Blockchain deconstructed (abstract)

Fritz Henglein
Department of Computer Science, University of Copenhagen (DIKU) and *Deon Digital AG*
henglein@diku.dk, henglein@deondigital.com

***Abstract*—We propose that blockchain/distributed ledger (DL) systems be characterized by three simultaneous general requirements: organizational and technical decentralization; tamper-proof recording of events and their evidence; and guaranteed resource (= asset) preservation. Including evidence extends blockchain/DL systems to serving as digital twins for physical processes and resources. Resource preservation generalizes the "no-double-spending" property to allowing dynamically adjustable and user-specific credit limits and having multiple, user-definable resources.**

We formulate a simple theorem that highlights that enforcing credit limits is essentially the *only* problem requiring more than point-to-point communication. In particular, without credit limit enforcement essentially all communication between authenticated parties in a (smart) contract can be kept completely private. Conversely, *some* privacy leakage to a third party is necessary for credit limit enforcement. This naturally gives rise to a lightweight architecture for permissioned blockchain/DL systems where all communication between parties is "off-chain" (= point-to-point or in separate private channels for multi-party contracts) and only resource transfers need to be validated by a decentralized system employing a suitable distributed consensus protocol. We point out that such consensus protocol need not reach agreement on a globally total order of transactions, which is the main cause of inefficiency in presently popular blockchain/DL systems, since resource transfers commute with each other and thus can be processed in any order with limited synchronization: only credit limit enforcement requires some communication amongst the on-chain nodes.

I. Elaboration

In terms of the REA accounting modeling [1]–[3], a blockchain/DL system records events such as transfers of *resources* and *information* between agents. The difference between resources and information is that the former must not be duplicated, whereas the latter can be freely copied. The system thus guarantees the invariant that the *sum* of all resources owned by anybody is invariant under *transfers*: transferring 50 ETH from account A to account B does not change the total amount of ETH. The system furthermore guarantees the no-double-spend property: the transfer is only *valid* and effected if account A contains at least 50 ETH; that is, A's balance must be nonnegative at all times. In other words, the no-double-spend property amounts to enforcing a credit limit of 0 on all accounts.

It is worthwhile keeping resource preservation separate from credit limit enforcement for two reasons. First, without credit limit enforcement no validation and thus no consensus amongst more than the involved parties is required.

Theorem: Assume all accounts have no credit limit. Let T be a set of resource transfers. Then all $t \in T$ are valid and commute with each other, that is they can be performed in arbitrary order.

In particular, if two authenticated agents agree on a contract involving resource transfers such as a loan agreement, they only need to have local communication: they need to agree on the sequence of events, including transfers, that have happened at any given point in time by sending signed messages and acknowledging their receipt. In case of disagreement a party to the contract can provide the cryptographically hashed sequence of signed message exchanges to a third party as tamper-proof evidence of the history of events. Note that tamper-proof recording does not require validation by a third party.

Second, nonzero credit limits can be agent-specific and context-dependent. For example, an airline may sell (transfer) more flight tickets or a car manufacturer more cars than it presently has in storage if it manages to produce them (just in) time. Or one designated agent—the central bank—may have a dynamic credit limit of *digital cash*, a fiat currency managed as a cryptocurrency on a blockchain/DL system. If all other agents have a zero credit limit this represents a full reserve system. If designated other agents—banks—have policy-controlled non-zero credit limits, this corresponds to a fractional reserve system. In both cases, cryptocurrency cannot only be issued, but also retired, for example as part of loan repayments.

The analysis suggests a blueprint for generalized permissioned blockchain/DL systems that are highly scalable: A distributed consensus network validating *only resource transfers*; all other messages are point-to-point and private, employing standard encryption and authentication technology such as TLS. The consensus network furthermore only needs to solve a simplified consensus problem: it need not agree on a total order of transactions nor even on a partial order; it only needs to ensure that the transfers its nodes validate are guaranteed or sufficiently unlikely to eventually violate the individual agents' credit limit requirements.

References

[1] W. E. McCarthy, "The REA accounting model: A generalized framework for accounting systems in a shared data environment," *The Accounting Review*, vol. LVII, no. 3, pp. 554–578, July 1982.

[2] J. Andersen, E. Elsborg, F. Henglein, J. G. Simonsen, and C. Stefansen, "Compositional specification of commercial contracts," *International Journal on Software Tools for Technology Transfer (STTT)*, vol. 8, no. 6, pp. 485–516, November 2006.

[3] F. Henglein, K. F. Larsen, J. G. Simonsen, and C. Stefansen, "POETS: Process-oriented event-driven transaction systems," *The Journal of Logic and Algebraic Programming*, vol. 78, no. 5, pp. 381–401, 2009.