GOVERNANCE AND BUSINESS MODELS OF BLOCKCHAIN TECHNOLOGIES AND NETWORKS

TNO innovation for life

AUTHORS
Dr. M. Oskar van Deventer,
Dr. Christopher Brewster,
Dr. Maarten Everts
TNO, June 2017

MANAGEMENT SUMMARY

BLOCKCHAIN TECHNOLOGY HAS ACQUIRED GREAT VISIBILITY IN THE LAST 2-3 YEARS, LARGELY DUE TO THE PROMISE OF SIGNIFICANT EFFICIENCY IMPROVEMENTS ("CUTTING OUT THE MIDDLEMAN") IN MANY BUSINESS SECTORS, INCLUDING FINANCE, INDUSTRY, LOGISTICS, ENERGY, HEALTH AND GOVERNMENT. WORLDWIDE, AS WELL AS IN THE NETHERLANDS, SECTORS ARE IDENTIFYING AND DESCRIBING USE CASES, PROOFS-OF-CONCEPT AND PILOTS TO STUDY THE POTENTIAL IMPACT OF BLOCKCHAIN TECHNOLOGIES. THESE ARE POTENTIAL FOUNDATIONS FOR FUTURE BUSINESS ECOSYSTEMS BUILT AROUND BLOCKCHAIN APPLICATIONS AND BLOCKCHAIN INFRASTRUCTURES.

When organisations or consortia are planning to deploy some of their applications or services on a blockchain, they are typically faced with a make-or-buy decision.
– Make: develop and deploy a new blockchain network.
– Buy: join an existing blockchain network that is run by others.
Business models and governance are important factors in this decision. An organisation should only join an existing blockchain network if its governance and business models are acceptable. And they would only develop and deploy their own blockchain network if proper governance and business models are in place.

This report provides an analysis of existing blockchain technologies (so called "fabrics") from the perspective of governance and business models. The purpose of the report is to provide knowledge and inspiration for organisations and consortia faced with the above-mentioned make-or-buy decision. The intended audience of this report are corporate and government organisations that consider offering or coordinating some of their services via blockchain. This report assumes a basic knowledge of blockchain technologies, including terminology like transaction, block, ledger, blockchain, smart contract and consensus.

Disclaimer: This work is based on a desk study by TNO in fall and winter 2016. Blockchain is a fast-moving set of technologies, so the reader is recommended to check the source references for the technology details.

1. TABLE OF CONTENTS

2. INTRODUCTION

Blockchain technology has acquired great visibility in the last 2-3 years, largely by promising significant efficiency improvements ("cutting out the middleman") in many business sectors, including finance, industry, logistics, energy, health and government. Numerous reports have been written by the major consulting companies about this technology[1,2] and there has been an explosion of venture capital investment. Currently over 1200 start-ups can be identified in this space apart from over 200 major corporations undertaking everything from proof-of-concepts to patent applications[3,4]. Worldwide, as well as in the Netherlands, sectors are identifying use cases, proofs-of-concept and pilots to study the potential impact of blockchain technologies. These are potential seeds for future business ecosystems around blockchain applications and blockchain infrastructures.

On a technical level, a blockchain can be seen as a network of computer nodes (owned by parties that do not necessarily trust one another), each of which
- keeps a copy of a so-called 'ledger' (block-chain), which is basically a database;
- may enable external parties to query and/or append data (transaction records) to the ledger;
- may allow code to be executed on the node, that queries and/or appends data to the ledger; and
- collaborates/communicates with the other nodes to ensure that the contents of their ledger corresponds with the contents of the ledgers of all other nodes.

Thus, the nodes must collaborate with one another and continuously agree on changes to be made and distributed across the nodes.

When organisations or consortia are planning to deploy some of their applications or services on a blockchain, they are faced with a make-or-buy decision.
- Make: develop and deploy a new blockchain network, i.e. become both blockchain application provider and blockchain service provider for the own blockchain application(s)
- Buy: join an existing blockchain network that is run by others, i.e. become only blockchain application provider and leave the running of the blockchain network to others.

1 *http://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf*

2 *https://www-935.ibm.com/services/us/gbs/thoughtleadership/blockchain/*

3 *https://www.blockchainangels.eu/startups/charts*

4 *https://outlierventures.io/corporate-blockchain/browse*

5 *http://ieeexplore.ieee.org/document/7163021/*

6 *https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review*

Business models and governance are important factors in this make-or-buy decision. The economic incentives between the different roles within the blockchain network need to be aligned, which requires proper business models. Maintenance of and changes to the blockchain network layer must be carefully coordinated, which requires proper governance. One would only join an existing blockchain network if its governance processes and business models are sufficiently trustworthy and realistic. And one would only develop and deploy an own blockchain network if proper governance and business models can be developed.

This report provides an analysis of existing blockchain initiatives from the perspective of governance and business models. The purpose of the report is to provide knowledge and inspiration for organisations and consortia that are faced with the above-mentioned make-or-buy decision.

The report assumes a basic knowledge of blockchain technology, including terminology like transaction, block, ledger, blockchain, smart contract and consensus. Recommended reading on this topic[5,6].

The report is structured as follows. Section 3 provides brief descriptions of a selection of blockchain technologies and networks, and the governance and business models are analysed for each technology and network. Section 4 provides a summary table of the essential aspects of governance and business models for the different blockchain technologies and networks. Section 5 provides the main conclusions.

FACED WITH A MAKE-OR-BUY DECISION

3. BLOCKCHAIN BUSINESS ECOSYSTEMS

THIS CHAPTER STUDIES A NUMBER OF BLOCKCHAIN TECHNOLOGIES AND ASSOCIATED BLOCKCHAIN NETWORKS THAT HAVE OBTAINED SIGNIFICANT PUBLIC VISIBILITY AND FOLLOWING. WE EXPLORE AND DISCUSS THEIR GENERAL GOAL AND APPROACH, THE GOVERNANCE OF THE BLOCKCHAIN TECHNOLOGY (SOURCE-CODE) DEVELOPMENT, THE GOVERNANCE OF THE ASSOCIATED BLOCKCHAIN NETWORKS, AS WELL AS THEIR UNDERLYING BUSINESS MODELS.

3.1. BITCOIN

GENERAL

Bitcoin is the well-known archetypal blockchain system, invented and started by the anonymous Satoshi Nakamoto[7]. Bitcoin is the combination of a technology, a network and an application for the creation and trading of the bitcoin cryptocurrency.
The system will not be described here in further detail.

The following functional roles can be (at least) distinguished in bitcoin.
- Users: the people that send and receive bitcoin payments, e.g. buyers, sellers and marketplaces
- Full nodes: nodes that validate transactions, and only relay valid transactions to other full nodes
- Miners: nodes that confirm transactions via proof-of-work
- Mining pools: groups of miners that work together to even
- Exchanges: places where people can buy or sell bitcoin for other currency
- Wallet software providers: developers that provide the software through which users can access and control their bitcoin funds
- Wallet service providers: service providers that keep bitcoin balances on behalf of their users

TECHNOLOGY AND NETWORK GOVERNANCE

The governance of bitcoin is through a “benevolent dictatorship”, similar to many open-source projects. Wladimir van der Laan[8] is the current maintainer of the bitcoin core software. Bitcoin Improvement Proposals[9] are typically discussed on the Reddit discussion forum and at other places. Bitcoin miners can vote for (or against) proposals via an informational field in their mined blocks. Proposals are only included into the bitcoin core software if there is community-wide consensus. Up till now, a proposal to improve the transaction speed proved to be highly controversial, and this has resulted in bellicose behaviour (“civil war”) on the part of participants in the discussions, including censorship at Reddit, DDoS attacks and personal threats[10].
Other proposals have been included smoothly without much controversy.
Upgrades to the bitcoin system and most other blockchains come in two flavours[11]. One flavour is where validation rules become more restrictive, which means that upgraded nodes do not validate all blocks that non-upgraded nodes would. An upgrade of this type is called “soft fork”. As long as the upgraded nodes are in the majority the blockchain converges. The other flavour is where validation rules become wider, which means that there are non-upgraded nodes do not validate some blocks that would be validated by upgraded nodes. An upgrade of this type is called a “hard fork”. Hard forks (i.e. non-backward-compatible patches) are persistent until all nodes are upgraded, and can cause a lot of confusion in e.g. wallet software.
So far, there have only been soft-fork upgrades to bitcoin, but hard forks are being anticipated in the future[12].

NETWORK BUSINESS MODEL

The business model for bitcoin miners and mining pools is straightforward. They provide a validation and confirmation service to bitcoin users, and they get rewarded in newly-minted bitcoins and transaction fees. The balance shifts gradually away from newly-minted bitcoins towards more transactions fees, according to the rules originally set by Satoshi Nakamoto. The business model is less clear for the bitcoin core project that maintains the core software. There has been a Bitcoin Foundation that went bankrupt, and there is MIT Media Lab’s Digital Currency Initiative, which funnels “unrestricted gifts” from sponsors[13].

As for the Bitcoin ecosystem as a whole, there is the inconvenient truth that much of Bitcoin’s value comes from illegal transactions (drugs, ransomware, ...), money laundering, tax evasion and storage of often illegally-obtained value.

7 *https://bitcoin.org/bitcoin.pdf*
8 *https://en.bitcoin.it/wiki/Wladimir_van_der_Laan*
9 *https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals*
10 *http://www.theverge.com/2016/2/9/10946072/bitcoin-core-classic-software-block-size-debate*
11 *https://www.weusecoins.com/hard-fork-soft-fork-differences/*
12 *http://www.coindesk.com/preparing-bitcoin-hard-fork*
13 *https://bitcoinmagazine.com/articles/who-funds-bitcoin-core-development-how-the-industry-supports-bitcoin-s-reference-client-1459967859*

3.2. ETHEREUM

GENERAL

Ethereum is a blockchain technology for the execution of "smart contracts". Smart contracts are typically small computer programs that contain business logic (e.g. if-then statements, or loops) to control some Ether funds.
Ether is the cryptocurrency that fuels the Ethereum blockchain. The amount of Ether needed, or actually of its derivative-cryptocurrency "gas", depends on the amount of CPU cycles on the blockchain needed to execute the transaction on the smart contract. In theory, any computable problem could be programmed as a smart contract on Ethereum, as Ethereum is Turing complete[14].
In practice, the main application is the control of Ether funds.

TECHNOLOGY AND NETWORK GOVERNANCE

Ethereum's governance is similar to Bitcoin in that it uses proof-of-work mining to reach consensus (for now—the plan is to eventually switch to proof-of-stake[15]) and a tricameral structure that requires a proposal from developers and approval from users and miners. The work is led by Vitalik Buterin[16], an active leader of the community for important protocol and economic decisions[17].

Buterin's leadership was seen in action during the "DAO Attack"[18]. "The DAO" ("Distributed Autonomous Organisation") was a smart contract deployed by the German company Slock.it. People could fund the smart contract and then vote on proposals how to invest the funded money. After raising over $150 000 000 in a couple of months, a vulnerability was discovered in the code of "The DAO" and a hacker started siphoning off Ether from the smart contract. Buterin stepped in and made the controversial decision to release a new version of Ethereum that would remove "The DAO" from existence and undo all financial transactions related to it. The decision lead to a hard-fork split of Ethereum into two separate blockchains: one with "The DAO" in and one without. A majority of miners and users followed Buterin's decision, and the other ("Ethereum Classic") blockchain quickly dropped in market capitalisation value, without disappearing nevertheless.

NETWORK BUSINESS MODEL

The business model for the Ethereum blockchain(s) is similar as for bitcoin. Miners validate and execute smart-contract transactions for Ethereum users, and they get rewarded in newly-minted ether and "gas" transaction fees. The development of the Ethereum software development is funded from Ether that was "pre-mined" by its developers. As such, Ethereum can be seen as an early example of an "Initial Coin Offering"[19], which is somewhat similar to an IPO (Initial Public Offering), with the crypto-currency Ether action as shares.

3.3. RIPPLE

GENERAL

Ripple[20] is an open-source payment protocol that forms the core of a blockchain-based business ecosystem.
The company Ripple Labs is the primary contributor of code to the consensus verification system behind Ripple. The Ripple system can be used to trade currencies and commodities including USD, EUR, RMB, YEN, gold, airline miles, and bitcoin, circumnavigating the fees and wait times of the traditional correspondent banking system.

TECHNOLOGY AND NETWORK GOVERNANCE

Ripple is a permissioned blockchain in which all participants are identified or identifiable. Each validating node, tracking node and application maintains its list of other nodes that they trust believe are unique, i.e. not (massively) colluding[21]. This approach makes the Ripple network robust against Sybil attacks.

In practice, the governance of the UNLs is work in progress. Ripple Labs provides a default UNL, which seems to be used by most users[22]. In the final scheme, so called "publishers" will publish lists of validators by public key. They will ensure validators accurately report their identity, jurisdiction, type of organization, and so on. Publishers will monitor the validators they publish to ensure they are operating reliably. Since validators must sign every proposal and validation, most types of misconduct will be easily provable.

The governance of changes in the Ripple system is using the Ripple consensus process itself. The amendments system provides a means of introducing new features to the decentralized Ripple consensus network without causing disruptions. An amendment normally requires 80% support for two weeks before it can apply[23]. Also proposals for changing values of fees and reserve requirements are governed by the Ripple consensus process[24].

14 *https://ethereum.stackexchange.com/questions/2464/what-does-it-mean-that-ethereum-is-turing-complete*
15 *https://en.bitcoin.it/wiki/Proof_of_Stake*
16 *https://twitter.com/VitalikButerin*
17 *https://thecontrol.co/the-governance-of-blockchains-5ba17a4f5da6*
18 *https://www.coindesk.com/understanding-dao-hack-journalists/*
19 *http://www.investopedia.com/terms/i/initial-coin-offering-ico.asp*
20 *https://en.wikipedia.org/wiki/Ripple_(payment_protocol)*
21 *https://wiki.ripple.com/Unique_Node_List*
22 *https://en.wikipedia.org/wiki/Ripple_(payment_protocol)*
23 *https://ripple.com/build/amendments/*
24 *https://ripple.com/build/fee-voting/*

NETWORK BUSINESS MODEL

The business model of validating nodes and tracking nodes is not explained in the Ripple documentation. It is made clear that validating nodes are not paid via transaction fees or other fees within the Ripple system. One could assume that the value comes from the use of the Ripple system by the validating-node organisation themselves and their customers.

The business model of Ripple Labs is via the Ripple crypto-currency XRP, which can be considered equity. One hundred billion units of XRP ("Ripple shares") have been created when Ripple got started (bitcoin connoisseurs would call this "pre-mining") and no more will be created as Ripple's architecture does not require mining. XRP serves as a bridge currency in the Ripple system[25]. Moreover, in order to keep the Ripple system stable and spam-free, transaction fees are paid by destroying XRP and each Ripple account is required to hold a minimum XRP reserve to remain active.

Ripple Labs' work on code and amendments is funded by selling XRP. Ripple Labs also invests ("distributes") in business development deals, incentives to liquidity providers who offer tighter spreads for payments, and selling XRP to institutional buyers interested in investing in XRP. Given that Ripple is the third largest cryptocurrency with a market capitalisation of near 300 million US dollar[26], the approach seems successful.

25 https://ripple.com/xrp/

26 https://coinmarketcap.com/currencies/ripple/

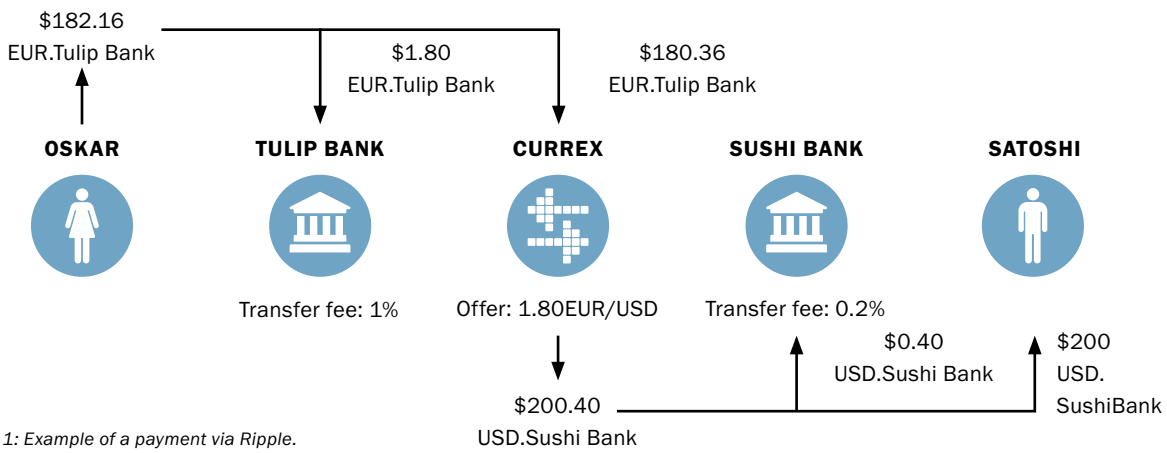

Figure 1: Example of a payment via Ripple.

3.4. HYPERLEDGER

GENERAL

The Hyperledger project[27] describes itself as follows: "The Hyperledger project is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration including leaders in finance, banking, IoT, supply chain, manufacturing and technology".

TECHNOLOGY GOVERNANCE

The Hyperledger project has a clear focus on industry and appears to be fairly formally organised (as opposed to many of the blockchain-related open source projects and startups). Hosted by Linux Foundation, the project has several staff members (8), a Technical Steering Committee (11), and a Governing Board (16). In addition, a wide range of 90+ companies and organisations have become a member of the Hyperledger project. The project is managed under an "open governance model", which is described in their charter[28]. This charter for example describes how there are three types of members (premier, general and associate) and that all premier and general members must be corporate members of the Linux Foundation to participate as a member in the Hyperledger project. Furthermore, the charter describes the different boards and committees that govern the project and the rules that apply. In terms of intellectual property, the charter states all new inbound code contribution shall be made under the Apache License.

Much of the project appears to be done and discussed in the open. For example, there are a number of public meetings of working groups and committees[29]:

- Hyperledger Project Technical Steering Committee
- Requirements Working Group
- Hyperledger Project - Fabric Technical Planning
- Hyperledger Arch Working Group - Biweekly meeting
- Hyperledger Identity Working Group - Biweekly meeting
- Hyperledger Protocol Working Group - Weekly meeting

The project has a number of blockchain-related subprojects under its wings, all still in what Hyperledger calls the incubation stage:

- Fabric
- Iroha
- Sawtooth Lake

These all provide permissioned blockchain implementations.

NETWORK GOVERNANCE

There is no single Hyperledger blockchain network, as the technology is designed to be used in many industry sectors and to have many network instances. The Hyperledger Fabric documentation describes the following roles and types of participants[30]. The process of admitting members and assigning their roles is handled by a (semi-) centralised membership service.

BLOCKCHAIN BUSINESS MODEL

There appears to be no explicit documentation or discussion on the business model for running/participating in a Hyperledger blockchain.

27 *https://www.hyperledger.org/*

28 *https://www.hyperledger.org/about/charter*

29 *https://wiki.hyperledger.org/community/calendar-public-meetings#hyperledger_arch_wg_biweekly_meeting*

30 *https://hyperledger-fabric.readthedocs.io/en/latest/glossary.html*

ROLES	
CHAIN MEMBER	Entities that do not participate in the validation process of a blockchain network, but help to maintain the integrity of a network. Unlike Chain transactors, chain members maintain a local copy of the ledger.
CHAIN TRANSACTOR	Entities that have permission to create transactions and query network data.
CHAIN VALIDATOR	Entities that own a stake of a chain network. Each chain validator has a voice in deciding whether a transaction is valid, therefore chain validators can interrogate all transactions sent to their chain.
CHAIN AUDITOR	Entities with the permission to interrogate transactions.

PARTICIPANTS	
SOLUTION USER	End users are agnostic about the details of chain networks, they typically initiate transactions on a chain network through applications made available by solutions providers. Roles: None
SOLUTION PROVIDER	Organizations that develop mobile and/or browser based applications for end (solution) users to access chain networks. Some application owners may also be network owners. Roles: Chain Transactor
NETWORK PROPRIETOR	Proprietor(s) setup and define the purpose of a chain network. They are the stakeholders of a network. Roles: Chain Transactor, Chain Validator
NETWORK OWNER	Owners are stakeholders of a network that can validate transactions. After a network is first launched, its proprietor (who then becomes an owner) will invite business partners to co-own the network (by assigning them validating nodes). Any new owner added to a network must be approved by its existing owners. Roles: Chain Transactor, Chain Validator
NETWORK MEMBER	Members are participants of a blockchain network that cannot validate transactions but has the right to add users to the network. Roles: Chain Transactor, Chain Member
NETWORK USERS	End users of a network are also solution users. Unlike network owners and members, users do not own nodes. They transact with the network through an entry point offered by a member or an owner node. Roles: Chain Transactor
NETWORK AUDITORS	Individuals or organizations with the permission to interrogate transactions. Roles: Chain Auditor

3.5. BIGCHAINDB

GENERAL

In contrast to Ethereum, Hyperledger or other blockchain projects described in this report, BigChainDB[31] does not build a full stack of Blockchain technologies, but rather offers an overlay onto existing database technologies to "blockchain-ify" them. They started with an initial open source database[32] and have added blockchain characteristics including decentralized control, immutability, and creation and movement of digital assets[33]. The main objective has been to overcome the widely recognised scaling problem that most blockchain projects suffer from. BigChainDB claims to be able to achieve over 1M transactions per second with this approach. The project sees itself as providing a technological component in a more conventional technology stack as shown in the following figure:

TECHNOLOGY GOVERNANCE

BigChainDB is run like many open source projects. The company Ascribe GmbH (now renamed into BigChainDB) initiated the project and its employees lead the project's development. All code is available on Github as well as extensive documentation and discussion boards/bug trackers. There are details provided on how to participate and contribute code and contributors need to sign an agreement. Final decisions on fundamental issues remain with the core BigChainDB team, and as such this does not differ from many company sponsored open source projects.

NETWORK GOVERNANCE

An instance of BigChainDB has to be initiated by a specific individual who then must add nodes to the instance. There is no voting mechanism or other governance structure to control the addition of nodes. In this regard, BigChainDB is obviously intended for a permissioned blockchain environment. Once nodes are up and running, then can vote to validate transactions in accordance with the consensus algorithm.

The consensus algorithm runs on each node and each transaction is assigned to a node for validation randomly, thereby each node having the same probability of receiving a transaction. Only a subset of nodes receive a transaction for validation at any given time. Each node stores a subset of the complete database as is common with modern databases using sharding but essentially all nodes are reading and writing to the same database (and not to their own copy). Nodes can drop in or out of the network without affecting the overall performance of the system.

BigChainDB is in the process of establishing a publicly running instance of BigChainDB, called the "Interplanetary Database" (IPDB), governed by 20 specially selected "caretakers" (private communication with Trent McConaghy, May 2017).

BLOCKCHAIN BUSINESS MODEL

The business model of running a BigChainDB network is similar to any distributed database setup. A single actor (such as a company) or a set of actors (for example a trade association) need to run such a network across their servers and how this gets funded/paid for is entirely extrinsic to the design of the technology.

The "Interplanetary Database" charges transactions fees for the amounts of stored data. The fees represent the net present value of the expected cost for storing the data for ever, taking into account hardware cost, operational cost and interest (private communication with Trent McConaghy, May 2017).

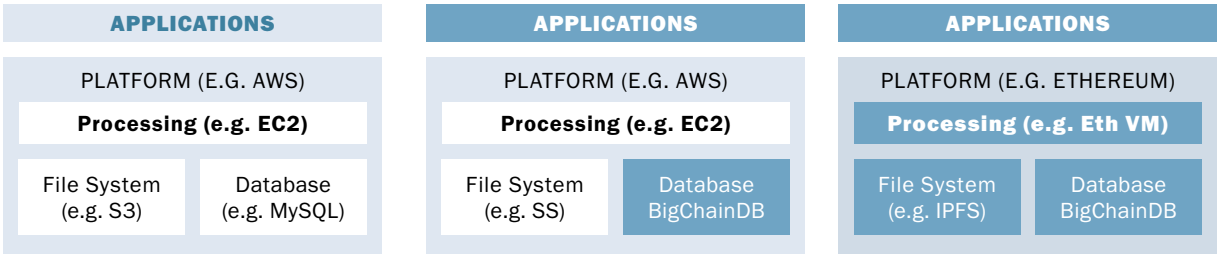

Figure 2: BigChainDB architectures (https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf).

3.6. CORDA

GENERAL

Corda[34] is an open-source distributed ledger platform developed by the R3 consortium[35]. Corda is specialized for use with regulated financial institution; all identities of participating parties are known.

Corda's aim is to provide a platform for companies to agree on collections of shared facts. However, in contrast with many other blockchain approaches, transaction data is not globally broadcast; only those who actually need to have access the transaction can actually access the data (typically the participants and/or regulators). This approach is reflected in the architecture. In a Corda network the following (types of) components can be identified:

- Nodes: participants in the network, provide storage for transactions (typically using a relational database).
- Identity and permissioning service: automates the process of provisioning TLS certificates.
- Network map service: publishes information about nodes on the network.
- Notary services: nodes that provide transaction ordering and timestamping services.
- Oracle services: a network service that is trusted to sign transactions containing statements about the world outside the ledger.

TECHNOLOGY GOVERNANCE

The community discussion about the project takes place at:

- Github[36], in the Issues
- An online forum dedicated to Corda[37]
- A Corda slack channel[38]

As Corda is a project from R3, the governance of R3 has a large influence on the governance of the Corda project itself. According to a blogpost[39], the Steering Committee of the R3 consortium at a certain point established an Architecture Working Group, chaired by Richard Gendal Brown. This working group consisted of hundreds of of senior architects, technologists and developers from the participating financial institutions.

Corda is in the proposal phase to be incorporated under the Hyperledger flag, so eventually the project governance will probably the same as is currently defined for Hyperledger (see also the section on Hyperledger).

NETWORK GOVERNANCE

Corda appears to support a somewhat fluid architecture; there can be multiple networks of notaries and nodes who decide for themselves who they conduct business with.

As Corda is a permissioned ledger, participating requires obtaining an identity signed by a root authority. Although not explicitly stated, this root authority is probably managed by the "Identity and permissioning service". Corda does use standard PKIX infrastructure to connect public keys to identities and "names" in the system are actually X.500 names. This means existing PKI infrastructure could be used to bootstrap identities in a Corda network. The documentation also explicitly states that an identity does not have to be a legal or true identity; a permissioning system can implement any policy it likes as long as the identities are it signs are globally unique.

In the Corda project, so-called Oracles interface the real world with the network; they sign transactions containing statements about the real world. Of course these oracles need to obtain an identity from the identity service, but other than that it is up to the transaction submitters and smart contract authors to decide which oracle to trust.

The Corda project appears to try to keep agility in mind and explicitly think about upgrade paths. For example, for composite signatures they explicitly do not choose for cryptographic threshold schemes but instead use a simpler approach that is a bit less space efficient, but does allow the mixture of different public key cryptography algorithm, which allows old algorithms to be phased out without requiring all participants in a group to upgrade simultaneously. Similarly, signatures and public keys are not specified inside smart contracts, which does not require them to be updated on key changes.

Similarly, Corda allows multiple (distributed) notaries in its network, which also provides some agility. Notaries can for example compete on their availability, performance, and local jurisdictionally aspects. But it can also be used to phase-out and or upgrade notaries by running multiple in parallel. How such processes should or could be governed is not specified further.

NETWORK BUSINESS MODEL

No information.

21 *https://www.bigchaindb.com*
32 *https://www.rethinkdb.com*
33 *https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf*
34 *https://www.corda.net*
35 *https://www.r3.com*
36 *https://github.com/corda/corda*
37 *https://discourse.corda.net*
38 *https://slack.corda.net*
39 *https://www.corda.net/2016/10/r3-corda-makes-different*

3.7. QUORUM

GENERAL

Quorum[40] is an Ethereum-based distributed ledger protocol with transaction/contract privacy and a new consensus mechanism. It is created by JP Morgan, a large financial institution from the United States. Quorum is based on Ethereum and the source code includes a minimalistic fork of the Go Ethereum client. What quorum adds w.r.t. Ethereum is transaction and contract privacy[41], a voting-based consensus mechanism, network/peer permissions management and higher performance.

TECHNOLOGY GOVERNANCE

No information.

NETWORK GOVERNANCE

Quorum aims to have a pluggable consensus mechanism, but the initial consensus scheme provided is a time-based majority voting algorithm dubbed QuorumChain. In this consensus scheme there are three types of nodes:

- Maker nodes are responsible for making blocks.
- Voter nodes are responsible for voting on the validity of blocks and placing them onto the blockchain.
- Observer nodes are all other nodes; they simply receive and validate (new) blocks.

The governance of this consensus process is controlled by a smart contract running on top of the system[42].
The special smart contract called BlockVoting has lists of public keys of valid Maker and Voter nodes. Special functions can be called to add or remove Makers and Voter, and to change the number of votes needed for consensus. The initial set of makers and voters is defined in the genesis block description. Each node maintains a list of (public keys of) nodes that it is allowed to connect to and communicate with.

NETWORK BUSINESS MODEL

No information.

40 *https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum%20Whitepaper%20v0.1.pdf*

41 *https://github.com/jpmorganchase/quorum/wiki/Quorum-Overview*

42 *https://github.com/jpmorganchase/quorum/wiki*

43 *https://www.tezos.com/static/papers/position_paper.pdf*

44 *https://www.tezos.com/static/papers/white_paper.pdf*

3.8. TEZOS

GENERAL

Tezos[43] is a blockchain project that distinguishes itself from other project by claiming they are “the first and only blockchain implementation operating with decentralized governance”. While the project does not advertise itself as a permissioned blockchain, the decentralized governance aspect makes it interesting for further study in this document. An important distinguishing feature of Tezos is that the project explicitly takes on the challenge of governance of protocols in blockchains. Their approach is to look at blockchains in an abstract fashion and basically enforcing protocol changes/upgrades onto the ledger itself.

In the Tezos whitepaper[44] they distinguish three different “protocols”:

- The network protocol: discovers blocks and broadcasts transactions
- The transaction protocol: specifies what makes a transaction valid.
- The consensus protocol: forms consensus around a unique chain.

Although any consensus mechanism could be used in Tezos, the project itself has a strong preference for a proof-of-stake approach.

TECHNOLOGY AND NETWORK GOVERNANCE

The project started in 2014. The Tezos website indicates the number of people for the team, two companies as partners, and two advisors. It is unclear how the funding of the project is realised. Twitter messages and online news articles hint towards the sale of “Tezos coins”.

The Tezos project prides itself in supporting decentralized governance. This is implemented by starting with an initial protocol and using the distributed ledger itself to agree on the next version of the protocol. Specifically, for the seed protocol, the Tezos documentation states that amendments to the “blockchain protocol” are adopted in predetermined election cycles (the length of which can of course be changed through amendments). This process is divided into four steps:

- First quarter: Protocol amendments are suggested through the submission of a hash of a tarball containing the source code (currently in OCaml) that represent the new protocol. Stakeholders can vote on/approve any number of protocols.
- Second quarter: The amendments are voted upon. The options for stakeholders are: vote for, vote against, or abstain. Abstentions count towards the quorum.
- Third quarter: If 80% of the stakeholders agree, the amendment is approved and used to replace the currently running test protocol.
- Fourth quarter: If an amendment passes the third quarter successfully it runs for a while in the testnet. The stakeholders then vote a second time whether the

test protocol running on testnet should be promoted to the main protocol.

NETWORK BUSINESS MODEL

No information.

3.9. MULTICHAIN

GENERAL

MultiChain[45] calls itself an "open source private blockchain platform". It is indeed a platform for private, permissioned blockchains aimed at financial transactions (both currency and assets). MultiChain is based on Bitcoin Core, the reference software for the bitcoin network, and tries to remain compatible with bitcoin's protocol as much as possible, but without using its PoW consensus scheme.

TECHNOLOGY GOVERNANCE

Although MultiChain calls itself an "open source platform", the main website does not refer to a source code repository. Their developer page[46] states that source code will be available in the beta phase (currently still alpha) under a GPL3 license, but that commercial licenses will be available.
So development does not happen in the open.

NETWORK GOVERNANCEE

In MultiChain public key cryptography is also used (besides signature on transactions) to control the permissions in the systeM[47]. Types of permissions and privileges include:

- Permission to connect to a node
- Permission to send and/or receive transactions
- Permission to confirm transactions ("mining")
- Permission to manage the permissions/privileges of other users

Any changes in permissions (i.e., granting and revoking) are submitted to the network in special transactions containing metadata. Changing administrator or mining privileges requires additional action: a minimum (unspecified) proportion of the administrators must vote to make a change. The miner of the "genesis" block is the initial administrator when a blockchain is initiated. Any further changes in permissions are managed "on the chain", although there are some additional rules to make sure these permission changes do not influence the transactions ordering and consensus.

NETWORK BUSINESS MODEL

In a MultiChain blockchain, transaction fees and block rewards are zero by default. Costs might be recovered through for example annual service fees, and could be paid through traditional off-blockchain means. MultiChain can however be configured to have block rewards that return the chain's native currency

45 *https://www.multichain.com*
46 *https://www.multichain.com/developers*
47 *https://www.multichain.com/download/MultiChain-White-Paper.pdf*

4. SUMMARY TABLES

TECHNOLOGY	GOVERNANCE	
	TECHNOLOGY	NETWORK
BITCOIN	Benevolent dictator, community process, voting via mining	
ETHEREUM	Benevolent dictator, community process, voting via mining	
RIPPLE	Ripple labs foundation, voting via Ripple consensus mechanism	
HYPERLEDGER FABRIC	Consortium agreement, formal management structure	No information, may differ per instance
BIGCHAINDB	BigchainDB company	20 caretakers of the BigchainDB-based Interplanetary Database
CORDA	Consortium agreement, central identity and permissioning service	
QUORUM	No information	Via a smart contract running on the system
TEZOS	No information	Decentralized governance with election cycles
MULTICHAIN	No information	Voting by administrators

TECHNOLOGY	BUSINESS MODEL	
	TECHNOLOGY	NETWORK
BITCOIN	Foundation, donations	New bitcoins, transaction fees per stored kB
ETHEREUM	Pre-mined ether	New ether, transaction fees per used CPU cycles
RIPPLE	Pre-mined XRP Back-end integration	No information, unclear
HYPERLEDGER FABRIC	Company sponsored	No information, may be different per instance
BIGCHAINDB	Company sponsored	Transaction fees per stored GB
CORDA	R3 consortium project	No information
QUORUM	No information	No information
TEZOS	Sale of Tezos coins?	No information
MULTICHAIN	No information	Off-blockchain service fees

Given the above analytical framework, any organisation seeking to use blockchain technology should assess the governance requirements (both in the short and long term) of their use case, as well as the business models, so as to identify the most suitable technology (or set of technologies) and to make an informed decision to join an existing blockchain network or initiate a new one.

5. CONCLUSIONS

When organisations or consortia are faced with a make-or-buy decision for the blockchain network on which they will run their applications, they first need to establish trust and confidence in the selected open-source blockchain technology. Important factors in this are the governance of the project that creates the source code of the blockchain technology and the associated business models. Moreover, a "buy" decision to select a specific blockchain network to run the blockchain requires trust and confidence in the governance and business model of the selected blockchain network. And a "make" decision to initiate an own blockchain network instance (based on existing open-source blockchain technology) requires the development of own governance solutions and business model, which may be inspired by existing blockchain networks. This report provides some insights in governance and business models of blockchain projects and networks, which may aid the above-mentioned make-or-buy decision.

There is a wide variety of blockchain technologies. Some are monolithic (Bitcoin, Ripple), other are highly modular (Hyperledger). Some are unpermissioned (Bitcoin, Ethereum), other are permissioned (Ripple, Hyperledger). Some are single-purpose (Bitcoin, Ripple, Corda), other are more general-purpose (Ethereum, Hyperledger). Some have a single main deployment (Bitcoin, Ethereum, Ripple), other are designed to have many independent deployments (Hyperledger). All this variety is reflected in varieties of governance and business models.

As for governance, most blockchain technologies are open source, but the governance over the code varies between the classic "benevolent dictatorship" (Bitcoin, Ethereum), controlling foundation/enterprise (Ripple, Corda) and fully-fledged standards developing organisation (Hyperledger). Many of the systems use their own consensus infrastructure for governance of changes to the infrastructure, e.g. Bitcoin miners include their votes on Bitcoin Improvement Proposals in mined blocks, and Ripple validators use their consensus infrastructure also to accept/reject new features and fee change proposals.

The business models of the various open-source projects associated with the blockchain technologies varies. Projects with a cryptocurrency often use that cryptocurrency as equity to finance the project (pre-mined ETH, XRP), as well as libertarian philanthropy. For corporate-oriented projects (Ripple, Hyperledger), application development and system integration may justify the investments in open-source code.

The business model of many blockchain networks is via transactions fees. Cryptocurrency-fueled blockchain networks (Bitcoin, Ethereum) reward their miners/validators with newly minted cryptocurrency (BTC, ETH) and transaction fees per stored kB of transactors or per used CPU cycle. The permissioned Interplanetary Database (BigchainDB) charges storage fees per stored GB. The business model of other blockchain networks is less clear (e.g. Ripple), or left to the implementors of the specific blockchain network instance (e.g. Hyperledger).

ALL THIS VARIETY IS REFLECTED IN VARIETIES OF GOVERNANCE AND BUSINESS MODELS.

For more information,
please contact
Dr. M. Oskar van Deventer
E Oskar.vandeventer@tno.nl
M +31 88 866 70 78

Blockchain.tno.nl

BLOCKCHAIN.TNO.NL