Teleport: anonymity through off-blockchain transaction information transfer

A Dark Paper for BTCD

Captain James Lee
Contact: PM jl777 on NXTforum.org
August, 2014

Summary

Alice acquires a treasure map drawn by pirate Jack Sparrow. Understanding that some pirates may be untrustworthy, Alice digs up the treasure and moves it to a different chest in another location. She copies the map and updates it with a new 'X marks the spot', crossing out the previous one and discarding the old map. Alice loses her new map to Bob in a game of chance. Bob, suspecting that Alice may have kept a copy of the map, moves the treasure, makes a copy of the map himself and updates it with a new 'X', again discarding the original. He later uses the new map as payment for Catherine. In such fashion, the map

and the location of the treasure change hands many times over. However, ***if care is taken when passing each map on, then there is no evidence for the identity of any of the previous owners****. The only thing we know for sure is that the treasure and the first map once belonged to Jack Sparrow.*

Teleport uses packages called telepods to send all the information required to make a transaction to the desired recipient, over a secure connection *outside of the blockchain*. Telepods are cloned by the recipient to prevent double spending, and sent to the next recipient when desired – or else emptied onto a previously-used account on the blockchain again. The contents of the telepod are therefore recorded on the blockchain at the point of cloning. However, if a completely new address is used every time, there is no way to know who has held the telepod over the course of its lifespan. The only thing that may conceivably be inferred is the original creator of the telepod.

Part I

Current approaches and limitations to

privacy

Introduction

Bitcoin has been a hugely successful implementation of peer-to-peer cash. The use of proof-of-work and blockchain technology allows users to establish consensus and prove ownership with no centralised authority, enabling fast, secure and almost free transfer of money over the internet for the first time.

However, the transparency with which this system necessarily operates is a double-edged sword. On the one hand, it prevents fraud: everyone on the network can see the contents of any address and whether a new transaction is consistent with the existing blockchain, the shared ledger of previous transactions. But this transparency also means that privacy is almost impossible.

There are several ways in which privacy may be compromised. Three of the chief means in which blockchain analysis can be used include:

1) Transaction linkage

Although each map bears only one current location for the treasure, 'X', evidence for every previous location is preserved. The discarded maps

show incrementally more disused marks, so that by studying previous maps a perfect history can be constructed of where the treasure has been buried for each successive owner. In itself, this may pose no problem, especially if there is no other information to identify the owner. However, as soon as additional details are included on the map – such as locations for other hoards of treasure, frequented taverns, and so on – then deductions may start to be made about who they are.

Although Bitcoin payments are often described as anonymous, they are really pseudonymous: the identity of the owner of a given address may not be known, but there is a permanent record of every transaction into and out of every account. Nakamoto's original paper acknowledges this:

> 'The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method... The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.'

[Image: tx linkage]

Every bitcoin transaction is traceable back to the block from which it was mined, as well as to every other address with which transactions have occurred. Moreover, this information may be linked to individuals through various means, as described below.

2) Fingerprinting

Intending to transition from a life upon the high seas to one as an honourable businessman, Bootstrap Bill makes it known that he wants to use his savings of 197 gold coins to purchase a large amount of jute. The East India Trading Company recognises this move as a threat to their monopoly on the jute trade. Although the sale goes ahead in secret, the Company knows the going price for jute, 4.63 gold coins per metric bushel. They therefore know that Bill has probably purchased in the region of 43 metric bushels of jute. Spies are instructed to look through merchants' accounts for the previous week for such an amount, in the hope of tracking Bill and stopping him from selling his goods.

Every transaction is time-stamped, and the entire blockchain can be viewed by anyone. If Alice is known to have made a transaction to Bob around a

certain time, and there is only one transaction recorded during the relevant period, then clearly the sending address belongs to Alice and the recipient's address belongs to Bob. Even if a large number of transactions occur in that interval, it may be possible to build up a picture over time based on statistical probabilities. This approach, called Transaction Fingerprinting, has successfully been used to identify owners of specific addresses:

> 'First, we developed a system for scraping bitcoin addresses from public forums. Second, we include a mechanism for matching users to transactions using incomplete transaction information. For example, suppose we hear Bob say to Alice: "I sent you $100 in bitcoins yesterday at noon"; though we don't know the exact time of the transaction (since "at noon" could easily mean 11:50 or 12:10) or the exact amount in bitcoins (exchange rates fluctuate significantly), we can generate candidate transaction matches and associated matching probabilities.'

3) Mantissa attack

Realising that the East India Trading Company know of his plan and will be monitoring the seas to

eliminate the competition, Bootstrap Bill decides to sell the jute in three different locations. Meanwhile, the Company's spies have discovered Bill's purchase in the ledgers of a wealthy merchant, learning that he bought 41.94 metric bushels of jute. Bill sells his jute in batches of 20, 15 and 6.94 metric bushels. Round number consignments are frequently traded and prompt no questions. Unfortunately, the spies are alerted by the distinctive amount after the decimal point for the last sale, so the Company is able to determine where he sold it and therefore his most recent location.

Any amount of money can be sent with Bitcoin, and since the exchange value is floating and dollar-equivalent sums are often transacted, these amounts may not be round numbers – leading to a very specific mantissa or significand (the numbers after the decimal point). If an unusual amount is noticed – either because of its large size, or because it appears to be an otherwise arbitrary number – then a link may be made, since the odds of this being a coincidence are minimal. If Alice sends Bob 3.14159265 bitcoins then the blockchain can easily be scanned and any accounts transacting that amount tagged. Even if there are

several addresses sending the relevant amount, some statistical correlations can be made.

> ‘Order books for Bitcoin exchanges are typically available to support trading tools. As orders are often placed in Bitcoin values converted from other currencies, they have a precise decimal value with eight significant digits. It may be possible to find transactions with corresponding amounts and thus map public-keys and transactions to the exchanges.’

Using a combination of these approaches, it is entirely possible to track payments through the blockchain and trace them to individuals. This ultimately makes Bitcoin ‘more traceable than cash... you have to go to great lengths to cover your tracks.’

Current solutions

There are a number of cryptocurrencies that offer privacy features by mitigating against such attacks in different ways, with varying degrees of success. None is entirely satisfactory – either because the level of anonymity gained is limited, in theory or in practice, and/or because the solutions raise other issues with regards to the long-term viability of the cryptocurrency.

While no technical solution can solve all aspects of the problem, especially against a determined attacker with almost unlimited resources, there are methods than can be used to protect the privacy of cryptocurrency users.

It seems counterintuitive that it could be possible both to enjoy the benefits of a publicly and permanently available blockchain, and to maintain the privacy of its users. However, this does indeed become possible to a significant degree with the use of certain processes and advanced mathematical techniques.

Mixing

A hoard of 143 gold coins is liberated from a chest belonging to Captain Crunch. Should the thief be intercepted with the gold in his possession, his crime will be known. To disguise the theft, the culprit deposits sets of 1, 10 and 100 coins with a series of trusted pirate acquaintances, to be recovered at a later time in a series of arbitrary amounts. Since the stolen coins are mixed with other coins in the chests, it is very difficult to prove which coins really belong to Captain Crunch – even if they could be traced to these locations. As an aside, it is worth remembering that there is

limited honour among pirates, so the thief may find he has been double-crossed when he tries to reclaim his loot.

[Image similar to: HYPERLINK "https://www.darkcoin.io/downloads/DarkcoinWhitepaper.pdf"https://www.darkcoin.io/downloads/DarkcoinWhitepaper.pdf p. 3]

Mixing services combine coins from many different sources before sending them back to their original owners (usually for a fee), with the intention of obscuring where the funds originated. In their simplest form, mixers are operated by individuals and users are simply required to trust them to return their funds. This is particularly unsatisfactory since they are often operated anonymously.

More sophisticated forms of mixing have been automated and incorporated into the protocols of different cryptocurrencies. For example, Darkcoin uses an implementation of CoinJoin called DarkSend. This optional facility collects together inputs of the same size (denominations in powers of 10 are used – 1 DRK, 10 DRK, 100 DRK and so on) into a DarkSend Pool. Coins are mixed within the DarkSend Pool and are returned to their owners

in a series of different amounts. The DarkSend Pool is operated by a master node elected from its participants.

Ring signatures

Most treasure chests can only be opened with a single key, carefully guarded by the owner. However, it is known that a particular treasure chest can be opened by several people: using the key owned by the Flying Dutchman; a skeleton key belonging to Hector Barbossa; the ancient tool possessed by Guybrush Threepwood; or the toothpick belonging to the Dread Pirate Roberts. When the treasure chest is opened, there is no way of telling which of these four keys has been used.

Image: ring signature representation

A second approach to obscuring the identity of the sender is to sign the transaction using one of a number of possible keys. This is made possible by the development of ring signatures, of which CryptoNote (also employed by Monero and several other cryptocurrencies) is the best-known implementation.

Ring signature is a more sophisticated scheme, which in fact may demand several different public keys for verification. In the case of ring signature, we have a group of individuals, each with their own secret and public key. The statement proved by ring signatures is that the signer of a given message is a member of the group. The main distinction with the ordinary digital signature schemes is that the signer needs a single secret key, but a verifier cannot establish the exact identity of the signer. Therefore, if you encounter a ring signature with the public keys of Alice, Bob and Carol, you can only claim that one of these individuals was the signer but you will not be able to pinpoint him or her.

Drawbacks and vulnerabilities

As stated above, none of the existing solutions are truly satisfactory, though for different reasons. Coin mixing solutions are effective in some circumstances but are relatively trivial to deanonymise at the level discussed in this paper, where privacy centres around transactions between single users. Increases in computer power may

render past mixing routinely transparent in the future. To compound matters, large quantities of coins are hard to anonymise quickly, unless there are similarly large sums with which to mix them.

Ring signatures are substantially more powerful, since each transaction provides only statistical correlations. Assuming each transaction has 10 possible parties involved, with any length of chaining the power of statistical linkage quickly reduces to the level of background noise. Coins based on CryptoNote may (like DarkSend) also minimise the problem of a Mantissa attack by splitting all of the transactions into power-of-10 outputs (for example, 1.23 RingCoins would be treated as 1 RC + 0.2 RC + 0.03 RC). Thus a transaction is obscured, though some weak correlations are still possible.

Centralisation and money flow

The centralisation inherent in most mixing services represents a clear vulnerability. Where trust in an individual is required, this constitutes an unacceptable solution for most users. Additionally,

> ‘[DarkSend] Masternodes can be controlled and thus the controller of the Masternode can learn about a certain transaction, if they were

> inclined to. There is a negative incentive to own many masternodes through their high price (so if a government agency wanted to own all masternodes that would escalate the cost of owning the nodes to a very high price) but this in itself does not prevent the mapping of the network to a certain degree. The next versions of DarkSend aim to improve on this aspect in particular.'

Mixing using protocols such as CoinJoin 'obfuscates money flows, and not account balances', meaning that information on and off the blockchain can still be analysed to build up a picture of accounts usage and owner identity.

Blockchain bloat

Ring signatures typically offer a superior degree of privacy over mixing solutions. Unfortunately, one of the major issues with cryptocurrencies that derive their privacy from ring signatures is blockchain bloat. Bitcoin blocks may contain several hundred transactions within a package of 200-400 Kb. Monero block sizes regularly exceed 10Kb and often 20Kb but contain just a handful of transactions. At the beginning of August 2014, Bitcoin's blockchain was around 20 Gb. (Most of

the increase occurred in the last two years, which account for over 90 percent of Bitcoin's 43 million total transactions and 313,000 blocks at that time.) By contrast, Monero's blockchain stood at around 2 Gb after just three months and 170,000 transactions: an order-of-magnitude difference. These and other issues were noted by one reviewer:

> 'There are some critical problems with CryptoNote. The size of the the entire project is just enormous. Key sizes are double the usual size. Unspent transaction output sets and key image sets both grow in an uncontrolled way. Most troubling is the centralization point of allowing an anonymous person on the internet choosing all of our elliptic curve constants without explaining himself.'

It is rightly acknowledged that 'CryptoNote is absolutely spectacular' and the advances it offers groundbreaking. Nevertheless, unless addressed, the blockchain bloat associated with the use of ring signatures is likely to limit widespread adoption of the cryptocurrencies based on them.

Part II

Teleport: a new approach

Teleport is a different approach to privacy that seeks to use one of the very features of cryptocurrency networks that limit anonymity under normal circumstances: transaction linkage. Teleport occurs off the blockchain but is verified using the blockchain, utilising the benefits of a public record without suffering its drawbacks.

Teleport uses '**telepods**' – packages of information containing everything required to make a transaction – to transfer funds securely and outside of the blockchain to the intended recipient. The recipient may or may not choose to remove the funds from 'hyperspace' at this point, depending on whether they trust the sender (in most cases, they will not; however, the eventuality that trust exists or that sender and recipient are the same person must be considered).

Key to Teleport is that users are sending the *capability of making a transaction* to their recipient, not actually *making a transaction* to the

recipient.

Similar to the example of the pirate's treasure map, an illustration can be made by analogy with Bitcoin paper wallets. These can be printed out and mailed to another person, who sweeps the balance into a new address that has never been used to stop the first owner from spending it. They then print a new paper wallet. The balance of an account may change hands many hundreds of times in this way. **The only evidence on the blockchain is a series of anonymous addresses, with just one incoming and one outgoing transaction each, leading back only to the first owner.**

In the original Bitcoin white paper, Satoshi Nakamoto anticipated the privacy issues that a public and transparent blockchain would raise, and suggested using a unique address for every transaction as a solution:

> 'As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is

revealed, linking could reveal other transactions that belonged to the same owner.'

However, even if every user avoided compromise through transaction linkage by following this as best practice, transactions could still be traced through other means, including Fingerprinting and Mantissa correlations. Teleport dramatically reduces exposure to all of these.

One-time addresses used to avoid Transaction linkage

Off-blockchain transmission and variable redemption time mitigates Fingerprinting

Standard denomination telepods to circumvent Mantissa correlation

Before describing Teleport in more detail, it is necessary to summarise the conditions and infrastructure within which transactions of telepods should occur, and what this enables.

Prerequisites for privacy

Captain Morgan recognises that although the system of using maps to carry value rather than handing over treasure itself is effective, the participants could potentially be identified if they

were seen together or if a trail could later be reconstructed from one to the other. Not wishing to be compromised in any way, he adopts a complex but highly effective strategy of disguising himself as a barmaid, using backstreets rather than main thoroughfares to get to the rendezvous point, and only travelling at night.

The public record of the blockchain is the primary threat to users' anonymity under normal circumstances. Clearly, if transaction information is being sent off-blockchain, then communication between users must be kept private if overall anonymity is to be maintained. In the case of BitcoinDark (BTCD), which uses the measures described below, the necessary features are built into the client to enable the full benefits of Teleport. Teleport will also enable the anonymisation of other cryptocurrencies, for a minimal transaction fee.

The most basic privacy required by users is the ability to keep their IP address from being discovered. Any efforts to ensure the privacy of cryptocurrency transactions can be rendered useless by allowing third parties to trace this. For example, if a private cryptocurrency payment is sent to an online store but the user's IP address is

visible, all payments received around that time are probabilistically linked to that computer. Information gleaned from the shipping address and any other personal details submitted can quickly be pieced together to discover the customer's identity.

PrivacyServers

Captain Morgan refines his secret messaging plan by enlisting the help of a community of like-minded pirates to act as couriers for different sections of the journey. Each one passes the message to the next, until the final one gives it to the recipient and records delivery to satisfy Captain Morgan's rigorous accounting procedures. To ensure that none of the couriers is compromised, each one only receives instructions on where the next courier is located when he is given the message. Couriers have no idea of the identity or movements of previous or subsequent couriers in the chain.

The solution to the problem of information leakage is the privacyServer. Any user can run their own privacyServer simply by running a VPS, so there is no need to trust any third party other than the VPS provider.

The privacyServer is only able to see who a given user is in contact with, since all communication

other than the initial setup and intentionally public information is fully encrypted using Daniel Bernstein's Networking and Cryptography library (NaCl). A session-based keypair is generated at the beginning of every session, so even in the event of any single key being compromised, exposure is time-limited. Additionally, all communications are time-stamped and tokenised to provide verification that an account is not being spoofed.

Using onion routing, the encrypted packet sent to the privacyServer only has the address of the destination and the encrypted data. The privacyServer sends the encrypted data to the destination. (Currently this information leakage is deemed to be minor; however, in order to address this an additional onion layer will be added, so that a random privacyServer will be chosen to be the destination that the user's privacyServer sees. Thus even the user's own privacyServer cannot glean any useful information. This protects against breaches at the level of the VPS provider.)

Graphic:

"xxx".() indicates the contents of () are only decodable by "xxx". [] indicates a data packet

[user's privacyServer.([jump privacyServer.
([actual destination.(encrypted data)]))]

Anyone monitoring internet traffic will only see that a user has sent a packet to their privacyServer. If the user's privacyServer has been infiltrated, it will be known that they are sending via the jump privacyServer, which was chosen at random. This randomly-selected jump privacyServer will have to be compromised even to find out the final recipient to whom the package was ultimately addressed. As a rule, the encrypted data is also tokenised so that the final recipient can be confident that whoever sent the message at least had access to the sender's account password.

Broadcasting

Rather proud of his courier network, which he knows will satisfy the vast majority of treasure movers' requirements, Captain Morgan nevertheless wishes to develop a premium service that offers still higher levels of privacy for his corporate clients. Understanding that an organisation with unlimited resources (such as the East India Trading Company) could theoretically infiltrate part of his network and learn some

information about his business dealings, he hits upon a new idea. Instead of passing the map from one courier to the next in person, he will arrange to have each one simply display a version of the message in a public place such as the market, for anyone to see. So long as he can write it in a form that only the intended courier will understand, there will be no trail at all between any of them. Indeed, if he is careful, no one else will even know what they are looking at...

Once effective privacyServers exist, point-to-point secure communication is possible. This is a prerequisite for secure implementation of Teleport.

There are remote possibilities in which some path information is obtainable, so for the most secure communications, a broadcast path will be used. This simply takes the form of:

[Graphic]

[broadcast.(encrypted data)]

In this instance, there is no stated destination address. Although it may seem contradictory to broadcast a message to the entire network to

maintain privacy, by sending it to everybody the same amount of information is leaked as sending it to nobody, since everybody is treated the same.

In addition to the destination address the public key of the sender is also sent. This allows the receiver to decode the encrypted packet. If this public key is the same as the public key broadcast, then it is the same as announcing who the communication is from; therefore a second keypair is used for these broadcasts. This can be a one-time keypair in each instance. In order to be able to encrypt the packet in the first place, the destination's public key needs to be known. However, this public key can simply be broadcast in plaintext.

The encrypted data is broadcast using this public key. All of the nodes will try to decode all of the broadcast packets, but only the intended recipient will be able to decode it successfully: everyone receives the packet but to everyone except the intended receiver the contents are meaningless.

Multi-signature capability

One final refinement affords Captain Morgan maximum peace of mind that his messages will not be intercepted. Whereas previously he has sent

copies of the full map, albeit indirectly, he decides to copy the map several times, cut it into pieces and use his marketplace system to give them all to members of his courier network. To complicate matters further, a proportion of the couriers in the chain are instructed to destroy their pieces of the map rather than to pass them on. The final recipient will slowly be able to piece together the map from fragments delivered at random, but anyone observing or any spy in the network will never know the whole picture.

Additional security measures can be established against an attacker that is able to log all the packets between nodes and infiltrate some privacy servers. To this aim, an 'M of N' approach to receiving a packet is suggested.

At the point of transmitting a telepod, each one is split into N pieces and sent to N random recipients, with a random number M of these forwarding to the final destination. This incorporates aspects of another onion layer, but with M of N ability a statistical retransmit will create additional obstacles for correlation.

Image: 6-of-8 representation for reconstructing

data

For example, if M = 6 and N = 16 (that is, each telepod is split into 16 pieces and 6 are required by the recipient), and each receiving node has a 50 percent retransmit chance, then on average 8 parts will get through, which is enough for the receiver to reconstruct the message. In the event that not enough pieces arrive, a confirmation packet is not sent back to the original sender, who will then retransmit. This return path can also be M-of-N split sent to minimise the correlations that are possible. The BitcoinDark implementation explored below will allow values of M and N up to 254.

If a significant percentage of nodes are participating in retransmission, then when a node initiates a Teleport, doubt is necessarily created as to whether it is a retransmit or the start of a Teleport. (This requires the introduction of random delays between receipt and rebroadcast.)

A separate use case for the M-of-N approach is to be able to create distributed cold storage of telepods. One part can be placed in encrypted online storage, another on an offline medium such

as a USB drive. With a 2-of-3 approach, the final part cannot be used without one of these other pieces. One application would be for donations to be split among a group of N people, M of whom would need to produce their telepods for the funds to become available.

(**Note:** the 'multisignature' capability used by BitcoinDark is actually an implementation of Shamir's Secret Sharing, though this has the same effect of requiring some or all parts of a packet of information to be combined to reconstruct the data.)

By selecting different levels of privacy, different levels of onion routing and broadcasting can be chosen. Maximum privacy is unnecessary for non-sensitive matters, especially since the more privacy is required, the longer the transaction will take to complete.

Overview of the BitcoinDark implementation of Teleport

Once the infrastructure of a secure network provided by the privacyServers is in place, Teleport becomes possible. BitcoinDark uses an implementation of the Teleport idea to enable

trustless private transactions.

Teleport transmits funds via telepods by transporters. All the information needed to spend funds is included in the telepod and sent via the encrypted network to the destination. Note that this is not the same as making a transaction itself: the recipient can choose if and when to execute the contents of the telepod. Only at this point is the transaction made from the sender's to the recipient's address – though in most cases this will happen immediately to avoid double spending.

Each telepod uses a newly-created address for the sole purposes of the teleport. Funds are sent from a transporter account – the originator of any given set of telepods, who will remain on public record – to standard-denomination telepods, which execute transactions of 1, 5, 10, 50, 100 coins, and so on.

Image: Standard-denomination pods travelling to new owner, being recombined, and sent on to new ones

Off-blockchain transfers

Captain Ironhook has a treasure-transfer outfit. He

hides treasure in various locations and prepares numerous maps, ready to give to customers, but leaves them to age and yellow in his office. So long as he does not need to spend the treasure himself, there is no disadvantage to this approach. Quite the opposite, since older maps are likely to raise less suspicion than new ones, on which the ink is still drying.

At this point, there is no activity on the blockchain. The telepod is in 'hyperspace', outside of the blockchain. The funds within it have not yet been spent, and so they remain in the issuing transporter's account. If the recipient trusts the sender to not double spend, these telepods can simply remain in storage – the longer the better. Under normal circumstances this will not be the case. However, there may be conditions when this occurs, either where there is a transaction between trusted parties, or where the sender and recipient are the same person.

The normal case will be that the recipient immediately clones the telepods. This involves executing the transaction held within them, so that the sender cannot double spend, and creating a new telepod using the funds released. After cloning is completed, the recipient can credit the sender

with carrying out proper payment.

Because the address to which the telepod has been sent has never been used before, and will never be used again after the telepod has been passed on, it is still considered to be in hyperspace. There is no interaction with an address that can be linked to other addresses through the blockchain, save for the originating transporter account.

Image: complex web of addresses, with one-dimensional clone line from telepod originator

No blockchain bloating occurs: there has just been a single ordinary spend transaction. And, whilst the blockchain records the fact that the telepod has been cloned, there is no information available – on or off the blockchain – about who carried out the cloning. Save for the transporter account that created the initial telepods, all telepods are clones of prior telepods, with no transaction history of their own outside of that line. The contents of a telepod are identical to the one that existed before it, with the same amount of funds being passed on to the new clone. (Over time, transaction fees will reduce the amounts in the telepods, but this can be

ignored for now.) The address of the first telepod is known, though if this account itself was a fresh account funded via semi-obsfucated sources such as an exchange, then even the identity of the original creator can be in doubt.

Example

Alice creates a new telepod (TP). She sends this telepod to Bob, who immediately clones it (TP') and sends it to Catherine, who also clones it (TP'').

On the blockchain, it is evident that the unspent outputs for TP were used to create TP', which was then used to create TP''. This only traces back to Alice, since the addresses TP' and TP'' have never been used before, and are only used once to clone the next generation of telepod. So long as the telepod is not spent in the normal way, in a correlatable transaction, *the only thing the blockchain shows is that somebody – maybe even Alice herself – cloned TP and TP'*.

The telepods are cloned and passed around to conduct commerce in private. Only the immediate sender and recipient know about each other, and even that can be prevented by using onion or broadcast routing. This enables totally anonymous

donations, by means of a telepod sent via broadcast using a one-time throwaway public key and sending address.

Privacy gains

The East India Trading Company keeps a record of every transaction it makes in its ledgers, protected from unwanted readers by a sophisticated code. Captain Pugwash uses a similarly complex code, but instead of recording transactions between people like the Company, he prefers to use his system of maps and leave the question of creating an identity for the new owner to decide. Even if his code is broken at some point in the future, there will be nothing to track that leads back to them, unless they want it to.

Although mixing and ring signatures provide a significant degree of anonymity, they are both vulnerable to advances in computing that would render them worthless. In the case of ring signatures, there is doubt as to who is sending coins due to R different signatures being possible. With real-world usage of R=10, this gives results of 10 percent → 1 percent → 0.1 percent for each generation. However, all these transactions remain

on the blockchain, and so if at any point in the future the encryption is cracked (which may be possible with advances in quantum computing), then a ring signature blockchain will become as transparent as Bitcoin's blockchain is now.

Let us assume that the attacker has somehow detected that an account is using Teleport. With proper use of privacyServers, this information should be very difficult to determine, and so this is an extreme scenario. Nevertheless, this case assumes that a user is known to have cloned a number of telepods during some specific period of time.

There are two concealing factors here. One is the total number of telepods cloned during this interval. Whilst Teleport remains its infancy, this number could well be smaller than 10, and thus provides less privacy than ring signatures in this respect. However, as the corresponding network grows, ring signature solutions will suffer from extreme blockchain bloat, and so the protection offered is relatively fixed: a ring signature with 10 keys is viable, whereas one with 100 or 1,000 is not. Conversely, though, as Teleport usage grows, the privacy level automatically increases at the same rate. 1,000 clones in the given interval means

a 1/1,000 chance of being identified correctly.

To receive a telepod, somebody must have sent it. On the sender's side, the situation is even more favourable. The possible senders to be analysed are all possible prior recipients from the time the specific telepod was cloned. In order to gain more privacy, telepods simply need to be stored for a longer period of time. If the receive side is at 1/10 probability and a telepod is stored for 100 times the reception window being used, the correlatability of the sender is 1/(10 * 100). Similar to the situation on the receiving side, the more Teleports that occur, the greater the privacy – all without any blockchain bloat.

In the case that the encryption for Teleporting is broken by advances in quantum computing, there is far better long-term protection than any system that records everything on the blockchain. Since the Teleporting is carried out off blockchain, there is no permanent record to be analysed: what happens in Teleporting, stays in Teleporting.

Funding transactions

Every time a map changes hands, the treasure must be moved to a different location determined by the new owner for safekeeping. The only way to

achieve this is by hiring a cart to carry it. Therefore every time treasure is moved, it logically follows that a cart must have been acquired for the purpose. By following this line of inquiry with local (and usually cooperative) cart providers, it may well be possible to establish the identity of the customer. Thus the necessity of carrying out a small transaction threatens to compromise the secrecy of the whole undertaking. Since providing facilities to move treasure and create new maps in secret is fundamental to the health of the pirate economy, it is deemed prudent to make a set of carts available for general use at no cost to the users.

In the overview above, transaction fees were ignored for the sake of simplicity. In a real-world implementation, though, these fees significantly complicate matters. Of course, each telepod could pay the fees out of its own balance every time it was cloned, the minor loss being the minimal price that the new owner pays for privacy.

However, this would necessarily mean that the telepods no longer had the same values, destroying the advantages of creating standard-denomination pods (resistance to Mantissa analysis). Information would be leaked, which could lead to

compromised identity. This means each telepod needs a small additional input to offset the transaction fee and keep its value constant. Since this transaction fee input must come from somewhere, it risks contaminating the entire telepod and leaving a trail back to the owner or another party in the system.

Finding a clean source of change is critical. This source is called a minipod. Minipods could be created in several ways.

One approach is to simply wait for a (small-denomination) telepod to arrive, and then use this as the minipod. One small telepod can be kept in hyperspace by the owner, and used to fund all other telepods required for the foreseeable future (since transaction fees are typically very small as an overall proportion of the funds being transferred).

Image: faucet payment and main account combining for transaction to next owner

Arguably a better solution is to have a minipod faucet that sends out pre-made and pre-aged minipods on request, via the encrypted network.

Ideally, large numbers of minipods will be created in the same block so they all look the same. Let us assume that this mechanism is available. Now, when the transaction fee is replaced when cloning a telepod, it will link back to the original creator of the telepod line, and to the faucet (which is itself a telepod issuer).

Telepod volume

One-Eyed Willie keeps most of his treasure in cold storage, safe behind a complex series of traps and puzzles in his favourite cave. For satisfying the needs of day-to-day trading, he requires a number of maps ready to go. As well as ensuring a ready supply of unit hoards (consisting of a single gold coin) buried and ready to go, he maintains a running total of larger-denomination chests and maps. Once he has passed a map on, he always destroys any old copies, just in case they fall into the hands of the East India Trading Company or a gang of enterprising pre-teens.

Since it makes sense to create as many telepods as are needed but no more (due to the costs involved in tying up funds), there needs to be a mechanism for satisfying a given level of requests for Teleport in the most efficient manner. Suppose that the

demand is for X coins, delivered in batches of standard-denomination pods.

We can assume an uncontaminated minipod will always be available from the faucet, since this is cheap to arrange, so the problem reduces to finding the best set of available telepods to fulfil the total required. The older the clone date, the more protection exists. However, a simple ‘first fit’ method will not work so well, as there is also the issue of matching the *total* amount X with the right denominations. However a simplified approach provides a good starting point.

Take the first N telepods, such that the total value of these N telepods >= X, but sum of N-1 < X. It is good practice to prevent telepod sets that have not aged enough from being used, and this can be passed in as a parameter. Using this parameter (or a default), we will also have a list of potential replacement telepods that are a little younger than the initial set, but still older than specified. Ideally, the selected telepods would exactly match X with the least number of telepods used, in order to reduce the number of packets that need to be sent. There may be a deterministic algorithm to solve this perfectly, but with the expected number of telepods and speed of the average CPU, this is a

simple problem for a genetic algorithm to find the fittest set. Using a genetic approach also allows flexibility in the criteria for the selection set. Different users may have different requirements.

Assuming these requirements have been met, we have the set of selected telepods that now need to be sent to the recipient. In the event there is not an exact match for X, issues arise regarding where to send the change without resulting in contamination. To sidestep this issue, in addition to the minipod faucet that will patch transaction fees, the system also requires a supply of telepods that are of the lowest denomination supported by Teleport. Since standard recommended denominations include 1 and 5, no user will ever require more than 4 of these unit pods. (It makes sense for transporter accounts to store a larger number based on likely estimations of demand, since then more than one Teleport order can be fulfilled without waiting for more telepods to age.)

There should therefore always be an exact match between the order sum X and the total value of the telepods. They can then be sent to the recipient, to await confirmation of successful cloning. In order to minimise timing attacks, the acceptance procedure should be randomly spread out over a

set amount of time. Again, a user-specifiable parameter with some reasonable minimum requirement is a practical approach. The recipient can also immediately acknowledge receipt of all telepods without cloning, in the case that the sender is trusted not to double spend. While this is not realistic for arm's-length transactions, for transfers internal to a single organisation it avoids needless cloning and the expenses and loss of ageing that creates. If a user is creating telepods for their own purposes and later use, again there is no risk of lost funds.

Upon receipt of acceptance, the sender deletes the telepods. This is a potential (edge case) information leak if the sender prevents deletion, but it can never raise the possibility that an untrusted sender will double spend. It is also in the interest of the sender to delete the telepods, as the sender's privacy is at risk (again, in extreme cases) as long as these files remain on their system.

Receiving telepods

Roger the Cabin Boy has received his monthly pay in the form of a set of standard-denomination treasure maps, delivered over the course of the last week by the pirates' courier network. Broadly

trusting his employer, Captain Pugwash, he has a choice about when to move the treasure and copy the maps, and does not have to do this all at once. He decides to wait until Saturday to recover some of the treasure, since many other people will have just been paid and will be engaged in digging. The more people are active at any one time, the less his own activities will raise the suspicions of the East India Tea Company.

The final part of the telepod transaction process is reception. As the telepods arrive, they are processed according to the stated trust level and user parameters. In the case of a trusted sender, the telepods are verified to contain proper unspent outputs on the blockchain and acceptance is given. (A higher-level packet that describes the entire set can be used to identify any packets lost in transit and to make the accounting simpler, though this is not required for the proof-of-concept to work.)

In the expected event of an arm's-length sender, the recipient should immediately clone each telepod, thus preventing double spend by the sender. Of course, in the event the sender *does* double spend, then the recipient simply rejects the payment, or pro-rates the amount double spent. Thus a double spend is an inconvenience but poses

no threat of fraud.

The cloning process involves taking the unspent amount in the telepod, adding the transaction fee equivalent from the minipod, and sending the funds to a newly-generated telepod address. After the cloning process is completed, the telepods begin aging and can become part of outbound teleports when a satisfactory age threshold is reached.

The issue arises of when to clone each telepod received in the set. To simplify the processing logic, it is recommended to await the arrival of all telepods, as specified in the summary packet. This allows a retransmission process to complete before proceeding to the cloning stage. The problem with cloning all the telepods at the same time is that this results in a much easier target to correlate, especially if the total amount is substantial. In addition to a general minimum time to wait before cloning takes place, there need to be provisions for processing larger amounts. Ideally, the total amount being processed by the entire network would be used to determine the recommended duration of the cloning process. Instead of specifying an arbitrary time limit, a privacy level can be chosen such that all telepods are part of a

large enough global set. The reception side is far more critical than the sending side, due to the significantly smaller timeframe over which this needs to occur. This may result in delays early on in the implementation of Teleport.

As the overall Teleport activity increases, these undesirable delays will be dramatically reduced, or even eliminated totally: Teleport works better and faster the more overall activity there is.

Leaving hyperspace

Roger the Cabin Boy has won a number of maps in a game of chance. The problem arises that although the maps have changed hands anonymously dozens of times in that form, when he actually needs to ***spend*** *the treasure in the chests he risks creating a link that could be followed back to him. The simple answer is that all of the maps were originally created by the legendary pirate, Jack Sparrow, and can be traced back to him. (Since Jack knew this all along, this is of no consequence to him.) So Roger can return the maps to Jack Sparrow in return for regular payment in whatever currency he prefers, and there will never be any evidence that Roger has dealt in the maps at all.*

This system describes the creation and continued use of telepods within hyperspace, or within a set of transactions that have no further relationship with the blockchain and addresses that can be identified by their associations – either other addresses to which they are linked, or other information available through external means.

For some privacy-oriented activities, the telepods will continue circulating in hyperspace and will never have to rejoin the main (monitored) blockchain. This would provide the optimum circumstances for using Teleport.

There will naturally be cases where users want to cash out telepods so that they can spend the funds within them, outside the Teleport ecosystem. This represents a significant vulnerability. Just as the original creation of a telepod is traceable to the address that first created it, so the address to which the telepod is cashed out for general use will also be visible.

Fortunately, there are effective ways to circumvent this problem. Some users will be content to move funds directly into their day-to-day accounts, especially if the transactions are obfuscated by other means (use of mixers, for example, is not

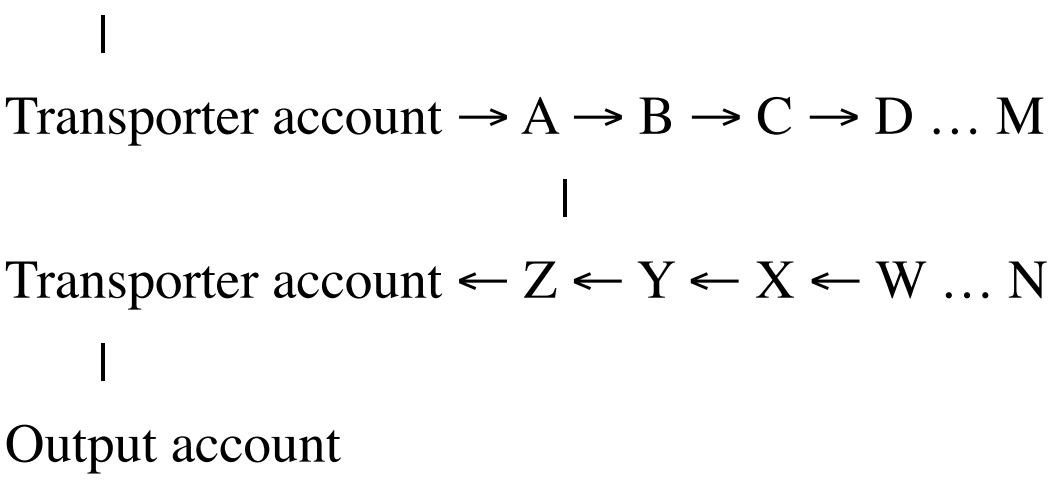
precluded by Teleport). However, for the highest levels of privacy, the following methods are recommended:

Anonymous bank card. Through a partnership with cryptocurrency payment processor Coinomat, BTCD balances can be withdrawn to a bank card. When funds are sent to the linked deposit address, they appear on the card's cash balance. This can then be used for online purchases and even ATM withdrawals. If the cards are delivered by mail then there is a potential risk; the ideal solution to this is purchase for cash. This telepod → fiat exit path offers a total anonymous ecosystem for cryptocurrencies.

Blockchain withdrawals via the originating account. In many cases, owners will want to 'withdraw' the contents of their telepods to the blockchain, in order to use the funds as normal – purchasing goods online directly with the cryptocurrency, converting to other currencies via exchanges, and so on. Since this represents a second point of vulnerability (the first being the original telepod creator), it makes sense to combine the two. Thus anyone wishing to cash out their telepods may do so *via the original issuer*. To the outside observer, the line of transactions simply

follows a loop from the originator back to the originator, via an unspecified number of clone addresses:

[Graphic]



Conclusion

Captain Kidd has devised a cipher with which to record the location of his treasure. Whilst adequate for the limited threat posed by his own circle of acquaintances, after the treacherous business with William Legrand he decides that extra precautions

would be wise. Kidd uses his cipher to encode the location of his replacement treasure chest, and then buries these instructions in a second location, marked on a treasure map in the established fashion – thereby cumulatively gaining the benefits of both forms of secrecy.

Teleport offers robust anonymity for cryptocurrency users – initially BitcoinDark users, though the protocol will allow other cryptocurrencies to be anonymised through the BTCD system for only minimal transaction fees. Teleport's exceptional level of privacy is achieved not by mathematically superior encryption or more sophisticated mixing processes, but by enabling transaction information to be sent outside of the blockchain within a complete ecosystem designed for privacy from the ground up.

It is anticipated that BitcoinDark will naturally compete with other cryptocurrencies offering anonymity features, including Darkcoin and Monero, which use variations of mixing and ring signatures respectively. Whilst no solution can ever be perfect, the addition of a wholly different approach to the current cryptocurrency landscape must be welcomed. The CryptoNote white paper points out that the currency is not considered a full

replacement for Bitcoin, but that there are advantages to having competing currencies: these are the circumstances under which innovation and improvement occur.

Bitcoin's immense network effect means that there is little chance in the medium term of another cryptocurrency unseating it. As the established digital currency for internet commerce, it makes no sense for users to switch to another form of cryptocurrency without good reason – though for private transactions they may choose another currency. Nevertheless, Teleport's versatility as a complete system rather than as an cryptocurrency-specific algorithm mean that in those circumstances where privacy is required by Bitcoin or another 'transparent' cryptocurrency, this eventuality is also covered by using BTCD through a third-party service.

There is also nothing to stop existing privacy-oriented cryptocurrencies from adding Teleport to their approach, either before or after native measures are taken. This layered use of anonymity protocols will provide exceptionally strong privacy for the most sensitive applications.

Further reading

Evan Duffield and Kyle Hagen (2014). *Darkcoin: Peer-to-Peer Currency with Anonymous Blockchain Transactions and an Improved Proof-of-Work System*. HYPERLINK "https://www.darkcoin.io/downloads/DarkcoinWhitepaper.pdf"https://www.darkcoin.io/downloads/DarkcoinWhitepaper.pdf

Michael Fleder, Michael S. Kester and Sudeep Pillai (2014). *Bitcoin Transaction Graph Analysis*. HYPERLINK "http://people.csail.mit.edu/spillai/data/papers/bitcoin-transaction-graph-analysis.pdf"http://people.csail.mit.edu/spillai/data/papers/bitcoin-transaction-graph-analysis.pdf

Satoshi Nakamoto (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. HYPERLINK "https://bitcoin.org/bitcoin.pdf"https://bitcoin.org/bitcoin.pdf

Surae Noether (2014). Review of CryptoNote White Paper. HYPERLINK "http://monero.cc/downloads/whitepaper_review.pdf"http://monero.cc/downloads/whitepaper_review.pdf

Fergal Reid and Martin Harrigan (2011). *An*

Analysis of Anonymity in the Bitcoin System. HYPERLINK "http://arxiv.org/pdf/1107.4524.pdf"http://arxiv.org/pdf/1107.4524.pdf

Nicholas van Saberhagen (2013). *CryptoNote v 2.0*. HYPERLINK "https://cryptonote.org/whitepaper.pdf"https://cryptonote.org/whitepaper.pdf

Satoshi Nakamoto (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. HYPERLINK "https://bitcoin.org/bitcoin.pdf"https://bitcoin.org/bitcoin.pdf

See Fergal Reid and Martin Harrigan (2011). *An Analysis of Anonymity in the Bitcoin System*. HYPERLINK "http://arxiv.org/pdf/1107.4524.pdf"http://arxiv.org/pdf/1107.4524.pdf

Nakamoto (2008).

Michael Fleder, Michael S. Kester and Sudeep Pillai (2014). Bitcoin Transaction Graph Analysis. HYPERLINK "http://people.csail.mit.edu/spillai/data/papers/bitcoin-transaction-graph-analysis.pdf"http://people.csail.mit.edu/spillai/data/papers/bitcoin-transaction-graph-analysis.pdf

Reid and Harrigan (2011).

Jinyoung Lee Englund, spokeswoman for the Bitcoin Foundation. See ‘Silk Road arrest exposes a

hidden Internet', HYPERLINK "http://articles.baltimoresun.com/2013-10-06/news/bs-md-silk-road-tech-20131006_1_silk-road-deep-web-internet-privacy/2"http://articles.baltimoresun.com/2013-10-06/news/bs-md-silk-road-tech-20131006_1_silk-road-deep-web-internet-privacy/2

CoinJoin was first described in HYPERLINK "https://bitcointalk.org/index.php?topic=279249.0"https://bitcointalk.org/index.php?topic=279249.0

See Evan Duffield and Kyle Hagen (2014). *Darkcoin: Peer-to-Peer Currency with Anonymous Blockchain Transactions and an Improved Proof-of-Work System*. HYPERLINK "https://www.darkcoin.io/downloads/DarkcoinWhitepaper.pdf"https://www.darkcoin.io/downloads/DarkcoinWhitepaper.pdf

HYPERLINK "https://cryptonote.org/coins.php" https://cryptonote.org/coins.php

Nicholas van Saberhagen (2013). *CryptoNote v 2.0*. HYPERLINK "https://cryptonote.org/whitepaper.pdf"https://cryptonote.org/whitepaper.pdf

'Untraceable Payments', HYPERLINK "https://cryptonote.org/inside.php"https://cryptonote.org/inside.php

HYPERLINK "http://wiki.darkcoin.eu/wiki/FAQ" \l "What_can_I_expect_in_terms_of_traceability.3F" http://wiki.darkcoin.eu/wiki/FAQ#What_can_I_expect_in_terms_of_traceability.3F

HYPERLINK "https://blockchain.info/" https://blockchain.info/

HYPERLINK "http://monerochain.info/"http://monerochain.info/

HYPERLINK "https://blockchain.info/charts/blocks-size" https://blockchain.info/charts/blocks-size

HYPERLINK "https://blockchain.info/charts/n-transactions-total" https://blockchain.info/charts/n-transactions-total

HYPERLINK "https://blockexplorer.com/" https://blockexplorer.com/

Surae Noether (2014). Review of CryptoNote White Paper. HYPERLINK "http://monero.cc/downloads/whitepaper_review.pdf"http://monero.cc/downloads/whitepaper_review.pdf

Nakamoto (2008).

HYPERLINK "https://github.com/cryptosphere/rbnacl" https://github.com/cryptosphere/rbnacl

Adi Shamir (1979). How to share a secret. HYPERLINK "http://dl.acm.org/citation.cfm?doid=359168.359176"http://dl.acm.org/citation.cfm?doid=359168.359176

HYPERLINK "https://coinomat.com/" https://coinomat.com/