


August, 2015

MoneyCircles.com

Proof of concept implementation - Fully verifiable Fiat pegged peer-to-peer lending backed by a private blockchain

Authored by Aron van Ammers & Jamie Burke
Contributions by Adrian Davies
POC developed by BlockStars.io, funded by OutlierVentures.io

1 Abstract

MoneyCircles.com[1] offers a new way of lending which is more ethical, social, and enables better financial characteristics than the current options for both savers and borrowers. The core of MoneyCircles is based on smart contracts[2] on a blockchain, to provide cryptographically verifiable honest behaviour.

The proof of concept leverages smart contracts on a private blockchain based on Ethereum[3] to govern the core financial logic and data. Funds are stored and transferred denominated in British Pounds using Uphold, formerly known as Bitreserve[4]. The smart contracts provide a high grade of transparency and verifiability of the service in an automated fashion.

The proof of concept implementation is live and can be reached through the following URL: http://www.moneycircles.com/proofofconcept

---

[1] "MoneyCircles." 2003. 1 Oct. 2015 <http://www.moneycircles.com/>
[2] "Nick Szabo -- The Idea of Smart Contracts." 2002. 6 Oct. 2015 <http://szabo.best.vwh.net/smart_contracts_idea.html>
[3] "Ethereum Frontier." 2014. 29 Sep. 2015 <https://www.ethereum.org/>
[4] <http://en.wikipedia.org/wiki/Bitreserve>
[5] "CC BY-NC 4.0 - Creative Commons." 2013. 6 Oct. 2015 <https://creativecommons.org/licenses/by-nc/4.0/>

2 Ambition

MoneyCircles.com is financed by Outlier Ventures Ltd, a European blockchain startup incubator, and delivered through its development subsiduary Block Stars Ltd. The ambition for the proof-of-concept is to demonstrate technically how blockchain technology can be applied to peer-to-peer lending in a usable way. The end purpose is to raise funds for Money Circles Ltd to commercially exploit and scale the opportunity.

3 Background

3.1 The current state of saving and lending

The current possibilities for lending money are limited, impersonal and suboptimal. Many groups of people, especially younger generations such as Generation Y[6], are managing a permanent state of indebtedness and struggle to access traditional credit markets due to restrictive credit scoring. In the West many are forced into a monthly cycle of managing payday loans with exorbitant interest and repayment rates, or using unofficial lines of credit such as late-payment of mobile phone bills, rent or council tax[7].

Equally the possibilities for saving money and receiving good interest are also poor: the interest rate on savings accounts is lower than the current inflation rate in most countries, driven by negative rates in the broader credit market[8].

Perversely traditional financial institutions, including high-street banks and credit unions, often fail to maximise returns on deposits through loan books. Challenger services often focus on new or improved customer experiences rather than ways to tackle this broken credit market. Often due to their own inherent fragility they are more rather than less risk averse.

We believe decentralised peer-to-peer lending could help create an alternative savings and loans marketplace to better optimise this disparity in the credit market.

3.2 Peer-to-peer lending

An emerging way of lending, which PwC predicts will swell from $5.5bn to $150bn by 2025[9], is peer-to-peer lending. A person or organisation in need of a loan can post their borrowing needs, often within a fixed structure, on a peer-to-peer lending platform. Others can invest in this loan by funding it

---

[6] "Millennials - Wikipedia, the free encyclopedia." 2011. 6 Oct. 2015 <https://en.wikipedia.org/wiki/Millennials>

[7] "Generation Y turning to high-cost credit - Citizens Advice." 2015. 6 Oct. 2015 <https://www.citizensadvice.org.uk/about-us/how-citizens-advice-works/media/press-releases/generation-y-turning-to-high-cost-credit/>

[8] "The Economist explains: Why negative interest rates have ..." 2015. 6 Oct. 2015 <http://www.economist.com/blogs/economist-explains/2015/02/economist-explains-15>

[9] "Peer to Peer Lending Platforms: PwC." 2015. 6 Oct. 2015 <http://www.pwc.com/us/en/consumer-finance/publications/peer-to-peer-lending.html>

partially or fully with fixed rates of return. Repayment is carried out with the peer-to-peer lending platform as a mediator.

Lending Club is the largest consumer finance platform, based in the US, with $11,167,217,348 in loans as of 06/30/15[10]. However whilst consumer peer-to-peer finance is growing, it is being outpaced by the equivalent business lending marketplace[11]. Initially both were meant as a way for the public to disintermediate financial institutions, however now around 4/5 of lenders on these platforms are hedge funds, pensions and banks chasing higher rates of return. Some of the best examples of this include Citi Group agreeing a $150m tie-up with Lending Club in 2015 and Citizens Bank buying $200m of loans from SoFi (a student loan focused platform) and committing to $300m more.[12]

It is common that P2P platforms will have fixed loan and interest sizes, rates as well as risk profiles based on their business models. Some platforms like UK market-leader Zopa pride themselves on rejecting at least 50% of loan applicants[13] with rumours it's closer to 80%[14], so it is our belief these platforms do not address the fundamental problems of those currently outside of the credit marketplace.

3.3 Credit unions

A more ethical and social way of lending money within a group of people, common in many countries and of growing import in the UK, is the credit union, a form of cooperative. Based on a 'common bond' like profession or geographical location, people can join the credit union and either deposit their savings or get a loan. Lenders are also often encouraged to save once they have paid back borrowing. In all they promise a more ethical and social way of lending with greater levels of inclusion.

Penetration is at its highest in the developing world like Latin America, Africa and Asia but there are high penetration rates in developed countries like; 30% in Australia, 45% in USA, 43% in Canada, with the largest of 73% in Ireland[15].

There are 56,000 credit unions in 101 countries with more than 200 million members and assets of $1.7 trillion. However the threshold for the average person to set up a new credit union is still high as it requires a significant initial amount of deposit, and in the West credit unions are significantly regulated by financial services authorities. This means they serve large catch-all groups of people rather than the true long-tail of social identities and networks. It is this better representation of our real social lives which a less centralised blockchain solution could cater for.

---

[10] "Lending Club Statistics - Lending Club." 2008. 5 Oct. 2015 <https://www.lendingclub.com/info/statistics.action>
[11] "P2P business lending to eclipse consumer sector - FT.com." 2015. 5 Oct. 2015 <http://www.ft.com/cms/s/0/80a87516-1513-11e5-9509-00144feabdc0.html>
[12] "The sharing economy - Financial Times." 2015. 6 Oct. 2015 <http://www.ft.com/cms/s/0/62f2737e-6210-11e5-9846-de406ccb37f2.html>
[13] "Is P2P for loans or investment worth the risk? - Choose." 2012. 6 Oct. 2015 <http://www.choose.net/money/guide/faqs/peer-to-peer-lending-worth-risk.html>
[14] "Nuzzel - 'Four in five peer-to-peer borrowers rejected'." 2015. 6 Oct. 2015 <http://nuzzel.com/story/09052015/expressandstar/four_in_five_peertopeer_borrowers_rejected>
[15] "2012 Statistical Report - World Council of Credit Unions." 2013. 5 Oct. 2015 <https://www.woccu.org/documents/2012_Statistical_Report>

Credit unions are still currently run in a very manual and labour intensive way disconnected from one another and functioning in silos. Knowing and having a personal relationship with members is part of their appeal and why they often have comparatively low default rates from borrowers, even when serving some of the most underprivileged areas. For example, despite being home to some of the UK's most economically deprived areas and lending to what are often perceived as the highest risk borrowers, some large credit unions in Liverpool have bad debt rates of under 2%. We believe a lot of the administrative tasks of credit unions could be automated partly or entirely via smart contracts.

Because they are small financial institutions, with lighter regulatory requirements than banks, they often have issues with governance. Fraud and embezzlement are serious problems in both more mature and developing markets equally.[16] A public, transparent and verifiable ledger that can be highly automated, such as a blockchain, offer huge benefits for governance and building trust.

3.4 Cryptocurrencies on a blockchain

A promising recent development in the fintech community is the rise of Bitcoin and other decentralised cryptocurrencies. Cryptocurrencies exist only in digital form and are, on a technical level, highly secure. At the core of most cryptocurrencies is a "blockchain", a public ledger the consistency of which is guaranteed by cryptographical rules.

Because cryptocurrencies are decentralised they don't require central bank or institution to manage them. They offer many options which are impossible with traditional cash and bank accounts, like escrow arrangements and multi-party transactions. As cryptocurrencies are currently largely unregulated in most countries, yet can be used to store and transfer real value, they offer much potential for use in financial services such as lending.

3.5 Smart contracts

A smart contract is a computer protocol that facilitates, verifies, or enforces the negotiation or performance of a contract. Another way to see it is as a traditional contract textual document, formalised and translated to executable and verifiable computer code. The clauses of the contract which would normally be interpreted by humans in the case of smart contracts are interpreted by computers. A trustable smart contract implementation offers great benefits to the contract parties, because they can trust that no party can break the contract. Compared to traditional contracts, great cost savings can be achieved on execution of the contract because no intervention of expensive qualified labour is necessary.

Blockchain technology could offer the base to realise a trustable smart contracts implementation. Several initiatives to realise smart contracts on a blockchain are under way.

[16] "The Dirty Dozen: 12 Notorious Credit Union Heists." 2012. 5 Oct. 2015 <http://www.cutimes.com/2012/10/01/the-dirty-dozen-12-notorious-credit-union-heists>

4 Vision

4.1 Social Lending

MoneyCircles technology can enable people to save and borrow by 'common bond', similar to credit unions, in circles. The difference being users can create circles for any given niche such as friends and family, local small community groups or specific social causes. These circles would assume set treasury and solvency rules, and importantly reside in a fluid financial network. This means that each circle would be its own distinct financial entity, but both money, identity and reputation are shared. We believe this would enable a financial social network with easier switching to truly reflect our diverse relationships and social selves.

4.2 True Peer-to-Peer Lending

Because the network is technically based on cryptocurrency, blockchain and smart contracts with irrefutable rules, trust is established without the requirement of an institutional body of a bank or credit union. In fact in theory the concept could exist without the need for any central party at all. Peers could truly save and lend with one another without the need of an intermediary. However we believe we are many years away from such an extreme disruption to financial services.

In the case of this proof-of-concept both Moneycircles and the Uphold platform do play a central role, albeit limited, automated and with full transparency and traceability. The trustless, fully digital structure also has cost efficiencies through automation, and as a network of circles in duplication of tasks. In the end the hard benefit for consumers is it would enable better rates and conditions for both savers and borrowers.

4.3 A Glass Bank

Financial institutions are suffering from a severe crisis of public trust[17], often further complicated by their diverse range of business activities. A circle would have a clear and limited purpose, as previously mentioned, governed by hard and unbreakable rules.

With credit unions, as relatively small and lightly regulated financial institutions, challenges with governance and control of funds is challenging. As previously discussed fraud by credit union directors and employees is not uncommon with 46% of CUNA Mutual fidelity bond claim dollars paid out between 2009 and 2013 due to employee dishonesty. Of the 192 credit unions that have failed in last decade, 78 were due to insider fraud[18]. Building savings and loans instruments on blockchains as their operational infrastructure almost entirely remove these problems and immediately restores trust.

Equally, with regard to peer-to-peer lending platforms, there haven't been many cases of platforms going financially insolvent. In the UK there are protections such as Financial Services Compensation Scheme (FSCS) but they do not cover p2p platforms and there is no real precedent for what happens

[17] "Trust in Financial Services - 2014 Edelman Trust Barometer." 2014. 5 Oct. 2015 <http://www.edelman.com/insights/intellectual-property/2014-edelman-trust-barometer/trust-in-business/trust-in-financial-services/>

[18] "Credit Union Times | Accurate and Timely CU News." 6 Oct. 2015 <http://www.cutimes.com/>

with funds and loans in the event of failure. In the case of Yes-secure which closed down in 2014 it is yet to repay everyone, plus interest[19].

The ambition of MoneyCircles.com is to make fraud and insolvency much less likely by effectively forming a “glass bank”. This idea was first introduced in 1931 as a futuristic solution for crimes in physical banks[20]. MoneyCircles aims to achieve it through profound transparency and technical enforcement of rules. A key component of this proof-of-concept is to visibly demonstrate both.

Also openness in data, all data relating to a circle's performance will be recorded and publicly verifiable on a blockchain, means that all circles can collectively learn from one another to improve towards an optimum market. This is in stark contrast to banks and other traditional financial institutions that are often being forced by regulators to share data to improve competitiveness and market performance[21].

5 Scope of work

5.1 Within scope

A proof of concept implementation of MoneyCircles was realised to test the viability of the concept and approach.

To realise MoneyCircles completely as envisioned would require several components which are not available in the current state of technology and services. The most important of those are:

- A mature, decentralised smart contracts platform
- A mature, decentralised way to handle identity and reputation
- Usable and secure methods to give end users access to a (partially) decentralised application from a broad range of (mobile) devices
- A decentralised way to store and interact with fiat currencies like Pound Sterling from smart contracts

Some of these requirements are however partially available. To realise a working product with what is available today, the proof of concept implementation is a partially decentralised hybrid solution making use of these platforms:

- Ethereum: smart contracts and proof of liability. A private blockchain based on Ethereum is used.
- Uphold: end user authentication and identity, fiat currency transactions and reserves.

The MoneyCircles proof of concept is realised as a web application which offers a social lending service by acting as a verifiably honest bridge between these platforms.

---

[19] "Is P2P for loans or investment worth the risk? - Choose." 2012. 6 Oct. 2015 <http://www.choose.net/money/guide/faqs/peer-to-peer-lending-worth-risk.html>
[20] "Glass Banks Will Foil Hold-Ups | Modern Mechanix." 2012. 4 Oct. 2015 <http://blog.modernmechanix.com/glass-banks-will-foil-hold-ups/>
[21] "UK banks forced to open up customer data to help challengers." 2015. 6 Oct. 2015 <http://www.ft.com/cms/s/0/5bcb559e-ce35-11e4-9712-00144feab7de.html>

5.2 Out of scope

For this to be a viable commercial product, MoneyCircles must comply with the regulatory environment. There are regulatory requirements such as KYC and AML, in short to guarantee MoneyCircles is actively seeking to counter money laundering and other criminal activities. Since the purpose of this proof-of-concept is to test technically what is possible and not to build an off-the-shelf product, this is left out of scope.

Furthermore the following aspects are left out of scope:

- On / off platform credit scoring
- Circle-specific and cross-circle reputation
- On / off platform loan default management
- Granular circle customisation

6 Implementation

6.1 Components

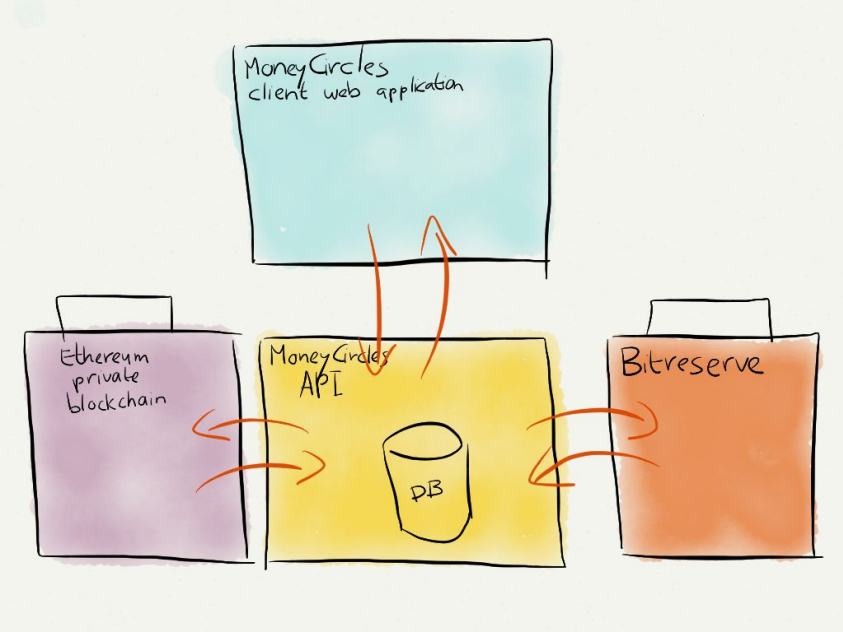
The proof of concept is realised as a Node.js[22] backend service accessed by a responsive AngularJS[23] web frontend. Smart contracts on an Ethereum private blockchain govern the core functions of circle membership, saving and lending.

Users access the service through the web application. The web application is developed in a mobile-first approach to be accessible by a wide range of end-user devices.

Technically adept users can access the smart contracts on the private blockchain and the Uphold API independent of the MoneyCircles API to verify its honest behaviour and solvency.

An overview of the components is provided in the diagram below.

[22] "Node.js." 2015. 29 Sep. 2015 <https://new.nodejs.org/>
[23] "AngularJS — Superheroic JavaScript MVW Framework." 2014. 29 Sep. 2015 <https://angularjs.org/>



6.1.1 Identity and authentication

The proof of concept leverages Uphold as an authentication provider. Users of the MoneyCircles proof of concept create an Uphold account and authenticate through OAuth. The service can then act on their behalf to transfer money between their Uphold account and circles.

6.1.2 Smart contracts

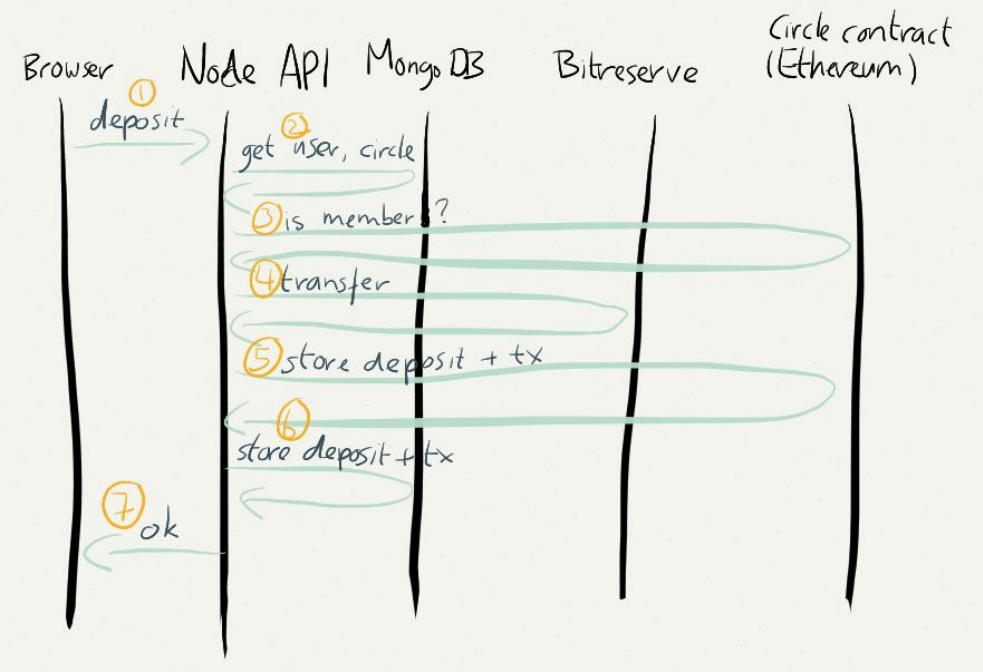
The smart contract backend provides governance and verifiability for the core data and logic of the service. Hence although the application is realised in a centralised form, its behaviour is directed by cryptographically verified data and logic.

Two types of smart contracts are deployed:

- Circle contract: each circle created in the system is deployed as an individual smart contract, forming the entry point to all its functions including management of members, deposits and loans.
- Loan contract: created by the circle contract on request of a loan, the loan contract this loan during its lifespan until repayment.

6.1.3 Interaction between the service and smart contracts

A typical interaction between the components is shown below. The diagram shows a simplified flow for a deposit of funds in a circle. The starting situation is that the user has authenticated with the services and is already a member of a circle.



A deposit comprises the following steps:

1. The user initiates the deposit from the web application in a web browser.
2. The API fetches data of the user and circle from MongoDB to handle the request.
3. The API checks with the circle smart contract to see whether the deposit can indeed be carried out, i.e. whether the user is indeed a member of this circle.
4. The API requests Uphold to transfer the funds from the user to the MoneyCircles vault.
5. The API registers the deposit in the circle contract, including the Uphold transaction ID.
6. The API registers the deposit in MongoDB.
7. The result is returned to the browser.

Ideally the processing of the request to deposit would be executed atomically: either it completes successfully and is stored correctly in all components of the system, or it fails and isn't stored anywhere. This would be the case in a fully smart-contract based approach. In our proof of concept approach this is not the case because of two reasons.

Firstly there is no atomic way to interact between the smart contract platform (a private Ethereum blockchain) and the store of value (Uphold). The MoneyCircles API service has to call both separately and in each of these calls an error could occur, resulting in an inconsistent state. The impact of this could be reduced by giving the MoneyCircles service rollback functionality so that in case of errors, the previous actions are rolled back. In a future version this might be realised.

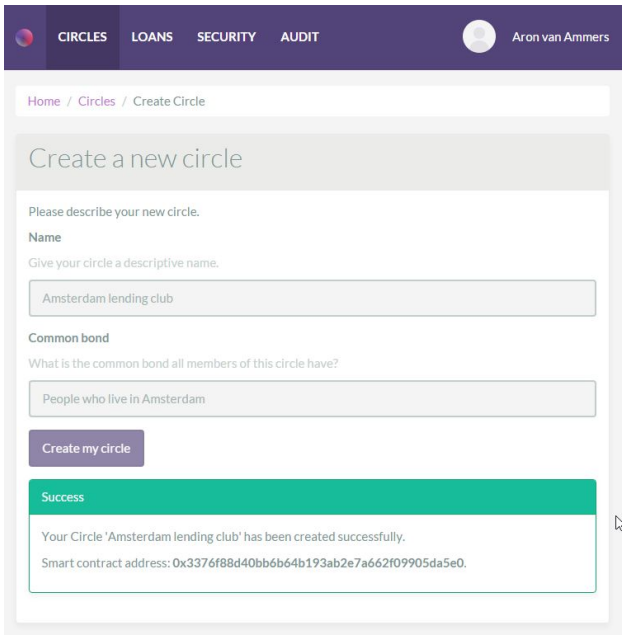
Second, the interaction diagram makes clear that there is some duplication in data between the MongoDB database and the smart contracts. We have chosen to use a MongoDB instance in the proof of concept for reasons of practicality and productivity. Although programming smart contracts in Ethereum has matured significantly since the first alpha versions, the possibilities are still limited in terms of storage, performance and development productivity.

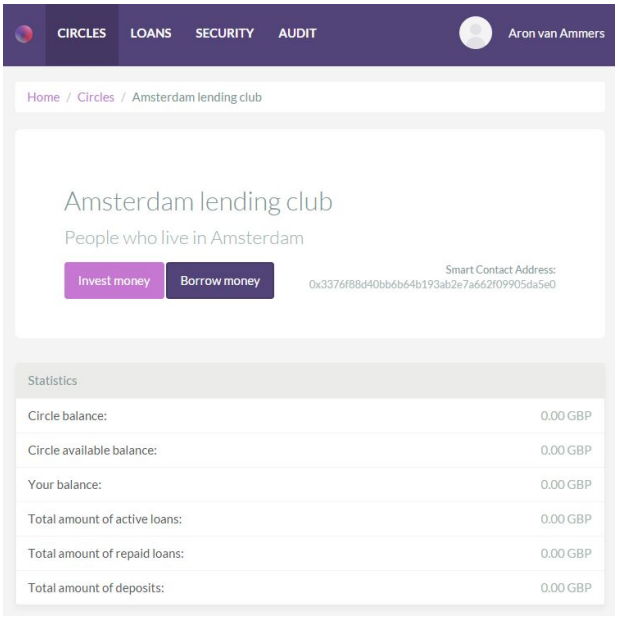
This duplication introduces the risk of inconsistency between the two data stores. If for example step 5 (registering in the smart contract) in the interaction diagram would be completed and step 6 (registering in MongoDB) would not, the deposit would be completed in terms of transfer of funds and registered in the smart contract, but not in the MongoDB backend. Dealing with this type of inconsistency is less of an issue than the issue described above; the smart contracts are considered the single source of truth with regard to transactions within MoneyCircles, hence transaction data in the MongoDB backend can be regenerated from the smart contract state.

6.2 Functionality

6.2.1 Circles and membership

Every user can create a new circle. Creating a new circle deploys a smart contract on the private blockchain which governs it. A reference to the smart contract is provided to enable end users to verify this governance.

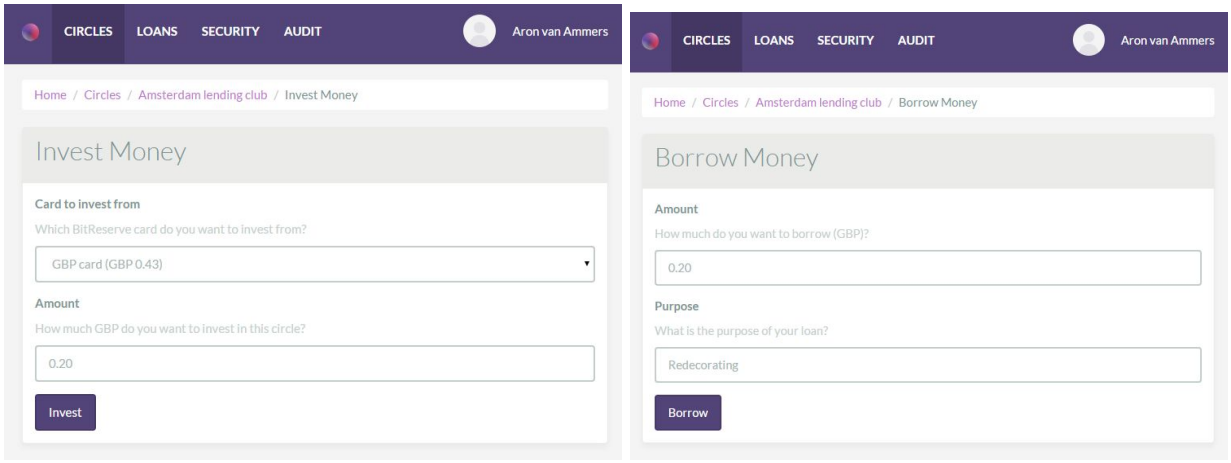




Other users can join the circle. Once they are a member of the circle they can start saving and lending.

6.2.2 Saving and lending

Members of circles can deposit funds into the circle. The funds of the circle comes available to all of its members to take out a loan.



Each of these actions is verified by smart contracts, and not approved if they would be outside of circle rules. The Uphold transaction ID's of all transactions are also registered in the smart contracts and presented to the users in order to provide a public record.

6.2.3 Circle minimum reserve

A minimum reserve of 20% of deposits is kept by each circle in order to deal with defaults. The amount above the minimum reserve is called the *available balance*. The circle contract will only allow taking out loans up to the available balance.

6.3 Transparency and verifiability

Built on the fact that all financial streams are governed and registered by smart contracts, several options are made available to inspect and verify the correct and honest functionality of the MoneyCircles proof of concept.

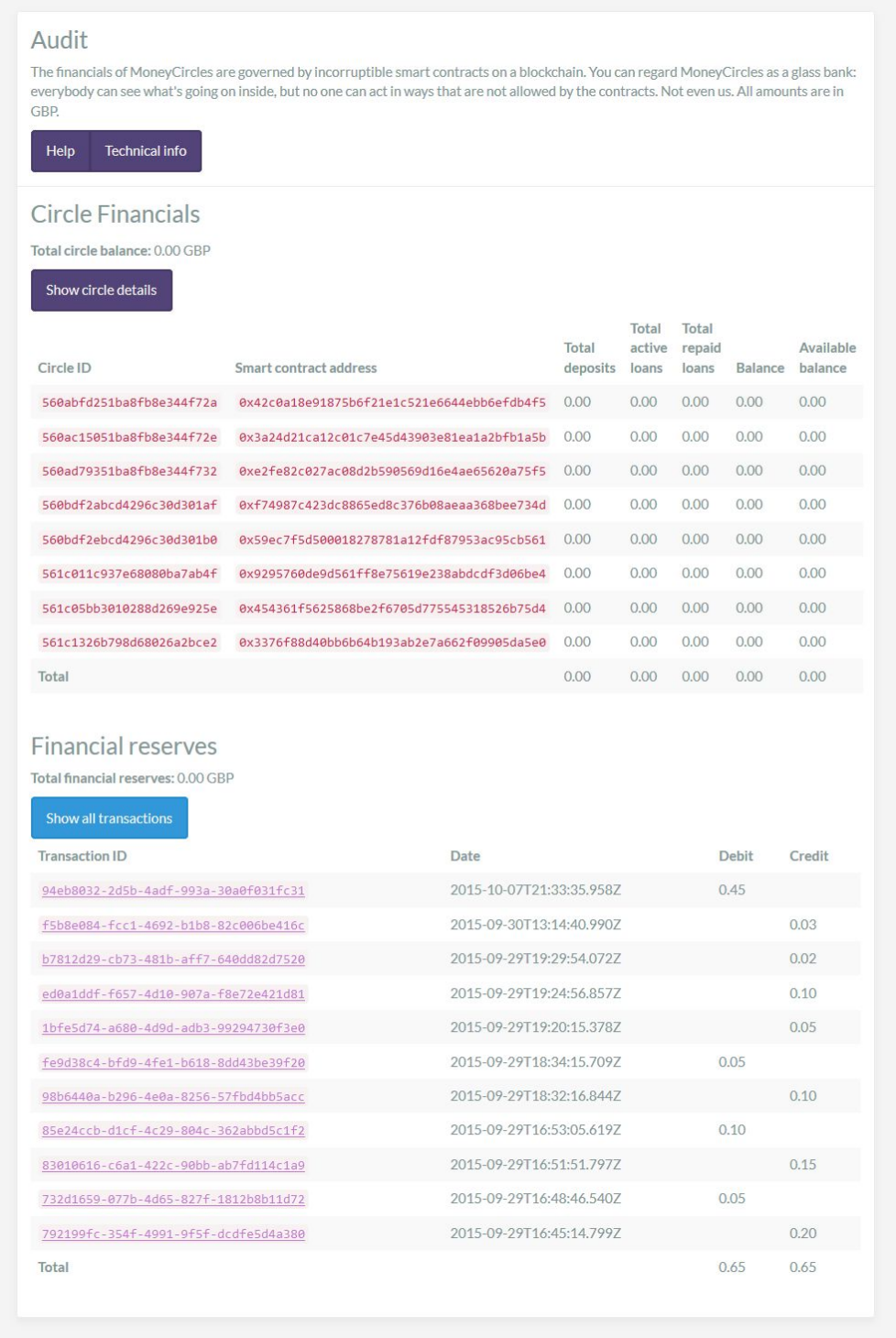
6.3.1 Audit trail

An audit trail page is provided in the application based on the data from the smart contracts and the transaction information provided by the Uphold API. This page is public and contains pseudonymised data so that outside users can inspect it.

Essentially the audit trail demonstrates:

1. Completeness: All transactions executed by users in the service have resulted in a real monetary transaction which can be inspected in the Uphold Reservechain.
2. Correctness: The shown amounts of deposits, loans, balances are calculated by the smart contracts, the logic of which can be inspected.
3. Solvency: The funds deposited by users in circles is still present in the MoneyCircles account. All transactions to the MoneyCircles account are shown and can be inspected in the Uphold Reservechain.

An example of the audit page is shown in the figure below.



Audit

The financials of MoneyCircles are governed by incorruptible smart contracts on a blockchain. You can regard MoneyCircles as a glass bank: everybody can see what's going on inside, but no one can act in ways that are not allowed by the contracts. Not even us. All amounts are in GBP.

Help | Technical info

Circle Financials

Total circle balance: 0.00 GBP

Show circle details

Circle ID	Smart contract address	Total deposits	Total active loans	Total repaid loans	Balance	Available balance
560abfd251ba8fb8e344f72a	0x42c0a18e91875b6f21e1c521e6644ebb6efdb4f5	0.00	0.00	0.00	0.00	0.00
560ac15051ba8fb8e344f72e	0x3a24d21ca12c01c7e45d43903e81ea1a2bfb1a5b	0.00	0.00	0.00	0.00	0.00
560ad79351ba8fb8e344f732	0xe2fe82c027ac08d2b590569d16e4ae65620a75f5	0.00	0.00	0.00	0.00	0.00
560bdf2abcd4296c30d301af	0xf74987c423dc8865ed8c376b08aeaa368bee734d	0.00	0.00	0.00	0.00	0.00
560bdf2ebcd4296c30d301b0	0x59ec7f5d500018278781a12fdf87953ac95cb561	0.00	0.00	0.00	0.00	0.00
561c011c937e68080ba7ab4f	0x9295760de9d561ff8e75619e238abdcdf3d06be4	0.00	0.00	0.00	0.00	0.00
561c05bb3010288d269e925e	0x454361f5625868be2f6705d775545318526b75d4	0.00	0.00	0.00	0.00	0.00
561c1326b798d68026a2bce2	0x3376f88d40bb6b64b193ab2e7a662f09905da5e0	0.00	0.00	0.00	0.00	0.00
Total		0.00	0.00	0.00	0.00	0.00

Financial reserves

Total financial reserves: 0.00 GBP

Show all transactions

Transaction ID	Date	Debit	Credit
94eb8032-2d5b-4adf-993a-30a0f031fc31	2015-10-07T21:33:35.958Z	0.45	
f5b8e084-fcc1-4692-b1b8-82c006be416c	2015-09-30T13:14:40.990Z		0.03
b7812d29-cb73-481b-aff7-640dd82d7520	2015-09-29T19:29:54.072Z		0.02
ed0a1ddf-f657-4d10-907a-f8e72e421d81	2015-09-29T19:24:56.857Z		0.10
1bfe5d74-a680-4d9d-adb3-99294730f3e0	2015-09-29T19:20:15.378Z		0.05
fe9d38c4-bfd9-4fe1-b618-8dd43be39f20	2015-09-29T18:34:15.709Z	0.05	
98b6440a-b296-4e0a-8256-57fbd4bb5acc	2015-09-29T18:32:16.844Z		0.10
85e24ccb-d1cf-4c29-804c-362abbd5c1f2	2015-09-29T16:53:05.619Z	0.10	
83010616-c6a1-422c-90bb-ab7fd114c1a9	2015-09-29T16:51:51.797Z		0.15
732d1659-077b-4d65-827f-1812b8b11d72	2015-09-29T16:48:46.540Z	0.05	
792199fc-354f-4991-9f5f-dcdfe5d4a380	2015-09-29T16:45:14.799Z		0.20
Total		0.65	0.65

The audit page provides a high level of traceability without compromising users' private data.

6.3.2 External verification

Although the MoneyCircles web application claims that it is governed by incorruptible smart contracts on a blockchain and provides consistent, detailed information on its transactions, it is still a centralised

web application. Users have no guarantee of the truth of these claims, and theoretically the web application could be dishonest or compromised. Technically adept users can verify the validity of the audit trail by examining it in detail.

6.3.2.1 Verification of the smart contracts

The private Ethereum blockchain on which the smart contracts run is open to the public in read-only format. Commits by external parties are not allowed. The Solidity[24] source code of the smart contracts is provided.

External auditors could verify properties such as:

- The smart contracts are deployed using the published source code.
- The smart contracts function as advertised: external auditors can examine and execute the smart contracts on their own blockchain, simulating the actions that have occurred in MoneyCircles, verifying that they lead to the same results.
- All displayed circle contracts exist on the blockchain, and no other circle contracts exist.
- All displayed loan contracts exist on the blockchain, and no other loan contracts exist.
- All displayed transaction ID's are registered in the smart contracts, and no other transaction ID's are registered.
- The same private blockchain is published at each moment; repetitive checking on different moment delivers the same blockchain data. The blockchain data published at moment T is contained in and added upon in the blockchain data published at moment T' after T.

6.3.2.2 Verification of the Uphold transactions and ledger

External auditors could verify properties such as:

- The financial transactions registered in the MoneyCircles smart contracts are executed as advertised. For example a deposit transaction in the smart contract for circle C by user U of 100 GBP can be publicly verified to be indeed a transaction of 100 GBP. However to verify that it is a transaction of user U to MoneyCircles, authentication of user U is needed.
- The Uphold account is backed up by real-world assets. Principally a balance in an Uphold account is an obligation from Uphold to its users, of whom the MoneyCircles proof of concept service is one. Uphold provides a public ledger of their obligations and assets in the Reserveledger[25].

7 Challenges

The proof of concept implementation leaves a set of challenges and risks. We explore the risks and suggest strategies to deal with them.

---

[24] "Solidity Tutorial · ethereum/wiki Wiki · GitHub." 2015. 1 Oct. 2015 <https://github.com/ethereum/wiki/wiki/Solidity-Tutorial>

[25] "Bitreserve - Transparency." 2014. 1 Oct. 2015 <https://bitreserve.org/en/transparency>

7.1 Technological risks

7.1.1 The MoneyCircles service gets compromised

A sound information security principle is to not think of the question *if* a service gets compromised, but *when*, and prepare for that moment to limit the impact as much as possible.

In the proof of concept implementation, development efforts were directed to other core objectives, hence little was done to reduce this impact. Authentication tokens for both the MoneyCircles account which secures the circle balances and the individual users accounts are kept in a MongoDB database. An attacker successfully compromising the server environment could therefore obtain these access tokens and act on behalf of the MoneyCircles account and the individual users' accounts.

The impact of this event can be dealt with by applying well-known information security strategies such as encryption and sharding.

Furthermore the permission structure of the Uphold API are coarse-grained: an application can either have permission to make any type of transaction, or none at all. That means that after having obtained the access tokens, the attacker could obtain all funds of the MoneyCircles accounts and all its users. We describe suggestions to Uphold to improve this below.

7.1.2 The Ethereum project gets discontinued

The proof of concept is built using blockchain technology from Ethereum. Ethereum is backed by the Ethereum Foundation, which was funded in one of the largest crowdfunding projects[26] in history. Recently however the organisation has admitted to be in a weak financial position[27] which could be considered a risk to the arising Ethereum crypto-economy and the further development and maintenance of the technology.

Considering the way in which the Ethereum blockchain technology is applied in the proof of concept we consider this a minor risk to MoneyCircles. Firstly, the Ethereum code is applied in the proof of concept as a private blockchain and hence serves a purpose independent from the public Ethereum blockchain. Furthermore, the code base of the Ethereum blockchain and specifically the virtual machine that runs the smart contracts has already been embraced by other projects including Tendermint[28] and the Eris Industries technology stack[29]. Finally, in the eventuality that the Ethereum Foundation would cease to exist, the open source code base is highly likely to be maintained and further developed by open source developers, either in an independent role or employed by businesses building on the technology.

---

[26] "List of highest funded crowdfunding projects - Wikipedia, the ..." 2014. 8 Oct. 2015 <https://en.wikipedia.org/wiki/List_of_highest_funded_crowdfunding_projects>
[27] "The Evolution of Ethereum - Ethereum Blog." 2015. 8 Oct. 2015 <https://blog.ethereum.org/2015/09/28/the-evolution-of-ethereum/>
[28] "Tendermint." 2014. 8 Oct. 2015 <http://tendermint.com/>
[29] "Eris Industries." 2014. 8 Oct. 2015 <https://erisindustries.com/>

7.2 Organisational risks

7.2.1 MoneyCircles misbehaves

Because of the high level of verifiability as described above, the MoneyCircles proof of concept service is highly transparent. Any misbehaviour can be detected quickly. However misbehaviour in this setup can not be *prevented*.

7.2.2 Uphold misbehaves or turns insolvent

Although Uphold provides a high grade of transparency into their services, it can not be considered an absolute impossibility that they would turn insolvent or that user funds would otherwise be at harm.

To reduce the impact of this eventuality, multiple different parties providing such services can be used.

7.2.3 Circle members or administrators misbehave

As end users access the functionality of MoneyCircles through the web application and have no way of directly accessing the funds of MoneyCircles or other users, they are bound by the same rules as the smart contracts. This limits the power of malicious users to damaging behaviour within the system, for example taking out a large loan and never paying it back. Reducing these risks is out of scope of the proof of concept and shall be explored in future versions.

7.3 Regulatory risks

7.3.1 Localized regulations on cryptography

The current government of the United Kingdom has indicated[30] that strong regulation on encryption is to be expected. This has led companies at the forefront of blockchain technology such as Eris Industries[31] to leave the UK, as their entire business is centered around cryptography.

The technological vision of MoneyCircles is also strongly based on the use of cryptography. As such any limitation or ban in the use of encryption forms a regulatory risk. An expert study[32] has however argumented that any exceptional access to encryption is both unfeasible and economically undesirable.

---

[30] "Can the government ban encryption? - BBC News - BBC.com." 2015. 7 Oct. 2015 <http://www.bbc.com/news/technology-30794953>

[31] "Company Blog | Eris Industries Statement on the ..." 2015. 7 Oct. 2015 <https://blog.erisindustries.com/2015/05/29/ei-comms-data-bill/>

[32] Abelson, H. "Keys Under Doormats: Mandating insecurity by requiring ..." 2015. <http://dspace.mit.edu/handle/1721.1/97690>

8 Short to mid-term further developments

8.1 Integration with bank accounts

As of Oct 14, 2014, Uphold supports deposits and withdrawals from UK and European bank accounts in the SEPA zone[33]. Shortly support for bank accounts on the ACH network in the United States will be added. This means that end users of MoneyCircles never have to deal with any form of cryptocurrency.

8.2 Multiple value ledgers

In the proof of concept Uphold is used to store and transact funds. Other such providers like Ripple[34] or OpenLedger[35] can be supported in a similar way. As explained above, the circle balance is backed up by the value storage network, in the proof of concept only Uphold. Supporting multiple such providers would allow for reduction of the risk for circle members that the the circle balance would be lost because of the eventuality that the service backing the balance would be insolvent.

8.3 Usable, secure access to decentralised services from mobile devices

One of the reasons to build our proof of concept using a centralised service is that there is currently no widely supported, usable and secure form of access to decentralised blockchain services. Participating in a fully decentralised blockchain ecosystem requires amongst others running fully equipped blockchain node and sophisticated private key management, something that cannot be expected from current mobile platforms nor from mainstream users. Promising developments in this area are under way and should be incorporated in the MoneyCircles architecture once they have reached maturity.

8.4 Recommendations to Uphold and similar service providers

8.4.1 Multiple, separate identities

Because of the current character of Uphold, the funds for all Circles are stored in a single account. This is suboptimal in terms of security and traceability. If a bad actor would gain access to this account, they would have access to all circle funds. Legitimate users of MoneyCircles users can explore their financial transactions with MoneyCircles in their Uphold transaction history, but from there they cannot trace the transactions back to the specific circle they interacted with.

For our use case and likely many others it would be good if a service building on Uphold would be able to instantiate multiple identities of itself. In the case of MoneyCircles that would mean that every circle is a first-class citizen in terms of financial transactions. Transactions would be traceable to the level of the circle not only in the smart contracts, but also in the financial transaction history.

---

[33] "Uphold - Welcome to Uphold. The Internet of Money™." 2015. 14 Oct. 2015 <https://uphold.com/en/blog/posts/uphold/welcome-to-uphold-the-internet-of-money>
[34] "Ripple." 2012. 1 Oct. 2015 <https://ripple.com/>
[35] "OpenLedger - Welcome." 2015. 1 Oct. 2015 <https://www.openledger.info/>

8.4.2 Limiting outgoing transactions

An authorised app on the Uphold platform currently has a lot of power, which might be abused by bad actors. Several measures could be taken to mitigate these risks. In conjunction with the fact that all transactions in MoneyCircles are verifiable and traceable, this would allow for preventing large-scale abuse and detecting it at an early stage.

8.4.2.1 Real-time fraud detection mechanisms

Services for real-time analysis and detection of usage patterns and (financial) transactions could be applied to mitigate both the impact of MoneyCircles user accounts being compromised and the risk of MoneyCircles being used for illegal activities such as money laundering.

An example are the the services of CryptoCorp[36]. CryptoCorp offers a transaction signing service which acts as a signer in 2-out-of-3 multisignature Bitcoin transactions, backed by fraud detection algorithms. Under normal circumstances, CryptoCorp will co-sign any transaction that the user signs. If however the fraud detection algorithm flags the transaction, it will not be signed. In such an event the application (such as MoneyCircles) can follow up accordingly.

8.4.2.2 More fine-grained security

The permissions for an application using the Uphold API currently have an “all or nothing” character. That means that each app that a user authenticates to make transaction on their behalf, could theoretically create transactions that would transfer out all the funds of their account.

Offering more fine-grained ways to give applications access to users’ accounts would limit these risks. For example an application could be given access only to a specific card.

8.4.2.3 Multi-signature accounts

Funds might be protected by introducing multi-signature requirements on Uphold accounts or cards, as is common in Bitcoin and other cryptocurrencies. Financial transactions would require approval of N out of M signers. For the case of MoneyCircles the required signers for transactions might be a quorum of administrators of circles, chosen by voting through smart contracts. Multi-signature verification could be made obligatory for transactions above a certain value.

8.4.2.4 Multi-factor security for high-value transactions

Uphold requires multi-factor authentication to log in. However once a user is logged in and an application has been authenticated to transact on their behalf, no further authentication is required. This requirement could be introduced for transactions above a certain value.

8.4.2.5 Time limits for transactions

Finally, Uphold users might be offered the option to lock their funds for a specific amount of time, or only allow outbound transactions up to a certain amount per day. This would limit the extent to which the funds of users and circles could be stolen by an attacker who compromised the system.

---

[36] "CryptoCorp | Innovating Bitcoin security with HDM technology." 2014. 7 Oct. 2015 <https://cryptocorp.co/>

8.4.3 Richer transaction explorer

The current Uphold transaction explorer exposes the sources of transactions. For example if an amount is transferred in transaction A, and transferred further in transaction B, the explorer for transaction B will list transaction A as its source. In that way the origin of funds can be traced in terms of the Uphold ledger.

However there is currently no accessible way to show that the amount of transaction A was further transferred in transaction B. Such functionality would help in proving that the money in a certain account is still held in that account, and hence proving the solvency of that account.

8.5 External oracles for a higher grade of decentralisation

Smart contracts in the Ethereum paradigm can not make calls to outside systems, data about the outside world has to be provided to them. A component providing data of the outside world to a smart contract is generally called an oracle[37]. Currently the MoneyCircles service is the sole provider of such data to its contracts. Any incorrectness in such data can be detected as described earlier, but not prevented. This could be improved by introducing external, independent oracles.

As an example, consider registering a deposit of 100 GBP into a circle. Currently the Uphold transaction ID is stored in the smart contract by the MoneyCircles service. The correctness of this transaction ID can be verified by external auditors.

In a scenario with external oracles, the MoneyCircles service would not have direct access to the operation “store deposit transaction” of the specific circle contract. Instead, a number of independent external parties (oracles) would have access. Say there would be three such oracles, and a minimum of two would be required to register the transaction. MoneyCircles would provide the transaction ID to the three oracles. Only if two out of three of the oracles confirmed that the transaction was correct would the smart contract register it and consider it as part of the circle balance.

8.6 Reputation and credit scoring

Reputation and credit scoring is achieved using MoneyCircles’ Trust Score system. This is used to assess a potential borrower’s likelihood, propensity and commitment to repay a loan. The Trust Score is partly determined by traditional data sources from Credit Reference Agencies, including credit and identity scores and weighted policy rule sets (e.g. recency of missed payments, defaults and County Court Judgements).

MoneyCircles would then add to the score using other data sources the member makes available to us, e.g. from social media sites which also provide an opportunity to screen scrape information from such services. MoneyCircles can then connect this with verification information based on handset information, IP address location etc.

Prior behaviour on the platform e.g. savings habit, repayment of other loans, 'references' given to other members of the circle who have repaid loans will also input to the trust score.

---

[37] "Ethereum and Oracles - Ethereum Blog." 2014. 6 Oct. 2015 <https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/>

Our approach is one of Whitelisting rather than blacklisting and would be configured by each circle where an administrator adds weight each data set in order of priority custom to the strength of the social bond.

Considerable work on decentralized reputation systems has been done in the OpenBazaar project[38], which might be applied or integrated in the MoneyCircles credit scoring mechanism.

8.7 Other possible developments

8.7.1 Tendermint blockchain

Ethereum is designed as a public, decentralised blockchain which requires tradeoffs in terms of efficiency. We apply the Ethereum technology to serve a different purpose: to govern the actions of a private system in a publicly verifiable way. This is suboptimal as the tradeoffs for a fully decentralised blockchain like proof of work are still applied.

Tendermint[39] is an approach to blockchains championed by Eris Industries[40] which is more fit for this purpose. It has all the characteristics and technical capabilities of the Ethereum smart contracts platform, but doesn't require proof of work. Exploring Tendermint as the smart contract backend would be a logical next step.

8.7.2 Verifiable bridge between smart contracts and fiat currency value storage

We have used Uphold to work with fiat currency in a programmable manner and smart contracts on an Ethereum private blockchain to effectuate and govern the transactions. As described above this introduces a risk of inconsistency between the two. The MoneyCircles service is responsible for dealing with this risk.

This risk could be eliminated if there were a common verifiable bridge between the smart contracts and the fiat currency value storage, concretely between Uphold and Ethereum smart contracts. Such a common bridge could be either realised by Uphold or a third party.

8.7.3 Working with fiat currency in Ethereum

Referring to and interacting with fiat currency in Ethereum contracts is a recurring theme in Ethereum development efforts. For example through the SchellingCoin[41] concept, data feeds of fiat currency rates might be provided to Ethereum contracts. It's not unthinkable that further innovation will lead to possibilities to directly work with fiat currency in Ethereum contracts.

---

[38] "Decentralized Reputation in OpenBazaar | OpenBazaar." 2015. 14 Oct. 2015 <https://blog.openbazaar.org/decentralized-reputation-in-openbazaar/>
[39] "Tendermint." 2014. 6 Oct. 2015 <http://tendermint.com/>
[40] "Eris Industries." 2014. 6 Oct. 2015 <https://erisindustries.com/>
[41] "SchellingCoin: A Minimal-Trust Universal Data Feed ..." 2014. 6 Oct. 2015 <https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/>

9 Long-term future developments

9.1 Circles as decentralised autonomous organisations

Decentralised smart contract technology on a blockchain can facilitate a new form of organisational structure: the decentralised autonomous organisation (DAO)[42]. DAOs are fully automated entities with no physical counterpart, existing only on a decentralised blockchain. They can act according to the functions encoded in their contracts, within the capabilities and limits of the platform they are deployed on.

Assuming the further evolution of smart contract and cryptocurrency technology, circles could ultimately become decentralised autonomous organisations. The fully automated circle would be owned by its members. The circle DAO would be the sole controller of the funds held in it. With the circle being a DAO, there would truly be no third party involved in the saving and lending between members.

9.2 Role of business/network operator

As circles become more and more autonomous, and it's smart contract software that takes care of carrying out business matters instead of a "business" in the form of an organization like Money Circles Ltd, the question arises what the role of a business like Money Circles Ltd might be.

We envision that such businesses will function as operators of the smart contract systems they create, and provide value-added services to the DAO's. The business won't service thousands or millions of end users directly, but provide the means to run DAO's and effectively service those as clients.

However we believe in the short to mid-term we are looking at degrees of decentralisation as is sensible and permitted by regulators required to bridge circles into the 'real world' financial system.

10 Regulatory Requirements

The regulatory framework that would govern MoneyCircles is dependent on whether it provides services directly to consumers or supplies the infrastructure to existing financial institutions. In the former case the regulatory framework is evolving, but e-money or P2P providers may simply be registered rather than authorised which would make establishing the company straight forward. As MoneyCircles does not hold deposits, circles would operate under existing institutional licenses.

MoneyCircles would meet Money Laundering Prevention and Know Your Customer requirements by utilising traditional identification data sets from credit reference agencies and will complement this using richer data sources, including information provided by a member's online presence, e.g. Facebook and LinkedIn. This can be achieved by using oracles to automate the process for cross-checking external data sources.

---

[42] "Decentralized autonomous organization - Wikipedia, the ..." 2015. 6 Oct. 2015 <https://en.wikipedia.org/wiki/Decentralized_autonomous_organization>

11 Conclusion

The MoneyCircles proof-of-concept technically demonstrates peer-to-peer lending in a social 'circle' using smart contracts on a blockchain. A private blockchain is useful to provide a high grade of correctness, transparency and verifiability. The honest behaviour of the service can be verified both by non-technical users and technical external auditors.

We believe the potential for such a solution to enable greater financial inclusion in the global consumer credit marketplace is very powerful, possibly liberating millions of people from a cycle of unsustainable indebtedness. Whilst we believe this technology has the potential to be incredibly disruptive, we don't believe this needs to be at the cost of existing financial institutions. In fact the emergent centralised peer-to-peer lending industry has clearly demonstrated traditional financial institutions are actively seeking new ways to put their money to use and earn better returns for their depositors / investors. This would be especially so if it brought all the added benefits of cost efficiencies, automation and incorruptible governance.

Whilst our ambition is to enable any one group of people to use circles for any purpose, to the exclusion of criminal purposes, this also includes existing financial institutions such as banks and credit unions. MoneyCircles when combined with decentralised reputational systems could enable financial institutions to lend more of their assets, improving liquidity – especially amongst the 525 credit unions in the UK (where only 50% of assets are on loan). Importantly MoneyCircles establishes an enhanced digital relationship with customers, consolidating relationships in a way that is relevant to their social use of technology.

If you are an investor interested in participating in our current subscription for Money Circles Ltd or member of the press please contact Jamie Burke on jb@outlierventures.io

If you are a financial institutional or fintech vendor who would like to collaborate or alternatively a group of people keen to test out the technology, please get in touch at info@moneycircles.com