

BBc Trust

— The Charter of Beyond Blockchain —

Kenji Saito and Takeshi Kubo
{ks91|t-kubo}@beyond-blockchain.org

October 31, 2017

0. Glossary

Actor	An entity that can sign transactions digitally.
Asset	A digitally represented record.
Commit	To make an irreversible entry of a transaction.
Data	Transactions and assets.
Ledger	A distributed system to store and process transactions.
Transaction	An event to change the state of an asset.
Storage	A distributed system to store assets.
User	A participant, possibly consisting of a group of actors.

1 Introduction

1.1 Objective

This document, “BBc Trust”, is a charter of Beyond Blockchain. It defines what users can trust about Beyond Blockchain products including BBc-1 (Beyond Blockchain One).

1.2 Overview of Blockchains

In general, a blockchain or related distributed ledger technology tries to realize the following within a defined set of users. In the case of an open public ledger, the set of users is the general public.

1. It maintains records so that their content and their existence cannot be denied by anyone.
 - The records can be automatically updated if and only if a legitimate user or users instructs so.
2. It assures that anyone can verify that.

3. It assures that no one can stop the above.

It can be abstracted as three layers of functions, each providing a type of correctness of transactions. Those layers are, ordered from the lowest, 1) guarantee of validity, 2) proof of existence, and 3) consensus on uniqueness. The layers are described in detail in later sections, as Beyond Blockchain also provides the corresponding functions.

Above these layers, a facility is often provided to describe rules (smart contracts) based on which validity of transactions is verified.

2 What Beyond Blockchain is Not

2.1 It is Not a Database

Beyond Blockchain does not guarantee that data is stored. It stores data in a best-effort basis, and it does not set either the minimal or maximal degree of certainties of data being stored.

If data is stored, the correctness of transactions described in the later sections is guaranteed, as long as cryptographic techniques being used are not compromised. At the same time, Beyond Blockchain provides facilities to upgrade cryptographic techniques being used.

2.2 It is Not a Blockchain

Beyond Blockchain does not realize a ledger as a chain of blocks locked with proofs of work. It is designed to avoid the following drawbacks of blockchains:

1. Lack of synchrony with real-time processes
2. Lack of confidentiality (although efforts have been made in recent developments of blockchains)
3. Oneness (all transactions are replicated to all fully capable nodes) as the fundamental cause of the following:
 - Lack of partition tolerance,
 - Lack of scalability, and
 - Lack of updatability.
4. Incentive Incompatibility that allows all applications to stop when all maintainers of the data leave as a result of the market value of the system's native currency tokens falling.

2.3 It is Not a Replication System

Beyond Blockchain is not primarily aiming for achieving fault-tolerance in existing services. It is not based on replication techniques such as state machine replication, where all transactions must have deterministic effects and must be totally ordered in the same way across the replicated servers.

This also means that Beyond Blockchain is not primarily a consensus system. In particular, Beyond Blockchain does not try to solve CUP (Consensus with Unknown Participants), which we believe is impossible.

3 Correctness : Guarantee of Validity

Beyond Blockchain, by design¹, guarantees the following:

- A transaction is immutable once committed.
- It is valid and consistent with the history of past transactions regarding the asset or assets.
- Only a legitimate user or users can commit a new transaction.
- No one can stop a legitimate user or users to do so.

4 Correctness : Proof of Existence

Beyond Blockchain provides proofs as the below:

- No one can delete an evidence of a past transaction.
- No one can create an evidence of a transaction that did not exist in the past.

5 Correctness : Consensus on Uniqueness

Users of Beyond Blockchain agree on the following:

- If two contradicting transactions are committed, both must be valid.
- To prevent damages from such an event actually taking place, the legitimate user or users responsible for the assets in question can select which transactions to commit.

¹Readers are reminded that an open source software is provided on an “as is” basis, without warranties or conditions of any kind.

- Beyond Blockchain provides some consensus mechanisms where such users consist of multiple replicated actors (which should often be the case because some level of fault tolerance would be required).

This is different from what blockchains provide, i.e., if there are two contradicting transactions, eventually, only the same one of them is observed in the users' views of the correct history.

6 Policies

6.1 Basically Free of charge

No cost should be imposed to the users to use the ledger functionality, to make possibilities of exploring applications of Beyond Blockchain open. Applications may define their own economy.

6.2 Scalable

The system should dynamically scale to meet the required level of traffic.

6.3 Updatable

New technology and techniques can be tested and deployed partially in the network without any permissions.

6.4 Incentive-Compatible

Incentives for new nodes to join and stay should be compatible with the dependability and sustainability of the system and applications.

— End of Document —