


4.2 Two Perspectives on Blockchains: Capabilities vs. Features

Søren Debois (IT University of Copenhagen, DK), Marlon Dumas (University of Tartu, EE), Stephan Haarmann (Hasso Plattner Institut, DE), Hans-Arno Jacobsen (TU München, DE), Mieke Jans (Hasselt University, BE), Jan Mendling (Wirtschaftsuniversität Wien, AT), Mark Staples (Data61, CSIRO –Sydney, AU), Barbara Weber (Technical University of Denmark – Lyngby, DK), Francesca Zerbato (University of Verona, IT), and Kaiwen Zhang (ETS – Montreal, CA)

License  Creative Commons BY 3.0 Unported license

© Søren Debois, Marlon Dumas, Stephan Haarmann, Hans-Arno Jacobsen, Mieke Jans, Jan Mendling, Mark Staples, Barbara Weber, Francesca Zerbato, Kaiwen Zhang

Blockchain technology is the subject of substantial enthusiasm and notable financial successes. For example in June 2018 alone, almost USD\$6B worth of tokens were issued in ICOs ¹.

Indications of widespread use of blockchain and distributed ledger technologies outside of tokens and cryptocurrency are emerging.

Prior work proposed different decision models with the goal to help answering the question “Do i need a blockchain for my application?” [21, 26, 39, 41, 42, 44, 50, 67, 68, 71]. Moreover, there are proposals to guide the design process (i.e., which blockchain configuration to best choose) (e.g., [68]). However, there is little work up to now that focuses on the business capabilities that might form part of a blockchain-based application supporting business operations and on how they link to blockchain features.

In the remainder, we proceed as follows. In Sect. 4.2.1 we provide the foundations of blockchain and distributed ledger technologies. Then, in Sect. 4.2.3 we give a list of business capabilities identified as key to blockchain. Moreover, in Sect. 4.2.4 we identify a list of blockchain features. Subsequently, we map features to blockchain capabilities. Finally, we outline potential future work in Sect. 4.2.5.

4.2.1 Background

In this section, we recall the main concepts of blockchain and distributed ledger technologies.

Blockchain and Distributed Ledger Technologies

Applications of blockchain typically shift trust from a third party (a bank, a government institution, a credit card company) onto something else, typically the technology of the chain itself. There are two reasons one might desire such a shift:

1. One does not wish to trust the third party. (Bitcoin: government-less money)
2. The third party is expensive. (Hypothetical example: Credit card companies.)

However, new applications might arise where there previously were no solution because involved parties could not or would not agree on a trusted third party. For example, Mærsk and other shipping companies always had the option of developing a global, centralised repository of shipping documents; however, presumably, who would control that repository prevented it from coming into existence.

We emphasise that in the absence of risk or trust issues, a blockchain has no purpose. In other words, *a blockchain is needed only if the data consumers and the data owner are in separate trust domains and the consumer has high-integrity requirements. There is no need*

¹ <https://www.coinschedule.com/stats.html>

for a blockchain when the data consumer(s) and data owner are in the same trust domain (e.g. inside a company).

To understand what capabilities are central to / indicative of such shifting of trust, we first (attempt) to clarify what is “trust” and what is “a capability”.

Definition of trust. Trust is the acceptance of risk. Such risk may arise either from, say, malicious intent, or unintentional byzantine errors (either because of incompetence or because of hostile environment)

Alternative viewpoint (solution-driven).

The benefits conferred from blockchain technology constitutes “affordances” (see: Gibson, J.J., *The Ecological Approach to Visual Perception*. 1979. Boston: Houghton-Mifflin) rather than a outright features:

- Having trust in a system without having a trusted third party;
- Lower cost for the service;
- Lower barrier of entry;
- More accessible than traditional services (strategic advantage);
- Elimination of TTP;
- Tolerance to failures (impact of failures).

4.2.2 Capabilities and the Resource-Based View of the Firm

Business each have a wide range of capabilities². Some are strategic capabilities which are key to the business’s sustainable competitive advantage, and are valuable and distinctive compared to other businesses. Strategic capabilities are sometimes called “core competencies”. Others are operational capabilities, which are necessary for the operation of the business, but will not be distinctive, and are more likely to be outsourced. A capability area may be strategic for one business, but operational for another.

Blockchains provide a mechanism allowing businesses to shift trust within the operation of their ecosystems. Often this is for disintermediation, stopping the centralised control of that capability by those third parties. This can be good for businesses that want to use that capability as an operational capability. However for trusted third-parties, this capability is a strategic capability, and blockchain may directly undermine the sustainability of their competitive advantage from that capability.

Definition of capability. “Capability thinking also means being aware of in what context the enterprise has the capacity and ability to offer business services that contribute to achieving business goals. The context basically captures what legal, technical, process, content, or other situation the business service is prepared for and what variations in providing the business service apply for what situation” [54].

4.2.3 Capabilities of Blockchain-Based Systems

Table 1 shows the main business capabilities resulting from our analysis and discussion. The list of business capabilities we have identified below is not exhaustive, and the capabilities

² Here we do not mean “object capabilities” which are secure references used in capability-based security models. We also do not mean software engineering capabilities captured for example in models such as CMMI.

■ **Table 1** Business capabilities for blockchain-based systems.

BC1: Voting <ul style="list-style-type: none"> ■ Anonymous voting ■ Delegatable voting (conditional voting with smart contracts) ■ Number of participants(N): un/bounded ■ Non-sellable 	Entry of votes submitted by different parties, tallying, and announcement of results.
BC2: Payment <ul style="list-style-type: none"> ■ Anonymous payments ■ Escrow payments ■ Variable payments ■ Complex conditional payment 	Transfer of cryptocurrency between different parties.
BC3: Asset transfer	The transfer of assets (cryptocurrency, tokens) from one party to another.
BC4: Settlement (payment vs. delivery)	Synchronisation of simultaneous asset transfers.
BC5: Exchanges	Settlement of particular assets.
BC6: Introductions	Connecting parties interested in being end-points of contacts
BC7: Referrals	Introductions where one or more party must be endorsed, authorised, and or made aware of by another.
BC8: Reputation	The reputation is a global score for participants representing trustworthiness.
BC9: Bookkeeping	Recording of transactions, typically for the purposes of financial reporting.
BC10: Brokering	Introductions for asset-transfer contracts.
BC11: Monitoring	The automated detection of transactions or contract executions satisfying particular, pre-defined properties.
BC12: Offering (incl. auctions)	Contract / transaction with initially undetermined counterparty.

may be interrelated (for example, settlement will involve payment). In addition, the business capabilities we have focussed on are multi-party capabilities, rather than capabilities that are mainly internal to a company.

4.2.4 Features of Blockchain-Based Systems

We then identified a list of blockchain features (system capabilities) as outlined in Table 2.

We then mapped the different business capabilities to the corresponding blockchain features (cf. Table 3). Optional features are listed in brackets.

A combination of the above described capabilities can be used to form a market.

Additionally, we identified the following inter-dependencies among features.

1. Audit Trail → Transactions → Signature → Encryption → Wallet information;
2. Contract → states → Verification;

■ **Table 2** Features of blockchain-based systems.

F1: Data access on-chain	Storage; universal access to data stored on the ledger for any processing node.
F2: Encryption	Ability to encrypt and decrypt data stored on the blockchain.
F3a: Channel	Need-to-know access to data. Access control list.
F3b. Vault/Wallet information	Access to private information necessary to operate on the blockchain, but should remain confidential (e.g. private keys).
F4: States	Ability to record state for assets defined on the ledger, and transition the states using smart contract executions.
F5: Audit trail	Ability to record and link events in a sequence (provenance, logging, states are chained).
F5b: Receipts	Ability to obtain a detailed record per transaction, indicating which assets were read and modified.
F6: Transactions	Ability to submit transactions.
F6b. Permissions to submit data on-chain. F7. Identity management	
F8: Contract	Ability to invoke programs through transactions, and store contracts on-chain.
F9: Process	
F10. Verification	Integrity check of the ledger, and contract execution.
F11: Time service	Authoritative source of physical time, and timestamping.
F12: Notary service	Ability to put trust in / responsibility for a particular computation step in a given participant.
F13: Oracles	Special case of notary which injects external information into the system. (A mechanism for ensuring integrity of data provided transparently by a trusted data source.)
F14: Tokens	
F15: Anonymization	
F15b: Pseudonymization	
F16: Watermarking	Ability to permanently fix a signature inside a document stored on the chain.
F17: Digital signature	Ability to attach a signature to a transaction / document on the chain.
F18: Event	Ability to send events between accounts, to trigger smart contract invocations, and to notify external subscribers.
F19: What-if analysis	Ability to query the projected impact of a transaction / contract execution on the current state of the blockchain [9].

■ **Table 3** Mapping Capabilities to Features.

Capabilities	Features
Voting	Transaction, Time service, (Anonymization, Notary, Identity Management, Tokens)
Payment	Transactions, Receipts, (Channel, Time service, Tokens)
Asset transfer	Transactions, Tokens, Watermarking, (Channel)
Settlement	Audit trail, Tokens, Notary, Contract
Exchanges	Transactions, Tokens, Assets transfer, Notary
Introductions	Process, Data access, Channel
Referrals	Transactions, Tokens, Identity Management
Reputation	Identity Management, Audit Trails, (Oracles)
Bookkeeping	Audit trails, Receipts, States
Brokering	Identity, Contract, Transactions, State, What-if
Monitoring	Audit trail, Events, Process, Contract (Time Service)
Offering (incl. auctions)	Transaction, Contract, Digital signature, (Time service, pseudonymization)

3. Time service → oracle → Notary;
4. Channel → Identity management → Encryption;
5. Tokens → Transactions.

4.2.5 Conclusion

This summary has taken initial steps towards identifying both the features that can reasonably expect to be supplied by a blockchain platform on the one hand; and the capabilities which applications for that platform may require on the other.

In the future we would like to investigate which features are supported by different blockchain platforms, to guide the decision which platform to choose.

Moreover, as another avenue of research we might look into different solution patterns on how to implement different features.

4.3 Factors Influencing Process Analytics on Distributed Ledgers

Claudio Di Ciccio (Wirtschaftsuniversität Wien, AT), Luciano García-Bañuelos (University of Tartu, EE), Mieke Jans (Hasselt University, BE), Jan Mendling (Wirtschaftsuniversität Wien, AT), Petr Novotny (IBM TJ Watson Research Center – Yorktown Heights, US), Ludwig Stage (Tübingen, DE)

License © Creative Commons BY 3.0 Unported license
 © Claudio Di Ciccio, Luciano García-Bañuelos, Mieke Jans, Jan Mendling, Petr Novotny, Ludwig Stage

Blockchains trace the sequence of tasks carried out in the course of business process executions by the totally ordered recording of transactions between involved parties, and additionally the logs of events registered by Smart Contracts. This leaves ample room for the ex-post analysis of conducted operations, for analytics, auditing, and mining purposes [40]. However,