PocketRep

A Decentralized Cryptocurrency Economy Reputation Platform

Summary: Trust between buyers and sellers is a foundation of any economic system. Problem of trust is especially difficult in a digital economy. Growth of online commerce was facilitated by a successful solution of a problem of trust via online reviews, search engines and credit card chargebacks. However, that success is creating centralization and a new set of major problems. PocketRep offers a solution that will replace many present-day functions of search engines and review platforms in a decentralized pseudonymous blockchain. PocketRep efficiently gathers information from cryptocurrency transactions across other blockchains. PocketRep does not require use of specific payment systems or wallets, can be used with any wallet and with major cryptocurrencies. Platform providers or sellers can create specific reputation categories using a special kind of transaction. Buyers and sellers go through simple prior steps to ensure that a cryptocurrency transaction on Bitcoin, Litecoin, Ether etc. allows the buyer to leave a valid review on PocketRep. These simple steps depend on cryptography, but are unseen by the buyer and seller and can be done automatically independent of their wallet software or payment method. Seller and buyer use PocketRep app or an API call to create a commitment prior to the purchase. After this commitment is accepted in a PocketRep blockchain, a resulting cryptocurrency purchase can happen. After the cryptocurrency payment, a valid review transaction can be completed on a PocketRep blockchain. All PocketRep personas are public keys and possible nicknames. No personal information is divulged at all. Pseudonymous reputation for PocketRep personas is visible on a blockchain and does not depend on a specific platform, thus removing Walled Gardens and points of centralization. Despite visibility of pseudonymous reputation, there is no link between transactions on different blockchains and specific PocketRep personas. Ring signatures are used to break that connection. Information in PocketRep blockchain can be searched to find verified reputable sellers of any kind, trending sellers, platforms, products. PocketRep blockchain is open sourced and powered by the token called Pocketcoin. Pocketcoin has built-in protection against 51% attacks, because review commitments act as effective notaries of PocketRep/Pocketcoin blockchain on Bitcoin, Ether and other blockchains.

Intro: Current State of Trust in a Digital Economy

Trust and information are foundations of any economic system. If trust is eroded and mechanisms to create trust do not exist, only a basic level of economic activity is possible. This is even more true for a digital economy. Cryptocurrencies such as Bitcoin provide a novel and ingenious way to remove some risk (clearing risk) in a transaction without a trusted third party. However, cryptocurrencies are not a panacea. There are some aspects of trust they are simply not designed to handle. Does this seller offer superior goods and service? Is this freelancer consistently doing a great job? Is this apartment best for a three day stay in Budapest? Those kinds of questions are typically answered today with online research using search engines (google) or various specialized platforms that contain reviews (airbnb, amazon, tripadvisor, yelp). From this simple example, we can see two aspects of trust in action. First, trust must be expressed in some way. For example, on Yelp, Airbnb etc. trust is expressed by leaving a good review (or a bad one)[1]. This is more or less direct expression of trust. If you use search engines such as Google to research a purchase, they will use many indirect channels. For example, a website of a seller might come up to the top without a single review (rare, but possible). That could happen, because essentially Google search engine sees other sites trusting the site of the seller, and if the other sites are also trusted – this gives indirect indication of trust. So, we can see two mechanisms of trust expression (reviews and proper links from trusted websites). We also see two corresponding ways of learning about that trust (reading reviews and using search engines). Such a system of building trust (along with credit card chargebacks) worked amazing wonders for a digital economy. We will not inundate readers with numbers and projections, suffice it to say that digital economy is a dominant economy and likely will become just about the only way that buyers & sellers meet and research each other's trust metrics.

However, the current trust system has hit serious roadblocks that make its future growth doubtful or at least suggest that this growth will benefit centralized entities disproportionally relative to consumers.

The first problem is fake reviews. It is a well known fact that many platforms contain lots of fake reviews, anywhere between 20-60%. In a well-known experiment a Londoner was able to create a non-existent restaurant called The Shed and take it up to #1 as the best restaurant in all of London on TripAdvisor[i], a widely used review site. A founder of Fakespot.com Ooi Ming estimated that 40% of reviews on Amazon are fake. Of course, Amazon has Verified Purchaser reviews and those are more expensive to fake en masse. If a Verified Purchaser also has a coherent story justifying their review, it becomes much more valid. That is why reviews on platforms like Airbnb are far more trustworthy, all reviewers are purchasers.

The second major problem is increasing ubiquity of Walled Garden strategies by leading providers. A Walled Garden is a closed ecosystem in which all operations are controlled by the ecosystem operator[ii]. This means, among other things, that any expression of trust within the ecosystem is walled off within that ecosystem and cannot be reliably ported to another platform. In essence, if you are selling something on Amazon, your reviews are stuck on Amazon and you can never take them with you. Amazon and others can simply corner the market with its size and stifle competition.

The third problem is related to the second one and it is censorship. Algorithms that google or facebook uses to deem content inappropriate are extremely opaque. And as those companies grow more and more powerful, they will have to worry about competition less and will use the power of trust to their benefit. This means that they can use their 'search engines' (using the term loosely) to increase your level of trust in something that does not objectively merit it. Only one and likely not the biggest example of that is a $4.2B fine that EU handed to Google for favoring its own comparison shopping tools over competition and demoting rival services. Essentially, Google and Amazon are huge gateways and they can sell whatever they want to sell, because their trust measurement algorithms are extremely opaque.

I. Cryptocurrency Transactions as Expressions of Trust on a Publicly Visible Ledger

Now, let's consider how cryptocurrencies fit into this picture. We can actually think of many cryptocurrency transactions as direct and public expressions of trust. How so? Every payment is public

[1] We will not for now touch on the veracity of the reviews on Yelp or any other platform, we will just look at the intent and how it is used in daily life.

on a blockchain (except privacy minded currencies like Monero, but even there transactions are still visible). If this transaction took place between two people – then it is an expression of trust. There are close to 200,00 daily transactions only in Bitcoin. If you add Litecoin, Ether you are looking at a staggering wealth of information on how people trust each other. If we could take that data and verify whether trust was fulfilled or failed, we would have a much better information set than search engines or review platforms. It would be better than search engines, because search engines deal with mostly indirect information about trust. And they have a power to bias that information in their favor. It would be better than review platforms, because every transaction would have a verified purchaser, the verification would be the same and buyer would not have to look in different places. All trusted sellers and counterparties would be found easily in one blockchain, the data would be objective and transparent. This is a difficult task, but we will show with PocketRep that is doable. Moreso, we will ensure that parties do not compromise their privacy if they do not want to, and are still able to partake in this new kind of peer-to-peer trust system without a trusted authority.

Goals of PocketRep reputation platform

Throughout the paper we will use terms Buyer and Sender to mean a person that is sending cryptocurrency and leaving a review. We will called Seller or Receiver the person who will receive both the cryptocurrency and a subsequent review.

A. Allow payers in cryptocurrency transactions to review the payee's pseudonymous identity called PocketRep Persona). Only actual payees can leave reviews, review requires a confirmed underlying transaction on a suitable blockchain.
B. Allow payee to present their aggregate reviews (PocketRep Score) as well as individual reviews and comments to anyone and anyone should be able to verify with a suitable app.
C. Allow cryptocurrency platforms, websites and sellers to create specialty reputations to enable narrow reviewing based on segment or specific goods/skills. Enable those platforms to easily embed PocketRep via a simple API into their marketplace.
D. Allow anyone to search PocketRep blockchain for trusted sellers in specific categories, trending categories (number of reviews is growing).

What PocketRep reputation does not do:

A. It does not create by default a persistent link to the identity of an individual. PocketRep public/private key represents a persona and a new persona may be created. Under certain settings some platforms can link the PocketRep Persona to the actual identity of the user on the platform and disallow user from using another PocketRep Persona.
B. Thus, PocketRep Score cannot be counted on to show all of the bad deeds of any person. The goal is to make it very costly to deceive people by having to 'burn' a good reputation.

Important Considerations:

Before we dive into the cryptography and design of the system, let's answer some questions that an astute reader is ready to ask.

A. There are risks with the review process that are simply not present in cryptocurrencies. For example, there is risk that Receiver with good reputation will want to cheat on this particular transaction and will want to divert the final review elsewhere (in cryptocurrency there is no risk that someone wants to divert payment away from himself).

B. Similarly, there is risk that Sender will want to direct review not to the Receiver, but elsewhere (whether to help or hurt some third party that was not party to this TX).

C. There is a risk that someone will want to try to use pre-existing TX on BTC blockchain (or another blockchain supported by PocketRep) to create reviews without actually transacting.
The first three risks are dealt with using cryptographic methods in Step 1 below.

D. Of course, there is the standard risk of fake reviews by performing meaningless transactions using cryptocurrency, a Cybil attack. We will spend a bit more time on this risk here. There are four major vectors of prevention of this type of an attack.

   1. Because reviews are public, reviews in short period of time can be viewed as less reliable. So, it takes time and effort to build a reputation using meaningless transactions.
   2. It takes transaction costs on cryptocurrency blockchains and eventually on PocketRep blockchain to leave reviews (not for the first year). It takes many good reviews to impact a reputation and if they have to be spread over time, the cost in money and time becomes significant.
   3. It is easier to burn a reputation than to build it. There is a typical percentage of bad reviews for good sellers, bad reviews beyond that will start hurting the reputation of a seller. So, investment of time and money to build up a reputation, even if successful, can only pay dividends if a seller keeps getting real good reviews.
   4. An analogy with search engines would be useful. When Google released its first search engine, it could be fooled with simple backlink strategies. However, over time Google found effective ways to deliver relevant content to the top of the search, despite manipulation. PocketRep is decentralized, but there are certainly ways to add rules to the blockchain consensus that would reject offenders who create fake reviews by sending money from one address to another or even using a cluster of addresses. Blockchains are public ledgers and it is much harder than it seems to create untraceable money flows. Any accounts that are used to inflate reputations could be clustered and traced with simple rules by PocketRep nodes (especially, since they are already uniting many blockchains). Of course, any such restriction can be overcome with sufficient Black Hat reviews, the question only is in cost, time, effort. Eventually, in order to leave an effective review, someone has to move money a few times, or exchange them between blockchains, give pauses to make it more believable, then write a believable comment. This would mean that PocketRep became extremely popular and community will be able to fight back by improving consensus algorithms that accept review as valid. This will not be much different than search engine arms race with Black Hat SEO and as long as it is expensive to fake a reputation, it can serve a valid social purpose.

Now we can move on to the description of the process.

II. The PocketRep Blockchain and Review Process

S. is the Sender – a person that pays someone money on a suitable blockchain and will have an opportunity to leave a review for R. (Receiver of both money and subsequent review)

Step 1 – R. sends Review Commitment signed by ks(R) draft to S. securely with add'l data

Overview: In this step a Recipient sends a draft of the Review Commitment to Sender for verification and signature. The communication happens over an encrypted channel through the PocketRep app or some other app that supports opens sourced PocketRep protocol. We are using a concept of stealth addresses and ring signatures that are similar (though not the same) to the ones used in a Cryptonote protocol. Some notation

$K(R)$ - Receiver's public key. It is really the PocketRep persona (though nicknames or emails can be used for communication, they will be resolved to this public key). It consists of two parts:

$Ks(R)$ – Receiver's 'send' address. This is the terminology of Cryptonote currencies, but the meaning is different in the review transactions on PocketRep.

$Kv(R)$ – Receiver's 'view' address.

$K(S)$ - Sender's public key. Consists of:

$Ks(S)$ – Sender's 'send' address

$Kv(S)$ – Sender's 'view' address

G –base point on an appropriate elliptic curve (in this case we are using Ed25519[iii] curve)

r, v – random numbers from the group

Here are various parts of that Commitment draft.

A. Review Commitment includes the R.'s BTC or other cryptoFX address (Ether, Litecoin etc). The reason it is done at this stage is to ensure that an existing cryptoFX transaction cannot be chosen arbitrarily to create a review.

B. Review Commitment includes one time receiver's address $K_O(R) = r * G + Ks(R) = r * G + ks(R) * G$. This is somewhat similar to the one-time stealth address in a Cryptonote whitepaper. Note, that essentially the Receiver is creating a one time address for himself, which is different from any cryptocurrency transaction. This ensures that the ultimate target of review is set and Sender cannot change the $K_O(R)$ is indeed related to the PocketRep ID $K(R)$. If this was not the case, the Sender could have manipulated the deal to actually review someone else. Also, receiver's stealth address is simplified relative to the CryptoNote protocol[2] . The resulting receiver's private key for the one time stealth address will thus be: $k_O(R) = r + ks(R)$.

C. R. also creates the one time stealth address on behalf of the Sender $K_O(S) = H\big(v * Kv(S)\big) * G + Ks(S)$ and adds it along with $v * G$ (similar to CryptoNote protocol) to enable S. to recover private key without knowing the random number v. The sender's one time private key that will be used to sign the Commitment Review and later sign the actual review is $k_O(s) = H\big(v * G *$

[2] The formula for a stealth address in Cryptonote protocol is $K_O(R) = H\big(r * Kv(S)\big) * \mathrm{G} + Ks(R)$. We simplified to have a more efficient zero knowledge proof later; it will enable us to leave verified reviews without connecting PocketRep personas to actual cryptocurrency transactions.

$kv(S)\big) + ks(S)$. Therefore Sender can recover $k_O(s)$ with the help of her private key $kv(S)$ and $v * G = V$, so that $k_O(s) = H\big(V * kv(S)\big) + ks(S)$

Note that $K_O(S)$ will now be locked and cannot be changed by the Sender (because Commitment will be signed by $k_O(R)$ which only Receiver possesses).

D. The whole Review Commitment TX carcass is signed by the Receiver with $k_O(R) = r + ks(R)$. This requires private key $ks(R)$ and knowledge of random value r. This is done to prevent reviews to non-participants in a transaction.

E. Last step is quite important, but not strictly a part of Review Commitment. Separately (not part of Review Commitment and does not go on blockchain) R. communicates ‘r’ in some encrypted form to S. to verify that the final review will actually go to the Receiver. This is to avoid a situation where a Receiver with good reputation intends to cheat and wants to divert this particular review to someone else’s one time address or to ‘nowhere’. To prevent such a bait and switch attempt, R. communicates ‘r’ to S. in some encrypted form. S. can verify that $K_O(R) = r * G + Ks(R)$ using the random value and Recever’s public send key. Note that the knowledge of random value does not allow Sender to recover Receiver’s one time private key, since that would still require solving a discrete log problem without knowing $ks(R)$.

Step 2 – S. sends the Review Commitment to PocketRep blockchain

Sender’s app/wallet performs the following steps and verifications :

- BTC Rec. Adr. matches the one receiving the funds
- $K_O(R) =?\ r * G + Ks(R)$
- $K_O(s) = H\big(v * G * kv(S)\big) * G + Ks(S).$
- The signature by $k_O(R)$ on the whole Review Commitment matches $K_O(R)$

If any verifications fail, Sender should know that review will not go to the Receiver of funds. An app being used by the Sender should flash a warning that there is a mistake or an attempt to bypass review.

Step 3 – PIN CODE

A PIN CODE will be calculated at this point. It is central to the review process, because it will be the marker that connects a Commitment on a PocketRep blockchain to the cryptocurrency transaction on an external blockchain. It also protects the integrity of PocketRep blockchain against 51% attack (discussed below) $PIN\ CODE =$ $RIGHT3(H(BTC\ Rec.Adr., PocketRep\ Previous\ Block\ Hash, Block\ Number))$

$RIGHT3$ is a function that accepts an alphanumeric string (such as a hash) and outputs 3 rightmost digits found in that string

The PIN Code will be used to link Review Commitment with cryptocurrency payment on an external blockchain (described in step 5 below).

Step 4 - Sender now signs the Commitment Review with ko(S)

Sender sends Review Commitment TX to Pocketrep blockchain. To summarize, it has the following components:

a. BTC Rec. Adr.
b. Recipient stealth address $K_O(R)$
c. Sender stealth address $K_O(S)$
d. Blockchain identifier $B = \{BTC, ETH, LTC, \ldots\}$
e. PIN code
f. Schnorr signature with $k_O(R)$ on the Hash(a,b,c,d) signed by the Receiver
g. Schnorr signature with $k_O(S)$ on the Hash(a,b,c,d,e,f)

All of these steps are happening in the background, in the interface the application simply shows Invitation to Review for Sender. Once accepted, the PIN CODE is received back by Sender's app/wallet from the first node and is shown in the app for the Sender to enter as last digits of amount.

At this point, PocketRep blockchain will perform the following verifications:

V1. Signature $k_O(S)$

V2. Signature on $k_O(R)$

V3. $PIN\ CODE = ?RIGHT3(H(BTC\ Rec.Adr., PocketRep\ Previous\ Block\ Hash, Block\ Number))$

It is possible that Commitment had to wait a block to get into the block chain, so two previous blocks are allowed as previous block hash.

Step 5 – CryptoFX Transaction to CryptoFX R. address in the Review Commitment

Sender now completes the CryptoFX transaction on a supported blockchain. Transaction goes to the CryptoFX Receiver address. That address is in the Commitment on PocketRep blockchain. The amount in the transaction needs to have the PIN CODE as the rightmost 3 digits of the amount[3]. Sender will have 60 minutes or 6 times the 10 minute block to complete the transaction, otherwise Commitment is invalidated.

[3] For Ethereum 999 WEI is far less than one cent. For most other blockchains, this is also true. At the Bitcoin price of $10,000, the maximum amount of 999 Satoshi would be about 10 cents. When PocketRep is integrated into a buyer-seller platform through the API or if CryptoFX payment itself is going through the PocketRep app, the PIN CODE amount between 001 and 999 Satoshi would automatically be added to price. Otherwise, it would be added manually by the Sender. As PocketRep gets more deeply integrated into payment platforms/wallets, there is ability to move away from the PIN CODE amount to using cryptographic methods to prove commitment (like signing with the same private key that was used in a CryptoFX transaction to verify ownership of a transaction).

Again, we are using Bitcoin only as one example, but PocketRep can support variety of blockchains such as Ether, Litecoin and even certain blockchains with anonymity properties based on various forms of zero knowledge.

When a cryptocurrency transaction is completed, it must conform to the prior PocketRep Review Commitment that is already on the PocketRep blockchain. It must go to the same receiver CryptoFX address and 3 rightmost digits of the amount must match the PIN CODE derived from the receiving public address and a timestamp.

Importantly, most nodes in PocketRep network must have received the Review Commitment before the CryptoFX transaction that it is committing to for obvious reasons.

Each node receiving the Review Commitment timestamps it in UNIX Epoch Time in milliseconds. Each node will find corresponding transactions on BTC, LTC, ETH etc. blockchains and will store them in the same Commitment/related payment table with timestamps. Later, in step 5, when the review actually occurs, every node will connect to 8 nodes and check that the median difference between Review Commitment and Cryptocurrency transaction is positive (i.e. that payment happened after the commitment). All PocketRep nodes are required to use NTP to synchronize their clocks[4]. Peers whose clocks drift more than 30 seconds are disconnected.

Step 6 – Anonymous ReviewTX using Ring Signatures

The motivation for this step is as follows. Our main goal with PocketRep to increase trust level of cryptocurrency transactions on all major blockchains and to increase cryptocurrency adoption as a method of payment, rather than a speculation play. However, we do not want to enable tracking of different transactions on cryptocurrency blockchains to one PocketRep ID, even though that ID is pseudonymous. As a first step towards protecting privacy rights of individuals, we integrated CryptoNote like ring signatures in the review process, along with unique ring decoy choosing (based on the specifics of the PocketRep platform) [5].

Let w be the message to sign with ring signatures, where w contains of:

-Review 1-10 stars

- Review comment hash and offset to find it in the blockchain (text of review will be stored in the Node in separate storage)

Sender would like to send the review to the public PocketRep ID of the Receiver, but we do not want to connect this review to a specific Review Commitment or to a specific CryptoFX payment on Bitcoin,

[4] Note, that the precise time is not relevant (though all nodes synchronize the time using NTP protocol). The reason TIMESTAMP is done on a node is that PIN CODE needs to be variable enough to be different for different transactions to the same Receiver address, yet this variability should be out of Sender's and Receiver's control, otherwise one or both of them could brute force a necessary PIN for a given BTC. Rec. Adr. If targeting a specific PIN for a given BTC. Rec. Adr. is possible, then reviews can be faked for those addresses that get regular payments in predictable amounts (e.g. subscriptions).

[5] We are also investigating newer methods that are not quite practical yet, but offer potential e.g. Bulletproofs.

Litecoin, Ether etc. blockchain. The reason for this is we do not want anyone to be able to link PocketRep ID (which is again, public) to many different transactions on Bitcoin or other blockchains. For this we need to define a set of Review Commitments, $C = \{C_1, C_2, \dots, C_n\}$ which occurred during time interval $T = \{t_s, t_e\}$. The time interval will be some period starting from the time of review going back 4 weeks. Commitments have to have verified to have qualifying transactions on blockchain. That means that a receiving address in a CryptoFX transaction (BTC. Rec. Adr.) must match the one in Review Commitment. It also means that most PocketRep nodes need to timestamp the CryptoFX transaction on blockchain B after the Review Commitment transaction (PocketRep nodes 'listen' and store 4 weeks of history on all applicable blockchains). It means that the PIN CODE in Review Commitment must match the rightmost 3 digits in the amount of the CryptoFX transaction. Once we have gathered our set of commitments, we need to create a zero knowledge proof[6] with three components:

a. Prove that reviewer possesses a one-time Sender's private key $k_{i,O}(S)$ to match $K_{i,O}(S)$that was used in Review Commitment C_i. Ring signatures are based on work of Fujisaki et al[iv]
b. We have to make sure that Sender cannot use the same unknown commitment C_i to leave two reviews. This is achieved in the same way as in CryptoNote protocol, using key image. The key image in this case is $\widehat{K} = k_{i,O}(R) * H(K_{i,O}(R))$. Blockchain will store key images and check for double spend or rather 'double review' as in CryptoNote protocol. This way one Sender's one time private key that is unique to a commitment can be used only once.
c. A separate proof can be performed to confirm that the recipient of the review is the same person as Receiver of funds with PocketRep ID $Ks(R)$ without disclosing which commitment is being referenced. In other words, reviewer knows such r on one of the commitments C_i that makes $r * G = K_{i,O}(R) - Ks(R)$. So, Sender (reviewer) sends the review to the public PocketRep ID, but doesn't confirm which exact Review Commitment gives her the right to review the Recipient, only that such a Commitment is connected to one of verified CryptoFX transactions on external blockchains and Sender knows both the private key from the Commitment (steps a and b above), as well as the PocketRep ID that was used to derive the one time address $K_O(R)$ that is part of the Review Commitment. As is clear from the formula above, this can be treated as ring signature with private key r on ring public keys $\{K_{1,O}(R) - Ks(R), K_{2,O}(R) - Ks(R), \dots, K_{n,O}(R) - Ks(R)\}$ with publicly known curve base point G. And this signature verification can be performed using Back's Linkable Spontaneous Anonymous Group signatures (reference).

To summarize, PocketRep blockchain performs the following verification steps on the Review Transaction:

V1. Verify ring signature to prove that reviewer possesses a one-time Sender's private key $k_{i,O}(S)$ to match $K_{i,O}(S)$that was used in Review Commitment C_i.

V2. Verify ring signature to prove that reviewer possesses the stylized private key to one of the valid commitments. In other words, that the reviewer knows such r on one of the commitments C_i that makes $r * G = K_{i,O}(R) - Ks(R)$

V3. That the Review Transaction is happening within 28 days of the commitment

[6] In the specific sense of ring signatures i.e. not disclosing which member of the ring actually signed.

V4. That Review Commitment at a given offset matches Review Commitment hash supplied in the review

V5. That Review Commitment referenced itself refers to a valid external blockchain payment with a

$$PIN\ CODE\ =?\ RIGHT3(H(BTC\ Rec.Adr.,PocketRep\ Previous\ Block\ Hash,Block\ Number))$$

This step verifies both the accuracy of the PIN Code and also that Commitment is found in the next block after previous block referenced (with a margin of one block, because Commitment may not have gotten in right away)

V6. That median time difference between Review Commitment/CryptoFX Payment based on querying 8 random nodes is positive (i.e. that payment happened after the commitment)

This is an additional protection against trying to find suitable transactions on cryptocurrency blockchains i.e. transactions that happen to match

$PIN\ CODE = RIGHT3(H(BTC\ Rec.Adr.,PocketRep\ Previous\ Block\ Hash,Block\ Number))$ in the last three digits of the amount.

Creation of Special Reputations "RepSpecTX"

PocketRep by default has one general reputation and offers ability to create Specialty Reputations with a special kind of transaction “RepSpecTX”. Specialty reputations have a very important on-chain property. They have a fixed easily recognizable prefix that resolves to a name, description and tags in all applications interfacing with PocketRep blockchain. Anyone can create a Specialty Reputation as long as they pick a unique name and pay a transaction fee to reserve the prefix, name, description, tags and logo on the blockchain. It is similar to creating a domain on the web. Here is what “RepSpecTX” transaction contains:

A. Address Prefix e.g. CBNB (should be under 8 characters).

B. Description "Addresses with prefix CBNB are used to leave reviews on the site cryptobnb.com only. We have the best decentralized platform for renting out apartments and we charge you less than 1% vs the 15% charged by Airbnb."

C. Add tags for quick search

D. Fee in Pocketcoin based on TX size.

E. Load a picture representing the reputation to store on node (hash in the transaction)

F. Another opportunity for platform owner might be to prepay transaction costs of anyone using their address prefix (especially if they can reserve it with a ‘key’) by connecting some additional amount in Pocketcoin in the RepSpecTX.

The special reputation prefix creation TX goes onto blockchain like other transactions, but nodes have special storage for it for easy reference and loading of data (similar to unspent UTXO in BTC).

As an enhancement, it is possible to offer users to close their reputation to outsiders by requiring a special key that could change, similar to an API key.

How Specialty Reputations Are Used:

1. When users open up PocketRep app for the first time, they can search by text, tags through hundreds or thousands (or more) of available reputations (by tags, reputations can also be suggested by interests etc.).

2. For each SpecRep they will see total number of reviews under it, to see how popular it is. They can click and explore these reputations. There are trending specialty reputations.

3. When someone advertises their reputation, PocketRep apps will immediately recognize it by the address prefix.

4. Anyone can use any reputation (just like anyone can post links to any site on the web), but they would be promoting someone else's reputation.

5. App can help user find PocketRep IDs that have the highest reputation for a given specialty reputation.

6. Platform owner could close the reputation by requiring a special other key (that is a future enhancement that requires work and will cost more).

Summary: We have described PocketRep – a decentralized pseudonymous trust system that allows for personal ownership of transaction based reputation and easy search for most reputable sellers in any category of goods or services imaginable. PocketRep has the potential to decentralize many of the activities that are at the core of digital economy, thereby creating immense value and distributing it to producers and consumers in a digital economy without creating centralized power structures.

Mining, Consensus Rules and 51% Attack

PocketRep is based on a proof-of-work mining algorithm similar to most standard cryptocurrencies. There is one important modification that makes PocketRep and Pocketcoin more resilient against 51% attacks that are becoming quite prevalent against the altcoins[7]. Recall that we have the following sequence of events when it comes to reviews:

Review Commitment >> Cryptocurrency Transaction >> Review

This chain provides a connection between PocketRep blockchain and external cryptocurrency blockchains. Recall that a value we called PIN Code is a three digit number derived from the rightmost digits of a cryptographic hash of external blockchain receiving address and PocketRep previous block hash. We can rely on this link to defend the PocketRep blockchain against the 51% attack. PocketRep blockchain has an additional consensus rule as follows:

Any reorganization of the PocketRep blockchain will have to go through an additional check. In addition to validity of proof of work chain of blocks, any block that is more than 5 blocks deep can be checked for correspondence with other blockchains. We have to assume that if someone went through the expense of adding a Review Commitment to the PocketRep, then they are likely to complete the resulting

[7] https://techcrunch.com/2018/07/22/rental-attacks-mean-that-blockchains-must-evolve-or-die/

transaction with the PIN code amount embedded in it. But the PIN Code is related to the PocketRep's previous block hash, because it is derived from its hash with the cryptocurrency Receiver address. This is not a direct relationship, as in 'delayed proof-of-work' where trusted nodes actually notarize blockchain's block on Bitcoin or some other blockchain with lots of hashing power. Essentially, users of PocketRep collectively act as notaries in a probabilistic sense. So, any node that is asked to reorg blockchain, can add a rule that any block that is more than 5 blocks old has to contain Commitments with PIN Codes that can be found on external (Bitcoin, Litecoin, Ether…) blockchains. Even if some Commitments will not result in a transaction, many or most will, because a Commitment is time and fees expanded specifically to create that transaction. So, a node can check that a block that is offered as a replacement as a supposedly longer proof-of-work chain actually has commitments that correspond to transactions on external blockchains. In other words a valid block can be displaced only by a block that not only is part of a longer proof-of-work chain, but also has more of its Commitments confirmed on external blockchains with PIN Codes that include a prior block hash from PocketRep[8]. Attacker could attack the proof-of-work hash preimage argument and create a longer chain. Attacker could also create lots of Review Commitments and manipulate timestamps on his nodes. But it would be extremely difficult to ensure that many of those commitments have corresponding Bitcoin, Litecoin, Ether etc. transactions with PIN Code amounts that match the relevant previous PocketRep blockhash.

Appendix A: **Choosing Ring Members**

PocketRep blockchain contains a public pseudonym. The reputation of the pseudonym and all its review transactions are public knowledge. We need this to have a verifiable reputation score and for enhancing trust in cryptocurrency transactions. However, at the same time, we would like to afford privacy to the individual behind the pseudonym. That is why in the final step we use ring signatures, a simple, but robust form of zero knowledge proof. Ring signatures are well studied and have been used successfully by cryptocurrencies to enhance privacy. However, our use is in PocketRep is different from use in cryptocurrencies. On one hand, review transactions do not have 'flows', meaning that once review is received, it is never sent on further. This complicates attacks on privacy, because one of the key ways they happen is by tracking flows over time.

On the other hand, Review Commitment and Review transaction refer to external blockchain public addresses and transactions. One of the weaknesses of blockchains (except Monero and some others) is that they allow for public address clustering based on various measures. So, we need to keep in mind that it is possible an attacker already clustered some addresses on external blockchains, for example bitcoin. Then they come to PocketRep looking to link those clusters to PocketRep personas. This presents a unique to the ring signature privacy mechanism. Self-contained blockchains do not have to deal with this threat. Intuitively, it is clear that if an attacker links enough transactions on an external blockchain, they can simply examine rings where this transaction was present and then identify the most frequent PocketRep persona that is the target of reviews using those rings. If rings are chosen,

[8] Of course, Commitment may not have gotten in for a block or two, so it is possible to refer to a hash of a block within 3 blocks of the verification.

randomly, there will be a high chance that they will succeed. Ring selection to defend against such an attack deserves a separate paper (which is forthcoming), however we will give an outline here.

Let's make some simple assumptions to test our hypothesis. We will assume that we are looking at some period over which 500 PocketRep personas have completed 10 transactions each on an external blockchain i.e. there are 10 rings leaving reviews for each PocketRep persona. We will assume a large ring size of 32 here. Further, we will assume that an attacker has been able to link 2,3,4,5 of those transactions somehow on that external blockchain. Of course, good privacy techniques should not allow an attacker to easily do that, but we will assume that cryptocurrency user did not use the best privacy techniques to begin with. We can first see what we are up against theoretically and then run a simulation.

Let's define:

PR_1 is the probability that any given cryptocurrency transaction is referenced in a given ring

$PR_1(10)$ is the probability that a given cryptocurrency transaction appears in one of 10 rings targeted to a specific PocketRep persona

$PR_1(10, X)$ is the probability that X transactions where $X = \{2,3,4,5\}$ all referenced in rings that are targeted toward a single PocketRep persona

$PR_{ANY}(10, X)$ - probability that X transactions appear in 10 rings with reviews for any given PocketRep persona (in other words in any of the 500 sets of 10 rings for each PocketRep persona)

$PR_1 = 32/5000$

$PR_1(10) = PR_1 * 10$

$PR_1(10, X) = PR_1(10, X)$ ^ X and finally $PR_{ANY}(10, X) = PR_1(10, X) * 500$

We can see that if an attacker is able to connect three transactions on an exernal blockchain and we pick ring members randomly, then probability that a random PocketRep persona will have all 3 in their 10 rings is only $PR_1(10, X) = 13.11\%$. For $X = 4$ such probability is .84%. Therefore, if there will be a PocketRep persona that has all these TX in their rings, they are likely the target. We could simply ignore this problem, since it originated on an external blockchain and not on PocketRep, but we would rather mitigate this type of an attack.

To that end, we propose to choose rings in a specific way, so as to thwart such an attacker.

Random Decoy Clustering algorithm description: When choosing 31 decoy ring members for any ring, do the following. Look back at all review commitments that had qualifying transactions on external blockchains. That will be the same overall set of decoys from which random decoys were chosen in our random algorithm above[9]. Instead of choosing decoys randomly, we will look at past rings where our genuine commitment was used. Using the notation from ring signature section, let's add a time dimension to it and call the set $C_t = \{C_1, C_2, \dots, C_n\}$ and our real commitment is say C_2. So, we will find all C_t where C_2 was already present and pick 3 other random companion commitments from those rings

[9] Since there is a period of 28 days to leave a review, this will only collect valid review commitments from the past 28 days.

only. Using 10 decoy ring 'farms' we will get 30 commitments and since we are using ring size of 32, we will simply get 4 instead of 3 from one random ring 'farm' to get a total of 31. It is not difficult to see that all Commitments (and thus related external blockchain transactions) will naturally cluster, but cluster in a random way interfering with the attackers ability to use breaches of privacy found on other blockchains through clusters.
We ran a simulation in Mathworks' Matlab to demonstrate the difference in the approaches. To measure results we introduce a measure we call Persona Ambiguity. It is related to $PR_1(10, X)$, but instead of probability, we measure how easy or difficult it is to cluster external blockchain transactions to PocketRep personas.

Defining Persona Ambiguity for three linked transactions on external blockchains:

Step 1: Attacker is able to link 3 addresses on an external blockchain.

Step 2: Attacker then observes that that are three commitments corresponding to those addresses on PocketRep blockchain. Since in the simulation we know which commitments are real and which are decoys, we give the attacker the benefit of the doubt and assume that he is correct and those 3 addresses are present in commitments and then reviews (together with decoys) to a single PocketRep Persona. To increase sample size, we will allow the attacker to correctly identify (without knowing he is correct) three transactions from each PocketRep Persona (there are 500 total, so attacker linked 500 sets of 3 transactions).

Step 3: In order to identify a single PocketRep persona, attacker looks at all of the rings where these commitments were used in a review ring and groups them by PocketRep Person – the recipient of a review.

Step 4: Any PocketRep persona that has these 3 transactions in distinct rings reviewing that persona is a suspect.

Step 5: Persona Ambiguity is calculated as total number of times the attacker is able to link a set of three transactions to some PocketRep Persona divided by the total number of PocketRep Personas.

The results of five simulation runs are as follows.

Random Decoy Selection	Random Decoy Clustering
1.22	12.63
1.2	12.44
1.2	12.38
1.25	13.04
1.2	12.71

First, let's consider Random Decoy Selection column. Note, that simulation differs somewhat from the theoretical probabilities we calculated above. Persona Ambiguity is the number of people that share links to a set of 3 external blockchain transactions. Because we gave attacker the power to correctly link the transactions, there will always be at least one target PocketRep Persona by construction. Random Decoy Selection is quite stable and on average it points to ~1.2 personas who share the three correctly chosen transactions. Simulation is modeled through time and there is some artificial clustering in early periods due to smaller number of decoy choices. That is why it shows a bit more ambiguity than statistical calculation of 13.11%, which would imply Persona Ambiguity of about 1.13 in a simulation. Regardless of whether it is 13.11% or closer to 20%, there is still a very high chance of connecting a cluster of external transactions to a PocketRep Persona.

However, if we look at our Random Decoy Clustering algorithm, we see that attacker's job is much harder. Because of random clustering, the three transactions can plausibly be connected to 12-13 PocketRep personas. Therefore, creating random clusters makes it more difficult for attackers who were able to link some transactions on external blockchains to perform a cross chain attack on privacy. Of course, if an attacker is able to consistently connect many of the external blockchain addresses, the efficacy of such clustering will decline. PocketRep researchers are researching solutions to this problem such as Bulletproofs[v] and ZK-STARKs[vi]. They are not practical yet, but have some features that show tremendous promise. This is especially true for Bulletproofs and batching capability which could be used in PocketRep.

[i] https://searchengineland.com/why-we-need-to-fight-fake-reviews-295005

[ii] https://medium.com/mediarithmics-what-is/what-is-a-walled-garden-and-why-it-is-the-strategy-of-google-facebook-and-amazon-ads-platform-296ddeb784b1

[iii] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted Edwards Curves, pages 389–405. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008

[iv] https://eprint.iacr.org/2006/389.pdf

[v] https://eprint.iacr.org/2017/1066.pdf

[vi] https://eprint.iacr.org/2018/046.pdf