knowledge of transaction data is an optional part of mining, which if completed, lets the miner claim a 5% higher block reward. The present invention, when implemented on a computer, is likely to be valuable as alternative currencies become accepted as a mainstream currency. As mining becomes more competitive, resulting in thinning profit margins, mining with proof of knowledge in accordance with the present invention will allow miners to maintain a significant financial gain and maintain decentralized mining procedures. The inventors have thus developed a mining process on a machine-readable alternative currency platform that can be configured to prove that a miner has knowledge of the transaction data they are mining. When mining with proof of knowledge is turned on, the miner can claim 5% more on the miner's block rewards.

Figure 2 shows one method in accordance with the present embodiment of implementing proof of knowledge on a computer-implemented program to manage virtual alternative currencies. In accordance with this embodiment a first step 220, in accordance with standard mining procedure, of building a block in a block chain by setting block header fields and gathering miner transactions, is accomplished. In a next step 222 of providing a bit flag specifying proof of knowledge in the block header, followed by step 224 of setting proof of knowledge data within the block header to zero. A next step, 226, of hashing the block header to produce the hash H. In a next step 228 of using H to pseudo-randomly select a transaction Tx from a block and the step 230 of setting the proof of knowledge data to a subset of the bits of Hx or a subset of the bits of Tx. In a next step, 232, of hashing the block header again with proof of knowledge data set in step 230, and determining if the difficulty
requirement is met, step 234. If step 234 is passed, then the proof of knowledge has been successfully created in the block chain, step 236. In accordance with this embodiment, if the difficulty requirement, step 234 is not met, the mining process to establish proof of knowledge continues on its next iteration, starting with incrementing the counter in the block header, step 236, and then returning to step 224.

In accordance with the present invention, once the proof of knowledge criteria has been implemented, verification steps are implemented in accordance with the present embodiment. In accordance with this embodiment, shown in Figure 3, step 340 of providing peers with block header and proof of knowledge data, as well as 1 block chain transaction (Tx 1) with proof that the transaction is in the block. In a next step 342 of setting proof of knowledge data in the block header to all zeroes and then hashing the block header (step 344). The result of step 344 is H, and in a next step, 346, of using H to pseudo-randomly select a transaction Tx from the block. In a next step 348, comparing Tx 1 from step 340 to Tx. If Tx 1 is the same transaction as Tx, then a next step 350 of setting the proof of knowledge data in the block header to a subset of the bits of Hx or a subset of the bits of Tx, and step 352 of hashing the block header with the pseudo-randomly selected data point, and a next step 354 of determining if the difficulty requirement is met in order for the next step of obtaining validation of proof of knowledge in a block chain, step 356. In accordance with this embodiment and step 348, if Tx 1 is not equivalent to Tx the verification step has failed resulting, in a step 358 of invalidating the proof of knowledge verification. Similarly, if the difficulty requirement is not met in step 354, then the verification step has failed resulting in the step 358 of invalidating the proof of knowledge verification.

One advantage of the present embodiment is that although the miner is required to know all of the transaction data in the block, verifying the work only requires one extra transaction from the block and a Merkle branch proving its inclusion within the block, and requires much less data compared to what is required to actually mine a block. This is especially advantageous for simplified payment verification nodes, which need to be able to verify block headers without downloading all of the block's data. To achieve this, mining with proof of knowledge is done by pseudo-randomly sampling transaction data. In addition, mining with proof of knowledge turned on will
not delay block chain transactions.

The result of using proof of knowledge on a machine-readable alternative currency platform is that miners are incentivized to build their own blocks rather than use the work given from the pool. Miners can still use pools to limit variance, but by incentivizing miners to know their own transaction data, no single user has control over a large portion of the network's hash power, thereby maintaining a decentralized mining network.

Additional Steps to Maintain a Decentralized Network

In addition to implementing proof of knowledge and tie breaking systems and methods to overcome growth hurdles with alternative currencies, the inventors further developed computer-implemented and machine-readable methods and systems that further help maintain decentralized alternative currencies, which when combined with the proof of knowledge or tie breaking technologies in accordance with the present invention, overcomes growth hurdles of alternative currencies.

As discussed in the background of the present invention, a major goal with current alternative currencies is to maintain a peer-to-peer based system with a decentralized repository. However, complex application specific integrated circuits (ASICS) hardware systems have been developed for mining with lower power and at lower costs than regular computer programs, making mining competitive and mostly profitable only for users with an investment in high powered ASIC hardware. As such, currently available alternative currencies are quickly falling into centralized mining locations, where only ASICS and those with access to ASICS have the power to mine, creating a few large pools of miners with mining power.

The inventors have thus developed systems and methods of developing small dynamic pools of trusted members in accordance with one present embodiment of the present invention, which prevents formation of large ASICS mining groups. In accordance with this embodiment, a server is devoted to creating and distributing private and public key pairs for each member of a pool. In accordance with this embodiment, private keys are randomly generated that allows users to sign into transaction and to
obtain money through the transaction. The public key is also random, and it allows a user to be paid by another source through the public key access.

In accordance with this embodiment, the miner in a pool who solves a block is entitled to spend the reward for that block. The methods and systems in accordance with the present invention will keep track of and redistribute rewards based on the private keys, once the miner who solves the block has produced a signature that is verified when the miner attempts to spend the block reward. Under this system, a pool with many anonymous miners is not feasible because all miners in the pool would be able to accept rewards according to their shares when others solve a block but then abscond the whole block reward when they are the one to solve a block. Thus, in accordance with the present invention, a certain level of trust is needed from peer to peer, because if a reward is not shared by the miner who solved a block, then the miner who solved a block would not be welcome to the pool, versus, a miner who shared their reward will also be able to obtain rewards proportional to their shares when other honest miners solve blocks. Instead of all miners in a pool trusting a pool operator, as is the case for many current pools, in accordance with the present embodiment, all members of a pool must trust all other members of the pool, resulting in a limited size of the pool, and resulting in more frequent financial rewards for miners and dis-incentivizing ASICS from joining a pool in accordance with the present invention.

Figure 4 shows an example of a dynamic mining pool in accordance with the present invention. In this embodiment, miners A, B, and C, shown as 660, are each shown being given a private and public key in accordance with the embodiments of the present invention. In accordance with this embodiment, the users must sign in on a server, shown as 662, with their private key to mine in the pool, and the users shall receive a proportional share of any reward when a block reward is granted, in accordance with the work each user put towards solving the block. ASICS are less likely to develop hardware that will centralize the present alternative currency because the private sign-in keys of the pools make creation of ASICS that would work with the present embodiment difficult to develop, and the ability for one miner to take
an entire reward for sharing a block unappealing to ASICS and large mining groups.

Accordingly, in one embodiment of the present invention of providing a machine-readable medium for exchanging alternative currencies, when executed by a machine, cause the machine to, provide private keys, 664, and public keys, 666, for each user; collect information of said user’s contribution when solving a problem, allowing the user who solved the problem to denote the problem has been solved and obtained the entire reward or request distribution of the reward amongst the users; and distributing a reward in accordance with the instructions of the user who solved the problem.

Chaining Algorithms
The inventors have also developed a unique way of chaining hashing algorithms by using the output from one algorithm to determine the next algorithm to use. In accordance with this method of chaining algorithms coded for alternative currency transactions, each algorithm unpredictable, making it more difficult to solve blocks and more resistant to ASICS. In accordance with this embodiment 5 randomized algorithms in a chained hash are provided, with Keccak executed first, and then the next 4 (JH, Grøsli, Skein, Blake) are executed in random order dependent on the results from Keccak. In accordance with this embodiment, after Keccak is executed, the lease significant 32 bits are used an integer to calculate the order of the next 4 hashes. The integer is modified by 24 and placed in a table to determine the next 4 hashes, resulting in unpredictable and harder to solve blocks for ASICS.

Additional Steps for Managing Block Chains
In addition to implementing proof of knowledge and tie breaking systems and methods to overcome growth hurdles with alternative currencies, the inventors further developed computer-implemented and machine-readable methods and systems that further help manage block chain size, including full node block chain processing, wallets for multiple currencies, and conversions to new systems which when combined with the proof of knowledge or tie breaking technologies in accordance with the present invention overcome growth hurdles of alternative currencies.
Full Node Block Chain Processing

In many current applications, an entire block chain must be parsed before the node can actively participate in transactions on the network. The currently available processes can be a time consuming process for most standard computers, which may take a week or more.

In accordance with one embodiment of the present invention, node participation in transactions on the network may be expedited. In accordance with this embodiment, nodes will first download all block headers and verify the basic validity of those headers. In accordance with this step, the nodes will have enough information to participate in the network as a light-weight node while a background thread runs, downloading block contents and then verifying the content starting at the genesis block. Certain features that rely on having the full block chain data set may be disabled temporarily while this process is running. During the initialization period described herein, the validity of transactions is established through other nodes' referral of transactions and the depth of the transactions within the block chain. The present embodiment makes alternative currencies much easier to use for everyday people, eliminating the need to wait several weeks before being able to participate.

Conversion to New Systems to Manage Block Chain Size

In yet another embodiment of the present invention, managing block chain size and conversion of alternative currencies to new block chains is a difficult challenge, as in order to be effective, miners may be required to update to a new block chain, and those who do not may be at risk of losing their transactions. The inventors have thus determined, in yet another embodiment of the present invention, a new alternative currency with a version control system which will allow easy one-way conversion from an older (version 1) version to a newer (version 2) version, such that old alternative currencies are exchangeable for new alternative currencies. In accordance with this embodiment, when an alternative currency needs to be improved, the present embodiment creates a new version 2 block chain upgrade. Some of the benefits of the new upgraded block chain in accordance with the present embodiment include, but
are not limited to, reducing chain size by dumping old transactions, allowing ease of migration to fix bugs, dis-incentivizing ASICS (defined above) from joining the mining pool, and the ability to reintroduce money that has not been transacted because private keys have been destroyed.

One hurdle with creating a new block chain for alternative currency upgrades is user adoption to the new block chain. In order to promote adoption, a version 3 block chain that accepts both version 1 and version 2 with the same specifications as version 1 is provided; since the specifications are the same as version 1, user adoption should be seamless and the block chain will be shorter, thereby allowing management of block chain size as user adoption grows, while still providing all of the benefits of the upgraded virtual alternative currency, version 2, described above. By providing a version 3 alternative currency in the manner described, a higher rate of conversions can be expected amongst users.

In accordance with this embodiment, further steps of providing an incentive for users to migrate alternative currencies to a new block chain, including the steps of providing a financial incentive for converting to a new block chain and/or for converting to a new alternative currency, and the steps of providing a third block chain with the same specifications as the old block chain, wherein the third block chain may be easier to convert for some users, and wherein the third block chain can readily be converted to the new block chain with updated specifications.

*Wallets for Multiple Alternative Currencies*

Another hurdle with alternative currencies is making the new block chains for new alternative currencies adaptable with multiple alternative currencies. In accordance with one embodiment of the present invention, wallets can access block chain information from multiple alternative currencies, allowing for ease of conversion to new alternative currencies. Additionally, a financial incentive may be provided for users converting an alternative currency to a currency managed with or provided with the embodiments of the present invention, in which case an exchange rate between each alternative currency will be provided. In accordance with this embodiment,
wallets keep track of other block chain headers up to a certain point while transactions are being verified.

*Checkout Benefits with Alternative Currency Payments*

In yet other embodiments of the present invention, using the systems and methods of the present invention may further result in cost savings for customers using alternative currencies, in addition to speedier checkout options using alternative currencies and the ability to manage different types of alternative currencies in block chain transactions and wallets, as disclosed herein. Methods of using alternative currencies in order to promote ease of checkout from multiple vendors, provide added discounts and promote payments of affiliate fees are disclosed herein. With regard to providing easy checkout methods, in accordance with one embodiment, users can checkout with multiple products from multiple vendors in one easy step, using the alternative currencies managed in accordance with the systems and methods of the present invention. In accordance with this embodiment, using alternative currencies managed in accordance with the systems and methods provided herein allows for additional savings that can be passed on to a user during checkout with coupons or savings obtained with, for instance, proof of knowledge turned on. By managing alternative currencies directly, a method of ensuring payments of affiliate fees, which are otherwise often lost in transactions between vendors and sites that redirect to a vendor site, is provided.

Each of the embodiments herein can be conducted over a network, using a machine-readable alternative currency platform including, for instance, a computer with a processor that may be used to read the alternative currency platform. It should be emphasized that the above-described embodiments of the present invention, particularly any "preferred" embodiments, are merely possible examples of implementations, merely set forth for a clear understanding of the principles of the invention. Many variations and modifications may be made to the above-described embodiments of the invention without departing substantially from the spirit and
principles of the invention. All such modifications and variations are intended to be included herein within the scope of this disclosure and the present invention and protected by the following claims.
CLAIMS:
1. A method of managing alternative currency block chain transactions on a machine-readable alternative currency platform, the method comprising the steps of:

   providing an alternative currency with a high new block chain generation rate on a machine-readable alternative currency platform;

   determining, at one or more nodes on a network, a tie in solving two or more block chains;

   analyzing on said machine-readable alternative currency platform said two or more block chains to determine the chain with the most destroyed alternative currency age;

   based on the analysis, choosing with said machine-readable alternative currency platform the block chain with the most destroyed alternative currency age; and,

   displaying for networks the block chain with the most destroyed alternative currency age, wherein the method results in an incentive for users to maintain unspent transactions based on amount and age in block chains and to increase destroyed alternative currency age in the event of a tie in solving two or more block chains on a network.

2. The method of managing alternative currency block chain transactions on said machine-readable alternative currency platform in accordance with claim 1, the method further comprising the steps of allowing a miner on a network to obtain the entire reward or request distribution of the reward amongst miners.

3. The method of managing alternative currency block chain transactions on said machine-readable alternative currency platform in accordance with claim 2, the
method further comprising the steps of promoting decentralized networks by promoting trust amongst miners.

4. The method of managing alternative currency block chain transactions on the machine-readable alternative currency platform in accordance with claim 1 further including the step of chaining hashing algorithms by using the output from one algorithm to determine the next algorithm.

5. The method of managing alternative currency block chain transactions on the machine-readable alternative currency platform in accordance with claim 4 further including the step of dis-incentivizing ASICS from mining on a block chain.

6. The method of managing alternative currency block chain transactions on said machine-readable alternative currency platform in accordance with claim 1 further including the step of allowing nodes to download all block headers and verify the basic validity of those headers to actively participate in block chain transactions.

7. The method of managing alternative currency block chain transactions on said machine-readable alternative currency platform in accordance with claim 1 further including the step of providing a computer-implemented version control system which will allow easy one-way conversion from an older (version 1) version to a newer (version 2) version, such that old alternative currencies are exchangeable for new alternative currencies.

8. The method of managing alternative currency block chain transactions on said machine-readable alternative currency platform in accordance with claim 1, the method comprising the steps of providing discounts during a checkout process.

9. A method of managing alternative currencies transactions using proof of knowledge of block chain transactions to improve miner reward and maintain a decentralized network on a machine-readable alternative currency platform, including the steps of:
building a block in a block chain by setting block header fields on the machine-readable alternative currencies;

gathering miner transactions on the machine-readable alternative currency platform;

providing a bit flag specifying proof of knowledge in said block chain on a network;

pseudo-randomly selecting transaction data for establishing data on proof of knowledge;

hashing the block header of the pseudo-randomly selected data point;

determining if a difficulty requirement is met; and,

verifying the proof of knowledge in said block chain on said network.

10. The method of managing alternative currencies transactions using proof of knowledge of block chain transactions to improve miner reward and maintain a decentralized network on a machine-readable alternative currency platform, with claim 9, the method further comprising the steps of allowing a miner on a network to obtain the entire reward or request distribution of the reward amongst miners.

11. The method of managing alternative currencies transactions using proof of knowledge of block chain transactions to improve miner reward and maintain a decentralized network on a machine-readable alternative currency platform, in accordance with claim 10, the method further comprising the steps of promoting decentralized networks by promoting trust amongst miners.
12. The method of managing alternative currencies transactions using proof of knowledge of block chain transactions to improve miner reward and maintain a decentralized network on a machine-readable alternative currency platform, in accordance with claim 9, further including the step of chaining hashing algorithms by using the output from one algorithm to determine the next algorithm.

13. The method of managing alternative currencies transactions using proof of knowledge of block chain transactions to improve miner reward and maintain a decentralized network on a machine-readable alternative currency platform, in accordance with claim 12, further including the step of dis-incentivizing ASICS from mining on a block chain.

14. The method of managing alternative currencies transactions using proof of knowledge of block chain transactions to improve miner reward and maintain a decentralized network on a machine-readable alternative currency platform, in accordance with claim 9, further including the step of allowing nodes to download all block headers and verify the basic validity of those headers to actively participate in block chain transactions.

15. The method of managing alternative currencies transactions using proof of knowledge of block chain transactions to improve miner reward and maintain a decentralized network on a machine-readable alternative currency platform, in accordance with claim 9, further including the step of providing a computer-implemented version control system which will allow easy one-way conversion from an older, version 1, version to a newer, version 2 version, such that old alternative currencies are exchangeable for new alternative currencies.

16. The method of managing alternative currencies transactions using proof of knowledge of block chain transactions to improve miner reward and maintain a decentralized network on a machine-readable alternative currency platform, in accordance with claim 9, the method comprising the steps of providing discounts during a checkout process.
Providing an alternative currency with a high new block chain generation rate on a machine-readable alternative currency platform

Determining, at one or more nodes on a network, a tie in solving two or more block chains

Analyzing on said machine-readable platform said two or more block chains to determine the chain with the most destroyed alternative currency age

Based on the analysis, choosing with a machine-implemented platform, the block chain with the most destroyed alternative currency age

Displaying for networks the block chain with the most destroyed alternative currency age, wherein the method results in an incentive for users to maintain unspent transactions based on amount and age in block chains and to increase destroyed alternative currency age in the event of a tie in solving two or more block chains on a network

FIGURE 1
Building a block in a block chain by setting block header fields and gathering miner transactions

Providing a bit flag specifying proof of knowledge in the block header

Setting proof of knowledge data within the block header to zero

Hashing the block header to produce the hash $H$

Using $H$ to pseudorandomly select a transaction $Tx$ from a block

Setting the proof of knowledge data to a subset of the bits of $H$ xor a subset of the bits of $Tx$

Hashing the block header again, with proof of knowledge data set in a prior step

Creating a block with proof of knowledge successfully

Incrementing the counter in the block header

Determining if the difficulty requirement is met

No

Yes

FIGURE 2

SUBSTITUTE SHEET (RULE 26)
Providing peers with block header and proof of knowledge data, as well as 1 block chain transaction (Tx 1) with proof that the transaction is in the block

Setting proof of knowledge data in the block header to all zeroes

Hashing the block header, with a result of H

Using H to pseudo-randomly select a transaction Tx from the block

Comparing Tx 1 from step 340 to Tx

Setting the proof of knowledge data in the block header to a subset of the bits of Hx or a subset of the bits of Tx

Hashing the block header with the pseudo-randomly selected data point

Determining if the difficulty requirement is met

FIGURE 3
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8): G06Q 20/00 (2015.01)
CPC: G06Q 20/3678; G06Q 20/06; G06Q 20/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8): G06Q 20/00 (2015.01); CPC: G06Q 20/3678; G06Q 20/06; G06Q 20/02

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
IPC(8): G06Q; CPC: G 06Q 20/10, G 06Q 20/367; USPC: 705/69; 705/65; 705/64; 705/37

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase (All); Google (Patents, Scholar, Web)
Search Terms: Currency, money, dough, tender, cash, bitcoin, Alternative, alternate, different, substitute, Transaction%, deal, bargain, Block w2 chain, Platform, staging, Generate*, Rate, Node%, network, Destroy*, ruin*, damage*, dismantle*, Age, life, maturity, Tie

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
</table>

Further documents are listed in the continuation of Box C.

Date of the actual completion of the international search
3 December 2015 (03.12.2015)

Date of mailing of the international search report
3 DEC 2015

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Authorized officer: Lee W. Young
PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

Form PCT/ISA/2 10 (second sheet) (January 2015)
This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. □ Claims Nos.:
   because they relate to subject matter not required to be searched by this Authority, namely:

2. □ Claims Nos.:
   because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. □ Claims Nos.:
   because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

This International Searching Authority found multiple inventions in this international application, as follows:

-Please See Continuation Sheet-

1. □ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. □ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. □ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos. 1-8

<table>
<thead>
<tr>
<th>Remark on Protest</th>
<th>□ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>□ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.</td>
</tr>
<tr>
<td></td>
<td>□ No protest accompanied the payment of additional search fees.</td>
</tr>
</tbody>
</table>
Continuation of Box No. III, Observations where unity of invention is lacking:

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1.

Group I: claims 1-8 are directed to a method of managing alternative currency block chain transactions to incent users to maintain unspent transactions based on amount and age.

Group II: claims 9-16 are directed to a method of managing alternative currencies transactions using proof of knowledge of block chain transactions.

The inventions listed as Groups I and II do not relate to a single general inventive concept under PCT Rule 13.1 because under PCT Rule 13.2 they lack the same or corresponding technical features for the following reasons:

Group II does not include the special technical features of: providing an alternative currency with a high new block chain generation rate, determining, at one or more nodes on a network, a tie in solving two or more block chains, analyzing the block chains to determine the chain with the most destroyed alternative currency age, based on the analysis, choosing the block chain with the most destroyed alternative currency age, and, displaying for networks the block chain with the most destroyed alternative currency age, wherein the method results in an incentive for users to maintain unspent transactions based on amount and age in block chains and to increase destroyed alternative currency age in the event of a tie in solving two or more block chains on a network of Group I.

Group I does not include the special technical features of: building a block in a block chain by setting block header fields, gathering miner transactions, providing a bit flag specifying proof of knowledge in said block chain on a network, pseudo-randomly selecting transaction data for establishing data on proof of knowledge, hashing the block header of the pseudo-randomly selected data point, determining if a difficulty requirement is met and, verifying the proof of knowledge in said block chain on said network of Group II.

Since each of these technical features are not common to the other group, unity of invention is lacking.

Non-special common features between Group 1 and Group 2 include: a machine-readable alternative currency and block chains. However, these features are obvious over the prior art and therefore not special technical features as evidenced by at least:

US 2015/0120106 A1 to Schwartz (28 July 2015) teaches a machine-readable scrip (Figs 2A, 2B and paras [0013]-[0021], [0030]);

US 2014/0201057 A1 to Shuster (17 July 2014) teaches a block chain related to a machine-readable alternative currency (Bitcoin - para [0059]).

Therefore the technical features common to Groups 1 and 2 are not special technical features.