

A Blockchain for Communities

Satish Babu *

Glenn McKnight †

July 2017

First introduced as a backing store for the Bitcoin peer-to-peer currency system, the Blockchain has acquired stature as a decentralized, peer-to-peer platform that has the capability not only to transact securely, but also to execute contracts. This paper outlines the Social Blockchain Platform, a computing platform ‘of Communities, for Communities and by Communities’, from farmers to fishers to consumers. The platform will provide the basic services of (a) recording ‘facts’ such as ownership, prices or production; (b) enabling transactions such as transfer of ownership or payments; (c) executing contracts. Together, these three services are considered sufficient to address the majority of the requirements of most communities. Several use cases—drawn from domains such as IoT, Financial Services, and generic, fact-based data repositories—are presented to provide a clear picture of the requirements of communities. Finally, limitations of the the blockchain platform when applied to community requirements is also discussed.

1 Introduction

Computational platforms based on the blockchain have exhibited explosive growth in the last few years. This is perhaps a testimony to the conceptual robustness of a secure, decentralized platform that permits a range of services. The practical use of the blockchain platform, as implemented by Ethereum and a few others, has shown abundant potential. At the same time, there have been difficulties in areas such as scaling to non-trivial sizes, managing short-term transaction bursts, and difficulties in joining initially (particularly participating as ‘full’ nodes that

require blockchain downloads that exceed 180 GB as of June 2017). However, these are seen as short-term difficulties that will not persist as the blockchain platform matures over time.

2 The Needs of Communities

The blockchain is itself a ‘community’-oriented technology, with the consensus process requiring community approval for on-chain transactions, often through proof-of-work or similar mechanisms. The ‘community’ in this cases refers to the network of nodes that process and store the blockchain.

In this paper, we take a broader view of the meaning of ‘community’, specifically referring to groups of people and/or ‘things’ (as defined in Internet of Things) that have specific requirements from the

*Chair, ISOC India Trivandrum (ISOC-TRV), and Member, IEEE Humanitarian Activities Committee. Email: sb@computer.org

†Member, Board of Trustees, Internet Society. Email: mcknight.glenn@gmail.com

blockchain. Examples communities include farmers, consumers, or milch animals that are computing-enabled through appropriate IoT hardware such as RFID tags and their controllers.

Communities have specific characteristics and needs that set them apart from generic users of the Blockchain. For instance,

1. Communities share common needs that may not exist outside them. For example, farmers may want a permanent record of prices of their produce in different markets, while dairy herd owners may want a record of the health of their animals.
2. Many communities are traditional or transitioning from traditional to modern (particularly in Developing Countries). The concept of “Trust” in communities may depend on a number of factors including origin and convention rather than institutional or individual factors.
3. Some communities are not be advanced users of technology and may have access only to rudimentary technologies (feature phones or entry-level Smartphones, low-bandwidth or intermittent access to the Internet)
4. Communities traditionally depend on intermediaries (“middle-men”) for many kinds of services, particularly financial. While intermediaries may be exploitative in many situations, they may also play valuable roles
5. Communities have different types of informational requirements. For instance, in the globalized world, communities that produce food—in agriculture, fisheries, and a range of related services (animal husbandry, poultry, apiculture etc)—have an important obligation to maintain traceability of a given product. In future, these kinds of requirements are likely to be even more demanding.
6. Communities in many parts of the world are looking for trustworthy information sources as well as repositories, as the general experience in most cases have been negative. Even

Governments—who are the traditional caretakers of communities—are seen not to have trusted repositories historically, particularly *vis-à-vis* land records, accountability/integrity of elected representatives, industrial activities and their externalities (eg., pollution), health records, or financial records.

3 Blockchain Services

While an exhaustive study on the potential community uses of the blockchain has not been conducted, a *prima facie* approach would be to provide for the following services:

1. Storage of ‘facts’: The blockchain should lend itself for the storage of any fact, such as the marks obtained by a student, the identify of a person (such as linking a crypto-identity with a national identity number), or the milk production by a cow on a given date. The main challenge here is that the facts occur off-chain, because of which validation of the facts become a problem. This is partly offset by the fact that this is a community application, and so the internal checks and balances should take care of authenticity of information.
2. Transactions: Transactions could be financial or otherwise (for instance, ownership transfer). For financial transactions, currency (fiat vs digital) would need to be addressed as well.
3. Contracts: A contract execution system will certainly add value to blockchain services. For instance, bankers and farmers may enter into a contract when the former advances a loan to the latter. Again, the currency aspect, as well as the legal aspects (to be considered later) needs to be addressed.

4 Instances of Potential Blockchain Requirements

There have been many broad claims made on the general use of the blockchain for higher community ob-

jectives such as ‘enabling financial services for the unreached’, ‘transforming democracy through a traceable voting system’, or ‘eliminating corruption in Development Governance and the Government’. While these may well be true, there are perhaps smaller, immediate applications of the blockchain that we can start with.

Here are a few specific use cases of the use of blockchain for community purposes:

4.1 Bookkeeping for Savings & Credit

Group-based savings and credit—otherwise called as Microfinance or Microcredit—is a very popular activity in different parts of the developing world. The rules and conventions of savings and lending is dynamic, diverse and often complex, which is at odds with the limited computing, storage and communications facilities available with the communities. It would help if blockchain-based technologies could either supplement traditional book-keeping (perhaps through “triple entry book-keeping”, where a third copy of each transactions is directed to the Blockchain), or supplant the traditional book-keeping completely using blockchains.

4.2 Dairy farmers

For dairy farmers, the following information would be useful if placed on the blockchain:

- Daily milk production of cows
- Health parameters (such as the oestrus cycle)
- Ownership of animals including ownership transfer
- Genealogy, particularly the sire-dam lineage

4.3 Forward Trading in Commodities

In several cases, farmers enter into contracts—in many cases, verbal contracts—with traders for forward trading. Forward trading could often be risky on either side, and may lead to disputes, particularly for verbal contracts. A blockchain-supported system would be useful to smoothen out this trade.

4.4 Food Production

Given the requirements of traceability—place and timestamp of origin as well as that of processing and marketing chain—producers will need to make available the entire flow of a product in order to ensure its compliance with food safety standards and to provide actionable tracking information in times of disease outbreaks such as *Salmonella* or *botulism*.

A blockchain-based traceability mechanism would serve the traceability/tracking requirement very well.

5 Community Blockchain: Other considerations

Community blockchains may not require the full, industry-strength, heavyweight implementations such as Ethereum. Additional considerations include the availability of mobile and lightweight wallets, preferential confirmation times (slower confirmation may be fine for fact storage, whereas transactions may need faster confirmation times) and proof-of-stake consensus instead of proof-of-work. However, these are all parameters that need fine-tuning based on trials.

6 Limitations that require further work

Blockchain technology, in its current state, is likely to encounter difficulties on some aspects. These include:

1. Interfacing with legal systems: At the very least, blockchain information needs to be accepted by the legal system as evidence in case of disputes (for instance ownership transfer or transactions). It would be even better if the legal system could enforce blockchain-based contracts. The topic is outside the scope of this paper, but it is likely that with some advocacy efforts, the legal system may be able to consider at least limited acceptance of evidence on the blockchain.
2. Identity-related issues: Personal identities are established in different ways in different places.

In India, we have Aadhar number, PAN number, passport (note: the passport number changes each time a new passport is issued), ration cards, and voter ID. There has to be some mechanism to link one or more of these with any given pseudo-anonymous crypto-id.

3. Information authenticity issues: For off-chain information that gets put online, there is the question of validation. If the data is not validated, we end up in a situation where incorrect data is stored on an immutable medium, with no easy way to invalidate it. Off-chain data validation (ie., how much milk did the cow really produce, and what was reported?) has to be explicitly made the responsibility of the institution/community that owns the blockchain.
4. Currency-related issues: There has to be an easy and “trustless” (ie., using only cryptographic identities and not the elaborate paper identification instruments) way to enable transactions, but interfacing with fiat currency is a challenge given floating currencies. Alternatively, contracts may be constructed based on fiat currency, in which case a new problem arises: who will bear the risk of cryptocurrency’s fluctuating exchange rate? At this time, it is not clear if a cryptocurrency can be pegged to a fiat currency or if a fiat currency can be digitized into a cryptocurrency.
5. Institutional mechanisms: This is a structural matter. It is assumed that in each case of a blockchain platform, there is a community that

owns or promotes it. For example, a group of farmers’ organizations may collectively create a blockchain platform for their transactions. This ownership is important for multiple reasons such as data validation, long-term stakeholding, coverage of costs, legal aspects (especially interfacing with the legal system), and routine administration/maintenance.

7 Implementation

Preliminary work on a proof-of-concept implementation on one of the existing blockchain platforms has been initiated. There are both on-chain and off-chain challenges in the reference implementation. These include Identification for humans and non-human entities (should we adopt the Government ID? In some cases the poorest of the poor are excluded from the Government ID systems...how do we handle these case?), the issue of interfacing with fiat currency, and achieving critical mass in terms of numbers, to name a few.

8 Conclusions

The blockchain provides a powerful platform that can be utilized by decentralized communities to effectively manage multiple financial and non-financial information. While there are several challenges still to be resolved, the potential of the platform is clear. A pilot implementation may be able to resolve the challenges and fine-tune the parameters of the system.