Converging Blockchain and Social Business for Socio-Economic Development

Raghava Rao Mukkamala[1,2], Ravi Vatrapu[1,2], Pradeep Kumar Ray[3], Gora Sengupta[4] and Sankar Halder[4]
[1]Centre for Business Data Analytics, Dept. of Digitalization, Copenhagen Business School, Denmark
[2]Department of Technology, Kristiania University College, Norway
[3]University of Michigan-Shanghai Jiao Tong University Joint Institute, China, [4]Mukti, India
{rrm.digi,vatrapu}@cbs.dk, pradeep.ray@sjtu.edu.cn, {gora.sengupta,sankar.halder}@muktiweb.org

***Abstract*—In recent years, there has been a growing research attention and practitioner interest in exploring the suitability of Blockchain technology for decentralised applications in multiple domains. This paper investigates the application of Blockchain technology to address some of the key challenges faced by the domain of Social Business (SB). SB is a business model for investments in social causes for the socio-economic development of under-privileged communities. We have modelled a small example of micro-credit use-case from microfinance activities of SB using a semi-formal modelling approach using Blockchain technology. We identified that the Blockchain technology provide solutions that enhance trust, transparency and auditability in SB activities. However, we have also identified challenges related to creating a native cryptocurrency for SB, and barriers to infrastructure and technology adoption by the different stakeholders in SB.**

***Index Terms*—Blockchain Technology, Social Business, Conceptual Design**

I. Introduction

Blockchain technologies continue to attract significant interest both from academic communities and industries [1]–[3]. Blockchain technology came into limelight when Bitcoin [4], a decentralised digital cash system that was introduced as a peer-to-peer cryptocurrency in 2009. The recent explosion of interest towards blockchain-based applications is both due to its disruptive & innovative nature as well as its strong underlying theoretical foundations of cryptography, distributed consensus algorithms, and decentralised databases. With the blockchain technology, the applications that once used to run through a trusted intermediary can now operate in a decentralised manner with the need of having central authority [1]. Because of this disruptive nature, blockchain has led to the evolution of many decentralised applications in multiple domains such as finance [5], healthcare [6] supply chains [3] etc.

Social Business (SB) is the term defined by the Nobel laureate Prof. Yunus to develop and apply a business model for investments for social causes such as poverty removal, healthcare and welfare activities that are not attractive from the perspective traditional profit-based business models [1]. For the purposes of this paper, the scope of an SB is restricted to being an entity whose primary goal is socio-economic development of the under-privileged. Typically it is "characterized primarily by humanitarian or cooperative, rather than commercial objectives, and pursues activities to relieve suffering, promote the interests of the poor, protect the environment, provide basic social services, or undertake community development" [7].

An SB obtains operating funds from soft loans or grants from sponsors (Social Investors) who may be individuals, philanthropic foundations, corporations under corporate social responsibility, national governments or international agencies such as the World Bank and United Nations. They allocates these funds to carry out the socio-economic development projects that an SB has identified. In the interests of continuing and sustained development activity, an SB needs to ensure that the flow of input funds remains commensurate with the nature and scale of its project activity, as well as in some cases ensure availability of operating expenses for solutions delivered in the past. All SB organisations need to raise funds from individuals and organisations and hence the donors (social investors) need to have the trust in SBs. Unfortunately, SBs do not have the financial resources (unlike governments and corporate sector) to develop the trust through promotions and other investments. Hence they rely on online software systems to operate at minimal overheads, otherwise precious donor funds would be consumed by the overheads (making less and less funds available for the target social causes). Therefore, blockchain technology could potentially could provide efficient and effective solutions for enhancing transparency, verifiability and auditability in distributed peer-peer systems networks underlying social businesses. In this paper, we examine the application of blockchain technology to SB for enhancing trust, transparency, privacy and auditability of the activities of SB. More specifically, we confine the scope of the paper to microfinance activities of SB and using a small micro-credit example as an use-case, we will investigate the suitability of blockchain technology for SB. Taking this into account, our overarching research question will be:

> *How can blockchain technology help in addressing the challenges faced by the Social Business organisations?*

The remainder of the paper is organized as follows. The sec. II 2 summarizes related work and followed by a description of challenges faced by SB in sec. III. We then provide a brief introduction to blockchain technology in sec. IV, a conceptual design and modelling of micro-credit use case with blockchain will be presented in sec. V. We will present

[1] http://socialbusinesspedia.com/

978-1-5386-5035-6/18/$31.00 ©2018 IEEE

opportunities and challenges of using blockchain for SB in sec. VI and conclude our work in sec. VII.

II. Related Work

Blockchain is an evolving technology with an increasing number of domain-specific applications in health care, supply chain management, information systems etc. However, to the best of our knowledge, the applicability of blockchain technology for social business has not been explored yet. In the health care domain, several studies explored blockchain technology for medical data access. A seminal and highly relevant contribution is [6], which proposes an architecture based on artificial intelligence and blockchain technology to enable control of patients' personal data including medical records. In supply chain management, [3] provided ontologies for the fundamental concepts of traceability in supply-chain provenance, and a formal ontological modelling approach to help the development of smart contracts for the blockchain-based solution using first-order logic in Prolog.

Within the information systems discipline, current research on blockchain technologies and cryptocurrencies is still in the nascent stage. That said, we gathered all the recent research papers from major information systems conferences and journals and the summary of review results is presented in the table I. First, the most notable research work on blockchain based technologies is [19], [20], which forecasts that in near future, blockchain technologies will empower organisations to implement solutions using distributed ledger technologies, which will handle contracts and transactions among the organisations in a decentralised manner without any need of having their own legal entities and finally will lead to the emergence of decentralised autonomous organisations. Second, several research frameworks [12], [16], [19] were proposed to study organisational adoption challenges and IT governance, e.g. in terms of decision rights, accountability, and incentives for the organisations which can reap the benefits from decentralised solutions using these technologies. Development of proof of concept prototypes for blockchain technologies using design science guidelines [10], [14], [17], [18] is also an increasing trend in recent years. Finally the research on the cryptocurrencies per se is rather limited [8] when compared to the more general research focus on blockchain based applications for organisations. In contrast to the extant research, our paper tries to identify opportunities and challenges of using blockchain technology to social business sector by modelling a micro-finance case study using semi-formal modeling approach using an open-source blockchain platform.

III. Social Businesses and Challenges

There have been persistent efforts towards social causes from Non-Government Organisations (NGOs), Corporate Social Responsibility (CSR) divisions of organisations, and Social Enterprises (SE). Although there are differences between SB, NGO,CSR and SE [22], all of these orgnasitaion types can be classified as social businesses for the purpose of this paper as we are addressing the problem of raising funds that is a common need across all of these organization types. SBs mostly operate at the grassroots level and are close to the action scene at deep interior locations where normally other providers would not be physically present. This increases their qualification for carrying out community development projects on behalf of corporates, international aid agencies or the government. Moreover, not-for-dividend SBs sometimes receive financial as well as professional assistance free of charge directly from individual sponsors when compared with for-profit entities. As such, transition to new technologies such as blockchain can confer them competitive advantages.

In this paper, we consider a Social Business that delivers micro-financing services from *social investor* funds to beneficiaries for the purpose of livelihood generation and social development. Traditionally a micro-finance operating SB collects sponsorships from social investors and softloans them to eligible borrowers for a pre-specified period of time for a pre-approved purpose. On expiry of the period the SB collects the maturity amount from the borrower and transfers it back to the social investor. Some relevant challenges traditionally faced by SBs in this context are noted below. While true for SBs in general, these challenges are particulary relevant for micro-finance operations and require spending of significant efforts and resources by the SBs to address them.

1) Maintaining a trust relationship with the social investor is a key factor in the SB's ability to receive their sponsorships consistently. The social investor sponsors the SB's activities based on the belief that the SB will deploy these funds in a timely manner, for the declared purpose and will do so in complete accordance with the local laws. This requires substantial time, resources and efforts by the SB.
2) The SB's activities in transferring the agreed amount of investor funds in a timely manner to the actual beneficiary needs to be visible to the social investor.
3) SBs must ensure that any personal data of the social investor (as well as beneficiaries) is kept secure.
4) Getting the social investors to follow local regulatory requirements for accepting of sponsorships by the SB may mean registering and following *know your customer* (KYC) type procedures. Although not their area of speciality, SBs may find themselves forced to follow banking type operational procedures.
5) Under existing operations, some social investors, especially international investors, could be averse to sharing personal information required for local registration processes due to reasons of security, and the SB could find itself spending substantial amounts of time and effort in trying to convince them to register and start sponsoring
6) Depending on the preferences of the social investors, the SB must ensure that sponsorhip transactions are kept private or made publicly visible.
7) Funds to carry on planned activities may not be available in a consistent and timely manner since this depends on the consistency of social investors.

Authors	**Focus**	**Theory / Method**	**Main Findings**
Glaser, F., et.al. (2014) [8]	User perspective in cryptocurrencies	Empirical case study	Indicated that new Bitcoin users rather use it as an asset with a speculative investment intention rather than as a currency.
Glaser, F., et.al. (2015) [9]	Decentralized Consensus Systems	Taxonomy	Provided a taxonomy for decentralised consensus systems and cryptocurrencies and an overview of different types of decentralised systems.
Beck, R., et.al. (2016) [10]	Trust-based payment	Design science, prototype	Prototype of trust-based coffee shop payment system to demonstrate blockchain technology and to identify strengths and weaknesses of technology.
Atzori,M. (2016) [11]	Democracy, state authority	Decentralized governance	Dominance of private powers in blockchain-based decentralized governance may lead to emergence of a stateless global society and dis-empowerment of citizens.
Risius, M., et.al. (2017) [12]	Blockchain Research	Framework for Social Media Research [13]	Research framework for blockchain based three activities (design & features, measurement & value, management & organization) at four levels of analysis (users & society, intermediaries, platforms, firms & industry).
Hyvaerinen, H., et.al. (2017) [14]	Blockchain prototype	Design Science Approach	Developed a blockchain-based prototype to demonstrate enhanced transparency regarding the flow of dividends and reduce tax frauds in public taxation sector.
Glaser, F. (2017) [15]	Blockchain research	Blockchain ontology	Domain concepts for blockchain-based systems and connecting technological implications to digital market models.
Notheisen, B., et.al. (2017) [16]	Blockchain Market	Blockchain Market Engineering Framework	Proposed a four-layered approach to blockchain research using market engineering framework: agent, application, infrastructure and environment.
Cholewa, J., et.al. (2017) [17]	Blockchain prototype	Design Science approach	Developed blockchain based proof of concept prototype for automated transaction of real-world assets such as cars registration.
Naerland, K. et.al. (2017) [18]	Blockchain prototype	Design Science approach	Design principles for applications that can mitigate transactional risk and uncertainty to decentralized inter-organizational environments
Beck, R., et.al. (2018) [19]	Blockchain economy	Decentralized autonomous organizations	IT governance Framework for blockchain economy along three dimensions: decision rights, accountability, and incentives and a case study of an emerging decentralized autonomous organizations
Beck, R (2018) [20]	Decentralized autonomous organizations	Orgnisational design	Blockchain empowers organizations to implement contracts and transactions without the need of having a central legal entity and therefore it will lead to emergence of decentralized autonomous organizations.
Salviotti,G., et.al.(2018) [21]	Business Application Landscape	Structured approach	Build a framework to classify blockchains based on protocols, consensus and permissions and application areas.

TABLE I
RELATED WORK ON BLOCKCHAIN AND CRYPTOCURRENCIES FROM INFORMATION SYSTEMS PERSPECTIVE

8) Lack of adequate human resources impacts on the timeliness and quality of the SB's products and/or services.
9) Success of an SB in the short or medium term could become a challenge for it in the longer term. While an SB could complete a project very successfully, subsequent operations could require up-scaling and a level of growth that the SB might not have the funding to handle. This in turn could lead to a substantial erosion of the good work done in the past.

From the above it can be seen that the typical SB is required to spend substantial time and effort in social investor creation, assurance and retention to ensure consistency of much required funds inflow. Central to these operations is the fact that under the current scenario it is solely the SB's authority that is used to enable trust in the system. Inability of the SB to create and continuously strengthen its trust relationship with the social investor could result in inconsistent funds flow eroding the SB's capability to perform its socio-economic development activities.

IV. BLOCKCHAIN TECHNOLOGY

Blockchain is the decentralized distributed datastore that is combined with guarantees against tamper-resistance of transactions/records using cryptographic methods. By using time-stamping of its transactions and messages, blockchain provides universally verifiable proofs for existence/absence of a transaction in the distributed database and the underlying cryptographic primitives using hash functions and digital signatures provide guarantee that these proofs are computationally secure and verifiable at any point in time. Blockchain is decentralized, jointly maintained by a plurality of independent parties/nodes and achieves consistency of transactions among distributed nodes by using distributed consensus protocols (such as Byzantine fault tolerance algorithm [23]) without the need of having a central authority. Blockchain transactions are transparent and visible to all users of the system (e.g. public blockchains) and at the same time blockchain provides anonymity to its users by allowing them create pseudo-anonymous transactions without the need for disclosing their personal information.

The disruptive and innovative nature of blockchain technology resulted in the evolution of many decentralized applications such as cryptocurrencies and smart contracts. Bitcoin, a decentralised cryptocurrency based on blockchain technology was introduced in 2009 [4] and as of 2018, Bitcoin is the largest cryptocurrency with a market capital of approximately more than 100 billion USD. Blockchain technology is built on three main concepts: a distributed database, a trust protocol and cryptography. In the following subsections we will explain them briefly.

A. Distributed database

Built on the concept of peer-to-peer networks and highly distributed storage systems [24], blockchain technology [25] can be considered as a distributed data store with state machine replication using peer-to-peer protocol, where the transactions are the atomic changes to the data store which are grouped into blocks [6]. Blockchain can be thought of a distributed log database where the records are batched into timestamped blocks and each of these blocks are identified by their cryptographic hash value [1].

B. The Trust Protocol

In order to avoid having to include a central, third party authority for enabling trust in the system, there needs to be some mechanism that establishes trust between the involved parties, which is achievable by distributed consensus of the involving parties. In blockchain this is done through a distributed consensus trust protocol. Although the protocol can vary slightly from system to system, the basic idea of achieving trust with the consensus among the involving parties remains the same. The two most widespread concepts of this protocol are proof-of-work and proof-of-stake anchoring schemes, which follow a Byzantine fault tolerance scheme [23] and will be further explained as follows.

Proof-of-work (PoW) refers to the idea that a service requester is required to solve a cryptographic puzzle (*computational work*) to participate in a network, as initially proposed in hashcash [26] as a counter measure for denial of service attack using CPU cost-functions. In blockchain and especially in Bitcoin [4], it is used as a verification technique for finding a suitable appropriate header for new blocks of data and to append them to the chain of blocks. To add a block, a node has to solve a cost-function (find the right *nonce*), which is a number that - combined with the merkle root [27], the previous' block hash and the rest of the block header - results in a pre-defined hash format with certain restrictions. At the same time, blocks can only be added to the longest valid chain (with the most proof-of work invested), to avoid 'dishonest' attempts of altering the blockchain ledger.

Proof-of-Stake (PoS) is another method for verifying and adding blocks to the blockchain. Instead of having a race to complete the next block the fastest, as in the case of PoW, the node that creates the next block is chosen [2]. The selection is based on a series of factors defined by the stakeholders. It is correlated to how much stake one has in the system and how long one has been a member of the system. Therefore, a node adds and verifies blocks according to how much stake they have in the system. Thereby, ownership will lead to actors behaving honestly, otherwise they would lose their stake, if they behave dishonestly. There are other anchoring schemes such as *proof of activity*, *proof of publication* etc. [2] to achieve consensus in the blockchain, but we skip their description due to space limitations.

C. Cryptographic Primitives

Hash Functions: The concept of hashing is used to ensure integrity of data. A hash function is an input independent average linear time algorithm that takes set of variables or data and transforms it into a fixed size hash digest [28]. A successful hash function has the following characteristics: *deterministic* - the same input always creates the same output, *efficient* - output is computed in a timely manner, *distributed* - evenly spread across the output range, meaning that similar data should not correlate to similar hashes, *preimage-resistance* - it needs to be infeasible to find the input x, based on the hash value ($h(x)$) and almost *collision resistance* - in general, no two different inputs x and y, create the same hash $h(x) = h(y) \implies x \equiv y$. The hash functions map any input string to a short fix-sized output string, so there will be a possibility of collisions between the hash values of two different input values in rare cases. However, the collision resistance property makes sure that it is hard to find if $x \neq y$ so that h(x) = h(y).

Digital Signatures: One of the main goals of blockchain technology is to able to verify authenticity and non-repudiation of data/transactions. Digital signature is a cryptographic scheme that guarantees two properties: *authenticity*, that the data/message created or owned by the known sender and the *non-repudiation* property guarantees that the data is not altered, using a pair of keys with an asymmetric cryptographic algorithm like RSA [29]. More secure versions of digital signatures such as Elliptic Curve Digital Signature Algorithm are used in the current blockchains.

D. How a blockchain works

The clients through which the blockchain users interact with the blockchain are normally known as nodes and each node can act as an entry point for many blockchain users. In general, each node will maintain it's own copy of blockchain and updates it's own copy via transactions, and thereby it maintains a copy of blockchain which is identical to the copies at the other nodes, at least until the last time when consensus among the nodes were reached.

Users who interact with blockchain will create a pair of keys (public and private) using asymmetric cryptography [29], where the private key will be used to sign their own transactions and the corresponding public key is normally used as an address on the network [1]. The advantage of using asymmetric cryptography is that brings in the guarantees of

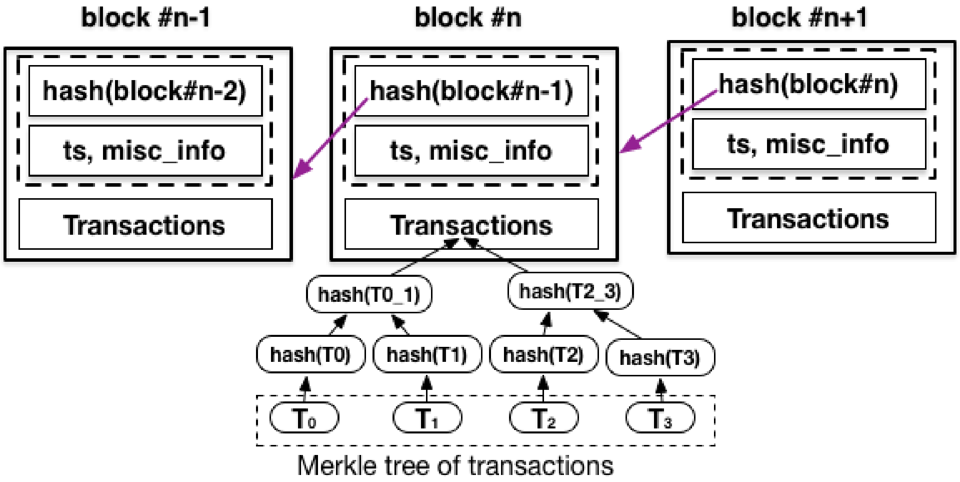

Fig. 1. Structure of a block in blockchain

authentication, integrity, and non-repudiation over the transactions. Every node broadcasts its respective user's signed transactions into the network by using one-hop peer i.e. to the adjacent peer.

Hash functions are extensively used in blockchain for integrity of data/transactions and for organising & linking data/transactions with blocks. The linking is done through the hashing of various elements in the block header containing hash of previous block, timestamp, and some miscellaneous information e.g. a nonce as shown in fig. 1. Each transaction is hashed, then the resulting hash of each transaction is hashed to build a tree structure until top node known as the Merkle root [27] is obtained. This type of organising of data allows secure and efficient verification of the contents of the blocks and also to summarise all the transactions in a block. Moreover the adjacent peers will make sure that the incoming transaction is valid, otherwise they will discard the invalid transaction. With this approach, valid transactions will only be propagated to the entire network eventually, while a invalid transaction will be dropped at the first hop peer. Moreover, valid transactions are collected, validated, ordered and packaged into a block during an agreed upon time interval, and properly linked to the hash value of the previously validated latest block (as shown in fig. 1) to form longest valid chain, which is known as *mining*. The mining node will broadcasts the newly formed block into the network and the choice of the node which will do the mining will be decided based on the type of the blockchain and the type of chosen anchoring scheme (sec. IV-B). Finally when the new block is arrived at a node, the node will verify whether the block contains valid transactions and also checks whether the new block is correctly linked using hash pointer to the previous block in the chain (fig. 1). If the block is validated correctly, then only it will be added to the local copy of the blockchain at the node. Using the above-described phenomenon the blockchain achieves the characteristics shown in Tab. II.

Immutability	Data once written to the chain cannot be changed or deleted without consensus
Decentralization	No single point of failure/control achieved by decentralised & distributed architecture
Transparency	All data sent through the blockchain is visible to all network participants
Pseudonymity	The identity of data senders and receivers is unknown
Chronology	Every transaction is time-stamped and can be traced back

TABLE II
CHARACTERISTICS OF THE BLOCKCHAIN

Based on the accessibility of blockchain, it can be broadly categorised as private and public. In case of public blockchain (permission-less network) anyone can join the network (e.g. bitcoin cryptocurrency), where as in case of private blockchains (or permissioned network), access is restricted to few users only [1]. Some blockchain platforms such as MultiChain [30] offers fine grained permissions such as connect (to see the contents of the chain), send (to transact), issue (to create new assets) etc.

V. Conceptual Design: Blockchain for Microfinance

Our motivation for this section is to take a simple social business use-case scenario (microfinance) and come up with a conceptual design using blockchain technology and use this as a basis for discussion about opportunities and challenges. We take the example of a Community Development Fund (CDF) operated by a SB organisation in Northern India, which is an autonomous micro-credit based community development program to promote economic empowerment of poor people through self-help employment and income generation by creating women entrepreneurs in the Indian villages. CDF comprises of many self-help groups (SHG) and one member from each SHG takes part in CDF to take the project autonomously forward. SB organisation provides/facilitates 0% interest loan

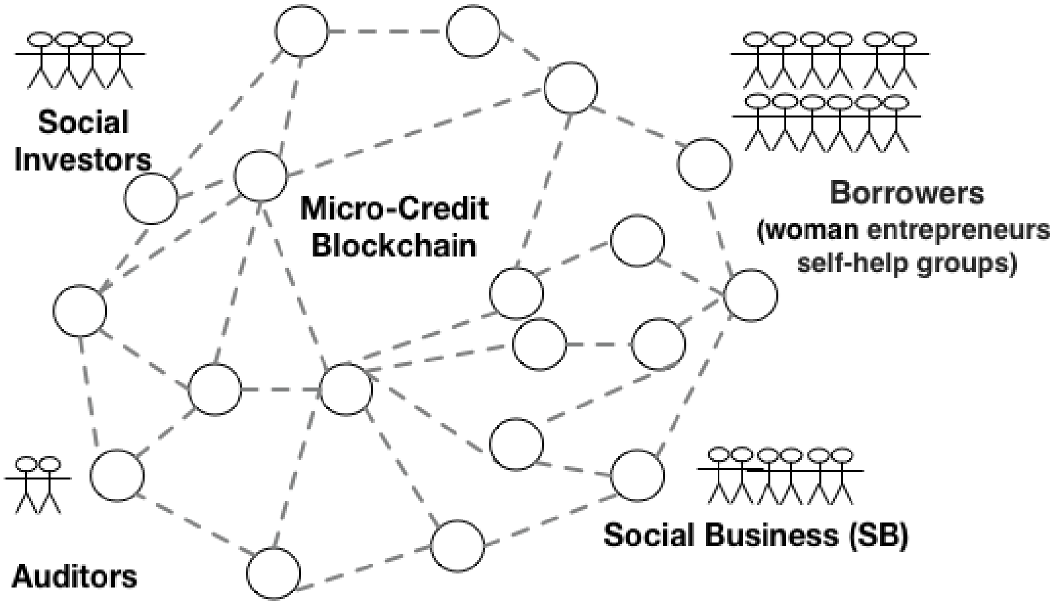

Fig. 2. System Architecture for BPDIMS

to SHG members after collecting funds from social investors, who are interested in lending their money for up-liftment of underprivileged people. As shown in fig. 2, the following are the main stakeholders involved in the Microfinance blockchain case study.

- Investors: Social investors who invest their money at 0% interest rate
- SB: SB organisation that selects women borrowers who need money for their small business
- Borrowers: Women from SHG, looking for loans of INR 10000-20000 ($150-300) for an year or so.
- Auditors: external people/entities/investors auditing the operations of CDF

The borrowers in the case study are screened and selected by the SB organisation for the lending money from investors. A social investor will lend money to the borrowers at 0% interest rate and after certain amount of time (e.g. 1 year), the borrower will repay the loan. SB organisation works at the grassroots level, on one hand to makes sure that the loans are going to the deserved women entrepreneurs and on the other hand approaches social investors for money to the loans.

A. *Conceptual Design*

To model the case study, we will use MultiChain [31], which is a open-source platform for building private blockchains. We have chosen to model micro-credit blockchain as a private blockchain (with public visibility) due to two main reasons: 1) to have control over who can perform a transaction (e.g. who can borrow) and which type of transactions are permitted 2) to have a simple and inexpensive mining scheme instead of having an expensive mining scheme like proof of work (e.g. bitcoin). Moreover, if the blockchain is private, problems related to its scalability such as block size, mining complexity etc. can be easily controlled and the blockchain will only contain respective interested transactions. Similar to public blockchains (e.g. cryptocurrencies), we assume that the user identity is managed by public-key cryptography, where each user will generate a pair of keys, keeping the private key as secret to themselves and using public key as an identity/address to send and receive assets/messages in the network. We also assume that digital *assets* are like cryptocurrencies and when once an asset is sent to a public key, then the asset can be spent using the corresponding private key, in the sense that access to private key is equivalent to ownership of asset/funds. Moreover, we also abstract away from the details of how assets are converted into funds (e.g. fiat money/currency) and we can assume that this conversion is happening outside the blockchain. In a simplistic scenario, the SB could act as an digital currency exchange, from whom assets can be exchanged with fiat currencies and also vice versa. Multichain offers different permissions [2] that can be granted on the addresses in blockchain and we assign permissions to different stakeholders as shown in tab. III. Even though the blockchain is private with restricted permissions, by default it has the public accessibility i.e.any one (including all stakeholders) can connect to it and verify the contents of it.

B. *Modelling the Use Case of Borrowing in Blockchain*

Using the primitives of Multichain, we will explain the Microfinance use-case esp. a borrower borrowing asset/funds from social investors. Multichain offers *transactions* for transfer of assets between different parties and it also offers *data streams* as an immutable (append-only) key-value pair timestamped database for facilitating message communication or data transfer.

[2] https://www.multichain.com/developers/permissions-management/

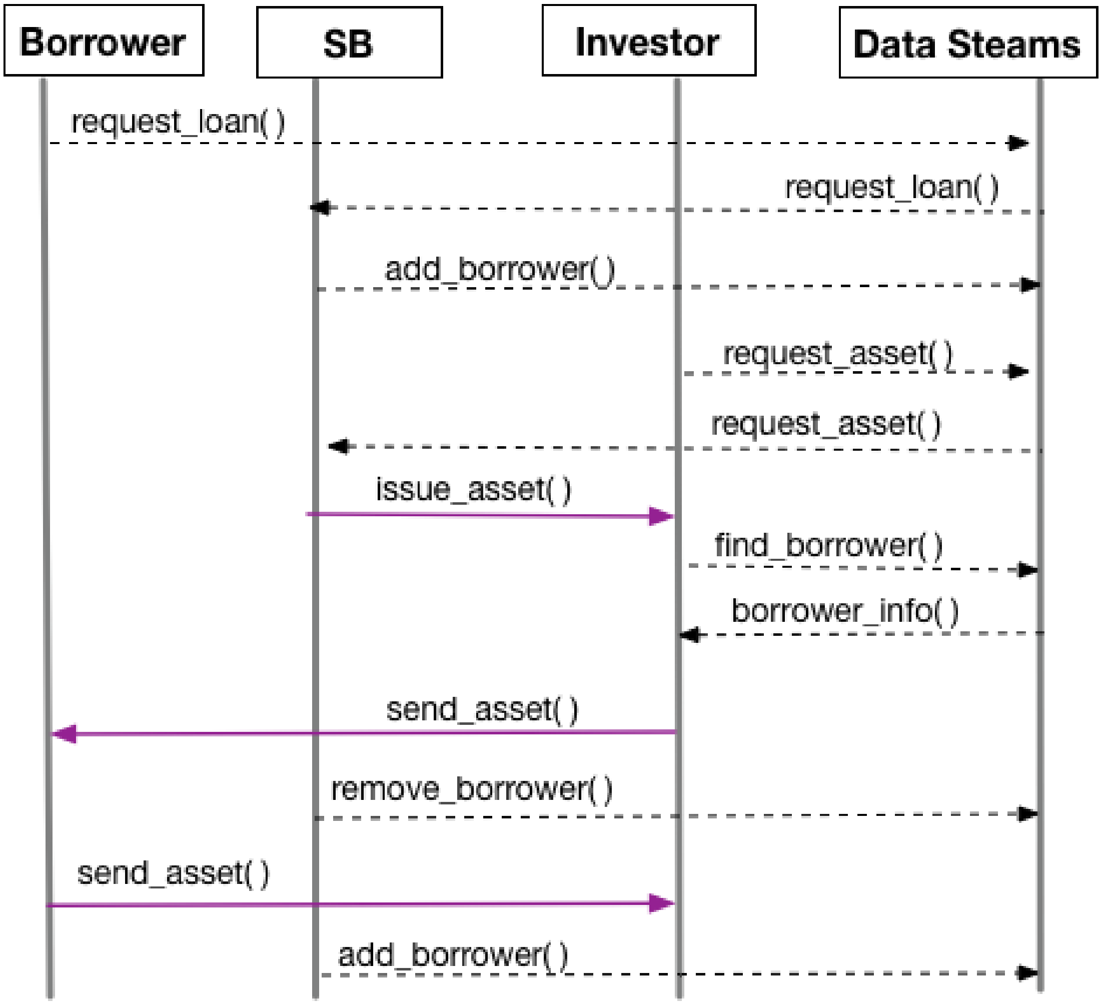

Fig. 3. Sequence of Steps in Borrowing Use-case

Users	Permissions	details
Investor, borrower	send, receive	to send and receive assets.
SB	admin, issue, send, receive, mine	grant permissions to users, issue assets, mine blocks etc.
auditors, public	connect, mine	connect to see blockchain's contents, mine (verify transactions, create new blocks)

TABLE III
STAKEHOLDERS' PERMISSION IN BLOCKCHAIN

Let us assume that n, b, i represents SB (e.g. NGO), borrower, and an investor respectively in the blockchain and let $(p_n \mid s_n)$, $(p_b \mid s_b)$, $(p_i \mid s_i)$ be their (public | private) keys respectively. We also assume the existence of appropriate data streams to publish requests/store data such as *borrowers_list*, *loan_requests*, *asset_requests* etc with suitable APIs to query and publish messages. The abstract description of sequence of steps/transactions in borrowing use-case is shown in fig. 3. The solid lines marked with purple colour are Multichain transactions and dotted lines represents non-transactional message communication or data transfer to the data streams.

• Borrower requesting loan
First, borrower will send a message using his private key (s_b) to the data stream *loan_requests*, and it will be received by the SB due to his subscription to the stream. It will be using the Multichain's *sendwithdata* API command as follows,

$$sendwithdata(p_n, -, obj)$$

where $obj = \{"for" : loan\_requests, "amount" : 5000, "key" : p_b, \ldots\}$ contains information about the stream details, and other meta information such as requested loan amount, information about the borrower such as public key etc. The SB will make suitable verification checks both on and off the blockchain (such as whether the borrower is a defaulter or does she fulfils the criteria etc. Then the borrower will be added to the *borrowers_list* where the borrower's public key (p_b) will be published.

• Investor obtaining an asset

A social investor who wants to fund the loans will first send a message to the data stream *asset_requests*, as the investor needs digital assets (like cryptocurrency) to lend/transfer to the borrowers. We assume that the investor paid/transferred the necessary funds, equivalent to digital asset to SB, which had happened outside of the blockchain before the issue of asset. After getting the message from the stream, the SB will perform *issue_asset()* transaction to issue digital asset to the investor using the following api command.

$$issue(p_i, asset_i, 10000)$$

where $asset_i, 10000$ are the name and quantity of the asset. Note that this is a transaction signed by the SB with his private key (s_n) to issue the digital asset to investor's public key (p_i), so that the investor can use his private key to transfer the asset to the borrowers.

- **Finding a borrower and transfer asset**

The investor will query the data stream *borrowers_list* to find a desired borrower and if the desired borrower is listed in the *borrowers_list*, then the investor will get his public key/address of the borrower (p_b) in return. Then investor can perform *send_asset()* transaction using his private key s_i as follows.

$$sendasset(p_b, asset_i, 5000)$$

Please note that since asset is transformed to address of the borrower (p_b), it guarantees that only the borrower can consume this asset using the respective private key (s_b). Simultaneously, the borrower will be removed from the *borrowers_list* until she had paid the loan.

- **Borrower repayment of loan to investor**

After certain amount of time, when borrower wants to repay the loan, then she can request the SB for the issue of an asset equivalent to the value of loan for example by repaying the dues to SB outside the blockchain. When the borrower receives the asset, she can then transfer to investor in the similar manner as explained previously and now the borrower can be again added to *borrowers_list* when she makes a request for a new loan.

C. Choice of Mining in the Blockchain

As the blockchain is private with restricted permissions, the nodes (decided by admin) who have the permission to *mine* will handle the processing of transactions and creating new blocks etc. The cost of mining is negligible in private blockchain as very little computing resources are needed and also there is no gold rush like in case of bitcoin and other cryptocurrencies. Therefore the miners in the proposed blockchain need not be paid any compensation for blocks or transaction fees. As explained in sec. III, SB (esp. NGOs) receives professional and infrastructure help from volunteers/sponsors, therefore in an idealistic scenario, mining activities can be completely to delegated to external entities such as volunteers/auditors/sponsors, who don't involve in the day-day activities of SB. This kind of arrangement will create high-trust and transparency in blockchain setup which is a key factor for attracting social investors. Alternatively, SB organisation can also setup nodes to handle mining by itself, but that can lead to monopolisation of mining process by the SB, which can compromise the blockchain network especially if the SB has deceptive intentions. In order to avoid such kind of monopolisation of mining process by few nodes, Multichain offers a configuration parameter $mining\ diversity \in \{0, 1\}$, and $mining\ diversity \geq 0.75$ will enforces round-robin schedule among the mining nodes. In blockchains systems with Byzantine fault tolerance algorithm [23] for distributed consensus, n consensus mining nodes can provide protection against local attacks in which the adversary controls at most $\frac{n-1}{3}$ consensus nodes. Therefore, even in the case if the SB needs to handle mining using m of its own nodes, then it should make sure that there are at least $n \geq 3m + 1$ additional mining nodes in the network that are controlled by external entities such as auditors/sponsors etc. If the SB maintains that ratio, then it can safely claim that it can not monopolise the blockchain network under any circumstances.

VI. Opportunities and Challenges of Using Blockchain

Taking the conceptual design from previous section as an example, we will outline how blockchain technology can address some of the challenges faced by the SB as mentioned in sec. III.

A. Opportunities

The following are the advantages that blockchain technology can bring in for SB,

1) **Trust Factors:** Blockchain technology can provide trust mechanisms for SB operations. For example, assets/funds transfer to borrower (public key p_b) in the conceptual design, guarantees that only the borrower (the holder of respective private key s_b) can consume the asset, which is like transferring funds directly to the borrower's bank account. Therefore, each stakeholder is in full control over assets they own by using their private keys and therefore no one else can spend one's assets. Additionally, use of underlying asymmetric cryptography will provide authentication, integrity and non-repudiation of transactions and data into the blockchain network. Altogether, use of blockchain will enable SB to build trust in the system, which is one of the key challenges faced by the SB.
2) **Transparency:** The public visibility of the proposed blockchain (even though it is permissioned) allows any one to connect to the network, download the contents of it and verify them. The transparency is a fundamental aspect that is built into blockahin to achieve verifiability [2], and therefore the fact that anyone can connect and verify will bring a lot of transparency into the operations of SB.
3) **Privacy:** Having great transparency in the system does not necessarily lead to privacy violations. Even though

we have not explicitly modelled how privacy is handled in our conceptual design, we will briefly sketch here how blockchain is good at handling privacy concerns. As explained previously in the design (sec. V-B) stakeholders interact in the network using their (public | private) key pairs only (not with their personal information), which will allow stakeholders (e.g. investors, borrowers) to conceal their identities to the public visibility of blockchain and at the same time they can reveal their identities to required entities or authorities. For example, using his public key an investor can conceal his identity in the network (e.g. from borrowers and public visibility of network), but at the same he can reveal his personal information securely to the SB (e.g. by encrypting his personal information with SB's p_n), so that only SB could be able to access this information (using s_n) to comply with the local regulations. Alternatively, some stakeholders (like SB) may not want to conceal their identity at all, in that case they can use their (public | private) keys from an X509 digital certificate issued by certification authority, which will reveal their public profile to the network.

4) **Decentralisation:** Blockchain is inherently distributed and that provides a few advantages [31]. First of all, control over the ledger or network is distributed across many entities (e.g. mining nodes), so no one (e.g. SB) can monopolise or compromise the network to decide which transactions are valid or confirmed unilaterally. Secondly, it will bring in robustness as failure or malfunctioning of a server will not stop processing of transactions in the network as a whole. Restoring a failure server is easy as the transactional state is replicated over different nodes, the failed server can easily restored by getting a copy from a one-hop peer.
5) **Auditability:** In the proposed design, blockchain is like a digital bookkeeping system, recording all the transactions, messages/data transfer in an immutable timestamped database, which leaves rich opportunities for auditing operations of blockchain. For example, one such audit could be to see whether there is any discrimination or partiality in screening the borrowers or granting loans etc. over a period of time as the auditors can get access to full blockchain entries since its inception. Moreover, auditors can also participate in the mining activities voluntarily as suggested in sec. V-C and in that case auditing can be performed as a continuous process (like monitoring) rather than periodically, which will be helpful in establishing further trust in operations of SB.

B. Challenges

Using blockchain technology for SB will also have certain challenges and some of them are listed as follows.

1) **Cryptocurrency:** In the proposed design, for the sake of simplicity, we have used a digital asset for handling of funds transfer from investors to borrowers. In a much more realistic design, a native cryptocurrency to blockchain (e.g. community-coin) would be more suitable to handle the funds transfer, which will eliminate the need of having SB as an intermediary in the funds transfer from investors to borrowers. Having a native cryptocurrency to blockchain will have challenges related to exchange with Fiat & other cryptocurrencies and also need to deal/comply with lot of financial registrations/regulations. Alternatively, if the blockchain is anchored to an existing cryptocurrency (e.g. bitcoin) then it has to deal with all the uncertainties, volatilities and price fluctuations of that cryptocurrency.
2) **Infrastructure and Deployment:** For implementing blockchain based solution, SB needs to find suitable professional, technical help to develop the solution. Moreover SB needs suitable infrastructure and nodes to run and mine the blockchain. Some of the stakeholders (e.g. borrowers) might not have the access/ability to use computers, but only to the devices like mobile phones. Hence there is also need for developing light-weight clients with mobile interfaces that can run on mobile phones, to interact with blockchain network.
3) **Training and Adoption:** Adopting to new technological developments like blockchain and smart contracts takes time and resources. The stakeholders involved need proper training and orientation to adopt to the new way of interactions in the blockchain. Therefore SBs need to spend their time and resources to train different stakeholders to make them adopt the new technologies.

Building on the discussion on opportunities & challenges and also based on the modelling of Microfinance use-case, we can infer that blockchain technology can provide value by enhancing trust, transparency and auditability in the operations of SB. Moreover, the applicability of blockchain technology can be easily extended to the other activities of SB, e.g. donations/products received from corporates or international aid agencies or the government. In such kind of activities, using blockchain technology can provide digital receipts, help in tracking of supply chain products, auditing and compliance to the regulations. Similarly, a number of related activities around SB can be complemented by using blockchain technologies as it can provide opportunities for add-on services such as promoting business opportunities for women entrepreneurs etc.

VII. Conclusion

In this work, we explored the suitability of blockchain technology in addressing some of the challenges faced by social business organisations. The contribution of our research is two-folds: first, we investigated the suitability of blockchain technology for SB by using semi-formal modelling approach and a conceptual design of microfinance use-case. We found that the use of blockchain technology can help social business in establishing and enhancing the trust relationship with social investors and sponsors. Second, we identified the opportunities that blockchain technology can provide for the domain of social business, especially in terms of transparency, auditability, privacy and decentralisation. Similarly, we also outlined the challenges in implementing a blockchain-based solution that a social presence organisation might need to address in terms of technology adoption, infrastructure, and most importantly on how to deal with financial transactions with a cryptocurrency.

Looking ahead, as part of our future work, we will (a) address the issues & challenges of having a native cryptocurrency or anchoring to an existing cryptocurrency, and (b) employ formal modelling approaches to understand the intricate complexities/complications around the cryptocurrency exchange/anchoring issues to come up with a good solution that will eliminate/remove the role of social business as an intermediary in the financial/monetary transactions. Eliminating SB from the role of intermediary in monetary transactions will lead to high trust in the activities of SB, which will result in attracting more social investors & donors. This will ultimately benefit the socio-economic development of under-privileged communities.

References

[1] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[2] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[3] H. M. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance," *Intelligent Systems in Accounting, Finance and Management*, vol. 25, no. 1, pp. 18–27, 2018.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[5] P. Treleaven, R. G. Brown, and D. Yang, "Blockchain technology in finance," *Computer*, vol. 50, no. 9, pp. 14–17, 2017.

[6] P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, E. Izumchenko, A. Aliper, K. Romantsov, A. Zhebrak, *et al.*, "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *Oncotarget*, vol. 9, no. 5, p. 5665, 2018.

[7] E. Werker and F. Z. Ahmed, "What do nongovernmental organizations do?," *Journal of Economic Perspectives*, vol. 22, no. 2, pp. 73–92, 2008.

[8] F. Glaser, K. Zimmermann, M. Haferkorn, M. Weber, and M. Siering, "Bitcoin-asset or currency? revealing users' hidden intentions," in *Twenty Second European Conference on Information Systems, Tel Aviv*, 2014.

[9] F. Glaser and L. Bezzenberger, "Beyond cryptocurrencies - a taxonomy of decentralized consensus systems," in *Proceedings of the 23rd European Conference on Information Systems (ECIS 2015)*, (Muenster, Germany), 2015.

[10] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, "Blockchain-the gateway to trust-free cryptographic transactions.," in *ECIS*, p. Research-Paper153, 2016.

[11] M. Atzori, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?," *Social Science Research Network Working Paper Series*, Jan. 2016.

[12] M. Risius and K. Spohrer, "A blockchain research framework," *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 385–409, 2017.

[13] S. Aral, C. Dellarocas, and D. Godes, "Introduction to the special issue-social media and business transformation: a framework for research," *Information Systems Research*, vol. 24, no. 1, pp. 3–13, 2013.

[14] H. Hyvärinen, M. Risius, and G. Friis, "A blockchain-based approach towards overcoming financial fraud in public sector services," *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 441–456, 2017.

[15] F. Glaser, "Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis," in *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

[16] B. Notheisen, F. Hawlitschek, and C. Weinhardt, "Breaking down the blockchain hype - towards a blockchain market engineering approach," in *Proceedings of the 25th European Conference on Information Systems (ECIS)*, 2017.

[17] J. B. Cholewa, A. P. Shanmugam, *et al.*, "Trading real-world assets on blockchain - an application of trust-free transaction systems in the market for lemons," *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 425–440, 2017.

[18] K. Naerland, C. Müller-Bloch, R. Beck, and S. Palmund, "Blockchain to rule the waves nascent design principles for reducing risk and uncertainty in decentralized environments," in *Proceedings International Conference on Information Systems (ICIS). 2017*, 2017.

[19] R. Beck, C. Müller-Bloch, and J. L. King, "Governance in the blockchain economy: A framework and research agenda," *Journal Of The Association For Information Systems*, 2018.

[20] R. Beck, "Beyond bitcoin: The rise of blockchain world," *Computer*, vol. 51, no. 2, pp. 54–58, 2018.

[21] G. Salviotti, L. M. De Rossi, and N. Abbatemarco, "A structured framework to assess the business application landscape of blockchain technologies.," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

[22] M. Mahfuz Ashraf, M. A. Razzaque, S.-T. Liaw, P. K. Ray, and M. R. Hasan, "Social business as an entrepreneurship model in emerging economy: Systematic review and case study," *Management Decision*, 2018.

[23] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.

[24] L. Xu, *Highly available distributed storage systems*. PhD thesis, California Institute of Technology, 1999.

[25] Multichain, "Multichain permissions management." https://www.multichain.com/developers/permissions-management/.

[26] A. Back, "Hashcash-a denial of service counter-measure." http://www.hashcash.org/papers/hashcash.pdf, 2002.

[27] R. C. Merkle, "Protocols for public key cryptosystems," in *Security and Privacy, 1980 IEEE Symposium on*, pp. 122–122, IEEE, 1980.

[28] J. Carter and M. N. Wegman, "Universal classes of hash functions," *Journal of Computer and System Sciences*, vol. 18, no. 2, pp. 143 – 154, 1979.

[29] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[30] C. S. Ltd, "multichain: Open platform for building blockchains."

[31] G. Greenspan, "Multichain private blockchain (white paper)." URl: http://www. multichain. com/download/MultiChain-White-Paper. pdf, 2015.