Anticoin, Beka, gamma & Gift Notes: A Crytpography-Based System Using Proof-of-Decentralization and Future-Determined Targets

Adam Z Winter
Seattle, WA, USA
adam@giftnotes.org
anticoins.org

The direction we are currently heading with proof-of-work algorithms devouring incredible amounts of energy is embarrassingly wasteful and simply not sustainable. Something must change.

Proposed is a new kind of virtual currency system that is non-volatile in value, capable of handling large amounts of transactions very quickly, viable for every-day use with low transaction fees, does not require staking, does not require large amounts of electrical energy or hashing power, cannot be attacked with large amounts of hashing power, provides equal opportunity for all to receive block rewards, is highly decentralized, extremely secure, open source, democratic, provides an open-protocol online personal identification layer [2], and benefits charities.

All of this is accomplished through the relationship between four separate types of coins within the system; Anticoin, Beka, gamma, and Gift Notes ("Notes"). Gift Notes will, initially, use existing gift-card technology to allow corporations to back the currency through purchase contracts and their goods, thereby removing volatility from the value of Notes by giving them tangible value and pairing with a nation's currency. As incentive to provide the physical infrastructure required (nodes), and further incentive to use the currency, block rewards will be awarded to participants (not "miners"). Participants will be anyone using the currency and/or providing a node. Block rewards will come in the form of Beka. However, Beka alone will not have the direct backing that Notes do until combined with Anticoin.

The entire supply of Anticoin will be issued at inception, as a means of raising the funds needed to bootstrap the system into existence. When a user deposits Anticoin and Beka to an address, the two annihilate each other and produce gamma. Gamma will, uniquely, be the currency accepted in an online auction system where newly-issued Notes will be auctioned off regularly. In essence, we'll say to a company, "We'll give you $9 if you give us $10 in store credit." The 10% difference will then be awarded to participants through the auction. This creates a kind of "DC bridge" between the rate that Beka will be awarded and the rate at which value can be added to the system, so that the value of Notes can be kept in solid state. Naturally, as Anticoin is destroyed, it will become scarcer and its value will increase, as will the value of Beka, which will have a decaying reward size.

The Central Guidance System (CGS): Imagine if Bitcoin were able to democratically change its parameters easily and without all the fuss. For example, the block size limit could be changed from 2 MB to 2.02 MB (the block size limit being the "parameter", and its value being changed). Whatever the arguments against changing the block size may be, an incremental change is much easier to agree to than a large one.

The Central Guidance System would only be capable of making incremental recommendations, and not able to enforce them. For example, the Central Guidance System could make a recommendation that the number of required signatures on a transaction be increased by one, or decreased by one, but the coding of all nodes would only allow such a change once every 6 months. In this way, all nodes can keep a default setting that automatically accepts recommendations made by the Central Guidance System, but always have the option to turn that setting off if they disagree with the direction things are heading, or have some reason to believe that the CGS has been hacked or corrupted. In this way, the Central Guidance System is like a driver of a vehicle that can keep the vehicle on the road and between the lines, but can't go bonkers and drive off a cliff.

It is very important to note that the entire system can still function on its own without the CGS. That is, if the CGS went offline, was hacked, or corrupted, everything else would continue as is until the CGS was secured again. The CGS will be a built-in functionality from the inception of the Anticoin system. Naturally, the people behind the CGS will be part of the larger, *democratic, non-profit*, organization that secures contracts with businesses and conducts the auctions.

Every coin in existence has a team of core developers who exert some amount of influence over how their coin operates. The Anticoin system will be the same in this regard, but the organization behind it will be a non-profit. The people who devote themselves to making it all happen will receive compensation for their very-valuable work, but as employees of a transparent organization. There will be no stock-holders in a corporate entity that the management must answer to. The shareholders will be the people who participate. That is, the shareholders will be the people who use Notes for payments and the people who provide the nodes. There will be no opportunity for the rich to buy all of these shares. Your stake will be inherent in the fact that you are an individual. The Anticoin system will be for the people. If you want to invest, buy Anticoin at the outset.

In addition to proposing changes to parameters, the CGS would also propose the minting of new Notes. This will work similarly to how a nation's treasury might work, where currency is regularly removed from circulation and new currency is placed into circulation. The big difference is that the people will vote whether or not to allow more Notes to be put into circulation. The CSG will propose a future transaction that will place new Notes into circulation, and the people will signal their willingness to accept that transaction within the transactions they sign. Upon approval, the new notes will be divided into appropriate-sized smaller chunks and auctioned. Naturally, the CSG will be required to provide and publish the evidence that shows the additional value has been secured to back the proposed Notes.

In their Bitcoin white paper, Satoshi Nakamoto[1] wrote:

The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. -Satoshi Nakamoto

Still, anyone able to allocate more processing power enjoys greater rewards and exerts more influence over that system. Now, we've seen the results of this with how a limited number of mining pools carry the vast majority of hashing power and have been able to exert that power significantly. This is not a decentralized system, and the level of democracy looks more like a boardroom meeting than what we should be able to accomplish in this age of technology.

Clearly, one-person-one-vote is the ideal. However, one might think that the attempt would be plagued with problems regarding identification, theft of identification, anonymity, and freedom....even if one might, at the same time, hold the belief that blockchain technology can revolutionize government elections. I will argue that online identification, theft of identification, and anonymity are already huge problems, and propose a system that is a solution to these, as well as means for securing a public ledger.

First, we need to address the elephant in the room, and the donkey. Governments are charged with protecting the people and fighting crime. It matters very, very, little your personal feelings about the reach of the government, as it pertains to capital offenses, terrorism, and taxes (just to name a few). Simply put, governments will always collect taxes and work to fight against the worst crimes, and often with a sledgehammer, not a scalpel. Thus, it is completely naive for anyone to think that if they keep making cryptocoins more anonymous, harder to trace, harder to tax, and generally better-for-use-by-criminals, that governments won't step in and slap down major regulations on the whole industry. The baby is being thrown out with the bathwater.

However, to have freedom and democracy in a currency, one should be able to choose whether or not they will identify themselves in a transaction, and also whether or not to *accept* a transaction from someone who chooses not to identify themselves.

To do this, two kinds of Note addresses will be used. Each will be identified by the first character in the address. One will be anonymous and function as most cryptocoin addresses do presently. The other will not contain the identity of the user, but will be traceable to the individual through a kind of registration, and the individual will be able to utilize this to prove their identity by signing an identification transaction. Through use, the individual's identification token should regularly move to a new address (with different private key and seed) in order to avoid overuse and to establish a list of historical addresses owned by the individual. The individual's own hardware device (computer) will constantly scan for unauthorized transactions that were signed using the individual's private key. If such a transaction is identified, the computer could then immediately issue a freeze transaction using one of the former private keys. All honest nodes in the system would then disregard any following transactions from the compromised account. If one is concerned about the security of that computer, then they should employ redundant computers. Everyone will have to employ a certain level of self-reliance, maybe even radical self-reliance. Also, any currency transactions issued before the freeze will be valid. There will be no chargebacks. Clearly, such an attempt at theft would have the currency sent to an anonymous address, and people can decide what they want to do with money that originates from such a place. (See **Unidentified Addresses** for more on this).

Storing the identities of people is a big burden for the organization to take on, and it will not be taken lightly. That said, this is not a system where unattended computers sit on check stands at the front of retail stores. Individuals, will have two options in registering their identification; ID-enabled and ID-disabled. The identification registration of a person who chooses ID-disabled will be kept offline in cold-storage and protected with great concern for its security. Part of the organization's budget will specifically be for hiring a team of attorneys who will be tasked with automatically reviewing any legal demand to turn over the identification of a person associated with an address. If you are this person, you will be notified and given the opportunity to provide your own legal representation. However, those who cannot afford an attorney will be provided a basic level of representation automatically, before any records are handed over. That said, legitimate criminal investigations will not be stonewalled.

Of course, those who choose the ID-enabled option will have their identification securely stored online in a way that the individual will control, and will be able to use this ability to prove their identity. You will own your identity. Your identity will not be a product for Facebook to sell [2].

It cannot be stressed enough the absolute dedication to protecting your identity that this organization must openly and transparently adhere to. If you're skeptical about the ability of an organization to protect your identity, please read on and understand just how many benefits there are to this system. Also, note that a nation's government can be used to fill this role, as they already have your identity. The question will remain whether that is the organization you want playing that role in your life.

You may have asked yourself why anyone would choose the ID-disabled option when they can just use an anonymous address. It is because only identified addresses will be eligible to receive block rewards and vote on parameter changes. When an individual creates a transaction that is properly broadcast into the network, that transaction will represent an entry in a raffle. Each block in the blockchain will be a separate raffle. This is how the need for proof-of-work systems and proof-of-stake systems will be eliminated.

Proof of Decentralization and Future-Determined Targets: Proof-of-work systems use a known target. You win a block reward by being the first to guess an answer that hits a pre-determined target. With this, there is only incentive to make as many guesses as you can as fast as you can. Thus, monumental amounts of electrical energy are used to do so. However, if the target is unknown, and only to be determined in the future, there is no use for high-speed hashing power. However, there is incentive to *use* the system, as each transaction represents the potential of a reward. One of our parameters will be a limit on the number of transactions an identified user can create, per block, that are eligible for a block reward. Of course, when a single transaction can contain multiple payments to multiple destinations, a limit of one transaction per minute may be sufficient. However, to make it simple, all transactions will be valid and accepted, but multiple transactions will cancel each other's eligibility for a block reward. That is, if only one transaction is created that minute, it will be eligible for a block reward, but if multiple transactions are created, none of them will be eligible. That way, users have the flexibility of being able to make multiple, but will be incentivized to consolidate their payments into single transactions. Still, an upper bound will have to be in place to make sure that the system can handle the load.

Time is another issue that we will improve upon here. Specifically, each block will represent one minute and contain only the transactions that were created in that minute. That is, block no. 42 will include only the transactions created in the 43rd minute since the system went live. Moreover, that block will contain *all* of the transactions created in that minute, with near-perfect accuracy. This will be accomplished by the fact that each block in the blockchain will not actually need to reference the one directly before it. This is accomplished simply by not allowing the block reward transaction to be created until a much later time when all transactions for that block have had more-than-ample time to propagate to all active nodes. For example, let's say we choose 24 hours to be the amount of time given to allow a transaction to propagate through the system. Then, on the 1,440th block after the block in question, all nodes should completely agree on all the transactions that were created 24 hours prior, and be in agreement as to who gets to sign a block reward to themselves and for how much.

Make note that it will not matter whether all computer clocks are perfectly synchronized with each other when creating transactions. That is, it doesn't really matter whether a transaction ends up in one block, or the one before it, or the one after it. Though, there will be a reliable system for rejecting any transactions that are egregiously back-dated in an attempt to insert a transaction into a past block. The following is an explanation of how this works.

The Consensus Algorithm: A transaction is created and relayed to a limited number (another parameter) of nodes, who each relay that transaction to no more than two other nodes, where the exchange between two computers can be modeled as the following conversation:

Node A: Hello, I have gift for you. It's a new transaction!

Node B: Sweet! My name is "N1jdfg55e1vg58ew7g1", and the parameters I adhere to are A=1, B=10, C=42, and D="6 months"[.......etc....] and the transactions I have from the last twenty blocks each hash to ["br54gr651rv654gedrg646e", "sf5g165vr15r4g5r4gr64", ..., and "fg5t4ht65h41g54r54g54"].

Node A: Great! Those are my parameters too! But it looks like our transaction histories only agree up to five blocks ago. Here's all the transactions that I have on record since then.

Node B: Perfect. I'll update my transaction record now......and I'm sending you the 102 transactions that I have that you didn't. Now, about that new transaction....

Node A: Yes, of course. I've written your name on it, put it in an envelope and signed the envelope.....and there you have it. Also, here's a list of my other close peers. Please don't relay this to one of them.

Node B: No problem, and Thank you! I'll be sure to send a new transaction your way sometime.

Node A: I would appreciate that very much. Thank you, goodbye.

Each node wants a new transaction sent to them because, when they sign it and pass it along, they also become eligible for a part of the block reward. In this way, nodes are incentivized to quickly pass transactions along. It is important to note that there is a big difference between the transactions that the two computers exchanged from their histories, and the new transaction. In order for a new transaction to be complete and eligible for a block reward, it must be sequentially signed by N signatories, where N is another parameter to be chosen. For example, let's take N to be ten. Then the new transaction would have to be signed off to ten nodes in a row before it is eligible for the next step to completion. With each node passing the new transaction to two other nodes (and no more than two), and other new transactions crossing paths with it, the transaction will very quickly find its way to all nodes.

If we assume that each interaction between two nodes takes as much as 20 seconds, then, when a node receives a new transaction that has been signed by X other nodes, the timestamp on the new transaction should not be longer than 20X seconds ago. If it is longer, an honest node will reject that new transaction and consider the possibility that the sending node was acting dishonestly. Naturally, some connections and computers may just be slow, but the transaction will be sent down more than 2^10 paths. One of those is likely to be fast enough to support the new transaction.

What if ten nodes collude to fake an old transaction? To combat this possibility, we will use a checkpoint where the transaction will pass into an inner circle of nodes who are the most transparent, most trusted, and (most importantly) have the most to lose by colluding with the ten dishonest nodes. The first node within this inner circle will timestamp the transaction and repeat the same steps of propagating that new transaction throughout the inner circle, requiring M more signatures (another parameter). At the end of this path, the transaction will finally be complete, and the first target will finally be established.

A new transaction will take many paths. Each of those paths will turn that transaction into a different version of itself. However, only one of these can be chosen as the eligible entry in the raffle. All nodes will agree that the hash of the transaction signed at its endpoint that is closest to the hash of the transaction at its creation will be the ultimate version of that transaction. That is, when the final node completes the transaction, the difference between its hash at that point and its original hash will be taken and that value will determine its fate. For whichever version of the transaction this value is the smallest that version will prevail. So, looking back at the interaction between Node A and Node B, they won't just compare which transactions they have, but which *versions* of those transactions, and adopt the appropriate one.

Now that we've successfully entered all of our transactions into the raffle, we can choose the winning ticket. We'll do this in a like manner, where the hash of each transaction is compared to the hash of all the transactions in the next block. Again, the one closest to that hash is the winning transaction. Since nobody will have enough information about all the transactions in a block as it is being created, nobody will be able to apply hashing power to find a self-rewarding transaction to slip into the previous block at the last second. 24 hours later, the dust will have settled on what transpired, and all will agree on who can write themselves a reward.

The nodes within the inner circle should be largely comprised of charitable non-profit entities. If the first node that a new transaction arrives at is the node that receives the largest portion of the block reward, then people will be able to support that charity by directing their new transactions to that node.

Attacks: Simulating the sequential signing of new transactions quickly would require individuals to hand over their private keys to someone who is inherently dishonest. Isolating a group of individual computers that only release a transaction when it's hash difference is low enough would be significantly slower. Either case would still require the collusion of multiple nodes from the inner circle. Still, after all this effort the only result would be ensuring that a particular version of the transaction was ultimately entered, not that it would be the final winning ticket.

Inner-circle nodes would have a higher standard for the speed that a transaction must be relayed at and much more difficulty back-dating a transaction without detection. More importantly, the regularity at which a node in the inner circle would exchange transactions would establish a clear history of which transactions it had at what time. That is, a node could not attempt to back-date a transaction and pass it along when it just finished passing along many transactions that were all newer. It would have had to have passed that transaction along at an earlier time if the transaction actually existed at that time. This can further be enforced by requiring a node in the inner circle to sign a statement of all known transactions at very regular intervals.

Enforcement will also be required of the rule that a node can only sign a transaction once and only pass a new transaction off to two other nodes (note that the inner circle will not be limited to only two). Proving that a node broke this rule would be as simple as providing three candidates for the same transaction that all have that node's signature. AI could easily be employed to scan the network and sniff these out. Any node could then broadcast a transaction which included this verifiable evidence and render that person ineligible to sign transactions or receive block rewards for some time. Though, they would still be able to create and receive transactions.

Without a limit on block size, the system could be subject to attack by flooding. However, if each node only accepts one newly created transaction from a given address and/or IP address, and only one newly created transaction from an unidentified address each minute, then the attacker would be very limited in their ability to flood the system.

Corporate Backing: The idea of corporate backing is analogous to the time when a nation's currency was backed by gold, and similar to Tether[3], which is backed by the US Dollar. In the case of Tether, for every one unit in circulation, there is supposed to be one US Dollar held in a bank account. Never mind what problems Tether may have with proving they have that money. The transaction fees are very high, and there's a whole gang of investors who expect a return. Those profits will come from the people who use Tether.

When a corporation issues store credit and receives the vast majority of that value in US Dollars, they are essentially taking a loan, and the people are "carrying the note." That is, they have received the money and, in return, given only a promise to provide some goods or services, at a later time. So, clearly, we cannot lend to them more than we believe they can pay back. That said, most people wouldn't doubt the ability of McDonald's to provide a million Big Macs in one day. In fact, a single day worth of revenues generated by the S&P 500 (just those 500 companies) would easily surpass the total value of Tether by an order of magnitude.

Furthermore, Tether is only worth whatever the US Dollar is worth. Likewise, if 200 Notes (♪200) will get you $200 worth of gift cards then the value of Notes will fluctuate with the value of the US Dollar. Ultimately, we will want to diverge from traditional gift cards and replace the backing with "commodities." Commodities is in quotes because I'm using the term very loosely. A 12oz cup of coffee from Starbucks isn't exactly a commodity, but there is plenty enough demand for it that it can serve that purpose in this system. Starbucks could change their US-Dollar price for a cup of coffee at any time, but the ones backing the Notes would already be paid for.

Auditing the outstanding Notes against available credit can be accomplished by each company having a page on their website that publishes their outstanding balance. This page should have an associated address for an API call that would allow an auditor to quickly gather all of those statements.

Transaction Fees: In US-Dollar-terms, transaction fees for Notes could be 0.1% with a minimum of one penny. So, it will cost a penny to send $10 or less, 10 cents to send $100, and $1 to send $1,000. There will be no maximum transaction fee. This will make transaction fees small, but affordable. With wide adoption, a significant amount of revenue will be provided to support the infrastructure and support charities by the pure volume of small, every-day, transactions. We would likely want to start out with the transaction fees higher than this. Anything less than 0.4% will compete with current debit cards. This is another parameter than can be adjusted over time.

Transaction fees for Anticoin, Beka, and gamma should be somewhat higher so that speculative investors, who may deal in large amounts of these, will contribute a little more; and to encourage the use of Notes for purchasing purposes, rather than one of these.

Unidentified Addresses: It is crucial that we, the free world, provide an anonymous and stable system to support the people living under oppressive regimes. One of the big claims of Bitcoin is that it's a system that cannot be shut down by a government. However, the value of Bitcoin falls dramatically every time a country moves to regulate it, or ban it outright. This puts a huge stress on the people who rely on Bitcoin (or other coins) for use as money, where their nation's currency has experienced hyper-inflation or collapsed altogether. We've already seen a number of regions where Bitcoin has become the de facto currency. These areas of the world would benefit greatly from a stable digital currency that their government could not control, as the infrastructure would largely be located outside of their borders.

On a technical note, unidentified nodes should be allowed to relay unidentified transactions with no consideration for the timestamp. In this way, transactions originating from within areas of the world without good connectivity, or oppressive regimes, will be able to reach an identified node with as much time as needed. The identified node will then timestamp the transaction and the transaction will go from there as though it were a new transaction created by that first identified node, still being eligible for the block reward (keeping in mind that the identified node is limited to one of these per block, and the first identified node can still only relay to two other nodes).

The Inner Circle: The hardware requirements for these nodes will be much higher. They will be required to store much more of the transaction history than other nodes. They will be required to supply data as requested by other nodes. They will be required to account for what transactions they were aware of and when. They will provide verification to the users that a transaction has been completed. As a large decentralized system within themselves, they will hold each other accountable and to a high standard. A high level of transparency should be demanded of these organizations, else they risk having transactions routed elsewhere. The people will vote with how they route their transactions, and these charities should compete to show that they make the most of what they are given. For the charitable non-profits, the needed hardware should be donated to them. This should provide a steady flow of revenue that they can rely on, and will do good things with.

Let's assume that this system could replace just 1% of the current debit card transactions each year: if we assume that volume to be somewhere around $2 trillion per year, and half of the transaction fees go to these nodes (the other half going to individual users), that would be roughly $800,000 per month going to these charities. If this system replaced half of the debit card usage, that would be around $41 million going to charity each month. Now, given that this is a value-stable coin, lenders would be able make loans in Notes without the risk associated with volatility. So, you can now have "credit card" accounts in

Notes and the total revenues from transaction fees are even greater. Of course, this is also how much wealth that would be distributed to the users, rather than the fat cats at the banks who are currently extracting much, much, more than this from the people. One might argue that it's worth trying this system just to remove that leech from our society.

To make a donation to help make all this happen:

Bitcoin: 114952J7QRveV3kNFxecNkTPRp7HqZwJzr

Ethereum: 0x4D599927Ef04bbC8bb6E55fA7d47f22f81165642

Lbry: bXWqpKW7k5j3gzsAU12ccQ2LkBGPTuQqug

Vertcoin: VdkYeB1Kiq1Za5PXAFFL7jxtWFnyU58sCd

References:

1. Nakamoto, Satoshi (31 October 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf

2. Johnson, Steven (16 January 2018). "Beyond the Bitcoin Bubble." https://mobile.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html

3. Tether : https://tether.to/