Version 1.4

MaidSafe.net announces project SAFE to the community

1. Introduction

Existing Internet infrastructure is increasingly unable to cope with the demands placed on it by over 2.4 billion connected people, a number that is predicted to grow to 3.6 billion by 2017. Today's architecture, where central intermediaries (servers) store and provide access to data is expensive and inefficient. Data centres use between 1.1% and 1.5% of the world's electricity (growing at 60% per annum) and represent significant expenditure for data centre owners, providers and businesses, who all have to pay to host user data and maintain the infrastructure. Security of user data has proven to be nearly impossible in today's networks with almost weekly reports of ID and password thefts.

To overcome these challenges a fresh approach is required, a solution that removes these inordinately expensive central points of failure, data leakage and bottlenecks. By developing a fully decentralised replacement for all Internet based services, Secure Access For Everyone (SAFE) will ensure the decentralised Internet is a reality, enabling:

- Autonomous handling of structured and unstructured data types
- Private and secure communications
- Data shared at the filesystem level worldwide, no need for http, smtp, ftp etc.
- Highly encrypted and private data at rest and in transit
- The ability for people to self-authenticate onto the network and join anonymously
- A network resistant to man-in-the-middle attacks or IP address identification
- A network that requires no administrators or human intervention of any kind
- No requirement for forward planning using infrastructure that automatically configures around its users in real-time (no data centres)
- A highly usable and free API that enables a plethora of developers to create the next wave of secure applications not currently possible with today's centralised architecture
- An underlying crypto currency called safecoin that will incentivise all actors in this ecosystem

SAFE is the culmination of 8 years of effort by MaidSafe.net and the continued and growing number of project developers. These developers will include MaidSafe.net and many other decentralised Internet application developers. Please see http://maidsafe.net for an introduction to the technology as well

as https://github.com/maidsafe/MaidSafe/wiki for access to project documentation and code.

The inclusion of a crypto currency is not new to the maidsafe core design. It is a logical step included in the initial design many years ago (2006). Importantly, **this proposal creates no founders pool or shares** but, incentivises funders, developers, users and satisfies existing investors in MaidSafe. This allows MaidSafe to clearly show this network truly belongs to us all and in perpetuity. It is a hugely important step to ensure the network is widely used and worked on by many hundreds of developers who can see the potential for a fully secured, unowned and decentralised Internet. The proposed crowd sale will seed the network, expand the developer base worldwide and push the whole proposition to the wider community in a manner that is extremely clear and logical.

MaidSafe Brief History

Formed in February 2006 with the intent to decentralise the Internet, the 14-strong team is based in Troon, Scotland. To reach this project stage, MaidSafe has taken investment from close friends and family, as well as supporters and Angel Investors. Further backing and supporters are required to push the platform out to the world and to incentivise network adoption.

It is also worth noting that the founder allocated all of his shares in MaidSafe to an employee share scheme (around 28%) and almost 50% of the business to a not for profit foundation. The MaidSafe Foundation will be a key player in this proposal and exists to ensure fair distribution of wealth, while helping to foster education and innovation. Based in Scotland, the laws and regulations surrounding such organisations ensure there can be no profit motive for trustees or members of the Foundation. This is an important model for managing many aspects of a decentralised project such as SAFE.

2. Project Status

At this time, MaidSafe has completed the foundation libraries and associated code. The API is being finalised in conjunction with application developers to ensure ease of use and this is being supplemented by examples and demonstrations. The network is preparing to go into wide scale testing and MaidSafe are hoping to implement this during the announcement of the funding round. At present, developers can download and run networks for test purposes.

Full public launch of the network will take place in the very near future. Earning capabilities will be added to nodes over a period of several weeks after the initial network testing is carried out and any issues and critical bugs are resolved. MaidSafe

will be hosting weekly public Google Hangouts over this period to answer any questions and assist application developers first hand.

3. Proof Of Resource

In many cryptocurrencies and decentralised networks a proof of something is required to allow the network to validate actions or services via a mathematically verifiable mechanism. In bitcoin this is achieved by a proof of work. This is essentially a hashing technique that requires significant (and growing) computer power to achieve. This technique allows bitcoin to confirm transactions and reward 'miners' with a block of coins randomly.

The SAFE network can validate nodes and their value to the network in a very accurate and cryptographically secure manner. The SAFE project will use this to create a **proof of resource** (see Appendix) which has some significant advantages. The resource in question is a computer's ability to store data chunks, which depends on CPU speed, bandwidth, disk space and on-line time, amongst others. This allows the proof to be a useful, measurable and an immediately verifiable entity. Proof of resource is a very efficient mechanism as its cost is very minimal.

Additionally, as a fully decentralised network, the SAFE approach allows transactions to be made and confirmed at network speed (under a second in some cases). This is due to a distributed Transaction Manager as opposed to a blockchain. In the SAFE network, a transaction management system can be linked or not. Bitcoin uses a linked blockchain (the chain term) that allows traversal of all transactions from the network start. SAFE has chosen an unlinked approach to the blockchain. Each user's account information is held by the group of nodes closest to it (according to the XOR address distance). The Transaction Manager only holds a temporary receipt object during the transaction procedure among users. This temporary receipt can be stored permanently allowing proof of the transaction to be maintained or destroyed immediately after the transaction is completed, leaving no trace on the network. In addition to allowing instant transfers of coins, this mechanism also allows an escrow model (a third party acts as moderator to resolve the payment dispute). This escrow mechanism is a core component of the currency.

4. Safecoin

For technical implementation details see the Appendix.

History has demonstrated that having the most cutting-edge technology does not in itself guarantee wide scale use. To ensure the SAFE network is fully and efficiently utilised, a token-based scheme is proposed where all stakeholder groups have the ability to earn these tokens (safecoins) in a manner that is both fair and equitable.

Safecoin (http://www.safecoin.io) may be earned, traded or purchased. The whole SAFE network is configured and designed to incentivise all parts of the community. The incentivisation is a critical component of a fully decentralised Internet. The MaidSafe code base is a part of this process, other application developers will add to this and be incentivised, users will be rewarded with safecoin for allowing their computer to be part of the network and funders who act as the catalyst will be able to buy safecoin (via intermediary MaidSafeCoin) directly, prior to the full network launch. This will allow sufficient resource to be made available to launch the network worldwide and application developers to release apps of significant value to us all. This project is simply the beginning of a new Internet, one that we all own and nobody controls, this is the "Internet sans frontieres!"

In essence, safecoin is a fair and transparent way of incentivising developers, backers and end users to use SAFE. As users trade their proof of resource, they are still earning safecoin as they are continuing to provide valuable network resources. Application developers can now use safecoin as their revenue model, enabling them to concentrate on providing amazing applications and not worry about revenue models and streams. Supporters can help to back a network that is focussed on providing common good while achieving returns that reward their willingness to take financial risk.

It is proposed that safecoin will have a predictable cap (2^{32}) with a value that is determined solely by the market. Safecoin will be a virtual currency with SAFE being used to complete transactions.

5. Project Proposition

Many of today's centralised systems use advertising to monetise their existence, or actually charge for resources that are in fact exponentially decreasing in value (CPU, disk space, bandwidth, etc.). MaidSafe proposes an approach that should not only make resources cheaper, but should also provide a crypto currency (safecoin) that will increase in value, facilitating exchange both on and off the SAFE network.

This paper demonstrates the creation of a fixed number of coins over time 2^{32} (~4 billion), which can be further subdivided to facilitate trading. This approach increases reuse of the coins, further incentivising miners. This proof of resource will represent disk space, CPU and bandwidth involved in storing shards of information. These resources will increase over time, creating a much desired increasing value for safecoin holders, while delivering exponential decreases in the cost of resources. The proof of resource algorithm will over time account for additional resources, such as proof of bandwidth, proof of CPU processing, etc.

In essence, this proposal will ensure computing resources are shared amongst all users at the lowest possible cost. MaidSafe believes this approach will provide the most cost-effective and efficient computing platform in the world, realising the company's vision of an Internet for everyone, free from spying, privacy erosion and data loss.

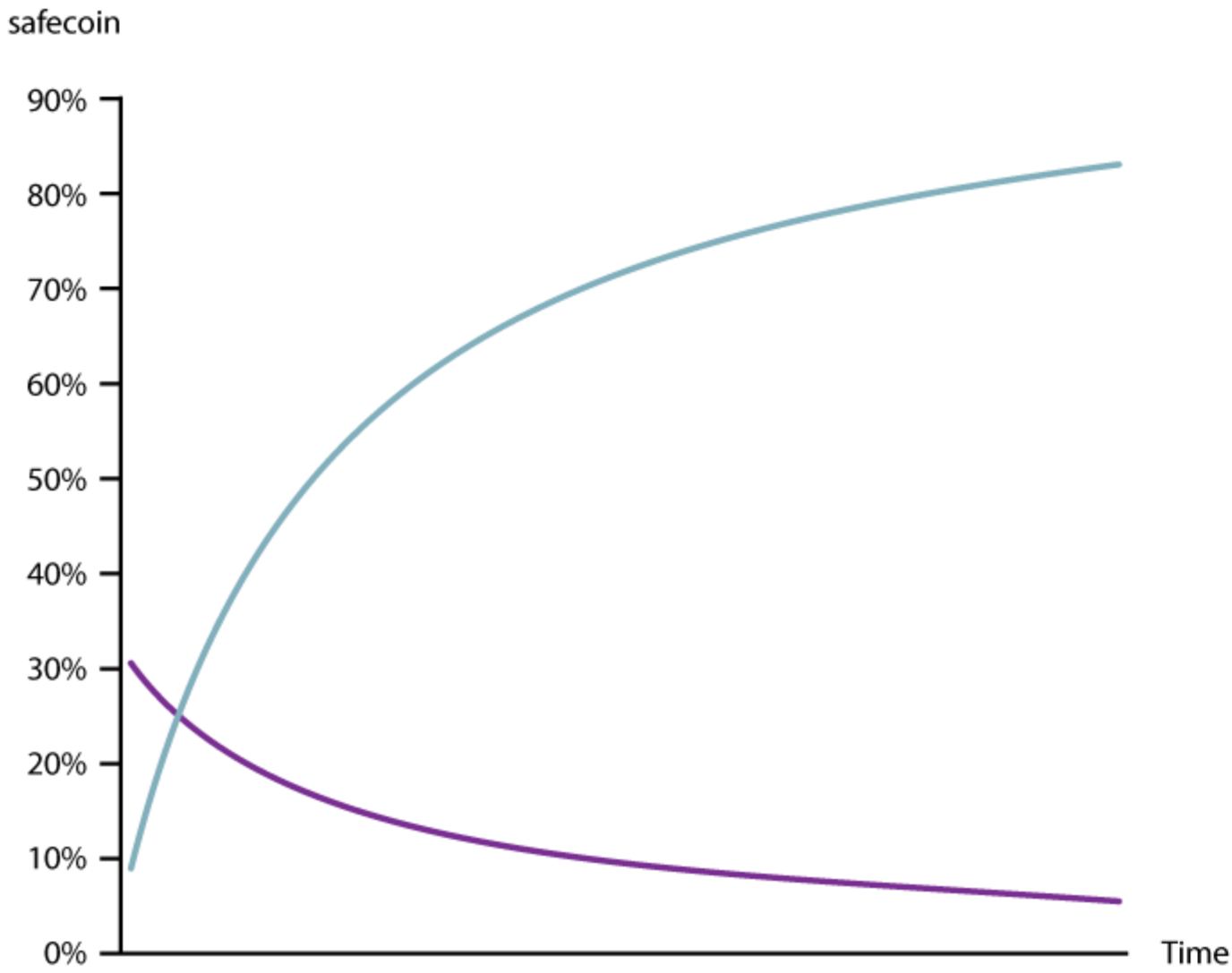
6. Incentivisation and Coin Distribution

The SAFE network is fully inclusive and enables everyone to get involved and become a part of the project, whether a supporter, end user, backer or developer.

End Users

As end users join the SAFE network anonymously, they will start a vault (a data storage and management location). This vault will add itself automatically to the network and start providing resources. These vaults require no setup and administration, they are a simple download and install. The network is designed to self-manage these resources and reward these 'farmers'(vault owners) accordingly in a random fashion, uniformly distributed across the network, thereby securing the network's data.

The earning speed is based on the storage space contributed to and verified by the network. For details of the calculation, please see Appendix 'Token System on MaidSafe Network'. Note the developer and crowd sale lines are obscured by the IP pool.



If people were to try and game the system by providing farmers to store data and then switch them off, they will simply remove their ability to earn. At some time in the future it is envisaged the network will be able to detect such data and remove it from the network. In the meantime, this kind of attack is costly to the perpetrators as their earning potential is adversely affected by their actions. This strategy also allows the network to arbitrate and manage resources mathematically and reduces the effects of the tragedy of the commons type deficiencies, requiring users to provide resources in an honest manner.

Unlike many currencies, the distribution of safecoin is backed by information. This information represents the world's data and grows exponentially. Unlike gold, which only increases at circa 1.5% per annum, the quantity of safecoin will initially burgeon. This is akin to the California gold rush, where the quantity of gold grew quickly with enthusiastic miners. In safecoin this is mirrored by the network building to the stage

where it is protecting all of the world’s data. During that time the mining frequency will be exponentially decreasing.

When all of the world’s data is secured, mining will naturally slow to a pace that just keeps up with the fungibility of the whole system and the increased resources under it's protection. This will be possible as people trade safecoin for network resources. These resources are initially data, but will likely grow to be bandwidth (to allow satellite and mesh networks) and processing power (for decentralised mass calculation work) amongst others.

The number of resources will be calculated by the network dynamically and in perpetuity. The value of individual safecoin will be market determined and this is an important notion. The number of coins in circulation is network led and the individual value is market driven. As people trade safecoin for goods and services this market value will be realised.

MaidSafe's figures forecast an estimated mining rate over time, this forecast is completely dependent on a number of assumptions including; speed of network adoption and the amount of data stored…etc. MaidSafe does not see this as an obstacle, rather a huge opportunity. Competing in today’s market using the SAFE proposition is an enormous advantage to developers (many of which are described in this paper) and to do so in an open network which is owned by no one is very compelling.

Backers

To allow distributed ownership of the network, MaidSafe will allocate 30% of the tokens on day 1. The coins allocated are fungible, particularly in the form of resources as backers reach their required returns or simply trade the coins. This allocation of safecoin will allow two separate entities to be rewarded:

a: Current MaidSafe investors/shareholders.

The current MaidSafe investors have invested for the past 8 years with complete faith and a strong desire to make a difference. These investors have been the very reason the technology is now developed and this proposal possible. Five percent of the safecoin issue will be laid aside for these investors and as safecoin is increasing in value, current investors will be able to swap their shareholding in MaidSafe.net for the coins. **The coins will be held by the MaidSafe Foundation for issuance at the request of each shareholder.** The safecoin here will be allocated at the point miners are introduced onto the network.

This allows investors to be rewarded for their help over the years and will also allow MaidSafe equity to return to being owned completely by the Foundation. This approach will ensure that MaidSafe as a company is not in charge of the SAFE

network and shareholders are treated with the respect they deserve. When they are allocated safecoin they can hold these as any backer will today.

b: Crowd Sale Participants

A crowd sale will enable everyone worldwide to seed and be a part of the SAFE project. This will last until MaidSafeCoin are sold out (circa $8million). If the all coins are not sold the event will end after 30 days. The crowd sale will enable a direct purchase up to ten percent of MaidSafeCoin. It is anticipated that soon after the crowd sale commences, MaidSafeCoin will be listed on exchanges and will be tradable, right up to the release of safecoin.

These crowd sale participants will be buying MaidSafeCoin, an intermediary coin that will be swapped on a 1:1 ratio for safecoin once the full SAFE network is launched. Purchases will be recorded in the bitcoin blockchain via the Master protocol suite. MaidSafe will be running a test net initially and will potentially need to bring the network up and down during testing. An intermediary coin is required as coins may be destroyed from time to time as the network is restarted

Particpants will be able to purchase MaidSafeCoins using either bitcoin or mastercoin with payments being made via a website: BuySafeCoins.com to the MaidSafe Foundations exodus address. This address will be published on both the crowd sale website, MaidSafe's own site and also the SAFE network site (www.safecoin.io) prior to the commencement of the crowd sale. Once funds have been received MaidSafeCoins will be automatically generated and will be sent to participants mastercoin wallet. If a participant does not already have one the wallets can be downloaded for free from: http://www.mastercoinwallets.org/. At present only Windows wallets are available, however a web wallet will be available soon.

The MaidSafe coins purchased will be credited as safecoins to the participants safecoin wallets as soon as the full network is launched and farmers appear online. This allows immediate benefit to the project and will demonstrate the desire of all backers to decentralise the Internet, enabling a plethora of new and exciting companies to emerge and provide true value at minimal cost.

Funds raised from this round will be held by the MaidSafe Foundation and will be utilised to house the MaidSafe core team and provide financial assistance for a period of three years. It is assumed that after three years, the core MaidSafe team will have grown significantly and introduced further innovations into the space. There is no founders pool and this is a very important aspect of this project. No team should be rewarded by safecoin who have not provided value in some respect.

Developers

MaidSafe proposes to reward developers in 2 ways. Firstly, safecoin can be earned by contributing bug fixes and code that are accepted into the master branch of the SAFE codebase. Secondly, developers that create apps that do not charge end users and are of benefit to the community will also be rewarded. The issuance mechanism for both groups will come via the MaidSafe Foundation. MaidSafe the company will also generate coins by providing P.O.R when they seed the network with several hundred nodes during final platform testing. This seeding stage will be public and others are welcome to contribute resources. It should be acknowledged that until the network is declared 'ready for general use' that the coins may be destroyed from time to time and the network restarted. There will be no private or hidden seeding of the network and announcements will be made at a minimum via the MaidSafe mailing list during these events.

15% of all safecoin earned will be allocated to the developer pool. This will ensure the developer community is highly motivated and rewarded for providing free-to-use applications and improvements to the underlying codebase that utilise safecoin as their revenue model. It is possible that 10% of these coins maybe recycled if a an idea of automated developer awards comes to fruition.

5% of the developer pool coins will be given to the core developement team. Without their hard work and dedication the SAFE network would simply not have been possible. A further $100k of safecoin will be allocated from the developer pool to those who gave their time and commitment to develop this white paper and for early project coordination. Without the efforts and expertise of these individuals this paper would not be as comprehensive and would have taken far longer to produce.

It is proposed that code commits and third party projects be chosen by polling the MaidSafe developer mailing list and payments will be allocated from the Foundation to successful projects/code enhancements.

The mining speed per vault is *projected* as:

Time	Number of coins
first day	800
first week	1800
first month	4000

Time	Number of coins
first year	19000

The size of the seeding network is estimated to be around 2,000 vaults, that being the case it is projected that the first month income will be around 8M coins and 38M in total during the first year.

Third party developers will also be incentivised outside of the token scheme. Choosing to develop their applications and businesses on the SAFE network will, when the network reaches critical mass, enable them to outperform all incumbents, while providing privacy and security to all their users. The network code is free to use and there are no upfront charges for API keys or developer programmes. Developers' customer acquisition costs will be a fraction of the levels compared to traditional architecture due to the lack of infrastructure costs.

7. SAFE Crowd Sale

The crowd sale will be operated as follows:

- A fixed number of MaidSafeCoin will be issued during the crowd sale
- The sale will last until all coins have been purchased (circa $8million) or 30 days has passed, whatever happens first
- Within that period, public funds in the form of bitcoin and mastercoin can be sent to exodus bitcoin address via www.BuySafeCoins.com
- Each participant will purchase an intermediary coin, MaidSafeCoin
- A quantity of 429,496,729 coins will be available for purchase, this equates to 10% of all safecoins
- Early buyer incentives are in place to reward early participation (see chart below)
- It is estimated that participants will purchase 17,000 MaidSafeCoins for 1 bitcoin
- All purchases and transctions will be recorded on the Bitcoin block chain via the Mastercoin protocol
- The deposit of funds in the exodus address will auto generate the appropriate level of MaidSafeCoins, they will be reciepted in the participants mastercoin wallet
- Once the full network is launched these will be traded on a 1:1 basis for safecoin
- Each participants safecoin wallet will be credited as the full network is launched and they create their SAFE network accounts
- In the event that not all coins are sold, the remaining coins will be burned
- All details are available at www.safecoin.io

Early buyer incentive

Time	% Bonus
week 1	40%
week 2	30%
week 3	20%
week 4	10%

After this stage is complete there will be no further opportunities of this sort available on the SAFE network with safecoin.

The incentivisation of decentralised application projects that are funded via safecoin should also ensure a very active participation into a very powerful ecosystem with a pre-prepared revenue model. It is also thought this model will encourage a more decentralised and distributed pool of backers. This model is very much in line with MaidSafe's core values and decentralisation in general, using logic and fairness with as few 'magic' numbers as possible.

It is interesting to note this crowd sale does not hold any safecoins for the founders; **no founders' pool is involved.**MaidSafe will work with the funds raised and commit to continue to develop the internal library code to earn coins in the future, provided the code is accepted by the community (as per the acceptance criteria agreed on at that time by the mailing list participants and Foundation board). It is also the founders' belief that if MaidSafe or any other group do not continue to innovate, they should not continue to strive as businesses. This allows the community to always be presented with the most efficient code and advancements to the system regardless of which entity makes those advances possible.

In this manner, **MaidSafe will 'eat at the same table' as all other developers in the SAFE network** and all application providers that will earn revenues via the safecoin model. It is envisaged that this approach is a very fresh and healthy model with the appropriate levels of risk and reward for all stakeholders.

8. The MaidSafe Foundation

The MaidSafe Foundation will initially:

- Hold and distribute safecoin for developer pools
- Manage issuance of MaidSafeCoin to funders and existing investors

- Hold all patents and use safecoin to pay for the upkeep and further patents for all projects (until this sphere cannot be litigated against, the MaidSafe Foundation will act as the holder of defensive patents, of which there is already a considerable worldwide portfolio, to protect the decentralised Internet).
- House the MaidSafe team in an HQ and provide funding for independent development pods, worldwide
- Provide finances for the core team and development pods for a period of at least three years (we have already started discussions with a person in San Francisco to begin this process immediately on funding, we hope to have at least six such pods, worldwide in year one)

No further actions can be taken by the Foundation, unless the authority is requested by the community to add additional objectives to this list.

Board members will be appointed from the community via polling. This board should be selected from as wide a catchment as possible and include 3rd party developers, core developers and members of other decentralised projects (e.g. Mastercoin, Invictus). The board members will be continually up for election. If the polling shows the community wish a member to be removed then the next meeting will remove that person and they should be replaced by the next in line, selected again via polls.

This group will ensure the correctness of the coin issuance and also that every project that is applicable is included in the polling system for funding of that project. The board can put forward their suggestions and conclusions for any funding for projects. The assurance of developer rewards will also be continuously-monitored and managed. This mandate will be kept as minimal as possible to prevent unfair or ill considered decision making.

An early project on the network will be a decentralised digital voting system. This system will be used to select and continually manage a member's position on the board.

APPENDIX

Token System on SAFE Network

Version 1.3

Last Updated 26 March 2014

1. Introduction

The SAFE network [ref Network] utilises a mathematically complete, peer-to-peer Public Key Infrastructure (PKI) authorisation on an autonomous network [ref Autonomous], secured key-value storage and reliable Kademlia based routing [ref Routing]. The network is designed to be decentralised and has the ability to get rid of Domain Name System (DNS). The PKI solution deployed within the SAFE network validates a user's identity with mathematical certainty.

Bitcoin [ref BitCoin] has proved the ability of crypto currencies to disrupt the status quo. Bitcoin proposed and executed a very innovative idea, coupled with a well-considered system design based on the block-chain and proof-of-work concepts. In essence, Bitcoin is a partially-decentralised (due to the use of the block chain) digital currency on a centralised network. MaidSafe propose a token based economic system on the SAFE network. In effect, a decentralised digital currency system on decentralised network.

2. Trusted Group

With the SAFE network, it can be assumed that the majority of a close group of nodes is trustable. While not impossible to generate a majority of malicious nodes in a close group around a particular target, it should be considered computationally unfeasible.

On the SAFE network, the following rules ensure a trusted group:

- It is hard to have a vault with a particular address (the address of a new vault will be defined by the network using the hash of the vault's credentials). In addition, each time a vault is switched off and then rejoins the network, it will be assigned a new address. Furthermore, the node will not be considered a full functional vault until the verification period is complete.
- When a request is emitted from a group, all group member's signatures will be attached. On the receiver side, a routing level find closest verification will be carried out to verify the senders are really closest nodes to the target. In addition, the public keys for the nodes will be downloaded from the network to validate signatures.
- The close group is not formed in a deterministic way (i.e. based on XOR distance as defined by Kademlia only). The close group of a target will only be formed when the target goes to the network. Unless the target is pre-known, it cannot tell whether two nodes are close.
- For sensitive data like currency or transaction, there is an additional level of protection : chained group. Chained group means the target is not only handled by the group around it, but also is managed by the other group chained to the target. The chain is established in a determistic way once the target is known, which allows verfication by public.
- The exchange of a vault between different users is not allowed. It is possible for a vault not to be linked to an account (unowned) and then linked to an account later (owned). However, once linked that vault cannot be detached.

Furthermore, there is the RUDP [ref RUDP] layer which encrypts communications between nodes to prevent the message content from being secretly modified by a third party. This ensures the request reflects the real intention of the sender.

Once the majority of the nodes inside the group have sent out a consistent request, it shall be considered valid.

Once the majority of the nodes have decided to perform the same action, the action shall be considered valid.

The Trusted Group feature, delivered by the SAFE network, ensures the system is secure as long as the majority of the nodes are honest and it is computationally / economically expensive to form a malicious node.

3. Transfer Mechanism

On the SAFE network, vaults assume various personas or roles [ref Persona], depending on the requests they receive. For example, the DataManager persona is responsible for managing the integrity and availability of a given piece of data on the network. A separate persona, the TransactionManager, is proposed to handle all the token-related transactions. A TransactionManager group will be a trusted group of nodes which are closest to any given transaction identity. The TransactionManager is responsible for the logic that enables transactions to be completed.

The transfer mechanism is defined as: ‘allowing a transaction (transfer of credit from A's wallet to B's wallet) between two user's persona groups to be completed’. The transaction shall be open and read only to public (allowing an upper layer third party broker app to validate there is transaction happening/completed).

The SAFE wallet is defined as : the place holding the credits (and the credit change history) for an account.

The procedure of a transfer (user_A transfers credit to user_B) can be illustrated as :

1. User A makes a function call : user_A.Transfer(user_B, amount, wallet)
2. When the Maid Manager group of user A receives a request, they :

   i) debit the amount from user A's wallet

   ii) send a request to the TransactionManager

   iii) send a notification to the upper layer API
3. When the Transaction Manager group receives a notification, they :

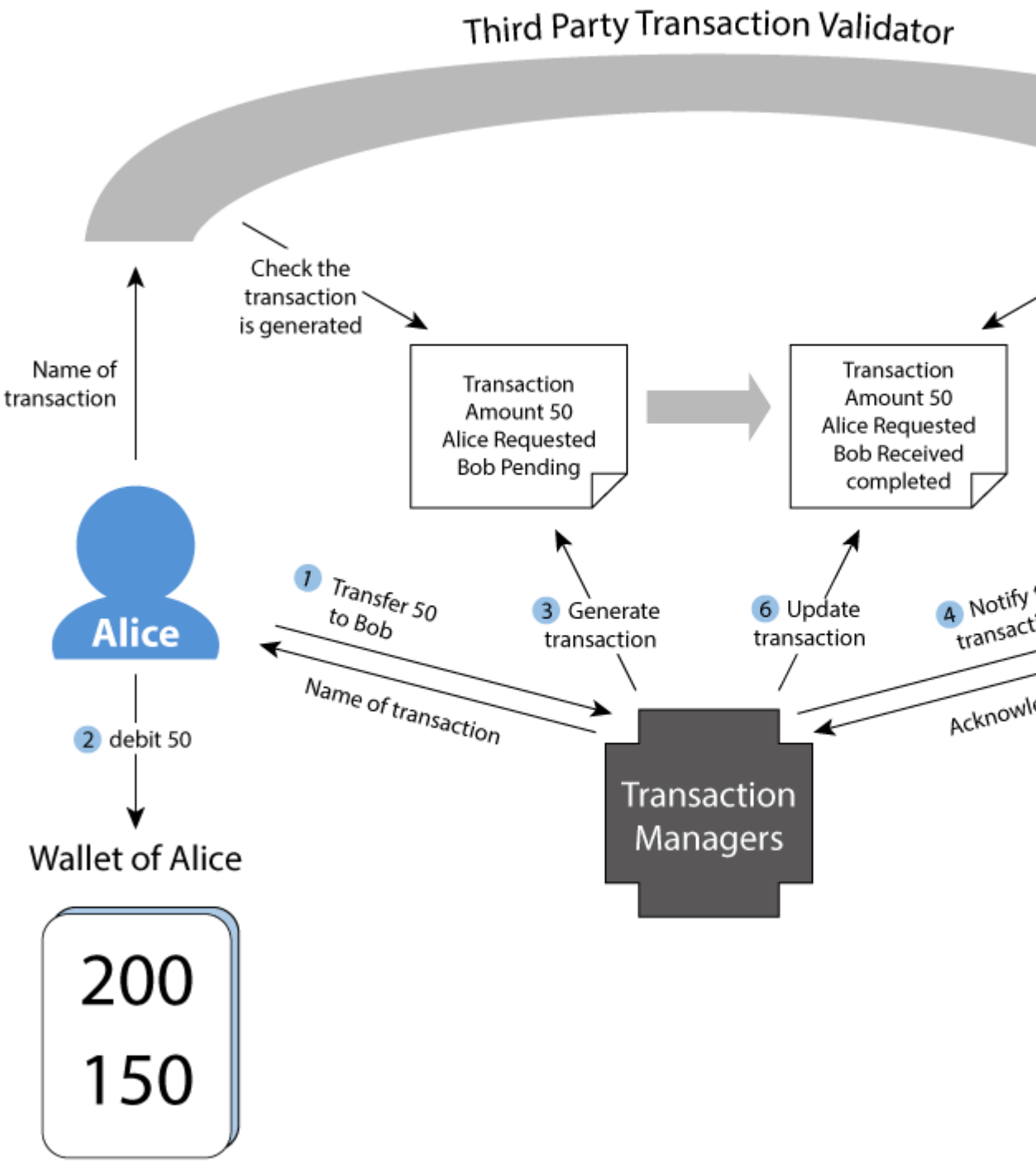
   i) send a notification to user B's persona

ii) create an internal transaction

4. When user B's Maid Manager group receives a valid notification they :

   i) send an acknowledgement to the TransactionManager group

   ii) credit user B's wallet with the amount



4. Proof Of Resource

On the SAFE network, a user contributes to the network by running a vault, which will handle requests and store data for others. The following parameters are used to measure a vault and a user account:

- stored_space: the total size of chunks that have been stored to that vault by the network
- lost_data: as data is stored on a node it may switch off or be otherwise unavailable, we consider this to be lost data. This is a critically important measure and in no way means the network has actually lost data as replicant copies are always available. This is a common practice for a node on the network.
- healthy_space (h.s.) : h.s. = stored_space - lost_data ------ ①
- available_space: the storage space a vault claimed (via the user) it can contribute to the network
- data_cost: data_cost will be calculated as the data_size that user stored to network. It will be refunded once user deletes the stored data. The client application has a local level deduplication, which will prevent a user from being charged twice when storing the same data again to the network.
- used_space: total data_cost of all the chunks that user put to network

The Proof Of Resource (P.O.R) is derived from healthy_space (which is a kind of QoS measurement)

- P.O.R will be updated when healthy_space updated in bi-direction

Δ P.O.R = Δ healthy_space ------ ②

This ensures P.O.R becomes a huge negative when the user transfers out P.O.R and then switches off their vault

- P.O.R will be checked when a user tries to PUT data. (used_space + data_cost) < P.O.R ------ ③

A user's initial allowance will be granted by setting used_space to negative claimed available_space. If any cheating is detected, the used_space will be changed to reflect that.

This will also cover for situations when a user's P.O.R drops by allowing the user to mutate his free allowance data.

- P.O.R is transferable among users
- P.O.R shall be an int in a unit directly derived from size unit KB (MB ...)
- The Maid Account will be the wallet of the P.O.R, and the Maid Manager group will be responsible for processing any updates.

- P.O.R shall be considered as a standard unit being recognized by all nodes across the SAFE network.

User A			User B	
Action	(used_space, stored_space, P.O.R)	Allowance	Action	(used_ stored_ P.C
Create Account	(0, 0, 0)	0	Create Account	(0, 0
Picked by Network To store 50 data	(0, 50, 50)	50	Never picked up or don't have a Vault	(0, 0
Store 20 data to network	(20, 50, 50)	30	Nothing Done	(0, 0
Sell 20 P.O.R to User B	(20, 50, 30)	10	Buy 20 P.O.R from User A	(0, 0
stored_space decreased by 10. Q.O.S drop or stored chunk removed by network	(20, 40, 20)	0	Store 10 data and get picked to store 10	(10, 1

5. Economic System With Two Types Of Token

P.O.R is proposed in order to facilitate the exchange of storage space on the SAFE network. However, as it doesn't have a predictable cap number, it may not be considered a genuine virtual currency. To provide a more robust form of exchange, MaidSafe proposes a token system that is totally independent of P.O.R, called safecoin. Safecoin will have a predicatable cap and will be injected into network using the storage space related mining procedure.

A bridge (converting rate) between P.O.R and safecoin can be established by the market solely. With third party upper layer broker applications, it will be possible to use safecoin to buy P.O.R or vice versa (user_A gives safecoin to user_B in exchange for user_B's P.O.R). It is expected that the per unit value of P.O.R will keep decreasing, while the per unit value of safecoin will continue to rise. In this way, it will be possible to buy more and more P.O.R with one safecoin. Safecoin will only be stored in the Maid Account wallet, this can only be updated by the Maid Manager group.

The value one safecoin represents will be recognised by all peers across the network and outside the network. If the economic system works as intended, safecoin will become a 'virtual currency' with the SAFE network being used to complete all transactions. Meanwhile, P.O.R will solely be used for exchanging space allowance among users.

A projection of P.O.R. is estimated as :

Network Wide Total Data	Copies	Traffic	De-Duplication Factor	P.O.R	Nodes	Data Pu Nod
1000	4	1	1	5000	100	10
3800	4	0.9	0.9	17100	200	19
10800	4	0.8	0.8	43200	400	27
27200	4	0.7	0.7	95200	800	34
64000	4	0.6	0.6	192000	1600	40
144000	4	0.5	0.5	360000	3200	45
313600	4	0.4	0.4	627200	6400	49
665600	4	0.3	0.3	998400	12800	52
1382400	4	0.2	0.2	1382400	25600	54

6. Safecoin Data Structure

Safecoin issuance will be capped at 2^32 (4.3 billion). Unlike P.O.R, which is just an integer number held in the Maid Account, each safecoin is represented by a special token type data. The data structure of such can be illustrated as :

Field	Content
Name	See below

Field	Content
Prev Owner	previous_owner
Curr Owner	$\text{Sign}(\text{current\_owner}, \text{version\_number})_{\text{previous\_owner}}$
Escrows	$\text{Sign}(\text{escrow\_1}, ..., \text{escrow\_n})_{\text{previous\_owner}}$
Escrow 1	$\text{Sign}(\text{owner})_{\text{escrow\_1}}$
...	...
Escrow n	$\text{Sign}(\text{owner})_{\text{escrow\_n}}$

The name of a safecoin is 64 bytes long to allow it to be a network-addressable object. However, the name has a particular format:

[32 bits: Token ID | 224 bits: ID padding | x bits (x <= 248): Subdivision bits | 248 - x: Random | 8 bits: Value of x]

The initial part (Token ID) inherently limits the total number of tokens available to 2^32 since each token must have a unique ID.

The second part (ID padding) must be predictable (e.g. it could just be all '0's, or it could be the ID concatenated 7 times). Its purpose is to force all subdivisions of a given coin token the same trusted group of vaults to eliminate the need for network traffic when handling such subdivisions.

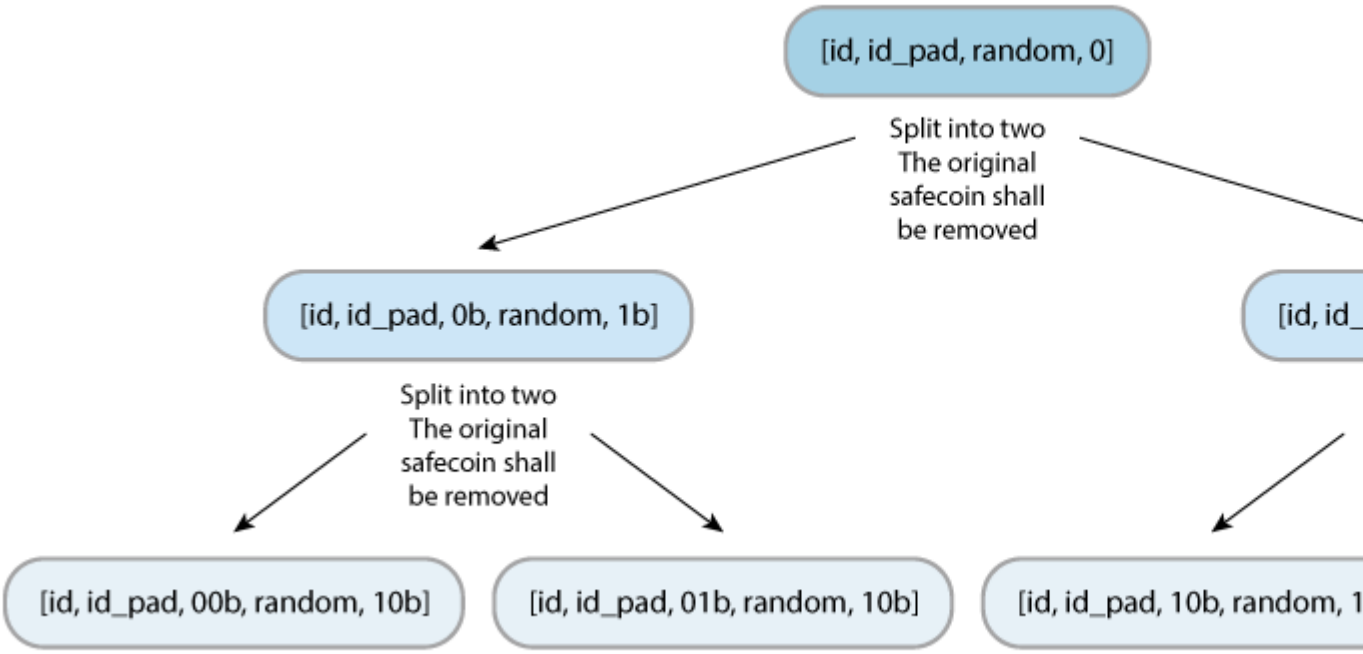
The third part defines the subdivision name. For example, if x == 1 (regardless of whether the value of that bit is 0 or 1) then that token represents a half of the original token.

The fourth part is random padding.

The fifth part indicates the level of subdivision of the original token, i.e. it contains the value of x.

This format allows the tokens to be split into 2^{248} parts if required. The splitting process will only allow the token (or subdivided token) to be bisected, so e.g. quartering a token would need to be done in 2 steps. When splitting a token, only the name changes; all other parts are copied to the new subdivisions. The split results

in 2 tokens, each representing a half of the original token value. This procedure is further illustrated in the following diagram.



The current_owner, together with the current version number, needs to be signed by the previous_owner, allowing a third party verification.

Escrows have the right to block / enable the access to the token by voting with majority (fill the correspondent excrow field with approved owner). i.e. only the majority of escrow approved owner will be allowed to update the token data.

This special safecoin data is being distributed by the DataManager and held in PmidManager's memory (shall never be stored to PmidNode as a chunk).

7. Safecoin Requests / Persona Roles

Safecoin data is one kind of data, so it has PUT and GET request being defined. However, unlike normal data, there is no DELETE request defined for it. The PUT request for safecoin is "no duplication allowed", i.e. if there is already a safecoin data having same name (first 32 bits), the new put request shall be rejected. This will be handled by the DataManager receiving the request.

A new request, EXCHANGE, is defined to allow approved requester update the pay_load of the token data. The rules defined as :

- Only the owner that be approved by the majority of escrows and owners (previous / current owners considered as approved themselves) can update all fields.

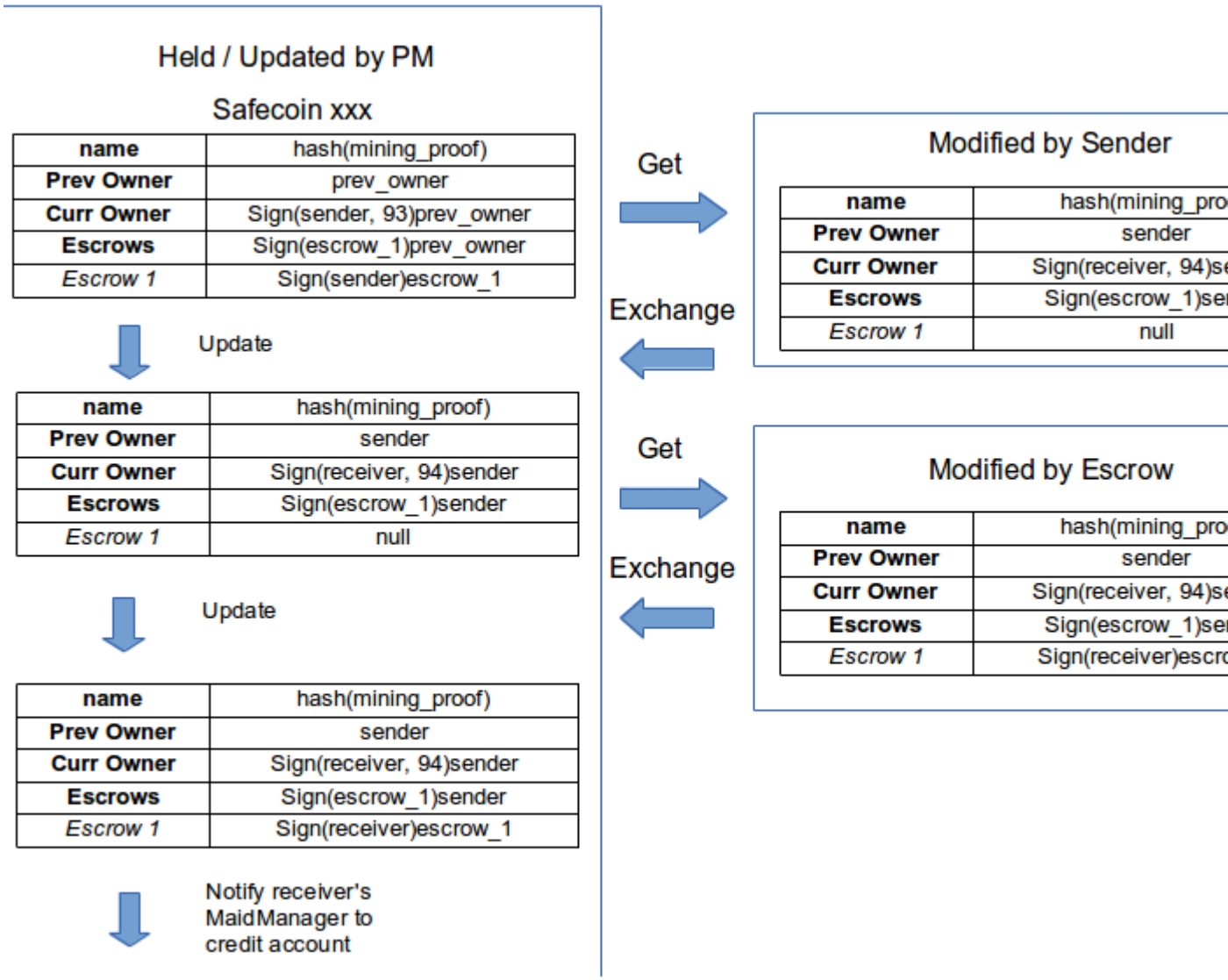
- Each escrow can only update their correspondent field once
- Each time prev / curr owner field get updated, the version_number must be increased by 1 step, and all escrow fields shall be erased

The above rules will be enforced by the PmidManager holding the safecoin data. As the ownership field, together with the escrow fields, are used as a 'transaction', the PmidManager effectively becomes the TransactionManager. In this instance, the safecoin data can also be considered as a receipt object as well.

The safecoin data also served as "wallet" to itself, i.e. a wallet that holds one token only. A user level bookkeeper, holding the list of token one user owns, can be completed as a client only application. That list of token information can be stored in user's local machine or uploaded to the network as encrypted data.

8. Safecoin Transaction Structure / Scenarios

The following diagram illustrates the evolve of RPC requests and safecoin data structure during a transaction process. It has the capability to support multiple escrows model (like multi-signature [ref Escrow] [ref BIP16/17] proposed for Bitcoin).



The following table illustrates the evolve of user account holding safecoins info, together with the safecoin data held by PmidManager.

Alice		Pmid Manager		Bob	
Action	***Account***	***Safecoin data***	***Request***	***Account***	***Action***
	(xxx, alice) (yyy, alice) (zzz, alice)	(yyy, prev_owner, Alice, 93, escrow_alice)		0	
Send 1 to Bob	(xxx, alice) (zzz, alice)	(yyy, alice, Bob, 94, Escrow_pending)	exchange	0	
	(xxx, alice) (zzz, alice)	(yyy, alice, Bob, 94, Escrow_bob)	exchange	(yyy, bob)	notification
		(ooo, bob, Bob, 0)	put	(yyy, bob) (ooo, bob)	mine success Notification
Send 1 to Bob	(zzz, alice)	(zzz, alice, Bob, 97, Null)	exchange	(yyy, bob) (ooo, bob) (zzz, bob)	notification

9. Mining Safecoin

Every mining interval, the Pmid Manager group around a vault will perform the mining for that vault. The Pmid Manager will generate a Random Attempt Target (R.A.T) based on the following calculation:

$R.A.T = Sign(Hash((merkle\_tree\_root + msg\_id) \text{ XOR } R.A.T\ prev))_{PmidManagerGroup}$ ------ ④

where : merkle_tree_root is generated from all the chunks stored on that vault

msg_id is the agreed random ID among the Pmid Manager group.

$Sign()_{PmidManagerGroup}$ means the PmidManager group in charge shall sign the hashed result. This makes RAT as proof of mining, allowing other vaults to verify.

The R.A.T will then be sent to the Data Manager as a PUT request, claiming the ownership of that token on behalf of that vault. If DataManager has no record of a token data bearing same token_index (first 32 bits), the token data will be passed to PmidManager to be held, and the correspodent MaidManager will be notified of the success. Otherwise, the request will be muted.

The mining interval allowed for a vault is determined by its contribution to the network. The interval is calculated as follows:

for each put attempts to the vault, when healthy_space is greater than group_average / 2 :

$MessageID \% (24 - round(\log_2(healthy\_space / 1MB))) == 0 \ ? \ true : false$ ------ ⑤

where : group_average is average healthy_space among the close group the vault belongs to

MessageID is the message_id from the put attempt request

This caps the quickest mining speed at one mining attempt per put attempt and set the slowest to be one mining attempt per 24 put attempts.

Given the collision probability against the accumulated number of attempts as shown in the following table. Where N is the total space (which is 4.3 billion in our case as the issuance of safecoin is capped at 2^{32}).

Collision Probability	Num of Attem
10%	0.105 N

Collision Probability	Num of Attem
20%	0.22 N
30%	0.36 N
40%	0.51 N
50%	0.69 N
60%	0.92 N
70%	1.2 N
80%	1.6 N
90%	2.3 N
95%	3 N

A projection of coin distribution can be illustrated as :

Year	Number Of Nodes	Average Data (GB) Per Node	Accumulated Attempts	Attempts Percentage	Coin Distributed
1	10000	16	88740000	2.07%	2.00%
2	50000	32	955700000	22.25%	20.00%
5	100000	64	4096000000	95.37%	70.00%
10	200000	128	17476200000	406.90%	98.00%
20	500000	256	92842500000	2161.66%	99.99%

10. Day 1 Injection

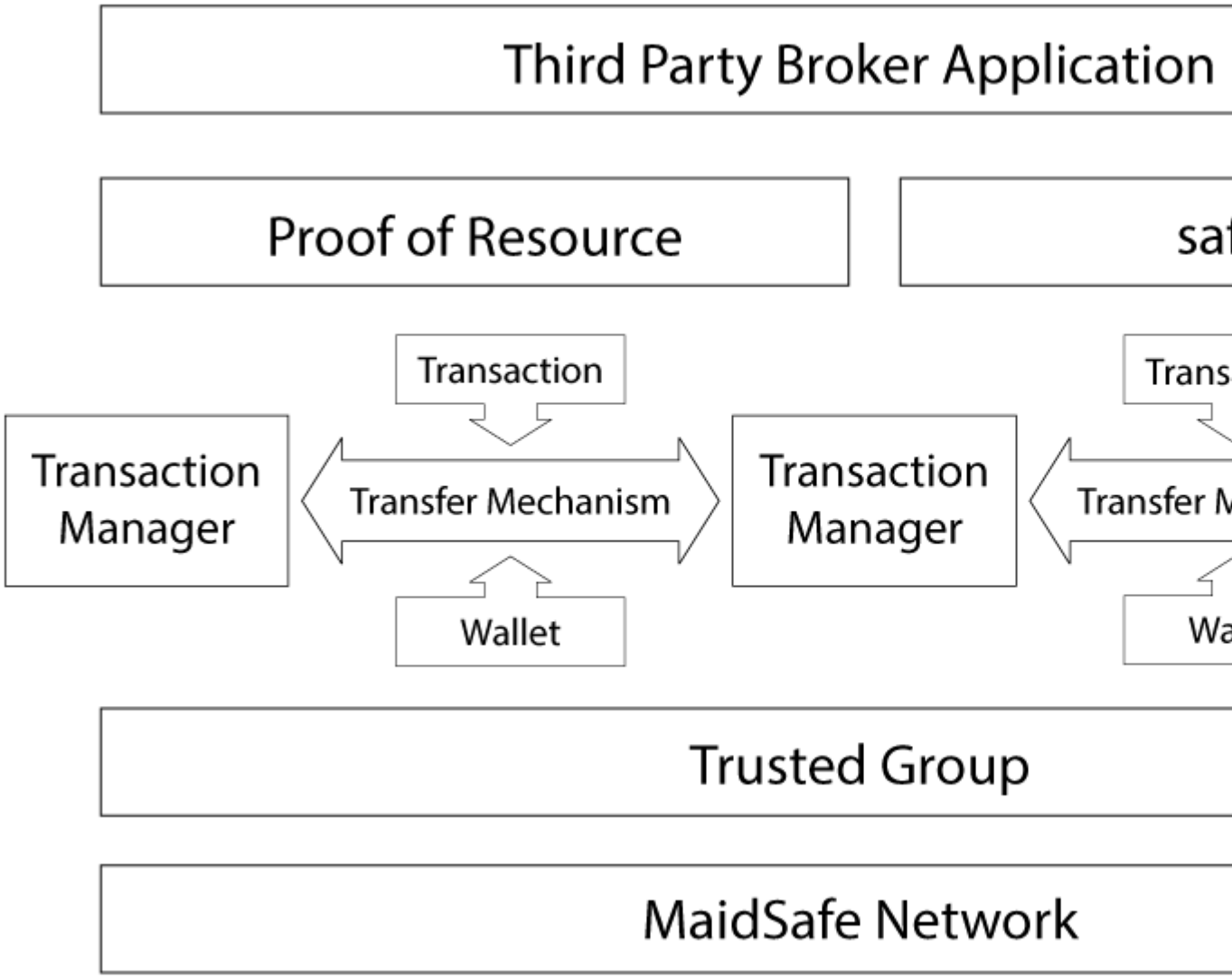
To reward investors and developers involved during the early stages of this project, it is proposed that 30% of all safecoins will be injected into the network on day 1. Up to 10% will be available for purchase via the crowd sale, 5% for the existing MaidSafe investors, 5% for the SAFE core development team and 10% for the general developer pool.

This 10% safecoin will require a storage space of 1TB, given the average SDV size is estimated to be 0.5kB. Vaults holding these SDV will gain P.O.R, which means the same amount of P.O.R is also injected into network. This ensures there is certain

amount of P.O.R available across the network for those client only users to startup with. This may be P.O.R given as gift or purchased from other users. As pointed out in the (table POR projection), sufficient P.O.R will be generated via user behaviour during the early stages, it is expected this initial injection will be enough to kick start the provision of storage to the public.

11. Summary

To conclude, MaidSafe proposed the SAFE network, an economic system that contains two types of token and relies on a trusted group. The transfer mechanism is advantageous in many respects and has the functionality to prevent double-spending, while enabling the verification of transactions immediately. Transaction Managers handling SDV data type are included into the SAFE network to manage tokens and transactions. Proof of Resource (P.O.R) is introduced to smooth the exchange of storage space, while safecoin is introduced to incentivise stakeholders throughout the network. The total cap of safecoin is set to be 4.3 billion. With the proposed mining procedure (and assumptions) it is estimated that half the total volume will issued during the first 5 years, with 95% issued after 10 years. End users will mine coins based on their ability to provide computing resources to the network and, in addition to the other benefits offered by SAFE, this will be their main incentive for contributing storage space. The tech stack of the token system is illustrated as .


Third Party Broker Application
Proof of Resource
sa
Transaction
Transaction Manager
Transfer Mechanism
Transaction Manager
Trans
Transfer M
Wallet
Wa
Trusted Group
MaidSafe Network