Blockchain & Business Process Management

Introduction

Business Process Management, or simply BPM, deals with the design, execution, monitoring and improvement of business processes and when it comes to *intra*-organizational, companies have long used and have available to them systems that support the enactment and execution of processes.

However, *inter*-organizational offer some inherent challenges, “challenges of joint design and a lack of mutual trust have hampered a broader uptake” (Mendling, 2018). In the context of BPM, “… blockchain offers a way to execute processes in a secure even in a network without any mutual trust between nodes”.

The Blockchain Technology

(Topic already devoloped in the Document Blockchain and Smart Contracts)

Challenges of the Blockchain Technology in the Context of BPM

In its current state, the Blockchain Technology still has room for improvement, mainly when it comes to general technological challenges it faces. Some of these can be addressed by using private or consortium blockchains instead of fully open ones (such as Ethereum) and others have already been addressed by the research community.

In general, these are the technological challenges faced by the technology:

Throughput; in the Ethereum blockchain is limited to approximately 15 transaction inclusions per second (tps) currently. In comparison, transaction volumes for the VISA payment network are 2,000 tps on average, with a tested capacity of up to 50,000 tps. However, the experimental Red Belly Blockchain which particularly caters to private or consortium blockchains has achieved a peak of 660,000 tps [https://www.redbelly.network/redbelly-network-whitepaper].

The latency also needs to be addressed. Transaction inclusion in the absence of network congestion takes a certain amount of time. Additionally, a number of confirmation blocks are typically recommended to ensure the transaction does not get removed due to accidental or malicious forking. This results in transactions being sometimes only being seen as committed (on average) after 60 minutes in Bitcoin, or 3 to 10 minutes in Ethereum. Even with improvements of techniques like the lightning network or side chains spawned off from the main chain, blockchains are unlikely to achieve latencies as low as centrally-controlled systems.

Size and bandwidth limitations are variations of the throughput issue: if the transaction volume of VISA were to be processed by Bitcoin, the full replication of the entire blockchain data structure would pose massive problems. [Yli-Huumo et al. 2016] quote 214 PB per year, thus posing a challenge in data storage and bandwidth. Private and consortium chains and concepts like the lightning network or side chains all aim to address these challenges. In this context it is worth noting that most everyday users can use wallets instead, which require only small amounts of storage.

Throughput in the Ethereum blockchain is limited to approx. 15 transaction inclusions per second (tps) currently. In comparison, transaction volumes for the VISA payment network are 2,000 tps on average, with a tested capacity of up to 50,000 tps.

However, the experimental Red Belly Blockchain which particularly caters to private or consortium blockchains has achieved more than 400,000 tps in a lab test4 .

Latency is also an issue. Transaction inclusion in the absence of network congestion takes a certain amount of time. In addition, a number of confirmation blocks are typically recommended to ensure the transaction does not get removed due to accidental or malicious forking. That means that transactions can be seen as committed after 60 minutes on average in Bitcoin, or 3 to 10 minutes in Ethereum. Even with improvements of techniques like the lightning network or side chains spawned off from the main chain, blockchains are unlikelyto achieve latencies as low as centrally-controlled systems.

Size and bandwidth limitations are variations of the throughput issue: if the transaction volume of VISA were to be processed by Bitcoin, the full replication of the entire blockchain data structure would pose massive problems. [Yli-Huumo et al. 2016] quote 214 PB per year, thus posing a challenge in data storage and bandwidth. Private and consortium chains and concepts like the lightning network or side chains all aim to address these challenges. In this context it is worth noting that most everyday users can use wallets instead, which require only small amounts of storage.

Usability is limited at this point, in terms of both developer support (lack of adequate tooling) +and end-user support (hard to use and understand). Recent advances on developer support include efforts by some of the authors towards model-driven development of blockchain applications.

Security will always pose a challenge on an open network like a public blockchain. Security is often discussed in terms of the CIA properties. First, confidentiality is per se low in a distributed system that replicates all data over its network, but can be addressed by targeted encryption . Second, integrity is a strong suit of blockchains, albeit challenges do exist [Eyal and Sirer 2014; Gervais et al. 2016]. Third, availability can be considered high in terms of reads from blockchain due to the wide replication, but is less favorable in terms of write availability [Weber et al. 2017]. New attack vectors exist around forking, e.g., through network segregation [Natoli and Gramoli 2017]. These are particularly relevant in private or consortium blockchains.

Wasted resources, particularly electricity, are due to the consensus mechanism, where miners constantly compete in a race to mine the next block for a high reward. In an empirical analysis, [Weber et al. 2017] found that about 10% of announced new blocks on the Ethereum network were uncles (forks of length 1). This can be seen as wasteful, but is just a small indication of the vast duplication of effort in proof-of-work mechanisms. Longer forks were extremely rare, so accidental forking seems unlikely in a well-connected network like the Internet – but could occur if larger nations were cut off temporarily or even permanently. Alternatives to the proof-of-work, like proof-of-stake [Bentov et al. 2016], have been discussed for a while and would be much more efficient. At the time of writing, they remain an unproven but highly interesting alternative. Proof-of-work makes very low assumptions in trusting other participants, which is well suited for an open network managing digital assets. Designing more efficient protocols without relaxing these assumptions has proven a challenge.

Hard forks are changes to the protocol of a blockchain which enable transactions or blocks which were previously considered invalid [Decker and Wattenhofer 2013]. They essentially change the rules of the game and therefore require adoption by a vast majority of the miners to be effective [Bonneau et al. 2015]. While hard forks can be controversial in public blockchains, as demonstrated by the split of the Ethereum blockchain into a hard forked main chain and Ethereum Classic (ETC), this is less of an issue for private and consortium blockchains where such a consensus is more easily found.

Business Process Management and the Blockchain

(Still in development).

References

Mendling J, Weber I, Van Der Aalst W, Brocke J, Cabanillas C, Daniel F, Debois S, Di Ciccio C, Dumas M, Dustdar S, Gal A, García-Bañuelos L, Governatori G, Hull R, La Rosa M, Leopold H, Leymann F, Recker J, Reichert M, Reijers H, Rinderlema S, Solti A, Rosemann M, Schulte S, Singh M, Slaats T, Staples M, Weber B, Weidlich M, Weske M, Xu X, Zhu L. (2018). Blockchains for Business Process Management – Challenges and Opportunities

J Yli-Huumo, D Ko, S Choi, S Park, and K Smolander. 2016. (2016). Where Is Current Research on Blockchain Technology? – ASystematic Review. PloSONE.
https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477

https://www.redbelly.network/redbelly-network-whitepaper