Safecoin: The Decentralised Network Token

Nick Lambert, Qi Ma and David Irvine

January 2015

Abstract

There are many examples of tokens (coins) being an effective mechanism for incentivising behaviour. These cases demonstrate the benefits of tokens in a wide variety of settings, but there is evidence that they are effective within a computer networking environment. This paper attempts to explain the reasoning behind safecoin, the digital token of the SAFE Network, a decentralised data and communications network. It is anticipated that the introduction of safecoin will incentivise behaviour that ensures the long term health of the network for all its users.

1 Token Economies

The use of tokens to incentivise behaviour is not novel and their use in multiple settings prove their utility. For example, token economy systems have been used to influence and guide behaviour in animals, prison populations, the military and education [12]. Doll et al. (2013) describe the nature of a token economy:

> "Within a token economy, tokens are most often a neutral stimulus in the form of points or tangible items that are awarded to economy participants for target behaviours."

In essence, tokens provide their holder with perceived economic or social benefit as a reward for acting out defined and desired actions. Bitcoin represents an excellent example of stimulating action (mining) through token reward. Its ability to eliminate double spending by harnessing the power of a distributed consensus network has given rise to a plethora of new digital currencies and assets. At the time of writing, there are currently 571 currencies listed on the leading cryptocurrency market capitalisation website [1].

However, it is the Bitcoin protocol and the additional features created by so called Bitcoin 2.0 technologies that are particularly interesting. The protocol enables additional features to be incorporated into the block chain (Bitcoin's immutable public ledger). These features include the ability for anyone to create digital assets or tokens that are cryptographically secured and inextricably tied to an ID on the network. These tokens can represent either ownership, or access to services.

The case for using tokens within a computer network is further strengthened by technologies that were restricted from reaching their potential in the absence of any incentivisation mechanism.

One such example is TOR, software that provides user anonymity by redirecting Internet traffic through a series of relays run by volunteers, who contribute their own computing resources to the TOR network. Current metrics from the network report that around 6500 relays are in operation while there are in excess of 2,000,000 directly connected users [3, 4]. In order that the network continues to expand, the project recognises that the current volunteer approach is not sufficient and incentives to run relays are required. One of the suggested solutions is TorCoin, a incentivisation mechanism that attempts to compensate users running relays. It is proposed that TorCoin will enable relays to mine for TorCoins once they have successfully trans-

ferred a batch of data packets across the network as a reward for providing bandwidth to the Tor network [5].

1.1 The SAFE Network

The SAFE (Secure Access For Everyone) Network, is a P2P decentralised data and communications network designed and built by MaidSafe.net and is currently in implementation phase [6]. The network will compliment all existing centralised web services and data centres with a secure and anonymous network comprised of the spare computing resources of its users. It is anticipated that this new network will provide a more secure and private experience, whilst achieving higher performance as the network reaches critical mass.

2 Safecoin

The requirement of users to contribute is an unmistakable part of any P2P network and the implementation of incentives is essential to ensure its health. The introduction of safecoin, the cryptographic token of the SAFE Network, is an approach designed to encourage a number of different users and contributors to the network.

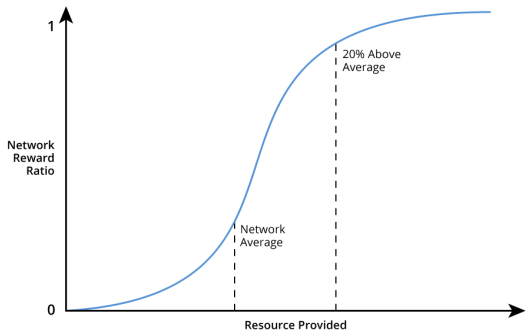
Safecoins can only exist on SAFE and it's distribution is handled entirely by the network on a per use basis. It is anticipated that 4.3 billion coins will be produced during the life of the network. Each safecoin has it's own unique identity and they are required to access services on the Safe Network. The type of services that will be available will depend on those being developed by third party developers. It is worth noting that any type of web service currently possible on the existing centralised Internet is possible on the SAFE Network. The cost for these services will be set by the service provider and it is anticipated that as more and more competing apps are developed that market forces will maintain prices at economic levels.

3 Obtaining Safecoin

Safecoin can be obtained through; farming, assisting with the maintenance of the underlying code, creating applications or by purchasing them.

Farming is a process akin to bitcoin mining, whereby users provide resource (storage space, CPU and bandwidth) to the network. When each user creates their credentials, they will set up a safecoin wallet via their SAFE Network client and this wallet identity will be cryptographically linked to their account. As figure 1 demonstrates, the safecoin earning algorithm is based on a Sigmoid curve, in that all vaults earn, slowly at first and the rate increases as the farmer stores up to the network average. The earning rate also takes into account the rank of the vault, a process whereby the network scores the usefulness of each node from 0 (being the worst) to 1 (the best). The safecoin farming rate is ultimately the result of the network rate, a balance of the demand and supply on the network, multiplied by the vault rank. The network rate will start to level at 20% above average, thus discouraging massive vaults which would bring centralisation to the network's farming process. Safecoin is allocated to them by the network and is paid to the successful node as data is retrieved from it (GETS), as opposed to when it is stored (PUTS).

FIG 1. Predicted Safecoin Farming Speed



The network automatically increases farming rewards as space is required and reduces them

as space becomes abundant. Data is evenly distributed on the network and therefore farmers looking to maximise their earnings may do so by running several average performance nodes rather than one high specification node.

3.1 Proof of Resource

Utilising a process called Proof of Resource (POR), the network is able to continually validate who and what is providing resource to it in a mathematically verifiable way. The network does this by attempting to store and retrieve data chunks onto/from its nodes. The ability for a node to carry out these actions will be determined by a combination of its CPU speed, bandwidth availability, unused storage capacity and on-line time. The SAFE Network uses a zero knowledge proof mechanism, where the network does not require to know the content of any data to be checked, but must know the data is in fact held and held in a manner that is accurate. Nodes that are either unreliable or are trying to game the network, by removing previously provided resource, are de ranked by the network if the node is unable to serve a chunk of data.

3.2 Core Development and Building Applications

It is also possible for core developers to earn safecoin by fixing bugs and developing new features for the underlying network. At the time of writing, this process has not yet been finalised. It is possible that code bounties will be raised by the core development team in conjunction with the SAFE project community. There are a number of existing platforms that facilitate the advertisement and management of code bounties, such as Bountysource and Bountify [7, 8].

People or companies building applications on the SAFE Network will also be able to earn safecoins. As they create and release new applications, they will code their SAFE wallet address into their application. Based on how much the application is used, the network will pay safecoins to the safecoin wallet address of the app creator. This provides a built in revenue stream for app developers, one that is directly proportional to how successful their application is.

3.3 Decentralised Exchanges

It will also be possible to buy safecoin. It is anticipated that these purchases will be made from decentralised peer to peer exchanges that will be built by third party developers. These exchanges will serve as platforms, enabling a buyer and seller to trade directly, potentially using multi signature (3 or more private keys are associated with an address, a majority must sign to make the transaction valid) technology to manage the transaction. It would also be possible to have centralised exchanges.

Exchanges are essential to the liquidity of safecoin as they ensure that people unwilling or unable (as they are using a mobile device) can still gain access to network services. Additionally, exchanges will also enable those earning safecoins to convert them into cash or into other cryptocurrencies.

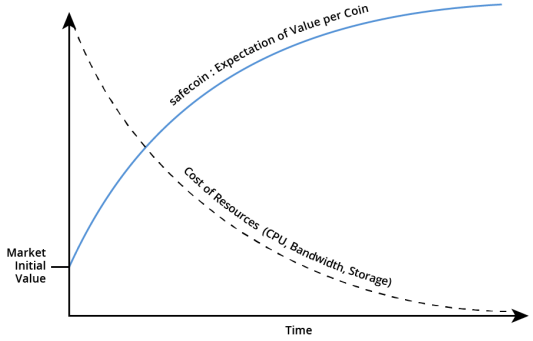
4 The Price of Safecoin

As with other digital coins, the exchange or purchase price of safecoin will be set by the market. This is a price established through the combination of supply and demand. As this paper has already described, the number of safecoins in circulation will increase based on network use. Almost all early safecoin holders will be farmers with this supply of resource creating both liquidity and distribution of wealth. It is anticipated that almost all users will possess at least a few safecoins in their wallet. Users may trade their safecoin for services on the network, or for cash (or another digital currency) using an exchange. The ratio of safecoin being saved (left in new wallets) versus the ratio being issued to Farmers will produce a price point. This point will be the market value of safecoin.

It is anticipated that as the number of applications on the network grows, the utility of safecoin will increase, helping to drive the price of the coin overtime. This, coupled with the increase supply of safecoin, will also potentially increase the stability of the coin. Safecoins will not have a finite quantity, as after the initial 4.3 billion are produced, a small percentage (dependent on usage) will be recycled in order to incentivise the storage of new data.

The number of resources or services it is possible to buy will not be linked to the exchange price. The amount of storage, for example, that each safecoin buys over time will increase, otherwise the network resources could become very expensive if allowed to rise in line with the exchange price. This is highlighted in figure 2.

FIG 2. Resources and Currency

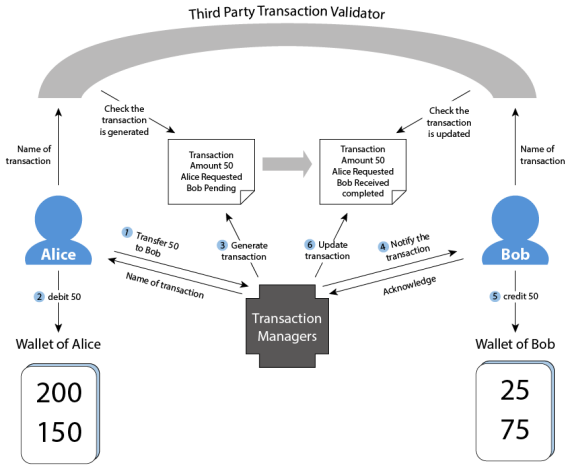


5 The Transaction Manager

Unlike Bitcoin, the SAFE Network does not use a block chain to manage ownership of coins. Conversely, the SAFE Network's Transaction Managers are unchained, meaning that only the past and current coin owner is known. It is helpful to think of safecoin as digital cash in this respect, providing safecoin users with more anonymity than they experience with bitcoin.

The Transaction Manager is a persona or role carried out by the SAFE Network's vaults. Vaults store data on a Farmer's computer and consist of a series of processes or roles that vary from managing the storage of data, managing other vaults and more importantly in this case, managing the processing and completion of transactions. The entire SAFE Network reaches decisions based on consensus of close groups of 32 nodes and the transaction manager is the trusted group closest to any given transaction identity. These close groups are chosen by the network based on the closeness of their IDs to the ID of the safecoin. Closeness in this respect refers to the XOR distance as opposed to geographical closeness [9].

FIG 3. Safecoin Transfer Mechanism



One of the major problems any virtual currency or coin must overcome is the ability to avoid double spending. Within the SAFE Network, transfer of data, safecoin included, is atomic, using a cryptographic signature to demonstrate that the last person who owned the safecoin has signed the coin over to the current owner. When the current owner spends the coin, they ask the network (their close group of 32) to accept a signed message transferring ownership to the new owner. This process is highlighted in figure 3. The knowledge of coin ownership (each has their own unique ID) is kept in several close groups and each group must agree upon and reach consensus (28 of 32) on the transfer of ownership before the transaction is processed and the ownership of the coin is transferred.

6 Minting safecoin

The transaction model, described in Section 5, enables safecoin ownership to be transferred. However, it will be possible, after the SAFE Network is launched, to mint safecoin in a more physical and anonymous way.

Minting safecoin can be achieved by the network enabling the registration of a special transaction with the transaction managers, that facilitates transfer of the ownship of the coin to any user that acknowledges the transaction. The minting process effectively removes the requirement for the transaction validation step from the Transaction Manager. When Alice wants to mint safecoin, she sends a request to Transaction Managers with a special request to transfer the coin(s) to anyone. The Transaction Managers, once they have confirmed by consensus that Alice is the current owner, will then generate the transaction. Once Alice receives the transaction name from the network, she can store it on an external storage device, such as a usb drive, together with a special validation signature which has been used as a salt when generating the previous sent request[1]. This salt is used to prevent Transaction Managers themselves trying to acknowledge the transaction to steal the coin.

When Bob receives the minted safecoin and decides he would like to spend them, he reads the transaction name and the validation signature from the storage device and then sends an acknowledgement to the network. Once the Transaction Managers receive the acknowledgement, the pre-generated transaction will be updated, thus completing the transfer of ownership of that coin(s) from Alice to Bob.

The benefit of using safecoin in this way is a reduction in the complexity of the transaction by removing the acknowledgement procedure, making minted safecoin similar to a cash note. It also means that Alice, in this case, no longer needs to worry about keeping her private key safe as the transaction has been pre generated. Minted safecoin is also more anonymous, eliminating the need to store safecoins only in a digital wallet that can be compromised should an adversory obtain access to a users SAFE Network credentials. However, there is risk that after the transfer transaction has been registered, if the owner loses the external storage device containing the safecoin(s), anyone will be able to claim ownership. However, this is no greater than the risk anyone undertakes when withdrawing cash from a bank, convenience comes at the price of security.

[1] A salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase

7 The Economics of Safecoin

Unlike many cryptocurrencies, whose creation is not backed by anything, the distribution of safecoin is backed by data. The generation of safecoin is entirely network led and they are only created as the network is used and data retrieved from network nodes. This activity is in contrast to currencies like bitcoin, whose coin distribution is arbitrarily set to 10 minute blocks. This means that if the SAFE Network is in great demand a large volume of safecoins will be created, while low demand will lead to minimal coins being generated. This demand generation cycle has a desirable affect in that it should ensure no over supply of safecoins, which may potentially lead to a unit price decrease. This is not to say that the price of safecoin will not be volatile, the comparatively small coin supply (Bitcoin's market capitalisation is currently $5.2 billion, whereas the US Dollar has around $17 trillion (M4 definition - notes, coins and bank accounts) in circulation) of cryptocurrencies makes this inevitable. However, it may provide greater stability in the long term [11].

In many respects, the underlying economics of safecoin can be directly compared to Cap and Trade Economics, a strategy utilised by governments in an attempt to limit the amount of greenhouse (GHG) emitted by private enterprises [16]. In the same way that the Cap and Trade system limits the overall emissions, en-

abling companies to pay for releasing GHGs, the safecoin cap will be influenced by the network average resources, with safecoins being traded to reach the market price.

Furthermore, current supply of traditional FIAT currencies has become elastic, with central banks of many nations engaging in quantitative easing, effectively printing money to ensure greater supply. Unfortunately this can have many negative consequences as printing money does not solve the underlying economic problems and can potentially lead to increases in inflation [2]. These drawbacks have led some economists to start calling for a return to the gold standard, a situation where supply of money was linked to the supply of gold, known to be valuable and very difficult to counterfeit [18].

With coin generation on the SAFE Network being directly linked to network use, the issuance of safecoins will be linked to supply and demand for data services. Data is valuable and is considered by some as becoming a commodity in its own right. The World Economic Forum has established data as an asset class [13]. The realisation of data having significant monetary value is also born out by recent valuations in technology companies, many of whom are not sustainable [17]. Having a network generated digital currency inextricably linked to a valuable commodity, has the potential for a stable environment, one that as the money supply increases, has the potential to be more resistant to price fluctuations.

8 A Revenue Model for a New Internet

In addition to incentivising user behaviour, safecoin may also provide an alternative revenue source for the Internet, in the shape of micro payments. It is possible to implement safecoin without transaction costs (although these could be added to aid security[2]) and high divisibility (coins are valued at $0.05 at the time of writing (Jan 2015) and have the potential to be divided up to 4.3 billion times) make them well suited to very low value transactions. Furthermore, the SAFE Networks ability to enable an unlimited number of transactions with confirmations at network speed equips it well for micro payments.

Micro payments are one of many ways to replace the current methods of funding today's centralised Internet, typically this is achieved through advertising. Large Internet companies, such as Google and Facebook, earn the vast majority of their revenue (91% and 89% respectively) by selling adverts at their users [15, 14]. This model has been criticised as it not only promotes increasing surveillance of user data, as advertisers require to know more and more about us, but also removes the rewards away from content creators [10].

It would be technically feasible, using safecoin on the SAFE Network, to pay for films on a cost per frame basis, with the user only paying for what they watch. This amount would automatically be deducted from the viewers safecoin wallet as they watch. A similar model could also be utilised for music, or for bloggers, with individual articles paid for via a paywall or on a voluntary basis. The decision about how to structure payment for their work would reside with the copyright owner. The SAFE Network enables an optional watermarking feature that serves to inform the user the identity of the content creator, however, this should not be confused with a DRM mechanism.

9 Conclusion

There are several examples of advanced technologies that did not reach their full potential as their incentives were poorly aligned. Tokens or coins have been used in a wide vareity of settings, including decentralised computer networks, to mo-

[2] An adversory could process a large number of transaction requests to the network in an attempt to overload it, the addition of a very small transaction fee may mitigate this risk.

tivate, influence and guide desired behaviour. Bitcoin in particular has shown that by properly aligning incentives, the health of the network is sufficiently increased as miners are compensated for providing their hashing power to the block chain.

It is anticipated that safecoin will provide sufficient incentives to ensure the long term health of the SAFE Network, encouraging end users to provide their resource, while enticing both application and core developers to assist in the continued growth of the network. It is hoped that by tying together supply and demand for data services, the SAFE Network economy will retain a natural balancing mechanism that increases the reward for space as it is required and reduces the reward when it is not.

Acknowledgment

Many thanks to the SAFE Network community, and in particular Yanick Vézina, for helping to proof read this paper.

[1] Crypto-currency market capitalizations. URL https://coinmarketcap.com/all/.

[2] Ecr research web page, November 2014. URL http://www.ecrresearch.com/world-economy/dangers-and-drawbacks-quantitative-easing.

[3] Tor metrics — relays and bridges in the network, November 2014. URL https://metrics.torproject.org/networksize.html.

[4] Tor metrics — direct users by country, November 2014. URL https://metrics.torproject.org/userstats-relay-country.html.

[5] Tor incentives roundup, November 2014. URL https://blog.torproject.org/blog/tor-incentives-research-roundup-goldstar-par-braids-lira-tears-and-torcoin.

[6] Maidsafe wikipedia, November 2014. URL http://en.wikipedia.org/wiki/MaidSafe.

[7] Bounty source web page, November 2014. URL https://www.bountysource.com/.

[8] Bountify web page, November 2014. URL https://bountify.co/.

[9] Kademlia wikipedia page, January 2015. URL http://en.wikipedia.org/wiki/Kademlia.

[10] The Atlantic. The internet's original sin, November 2014. URL http://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/.

[11] John Aziz. Does the federal reserve really control the money supply?, December 2014. URL http://theweek.com/article/index/244899/does-the-federal-reserve-really-control-the-money-supply.

[12] Anjali Barretto Christopher Doll, T. F. McLaughlin. The token economy: A recent review and evaluation, July 2013. URL http://www.insikapub.com/Vol-02/No-01/12IJBAS(2)(1).pdf.

[13] World Economic Forum. Personal data: The emergence of a new asset class, November 2014. URL http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

[14] Facebook Inc. Facebook reports fourth quarter and full year 2013 results, November 2014. URL http://investor.fb.com/releasedetail.cfm?ReleaseID=821954.

[15] Google Inc. 2013 financial tables, November 2014. URL https://investor.google.com/financial/2013/tables.html.

[16] Paul Krugman. The textbook economics of cap-and-trade, December 2014. URL http://krugman.blogs.nytimes.com/2009/09/27/the-textbook-economics-of-cap-and-trade/?_r=0.

[17] Joe McCann. Data is the most valuable commodity on earth, November 2014. URL http://subprint.com/blog/data-is-the-most-valuable-commodity-on-earth.

[18] BBC News Web Page. Gold v paper money, November 2014. URL http://www.bbc.co.uk/news/business-18644230.