FUTURIUM: Next Generation Internet

Position Paper

Blockchains and Smart Contracts – A Valuable Alternative for Distributed Data Bases?

Burkhard Stiller, Thomas Bocek
Communication Systems Group CSG, Department of Informatics IfI, University of Zürich UZH
[stiller¦bocek]@ifi.uzh.ch

With the advent of data bases and the increasing amount of data (big data) to be processed, the development of distributed data bases started, which took into consideration the role of underlying communication protocols to reach – besides pure accessibility – stability, reachability, and secured access. The operation of the CAP principle – "Consistency, Availability, and Partition Tolerance" – in this context is considered standard today.

However, any of those distributed data bases are administered by a human system administrator with various rights to maintain, handle, and operate such a data base. In case of unencrypted data base entries – forming rather the norm than an exception as of today – this administrator will have read/write access to the data base. Even in case of integrated logging mechanisms and signed confidentiality agreements, such distributed data bases face the risk of a non-trusted administrator to manipulate this data base.

Blockchains have solved this problem of missing trust by assuming that any participant participating in a public blockchain does not have to have any trusted relationship, neither beforehand nor by knowing someone's identity. Thus, blockchains are a type of distributed data base for everyone's access, reading from it and writing into it by following the blockchain's consensus protocol. Besides unforgeable entries stored in the blockchain, all historic data is permanently stored forever, unless the underlying cryptography – especially cryptographic hashing – will be broken. Thus, blockchains in their pure form never forget any detail.

While Bitcoin has reached a high public attention in the past years, and as it was outlined in [1], too, it is the first crypto currency making use of this blockchain approach. The storage of all transactions (the hand-over of Bob's *b* BTC to Alice) is performed by using account information for Bob and Alice (which are represented as a hash of its public key), which do not reveal their current physical identity. Although first approaches exist today to relate more than one transaction data to a set of transactions potentially can break the anonymity of Bitcoin. However, besides these account information the capability of a blockchain to relate any user (unknown to each other, as in a regular day-to-day payment process with cash, bills or coins) to perform such a crypto currency payment and to verify latest after 6 blocks of transactions being stored in the blockchain (by applying the consensus mechanism of Bitcoin, currently a Proof-of-Work (PoW) in terms of partial hash collisions using SHA256) that no double spending has occurred, determined the real advance in communications and distributed systems design.

Note that blockchains work due to the definition of communication protocols combined with state-of-the-art security algorithms. This is, however, extended by application- and domain-specific executable code – the Smart Contract –, which performs on transaction data (upon their write into the blockchain) procedures to check, validate, or activate data/actions. Thus, a very close relation of blockchains to legal and regulatory aspects (for the technology itself ***and*** their applications) arises, which a Future Internet needs to be aware of and has to handle before unfavorable best practices may become the norm.

While [1] nicely argues on the potential new applications and use cases in a variety of fields, the authors of this position paper here have provided input on a set of additional scenarios, including application areas besides the finance industry, cf. [2]. Besides the major challenges of blockchains listed in [2], the set of ***key technical challenges blockchains face*** as of today are categorized and collected as follows.

Scalability: Public blockchains – especially with respect to the Bitcoin or Ethereum examples, known as permissonless – have been operational for only a very limited period of time with only a smaller number of transactions. Thus, the blockchain itself, the distributed data base of all writes ever performed, will grow with the number of transactions. While this will lead to a storage problem – size-wise –, the scalability of blockchains in broader settings and applications is at stake. In addition, the main reason for such observations is linked to the additional question, which data has to be persisted in the blockchains, thus, how many bytes are needed to refer to critical transaction information.

Security: As indicated, blockchains rely on the public-private key security. However, the anonymity of stakeholders involved in transactions can be considered in certain applications a deficit besides, although being advantageous for cryptographic currencies. Thus, the final level of security achievable is to be determined, especially in the context of consensus protocols available today. While the PoW – as mentioned above – requires many hash calculations, incentives in a public blockchain are available today to operate a public blockchain. However, private blockchains do need different consensus mechanisms, such as a majority vote or a Proof-of-Stake (PoS), which determines a mechanism to enable coin owners to validate a block, for which they receive a reward if being successful. However, in such cases – also known a consortium-based or permissioned blockchains – the stakeholders involved have to show at least a partial trust between them due to, *e.g.*, the "Nothing-at-Stake" problem. The absolute or relative boundary between those blockchain types and their achievable security needs further investigation, including their consensus mechanisms.

Computing Power and Energy Efficiency: Especially the PoW consensus mechanisms give raise to questioning the computing power needs and their related energy efficiency. While calculations have shown that all transactions performed world-wide with Bitcoins in 2015 have reached approximately a 250-500 MW energy consumption level, it is more than obvious that more energy-efficient consensus mechanisms are a must for future use, especially in case of a widespread public use of permissionless blockchains in governmental or commercial settings.

Availability and Reliability: The use and access of data, which were generated more than a couple years ago, tends to become tedious as long-term archival work shows. Thus, the question arises how do private blockchains need to be treated, if they run operationally and if the underlying technology changes? The availability of old or even historic data access may become crucial. Furthermore, the reliability of a blockchain's operation is important. While distributed data bases – run in different geographical locations – operate with consistency mechanisms and provide respective mechanisms for data calibration, a lacking Internet access of blockchain stakeholders during longer periods of time leads to problems of sidechain integrations, availability of blockchains when blocked or censored, or collusion situations, where simply due to unreliable power supply of nodes or active attacks more than 50% of the stakeholders involved start to stretch the reality of transactions.

Smart Contracts: Any procedure to be automated does require application- and domain-specific executable code. While a distributed data base does allow for "Stored Procedures", code to be executed on the content of an entry during its write process, blockchains provide exactly that functionality in terms of Smart Contracts. However, the direct embedding of transactions, transaction data, and executable code in terms of Smart Contracts leads to the question of which programming language to use? While programming language experts acknowledge the fact that non-Turing-complete languages for Smart Contracts limit its usability, Turing-complete languages for Smart Contracts have been developed, which, *e.g.*, include loops. However, by applying those languages for Smart

Contracts, the testing, bug-fixing, and change of existing Smart Contracts in that language leads to the problem of "change the law" (cf. below) or "change the semantics", which needs careful considerations. Thus, the question is how much "power" does a Smart Contract language need to have to fulfill application demands, but how limited does it need to be at the same time to avoid mistakes, especially in case of public instances, a public blockchain.

Code is the Law: While the blockchain developers define the only and strict interpretation of a Smart Contract as the only valid one (the "Code is the Law" principle), the use of a non-Turing-complete programming language may support such a position. *E.g.*, Bitcoin defines Smart Contracts, which are limited to the transaction type of a crypto currency transaction. However, up to now a proof is unknown that Smart Contract programming languages do enable a unique interpretation of the code executed. Additionally, the applicability of limited Smart Contract languages to potentially reach into wider areas of applications may lead to restricted use, which contrasts with a more general Smart Contract scope. However, if the volition of a contract is not in line with the general Smart Contract, mediation is necessary. Current approaches with forking the blockchain, *e.g.*, after The DAO incident, should be avoided.

Law and Regulation: The set of legal and regulatory aspects to be investigated for blockchains relate to (a) the technology itself ***and*** (b) their applications at the same time. This close combination of technology-inherent and technology-driven demands is unique and poses a general juridical problem, since there exists a separation of (a) laws' applicability for dedicated or general application areas and (b) a regulation of technology use in more general terms. Meanwhile, regulations had been defined in the past, especially for competitive sectors or those, where customers can be effected negatively by lacking competition. Thus, an unlawful use of an application may have to be prohibited or prosecuted, but the technology itself, once accepted as a "common practice", shall not be effected at all. Finally, two important legal questions remain: (a) do a private blockchain and its Smart Contracts "belong" to private law or do the data persisted therein belong to public law and (b) which law will guide public blockchains and their use?

Public Perception and Acceptance: While the technology and its characteristics are available, at least partially tested, and more recently utilized, the fields of blockchain applications covers FinTech (financial), InsurTech (insurance), SCTech (supply chain), governments, and consortium-internal tasks. The key question remains in which sense and form the public, today's society, regions, or countries will perceive the value and security of blockchains in any of those fields of applications (or parts thereof)? How does a society accept a technology, which executes code and, in turn, determines a one-to-one mapping of laws or regulations in an automated manner?

Thus, besides the regulatory demands in the context of blockchain usage, identified in [1], and highly relevant for the finance industry and beyond, the pure technical perspectives of blockchains as outlined above do need a very careful and detailed investigation, for which the key directions have been outlined above. Additionally, the relation between such new technology and the varying jurisdictions in the world has to take into account a missing global approach and segregated regulation domains.

[1] Primavera De Filippi: *Position Paper on: Bitcoin, Blockchain, and the Future of the Internet;* in FUTURIUM, Next Generation Internet, https://ec.europa.eu/futurium/en/content/bitcoin-blockchain-and-future-internet, last accessed November 14, 2016.

[2] Thomas Bocek, Burkhard Stiller: *Smart Contracts – Blockchains in the Wings;* to appear in "Digital Markets Unleashed", Edts. Claudia Linnhoff-Popien, Ralf Schneider, Michael Zaddach; Springer Verlag, Heidelberg, Germany, 2016/2017.