Radoslaw Krzeski

Summary of Topic VI - Corda

Corda Introductory Whitepaper

The abstract describes a distributed ledger between distrusting nodes, allowing for a global database to record deals and obligations between institutions and people. The main difference from bitcoin seems to be the lack, or rather the absence, of ledger that needs synchronization on all connected nodes.

It supposed to transform the financial sector, both for clients and firms, with little friction involved between transaction. It is launched with legal frameworks and relies on proven technologies. Three main points of their philosophy are: engineering for the requirements of institutions, focus on non-functional requirements and extensibility.

The paper states that banks maintain their own ledgers, but ones that abide to the beliefs and rules of the financial institution. This might sometimes not match the views of its customers of transacting partners and causes costly delays. This is especially true for different technologies between different firms, where information sharing is not usual. The creators believe that blockchain technology can create authoritative systems between firms, a single global ledger for all agreements between firms recorded on it (firms agreeing to participate obviously).

A few examples are shown, where two parties can have their own records, but share discrepancies and duplications ("Bilateral – Reconciliation"). Another is where there is a third party involved to delegate critical processing ("Third Party/Market Infrastructure"). A last example is where to parties collaborate on a greater level and share a common exchange platform to pave way for new services or providers ("Shared Ledger Vision").

Such a shared idea will create large cost savings, fewer discrepancies and quicker agreement's. This is then expanded on a global scale, where the authoritative management is moved from within firms to being shared between firms.

The paper describes a few end-state principles:

- Facts recorded by the ledger are admissible evidence and legally binding.
- Fact recorded by the ledger are authoritative themselves and not "shadows".
- Facts are final and immutable, and processed with subsequent transaction. Firms are pressured to increase accuracy and quality.
- Any actor may, in principle, connect to ledger and record agreements with counterparts.
- Promoted open standard invite provides of different services, choices and competition.
- Only parties that are stakeholder or have legitimate reason have access to financial transactions.
- Interim states, where only business logic is shared.
- Support for code upgrades and explicit reference to solve disputes.
- Design will not necessarily be global, but a multi-layered ledger (and contain IP proprietary on a higher level).

I would say a weakness emerges when the paper says that is assumes a collaborative alliance with multiple financial institution. This is probably the hardest thing to solve and negotiate before the technology gathers form. A regulatory engagement is also key, but seeing how long it took bitcoin to become mainstream this might prove to be difficult.

The platform itself supports smart contracts, automatable by computer code, and are legally enforceable. The contracts have a set of key activities:

- Recording and managing shared data between parties.
- Making a workflow without a central controller and supporting consensus on a scale down individual deals.
- Can support inclusion of regulatory and supervisory observer nodes.
- Validating transactions solely between parties and support various consensus mechanisms.
- Support extended use of contracts, industry-standard tools and ability to restrict access.

It is envisioned to start on a global scale, with subgroups existing on the initial ledger. The "state object" is the primary digital document to record the record agreements of various scale. IT shared globally, but not visible to all. Hashes identify who has access.

An example is given where a State object can represent a cash claim against a bank or proving a credit relationship. Pre-agreed rules, timestamping, orchestrated framework and multi-steps protocols are all ingredients of Corda. Transactions are consumed and produce new state objects.

Two objects of consensus: transaction validity and transaction uniqueness. The last object will often require and observer, often an independent party.

Data is also defined as being "on" and "off" the ledger, depending on the transparency of the data and transactions. When a transaction find place, a function accepts or rejects a transaction as input and produces an output. The virtual machine

controlling this will be the Java Virtual Machine, due to the extensive libraries and resources, but locked in a strict sandbox with a standardized bytecode set.

In the end-game Corda is conceived to serve these main purposes; cash agreements, security(custody) and derivative agreements). These would involves storing the legal identity, current, amount etc.

Parts are stored in the Contract code, in addition to information in the Legal Prose. The protocol proposed has some similarities to the Bitcoin protocol in terms of the UTXO`s and immutable states. Corda is also Turing-complete, and can be written in any ordinary programming language. Corda has no Proof of Work or concept of mining in it.

In hindsight, it has a few similarities with Ethereum, in terms of smart contracts and can contain complex logic, but limits itself to financial transactions and on a decentralized, and maybe even isolated, state of function.

Gendal.me Article

Once again, the article specifically mentions that R3 is designing Corda for the use in financial agreements and between regulated financial institutions. The overarching benefits are limited sharing of data, choregraphed workflows without a central controller, multiple consensus mechanisms on individual level, enables regulatory and observatory nodes, transactions are validated by parties, ability to record legal prose documents, built on industry standards and has no native cryptocurrency.

As of April 05, 2016, they were still building the maturing code, and planned for an open source release. The system was built from the ground from (and for) a set of requirements, not purely on design purposes or the hype of blockchain. It is argued that Bitcoin was built on the requirements of how to “not have others spend my money”.

No matter how good a solution, if it does not solve a business/client problem, it will not be accepted.

The article has five main points that blockchain technology could offer, or uses as separate services:

Consensus: where a party to a shared fact, know that the fact is the same that other stakeholders see.

Validity: It allows to check the validity of a given fact, and defines the rules of the system.

Uniqueness: The ability to define two identical parts with each other and define which is the correct one.

Immutability: in the form that data can only keep building if it’s based on a larger base of an unchangeable body of previous activity.

Authentication: Usually trusted to private keys, getting rid of superusers og authoritative admins.

The paper argues that agreements today are usually stored on separate, different systems, which increase costs, rather than unify and validate transaction history. They also rely on messages, rather than actual statements of facts.

“What I see is what you see and we both know that we see the same thing and we both know that this is what has been reported to the regulator”

And this is to be controlled by the node entity that is Corda.

The below statements match for Corda according to the ones above.

Consensus: Mainly between participants.

Validity: Valid between stakeholders involved, and written on a contract-by-contract basis.

Uniqueness: More or less the same, but have additional abilities in terms of prioritizing consistency at the expense of availability.

Immutable and Authentication: Builds on the given knowledge base of previous blockchain technology.

Main differences are that it’s not a blockchain, rather a node network, and shared only between a set of parties. Main object are agreements, legal prose and the consensus system is built for financial transactions, along with a focus in interoperability and choreography between firms as they build agreements.

Built on the premise that no other platforms are addressing the problems they have stated (R3).

Docs.corda.net – Video

The video begins with the fact that a lot of people are involved when a traditional transaction is to take place. Distributed ledger technology is to take over now, to keep the transaction between Alice and Bob in sync, but also not to allow for changes of this data. Traditional blockchain is slow in terms of data sharing between nodes, and the fact that privacy is at stake, only the stakeholders really need to know about transactions. With a single deal, you are under control, and can plug in a service or regulator to keep all things clean between the parties. Built to deal with real business problems. Open source and works with industry languages.

References:

https://docs.corda.net/_static/corda-introductory-whitepaper.pdf

https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/

https://docs.corda.net/