Issues in Designing a Bitcoin-Like Community Currency

David Vandervort, Dale Gaucas, and Robert St Jacques

david.vandervort@xerox.com, dale.gaucas@xerox.com,
robert.stjacques@xerox.com
PARC, Webster, NY

Abstract. The invention of the Bitcoin protocol has opened the door to new forms of financial interaction. One such form may be to adapt Bitcoin technology for use as a community currency. A community currency is a form of money issued by a non-government entity to serve the economic or social interests of a group of people, often in a small geographic area. We propose a model of a community cryptocurrency that includes a community fund from which community members may take out loans if the community votes to approve them. We consider possible vulnerabilities and mitigations to issues that would affect this community fund, including issues of identity, voting protocols and funds management. We conclude that these vulnerabilities are, in most cases, amenable to technological mitigations that must be adaptable to both community values and changing conditions, emphasizing the need for careful currency design.

1 Background

Money issued by national governments is a dominant fixture of modern economic exchange. So called fiat currency is freely traded for goods and services, with its printing, issue and acceptance protected by law. Bitcoin and its derivatives are a different kind of currency, useable for many purchases despite being non-government issued and protected by no law. Community currencies, including such subtypes as Local Exchange Trading Systems (LETS), time banks and business trade exchanges, are similar non-state issued moneys that circulate in parallel with fiat currencies [1]. Purposes of community currencies often go beyond economic exchange to supporting values and causes including social, environmental or ethical dimensions [2].

Examples of community currencies include the Brixton Pound, Ithaca Hours and BerkShares. Each serves a different local area and evinces a different philosophy of society and economics in its construction. Bitcoin is a digital currency that was developed in order to remove the need for a central authority (i.e. banks) to mediate and clear transactions and to protect the privacy of those engaging in transactions [3]. This is clearly also a philosophy. In a sense, Bitcoin can be regarded as a community currency, with the community being those people who care about Bitcoin. They have shown the ability to work together toward goals large and small, to hold informative discussions, to build an economy and to help each other in times of need. It seems reasonable then, to consider ways in which Bitcoin technology could benefit other communities.

1.1 Cryptocurrencies

Because of its use of cryptographic methods to protect the integrity of transactions and of the currency itself, Bitcoin is known as a cryptocurrency. Advantages of Bitcoin include immutability of transactions, pseudonymity, distributed control that prevents manipulation by a central authority, complete transparency (as anyone, anywhere can download the blockchain and view all transactions) and strong cryptographic protection against tampering.

While Bitcoin was the first cryptocurrency, it was quickly followed by an explosion of currencies based on the same or very similar technology. There are a plethora of cryptocoins available besides Bitcoin, including Litecoin, Mastercoin, Primecoin, Marscoin, Zerocoin, Dogecoin, Reddcoin and many others. Many of these experiment with slight differences in the protocol to serve perceived needs of the community and the world.

Bitcoin is a software based system. Bitcoin transactions manipulate data to exchange ownership of bitcoins between addresses, with no requirement for physical exchanges of notes or coins. This allows complex scripting of behaviors, such as m of n (multi-signature) transactions and smart contracts [4]. It also means that any behavior that can be expressed in code can theoretically be encoded into a Bitcoin-like protocol. If this is true, then features found in community currencies may be added to Bitcoin to make something new.

2 Community Cryptocurrency Features

Community currencies include features beyond direct economic value that are intended to advance their goals. Two important features for the present discussion are demurrage and the maintenance of a fund for loans or grants. Demurrage is the practice of reducing the value of currency in proportion to the time it is held, rather than spent. Reportedly, the “peanuts” LETS currency in Chiba Prefecture in Japan charges a 1% fee per month on currency that is not used. Demurrage encourages people to keep circulating currency so as to avoid the loss of value. This is reportedly a significant factor in the success of Peanuts [5]. Note that the velocity of a community currency (roughly, the number of times a single note or coin is re-spent in the economy) can be quite high and demurrage is sometimes cited as one of the reasons [6].

A loan or grant fund is possibly one of the most powerful tools of development possessed by community currencies. The BerkShares currency maintains a loan fund for local businesses [7]. It is not unusual for hours based systems such as Ithaca Hours and Calgary dollars also to provide small loans or outright grants to local businesses [8]. Small business loans can be a driver of economic development. As well, personal loans and grants can be tools for assisting those in need. Loans can also be targeted at types of businesses, or interest rates tailored to meet social as well as economic goals.

Other possible features for community currencies include restriction to a small geographic area (geofencing), privileged transactions, interest payments and participant dividends. Because the last two features must have a source of funds, their implementation will likely involve draws from the same fund as loans and grants. For

that reason they will not be dealt with at length. The focus here is on the community loan and grant fund. For simplicity, this fund will be referred to in most instances as the community fund.

There have been several forays into using Bitcoin technology for community currencies. Examples include the following.

- Mazacoin (http://mazacoin.org). Mazacoin claims to be the national currency of the Lakota Nation, though it is unclear from reports if the officials of the nation share this view. The creator of Mazacoin pre-mined 25 million coins (meaning he created them before allowing others to mine for their own) to be set aside for a tribal fund that would give grants to individuals, businesses and non-profits focused on the tribe [9].
- IrishCoin (http://IrishCoin.org/). IrishCoin is targeted specifically at promoting tourism to Ireland and has allocated 7% of the total volume of the coin for distribution to businesses and organizations associated with that industry for use as a "discount token" [10].
- Marscoin (http://marscoin.org). This coin has the unusual goal of becoming the currency used by colonists on Mars[1]. Four hundred thousand coins were pre-mined and donated to the Mars Society, a not-for-profit organization that seeks to establish a colony on Mars. The eventual goal is for colonists to take the Marscoin blockchain with them to Mars and use it as the basis for a local economy [11].

These and similar examples of community cryptocurrencies adapt the Bitcoin protocol to serve their needs without significant new features. More extensive adaptations of existing Bitcoin features and new capabilities can increase differentiation and utility for community cryptocurrencies. The remainder of this paper will discuss integrating these extended features into a cryptocurrency so it may serve an individual community. A significant portion will be devoted to a vulnerability analysis of the community fund and to methods of community decision making, centered around the community fund.

2.1 Mining

One of the protections Bitcoin has against fraud and manipulation is that coins are created and transactions verified in a distributed manner. All the working nodes check each other's work. It is, however, a consensus algorithm, with the blockchain reflecting work that the majority of nodes agree on. This makes it vulnerable to what is known as a 51% attack. In this attack, one person, node or mining pool acquires enough power (possibly through having more or better hardware than other nodes) to force a consensus on its own terms. Thus this powerful unit can conceivably corner the market on coin creation or even insert fraudulent transactions into the blockchain [12].

In a community cryptocurrency limits to the participant pool imposed by geography, interest, or other factors may increase this risk. Careful attention must therefore be paid

[1] One of the authors of this paper (Vandervort) has mined Marscoin. His wallet currently holds 321.824521 Marscoin. He has no plan to go to Mars.

to the numbers of mining and verification nodes. It may be then that proof-of-stake algorithms may be safer for community cryptocurrencies than the Bitcoin proof-of-work method. Proof-of-stake protocols require participants to prove possession of some amount of the currency for a minimum period of time before being permitted to produce new blocks (and with them, new coins) [13]. One way of jump-starting this is for a small amount of currency to be automatically given to new members of the community, probably from the community fund. Membership may be determined simply by downloading a new wallet, registering a new identity (discussed below) or some other method.

2.2 Geofencing

Community currencies are often intended to serve a local geographic area. BerkShares and Ithaca Hours are examples of these kinds of community currencies. Implementing geographic limitations in a cryptocurrency may have wide ranging consequences and difficulties.

Thanks to the revolution in geopositioning systems (GPS), software can be aware of the location where it is being used. This is not universal as location is often considered private data and many people block it by default. For a community cryptocurrency, location data can be used to verify the location of transactions and even software downloads. However, locations can be spoofed, for example by accessing a download site through a virtual private network. The question of how to handle offline transactions, which may experience delays before being committed to the blockchain is also an issue, since verification of location information may not necessarily occur at the time of the transaction.

Even putting aside the possibility of spoofing IP addresses and other location identifiers, there are issues with geofencing a digital currency. Enforcing the restrictions means forcing both businesses that accept the currency and users who spend it to reveal location information. Many may find this intrusive and the pool of available users will then be reduced accordingly. The size of the area and the mobility of people within it is also an issue. What happens to someone who travels outside the area briefly then realizes a bill needs to be paid? Is the payment prevented from going through until the payer returns home? There are many other cases that could be imagined in which geographic restrictions are an impediment even to people who live and work within the assigned area. Softer restrictions that allow transactions outside the defined area seem more supportable but risk allowing the area to artificially widen. This may not be a disadvantage in practice as it allows the pool of participants to widen as well.

Mining for new coins is a different question. Should this be allowed outside the intended area? If communities answer yes, they run the risk that outsiders will come to dominate mining, removing control of the currency from its intended community. If, however, they discourage this option, the total number of mining nodes may be too low to keep the currency stable or to fend off attempts to take over 51% of the processing power.

It can be seen then, that enforcing geographic limits at the protocol or software levels may create complications for a currency and its users. This indicates that the best course may be for real human beings to concentrate on working with their neighbors and with

local businesses to make their currency popular in the local region rather than to use technology to enforce geographic restrictions. Therefore, at the current time geofencing related features are not recommended for community cryptocurrencies.

2.3 Privileged Transactions

Privileged transactions are those that the community encourages by providing extra incentives. These transactions are considered to advance community goals or express community values. Examples include giving bonus payments for services performed for the elderly, or discounts for purchases of environmentally friendly products. In each case, for the economic equation to work, the difference between the normal price and the privileged price must be made up from somewhere. The most logical source for these additional funds is the community fund (discussed below).

As a direct expression of the community's values, privileged transactions are a means of fostering community cohesion. Including this feature in a digital currency requires some method of indicating what types of transactions would be privileged and how much privilege they would receive. Privileges expressed numerically, such as discounts and bonuses, are the simplest to translate into rules that can be interpreted by software. Less deterministic privileges, such as a promise of invitations to dinner at some time in the future, might be specified by text strings but automating verification of their delivery is difficult. The Bitcoin protocol may enable creative solutions to this problem. For example, a promise of dinner can be encoded as a very small multi-signature transaction, that is completed when all parties are satisfied that the promise has been kept. Verification of some sort is important for the sake of transparency. When users can check in the blockchain to see that promises are being kept, their faith in the currency and the community is likely to be greater than cases where there is no such verification.

The problem of verification brings up another issue that is important to the design and function of a community currency: trust. In some communities, methods of verification might be relaxed as a show of trust among community members. In such communities it might be enough for someone to send an email to one of the community leaders describing the privileged transactions they have been involved in and asking for bonuses thus earned. Particularly in small groups where the members have considerable face-to-face contact this kind of informality may be acceptable. Whether this type of small, trusting community needs a cryptocurrency is another question. In any case, the ability to automatically adjust compensation for different types of transactions and to verify the accuracy and nature of payments is a significant advantage of software-based systems over more traditional paper currencies or even many electronic exchanges. The convenience of having an account automatically credited by the correct amount the moment the transaction takes place, rather than having to go to a local "bank" and exchange notes or access a website and enter verification details is a significant advantage of a Bitcoin-based model for these currencies.

2.4 Demurrage

In order to encourage economic transactions, some currencies use demurrage, meaning they reduce the value of unspent notes over time. This gives people holding them incentive to move them quickly in order to capture as much value as possible. This in turn may magnify the economic multiplier effect (or velocity) of such currencies. Though many factors may affect the velocity of a currency, demurrage appears to have been at least somewhat effective for several community currencies [14] making it a potentially desirable feature.

Administering demurrage means that the time of transfer of each note must be recorded so that the value can be properly calculated. In the physical world, this means that either a note must have a timestamp (or series of timestamps) on its face, or it must have an identifier such as a serial number that can be associated with the timestamps in a central registry. This second method of tracking time for notes and transactions is similar to the function of the Bitcoin blockchain, which directly incorporates timestamps into transaction block data [3]. There are, however, potential pitfalls. Differences in time zones, system clocks and even the representation of time in different programming languages may make it impractical to calculate reductions in value over short periods of time. Recalculating the value of a particular coin should probably be done on a scale of days or weeks rather than seconds or minutes.

It is essential, also, that changes in the value of currency be verified at the mining level, similar to the way transactions are incorporated into the blockchain. In fact, the simplest implementation is to remove some portion of currency at the time it is used and deposit that portion into the community fund. This implementation prevents unintentional destruction of the total value of the currency, which could adversely affect the stability of the currency over time. It could also help to keep the balance of the community fund healthy.

The question arises of the relationship between demurrage and a proof-of-stake system. One of the advantages of proof-of-stake is that it may allow anyone who has a stake to mine new coins. Typically, coins must be shown not just to exist but to be reasonably "fresh" [13]. If the rate at which demurrage removes value is too fast, it could then interfere with the ability to show stake, both by directly removing coins that would otherwise show stake and by encouraging people to spend their coins so quickly that they have little or no stake in their wallets for verification. Yet, if demurrage is too slow, it provides little incentive for people to spend their coins, defeating its purpose. Thus if both proof-of-stake and demurrage are implemented in the same currency, the rate of change must be carefully calibrated to encourage spending while preserving stake[2].

Related to demurrage is the payment of interest, which increases holdings over time rather than decreasing them. The money to pay interest must come from some source. That source is most probably the community fund. Interest incentivizes saving rather than spending, which may not be in the best interest of the community economy.

[2] As of this writing (September 2014), a USPTO patent application #20130346164, "Peer-to-peer (p2p) currency platform implementing demurrage," may affect implementations of demurrage. The application can be viewed at http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=/netahtml/PTO/srchnum.html&r=1&f=G&l=50&s1=20130346164.PGNR .

However, it also provides clear value, which may improve trust in the community. It can be used to demonstrate proof-of-stake by adding "fresh" currency to a wallet. Variation in interest rates, such as a reduction in interest payments when the community fund has a low balance, may offset the benefits, however.

2.5 The Community Loan Fund

Some community currencies maintain a fund that can be used to make small grants or loans, usually for the purposes of starting or improving small businesses. Such funds can be effective at building owner-operated businesses [15], therefore incorporation of loans or grants into a community currency may contribute toward community goals. There are two questions to consider in designing this capability. Where do the funds come from, and how are decisions made concerning their disbursement? We propose that the answers to both questions be incorporated directly into the currency software.

2.5.1 Adding to the Community Fund

In cryptocurrencies, the most common method of stocking the community fund is currently for the creator(s) to pre-mine some amount that they can keep under their control. This method is easy to implement by simply running the first mining node or a small number of such nodes, without allowing others to download the software and run their own nodes, until a sum deemed sufficient has been mined. The cryptocurrency community in general tends to frown on this practice since it allows an unscrupulous operator to introduce a currency that they control from the very beginning. Note again the issue of trust comes into play.

It is possible for cryptocurrencies to add coins to a general fund in other ways, for example by adding a small fee to all transactions, or to all transactions above a certain amount, which will be paid to an address associated with the fund. In a corollary to privileged transactions, it may be possible to charge an extra fee for discouraged transactions, such as buying gasoline, if the goals of the community are environmentally oriented. The Bitcoin protocol already uses transaction fees as a means of compensating miners. Adding another fee or increasing the fee slightly and splitting between two recipients are relatively simple modifications that can support a community fund without pre-mining.

A related method of adding currency to the community fund is to take a small portion of mining rewards for the fund. In current cryptocurrencies, a node that is the first to generate a solution for a block is given a reward in new coins. This is called mining the currency. In the Bitcoin network the current reward is 25 bitcoins per block. In a community cryptocurrency, splitting off a portion of the block reward for the community fund is feasible. Miner objections may be reduced if the amount remaining to them is enough for a profit, or if they perceive some other benefit such as a good reputation within the community. The reputation factor could be enhanced by allowing miners to adjust the amount deposited to the community fund, therefore making it more a donation than an involuntary side effect. Designers of community cryptocurrencies

may find it advisable to set a minimum donation, rather than depending entirely on the altruism of the miners.

2.5.2 Disbursing From the Community Fund

In traditional finance, the most common method of disbursing funds for loans and grants has been for a small number of administrative persons to make all decisions. Even in community currencies, this seems to be the default approach. So, for example, the creators of IrishCoin stocked a distribution fund by pre-mining and indicated a preference for distributing it to businesses and organizations associated with Irish tourism [10]. This approach requires no custom programming to implement in the current Bitcoin protocol.

Another method can be built that uses the distributed nature of the protocol to take the disbursement out of the hands of a few members and give it to the whole community. This would involve a multi-step process. First, a transaction of a new type, community loan, is created by any authorized user, which in many communities may include any member of the community. The amount of the transaction is the amount of the loan (or grant) from the community fund. Then members of the community submit transactions of another new type, vote. Each vote either approves or disapproves of the transaction. When a threshold is reached, the vote is finalized. If the loan is approved the funds are released to the address specified. If the loan is disapproved, the transaction is invalidated. The voting threshold for or against the loan will vary from community to community. Some will require a majority of voting members. Others will require a supermajority. Any amount that can be mathematically described can be conceived.

The advantages of a system where the community votes on the disbursement of funds are in increased trust among community members and commensurately increased investment in the goals and activities of the community. There are numerous difficulties created by the proposed system as well. The next sections of this paper will discuss the problem of identifying "voting" members of the community as well as the recipient of proposed loans. This will be followed by a discussion of potential vulnerabilities to the integrity of the community fund.

3 Challenges with a Cryptocurrency Community Fund

The community fund and votes concerning loans from it are where the community works together, expressing shared values and building economic and social structures to make the community stronger. Conversely, should the loan fund become depleted or weaknesses in the system of proposing and voting on loans develop, the community could suffer a loss of trust, cohesion and even economic viability. Our analysis identified three major areas where design must be carefully considered in order for a community fund regulated by community participation to be viable. Those areas are identification of community members, tallying of votes and regulation of loans. The issues related to these factors are often interrelated.

3.1 Identity

The original Bitcoin system is highly successful at allowing relatively anonymous, trustless transactions. In a community currency there are at least three reasons why identity might be revealed to some extent. It may be necessary to ensure the proper counting of votes, to validate the recipient of grants and loans and to find businesses that will accept the currency in payment. Serving these purposes may require different levels of disclosure of identifying information. For example, while identifying a loan recipient may require a full name and address, voting may require no more than a unique identifier. In other cases, some third party identifier or certificate issued by a provider who possesses but does not share more specific identification information, may be a good compromise between the extremes of full identification and full anonymity.

The level and type of identifier used may also vary depending on purposes. Businesses may prefer to be more open about their true name and location than people whose purpose is not business related. Registering clear identifying information as a public identity is a simple form of advertising. In communities with a strong local component, geographic coordinates might also be part of an identifier.

How identity data is stored and accessed is an important consideration. Do identities need to be registered directly in the blockchain (or some blockchain) or is it enough to have some identifier such as a username associated with a wallet address? Could a separate blockchain for identity be used, with transaction meta-data incorporating a hash of a location in the identity chain? In this case, is it enough to reference identities registered with some service such as Namecoin? While this low level of identification is suitable for many purposes, it seems likely that a higher level of disclosure is required in communities that vote on local issues, or in which reputation is important.

3.2 Voting

Voting is integral to the model of community currency being developed here. Voting is one way that people participate in the community which ties it closely to identity. In order to verify that only people who belong to the community cast votes, voters must be identified in some way. If, however, the community requires votes to be cast in secret, verification and tallying become separate steps. When using a structure such as a blockchain to store votes, meeting the goals of both secrecy and identity verification is a difficult technical problem.

In the physical world, voting is usually restricted to a specific time period. This makes sense especially when dealing with monetary loans, which may be time sensitive. Rules for determining winning and losing vary with locality and context. For a political election, the highest number of votes may win, or a majority (>50%) may be required with lower numbers resulting in a runoff. In a jury, unanimity may be required. In a legislature, some actions may pass by majority vote while others may require a supermajority. An additional concept to consider is the need for a quorum. This is the smallest number or percentage of the membership that must vote for results to be considered valid. Without a reasonable number for a quorum, a community risks having its resources come under the control of a small number of members. All of these

properties can be modeled in the community cryptocurrency software. As discussed above, votes are treated in this system as another form of transaction. Therefore, mining nodes may apply rules to voting transactions and voting blocks as the community requires, though choosing optimal values may be challenging.

3.3 Loan Regulation

In order for a loan fund to be viable, it must not loan out more currency than it has coming in and loans must be paid back in a timely manner. The way loans are proposed to and approved by the community influences these factors. Communities should consider factors such as who is allowed to propose loans. Should anyone be allowed or should it be restricted to members in good standing? Does a proposed loan have to be seconded before it is put up for a vote to the whole community? Should there be a maximum size to loans either in whole numbers or a percentage of available funds? Should loan recipients be allowed to receive new loans while a previous loan has not yet been paid back?

There must be some method of stocking the community loan fund. As mentioned above, methods include taking tithes from transactions or from miners. There may also be a tax on wallet balances above a certain amount or membership fees for businesses. Whatever method is used to fill the fund, it must be carefully balanced with outgoing loans. If the community fund becomes too large it may stifle other economic activity effectively creating deflation. If it is too small, loans will be choked off and economic growth may suffer.

In addition to the need to encode policy into software comes the question of how to change policy. Any policy may need to be revised to accommodate real world experiences. Perhaps if too many loans default, a temporary cap needs to be put in place, or certain members need to be permanently banned from proposing or receiving loans or grants. Creating a system that is comprehensive, secure and also responsive is a significant challenge for both currency designers and software developers.

4 Vulnerability Assessment

While Bitcoin transactions provide a level of protection of user identity, in a community fund this may be compromised to some extent. Businesses, including those operated by the self-employed, may desire more visibility to the community in order to advertise their services and so their names may accrue a good reputation. The counting of votes is tied to identity as well. Vote tallies must be accurate and, in many communities, secret, in order to ensure that the will of the community as to the disbursement of funds is not subverted. Similarly, the regulation of loans refers to the way in which loans are proposed, disbursed and even repaid.

In a community in which all the members know and trust each other, these problems may be ignored. In more common communities where self-interest sometimes conflicts with the community interest, controls are needed to mitigate potential risks. We analyze the risks from the point of view of the STRIDE framework, slightly modified to

accommodate analysis at the fund operation level rather than at the point of software implementation.

4.1 STRIDE Framework

STRIDE is an acronym for a common set of risks to software-based systems. It stands for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of Privilege [16]. Our analysis, however, is not of the software implementation but of potential risks at the community fund level, as the structure of the system must be determined before being implemented in software. Therefore we use the terms, plus one other, for structural issues that may impact fund operations. This gives the following categories for the analysis.

– Spoofing. When a person pretends to be another, the pretend identity is said to be spoofed. In this case, one person may spoof multiple identities and control multiple votes. Those identities may be created by the person who controls them or they may be hijacked from other users. This is not an issue for normal Bitcoin transactions, which do not support personal identifiers.

– Tampering. When transactions are changed after a user believes they are finalized, they have been tampered with. It is assumed that the nature of the Bitcoin blockchain will provide strong protection for completed transactions, including votes. This issue is therefore most prevalent at the software and communication levels and is not considered here.

– Repudiation. When a person rejects a transaction they have allegedly made they have repudiated that transaction. In standard Bitcoin practice, the blockchain provides strong protection against this as well. However, because the community system introduces a level of identity that is not present in the baseline Bitcoin protocol, there may be issues with repudiation here, particularly in voting.

– Information disclosure. Like repudiation and spoofing, the introduction of user identity creates the possibility of more personal information leaking than intended. This is highly sensitive to how much identity information a given community requires from its members. This is purely an implementation issue, not considered below.

– Denial of service. At the fund level, denial of service means that the community fund is depleted. In some communities this may be seen as only a temporary inconvenience. In others it may be a catastrophe. At some level, funds must be maintained.

– Elevation of privilege. When someone is able to access funds which they do not have the right to use, or to propose loans or open or close voting when they are not designated as having that authority, they are said to have elevated their privilege. This is very sensitive to community standards.

– Operational. In addition to the STRIDE categories described above, we use the operational category to show risks that may be aggravated or mitigated by the way community cryptocurrency features, such as voting, are designed.

Dropping the unused categories and adding the one new one, modifies the STRIDE framework to SRDEO. While less mnemonically satisfying, this is at least a good start on developing a framework for analyzing the structural weaknesses in a community cryptocurrency.

4.2 The Vulnerability Matrix

Using the SRDEO categories, and the classifications of voting, identity or loan problems, we have developed the matrix of potential problems in designing a community currency seen in table 1 (below). This list is not considered exhaustive but should contain the most prominent risks that must be considered when designing a currency for community use.

Table 1: Vulnerability matrix

Category	Issue	Effect	Mitigation strategy
Identity	Too few registered users (O).	Small coalition controls funds.	None (community has failed).
	Too many registered users (O).	No quorum, no completed votes.	Adjust quorum rules to accept lower percentages of voters.
	Spoofed identities (S, R, E).	People propose and vote on loans for themselves.	Require identity confirmation.
	Abandoned IDs (O).	No quorum, no completed votes.	Require proof of activity for voting.
Voting	Voter turnout too high (D).	If people are paid to vote, this could deplete funds.	Do not pay for votes or reduce payments once quorum is reached.
	Voter turnout too low (O).	No quorum, no completed votes.	Time limit voting period and reduce or eliminate quorum rules.
	Voter turnout too low due to apathy (O).	No quorum, no completed votes, few loan proposals.	Pay for votes. May pay for the first n votes or for votes in first t minutes or choose random sample of voters to be paid.
	Voter turnout low due to confusion about issues (O).	No quorum, no completed votes, voter dissatisfaction.	Require proposal summaries; use wallets or other means to support information dissemination and debate.
	Too many proposals to vote on (D).	Depleted funds, not enough votes on individual items.	Limit number of concurrent proposals or pay for votes on items that have not reached quorum.
	Falsified votes (S).	See spoofed IDs.	See spoofed IDs.

Loans	Not repaid (O).	Funds depleted.	Garnish payments after some time limit.
	Too many loans (D).	Funds depleted.	Set a maximum level of concurrent loans and/or increase interest rates.
	Too few loans (O).	Community loses credibility.	Reduce interest rates. Pay dividends to all community members.
	Too few transactions (O).	Funds depleted.	Introduce demurrage, transaction fees or request donations.

4.3 Mitigations

Multiple issues flow from insecure identity implementations. If a small number of people can control a large number of votes - that is more than one each - they can dictate who gets loans, including steering loans to themselves and their friends. One partial solution to this is to require that the identity of new voting members be verified by some number of previously existing members. It is a partial solution because it can never be guaranteed that those who provide verification will perform due diligence, such as meeting new members face to face, or that they will not be fooled. Therefore this is only a first level of protection. Some method of revoking voting privileges should exist as well, though this could also introduce the potential for problems if not carefully handled. Methods of temporarily suspending voting rights, loan proposal and loan receipt rights may also be necessary to police issues.

Controls can also be built that take note of community participation. For example, someone who has not posted a transaction of any kind within the last 30 days could be barred from voting or from proposing loans. This should discourage the creation of membership accounts solely intended to influence votes. There is a risk with this method that too many users will be barred if transaction volumes drop too low. This likely cannot be remedied by automatically or even manually adjusting the time period to allow more to vote. When participation is too low, the remedies are social. The community needs to be encouraged to participate more.

The problem of too frequent or too large loans is more readily amenable to software controls. With guidance from the world of banking and finance, formulae can be developed to balance loans that are being repaid, those that are not and the funds available to make more loans. The performance of the loan fund can be scored and loan proposals compared with currently advisable amounts before voting is allowed.

The danger of underperforming loans in community currencies is significant, especially if the community includes assisting the poor among its values. To at least partially offset this, repayment terms can be automated, for example garnishing 1% of every transaction which the loan recipient receives until the loan is repaid. This may be more reliable than mandating manual monthly payments.

Interest rates on community loans are often low or non-existent [6]. If the loan fund is low or the proposed loan high, a prudent policy might be to charge a higher rate of

interest than at other times. This would discourage depletion of the fund as well as bringing in extra revenue to rebuild it. Again, this can be expressed in software easily.

The mitigation efforts described here may be implemented in various ways to meet the needs and expectations of various communities. However, unless a community has perfect trust, the issues described must be considered and controls decided on before the currency is launched.

5 Conclusion and Future Research

It has been shown here that, while Bitcoin technology is a good fit for use as a community currency, significant modifications to the protocol are needed as well. The needs of a community cryptocurrency are more social, requiring degrees of identity and fiduciary care not found in the pseudonymous world of Bitcoin. These needs produce their own opportunities for economic engagement and community cohesion while also generating significant risks for collapse of a community using a currency with a flawed design. We discussed three major vulnerability areas in the community fund of a community cryptocurrency. In almost all cases we found possible mitigation strategies that could be built into the cryptocurrency software. The operation of these mitigations in practice and ways to adapt them to community values and changing conditions are important areas for future research.

While the modified STRIDE framework (SRDEO) makes a promising start on a method of analyzing the structure of community cryptocurrencies, improvements are possible. In particular the framework should consider attacks at the mining level, such as Sybil nodes and 51% type attacks. Whether these can be mitigated by requiring miners to provide a verifiable identity is an important question.

Different models of identity, including those based on a model such as Namecoin and more complex, more deterministic measures should be implemented and their risk models worked out in detail. Experimentation with different loan models, such as interest bearing, non-interest bearing and multi-party, as well as differing payback rates and garnished and voluntary payments, can yield unprecedented information about financial dynamics and human financial behavior.

The concept of a community cryptocurrency is one that joins the financial, technological and social worlds in new ways. Designing a currency that has a reasonable chance of working is only the beginning of the effort. In this paper we have tried to explore the most important variables and potential features at a high level. There are more levels and more variables still to be considered.

References

1. About. (n.d.). International Journal of Community Currency Research. Retrieved September 2, 2014, from http://ijccr.net/about/
2. Seyfang, G. (2002). Tackling social exclusion with community currencies: learning from LETS to Time banks. International Journal of Community Currency Research, 6(1), 1-11.

3. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Consulted, 1(2012), 28.
4. Butterin, V. (2014). A next-generation smart contract and decentralized application platform.
5. Lietaer, B. (2004). Complementary currencies in Japan today: History, originality and relevance. International Journal of Community Currency Research, 8(1), 1-23.
6. Lietaer, B., & Hallsmith, G. (2006). Community currency guide. Global Community Initiatives.http://www.lyttelton.net.nz/timebank/Community%20Currency%20Guide.pdf. Accessed on July, 20, 2007.
7. Hess, D. J. (2012). An Introduction to Localist Movements. of the American Sociological Association, Denver.
8. Mascornick, J. (2006). Local Currency Loans and Grants: Comparative Case Studies of Ithaca HOURS and Calgary Dollars (Doctoral dissertation, University of Montana).
9. Ecoffey, Brandon. "Oglala Sioux Tribe surprised by MazaCoin plan." Indianz. Native Sun News, 7 Mar. 2014. Web. 2 Sept. 2014. http://www.indianz.com/News/2014/012781.asp.
10. "IrishCoin." IrishCoin.org. N.p., n.d. Web. 2 Sept. 2014. http://irishcoin.org/irishcoin.html.
11. BitcoinForMars. Not every cause needs a coin but every planet does . (n.d.). Retrieved September 2, 2014, from http://marscoin.org/
12. Weaknesses. (2014, August 2). Retrieved September 2, 2014, from https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power
13. Bentov, I., Gabizon, A., & Mizrahi, A. (2014). Cryptocurrencies without Proof of Work. arXiv preprint arXiv:1406.5694.
14. De la Rosa, J. L., & Stodder, J. (2013). On Velocity in Several Complementary Currencies. In 2nd International Conference on Complementary and Community Currencies Systems, The Hague.
15. Williams, C. C., Aldridge, T., Lee, R., Leyshon, A., Thrift, N., & Tooke, J. (2001). Bridges into work? An evaluation of local exchange and trading schemes (LETS). Policy studies, 22(2), 119-132.
16. Shostack, Adam. Threat Modeling: Designing for Security. Indianapolis, IN: John Wiley & Sons, 2014.