Smart Contracts for Government Processes: Case Study and Prototype Implementation (Short paper) *

Magnus Krogsbøll[1], Liv Hartoft Borre[1], Tijs Slaats[2], and Søren Debois[1]

[1] IT University of Copenhagen, Copenhagen, Denmark
{magkr,livb,debois}@itu.dk
[2] University of Copenhagen, Copenhagen, Denmark
{slaats}@di.ku.dk

Abstract. We study blockchain-based integrity-protected smart contracts as an implementation mechanism for municipal government processes. To this end, we attempted a prototype implementation of such a process in collaboration with a Danish Municipality. We find that such an implementation is possible, despite the obvious confidentiality requirements, and that it does provide benefits: integrity guarantees, verifiability, direct collaboration and payments between the parties. These benefits come at the cost of latency, pr. transactions charges, immutability of errors, and a very concerning single point of failure the municipal government: losing blockchain private keys means losing control over municipal government casework, *with no recourse*. Our municipal government partner felt that altogether no immediately pressing problem was solved by the implementation, and that the latter risk clearly outweighed any benefits. We note that smart contract implementations of government processes needs to be immutable and outside of the government's control when running; however, they also need to be updatable when laws change, and provide an "out" for the rare case when errors in the contract implementation result in unlawful behaviour. We propose these conflicting requirements as a foundational research challenge for blockchain to be applicable to governmental processes.

Keywords: Applications of blockchain · Electronic government · Smart contracts · Ethereum · Governmental processes

1 Introduction

Municipal governments in modern democracies exercise *power* over their citizens: they decide who is or is not entitled to receive welfare benefits; which sports clubs receive financial support, which parents are unfit for their role. This power is checked by national or federal laws defining exactly how these decisions are made,

* **Acknowledgments:** Work supported by the Innovation Fund Denmark project *EcoKnow* (7050-00034A). We gratefully acknowledge Syddjurs Municipality for their contributions to the case study and insightful comments.

and appeals institutions providing redress to citizens who can prove that these laws were violated. Even so, for society to function, the public must *trust* that municipal governments mostly do right; that decisions are fair and in accordance with law; that appeals are mostly unnecessary, and that the successful appeal is the rare exception.

In this paper, we investigate to what extent we can supplant trust in municipal government with the integrity guarantees provided by smart contracts [3,18] running on a blockchain [14,17]. We do so by experiment: In collaboration with the Danish Syddjurs Municipality, we have constructed a prototype implementation of a specific social benefits process as an Ethereum smart contract. The implementation is available online [2].

The process is defined by §42 in the Danish Law on Social Service [7], which describes the circumstances under which parents are entitled to compensation for earnings lost due to the caring for a child with a long-term illness. The implementation revolves around an Ethereum smart contract which serves as an intermediary between the citizen, the municipal government caseworker, and the Appeals Board. This contract encodes (to an extent) the law: the caseworker records in the contract that necessary steps, like procuring documentation or conducting public hearings, has been taken; the contract does not allow decisions until all such steps require by law have been concluded.

We conducted this case study in collaboration with the Danish Syddjurs Municipality, who assisted us in both understanding the §42 process and in evaluating the eventual prototype.

Our key findings are that it *is* possible to replace part of the trust in municipal government with a smart contract while preserving the necessary confidentiality requirements. Doing so provides transparency to both the citizen, incontrovertible history for the appeals institution, and reduces the possibility for procedural errors by the municipal government, such as deciding upon a case without having procured all law-mandated documentation. It allows for streamlining of the process through semi-automated intervention by an appeals institution, and potentially removes the possibility for the municipality to ignore a reversal on appeal (which would otherwise have to be remedied in court).

Syddjurs Municipality expressed severe concerns that (a) the additional integrity guarantees provide no real-world benefit; (b) it remains unresolved who defines the smart contract and how it will be updated when the law changes; and, most severely, (c) the contract introduces a single-point of failure: should the municipal government leak the keys to the smart contract, they will have lost control of their processes (and payouts) *with no possible recourse*. We conclude that addressing this dichotomy between on the one hand providing trustworthy immutable contracts, on the other requiring the ability to support (1) constantly changing laws and (2) the reversal of outlier cases which were handled in an unlawful manner is a significant research challenge for blockchain to be applicable to governmental processes.

Related work. Ours is not the first to study applications of blockchain technology to governmental processes. Most notably, [23] considers such applications in

the abstract, proposing a number of possible applications and their trade-offs. However, that paper does not consider the question of who controls the eventual update of smart contracts and treats the subject purely in theory, whereas in the current paper we take an experimental approach. In [5] a case study of applying blockchain technologies to governmental processes is presented. Along similar lines, [6] provides an overview of a large set of ongoing governmental projects that include the application of blockchain technologies. This paper provides an analysis and discussion of the potential consequences of such projects for society at large. The paper [15] provides a brief overview of existing academic literature related to blockchain technologies and discusses potential applications in e-government, going in more detail on one proposed case study. Unlike the current paper, this study is however hypothetical, with no actual implementation to underpin it. For process management in general, opportunities and challenges for blockchain was discussed in [12], and implementation of generic "process engines" on Ethereum is well-studied [4,8,9].

Process. Our explorative case study proceeded as follows. Staff from the Syddjurs Municipality Digitalisation Office proposed the §42 process to us; then kindly provided both a presentation of their §42 workflows, an interview, and subsequent e-mail clarifications. Based on this information, we independently designed and implemented a smart-contract–based prototype system supporting this workflow. Finally, we evaluated this prototype jointly with Syddjurs Municipality Digitalisation Office staff and management. The present paper mirrors this structure: we first present the §42 process (Sec. 2); then present the prototype design and implementation (Sec. 3); and finally present findings based on the joint evaluation (Sec. 4).

2 The §42 Process

The process implemented in our experiment is defined in §42 of the Social Services Act [7], which describes how parents of children with disabilities or long-term illness may, under certain conditions, be compensated by the municipality for their loss of earnings due to the necessity of caring for the child at home. Citizens may appeal decisions, in which case the process includes the Appeals Board, a Danish public institution that may overrule municipal governments.

A recent study by the Appeals Board [1] found across-the-board issues in municipalities' execution of these processes, especially (1) failure to obtain sufficient information for lawful processing of a case, and (2) failure to sufficiently justify decisions. Note that while a smart contract may alleviate (1)—by requiring that documents are uploaded before a decision is made—it seems unlikely that (2) can be detected by automated methods, as we cannot (yet) automatically decide if the *contents* of those documents warrants a particular decision.

The process proceeds through 3 phases depicted in Figure 1; *decisions* are made along the way, and the process terminates on unfavourable decisions.

In **Phase 1** (Figure 2), the municipal government calls the parents for a guidance meeting. The caseworker may at this point decide that the parents' situation

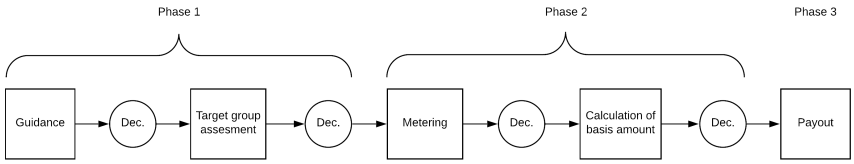

Fig. 1. The full §42 process

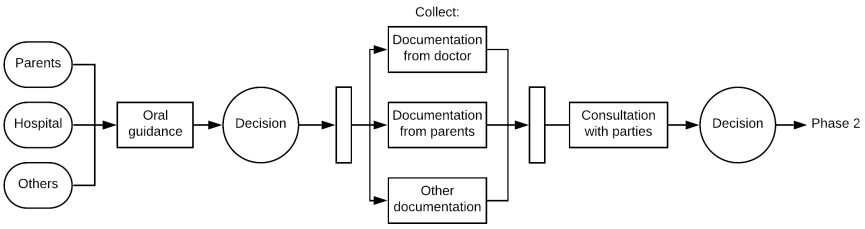

Fig. 2. Phase 1 of the §42 process

is out of scope for §42. Otherwise, the caseworker collects documentation to establish that care at home is (a) necessary and (b) most expedient. Again, the caseworker may at this point decide that (a) and (b) are not the case, and the parents not eligible. In **Phase 2**, the caseworker collects additional documentation to calculate lost earnings, and any possible offsetting absent of expenses (e.g., gasoline not used when not driving to work). In **Phase 3**, decisions are made regards to payouts. Each month the parents document their lost earnings, and the caseworker then issues a payout. Every six months the municipality must review the case from (repeat Phase 1), and every year the government updates their rate and the compensation has to be recalculated from Phase 2.

The citizen may appeal any decisions made (Fig. 3). The appealed decision is then either ratifies or amended by the caseworker. A ratified decision is immediately forarded to the appeals board, which eventually either ratifies, changes, disbands, or returns the decision; in the latter case requiring the municipal government to re-process the case from the *previous* decision onwards.

3 Prototype

The prototype system comprises a smart contract (enforcing the process), web-interfaces for each of the actors (citizen, municipal caseworker, appeals board), and a local database each for the municipality and the appeals board.

Each task in the is classified as either a decision; the acquisition or processing of data in the form of documents or numbers (say, a number of hours or the claimed amount); or payments. The smart contract accordingly implements a

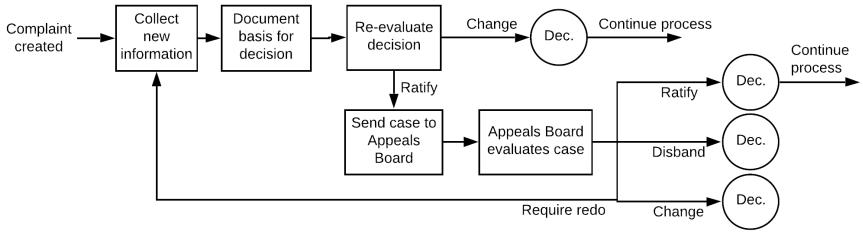

Fig. 3. The appeal process

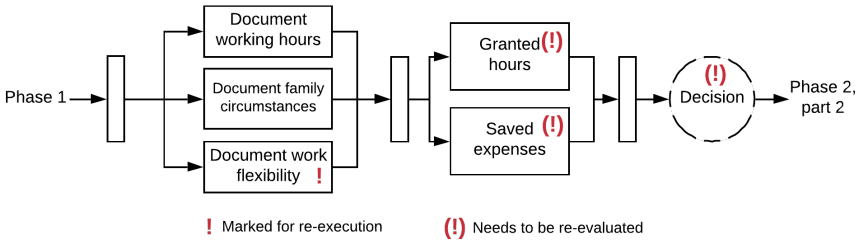

Fig. 4. Illustration of the Appeals Board marking a data in the process

simple process engine along the lines of [8,9]. The process itself is specified as a dependency graph over tasks; a task is only available for execution if all of its dependencies have been executed. A task can be marked as requiring re-execution (used in appeals, see below). The process model assigns roles to tasks (citizen, municipal caseworker, or appeals board), and implements role-based access control via Ethereum addresses.

An appeal of a decision interrupts the process and forces the municipality to review the case by marking the tasks after the previous decision as requiring re-execution. If the municipality changes its decision, the case continues (although the citizen may again appeal the changed decision). If the decision is re-executed with the same data (the same decision), the appeal and case is sent to the Appeals Board. Via the smart contract, the Appeals Board manifests its decision by marking tasks for re-execution, thereby forcing the municipality to re-evaluate the case; or by setting the process state outright, thereby overruling the decision. We illustrate the process state after an appeals decision in Figure 4.

Confidentiality and verifiability Data involved in the process is generally sensitive (e.g., the child's medical condition and the parents income), and so cannot be stored publicly on a blockchain. We store instead a hash of the information; the municipal government stores the actual data in a local database. With the hash public, a citizen can verify that the process really contains the data he has submitted. Similarly the appeals board, who must receive the actual data for the case from the municipality on a distinct, trusted channel, can similarly verify that the municipal government is forwarding the correct data.

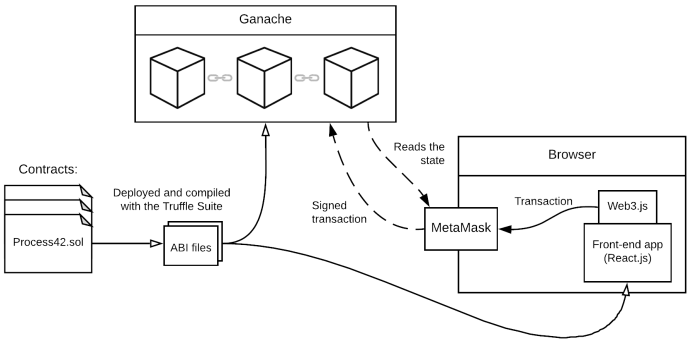

Fig. 5. Overview of communication with a local blockchain

In contrast to, e.g., [22], we do not decentralise *storage* of data: The municipal government and possibly the Appeals Board both retain—and have responsibility for—full local copies of the data involved in the case. The privacy of the citizen towards the municipal government is not an issue here: he has none[3].

Implementation. The system (Fig. 5) comprises *front-end* "React" webapps [16] for the citizen and the municipal caseworker, back-end smart contracts on the blockchain, and a local database for the municipal government. Each of actor (citizen, municipal caseworker, appeals board) interacts with the system through a web interface resembling contemporary case management systems in use at Syddjurs such as Acadre or the Open Case Manager. The *backend* consists of Ethereum contracts written in Solidity 0.5.0, deployed with Truffle [19]. The front-end application React [16] webapps uses the MetaMask [13] library to communicate with the blockchain. The prototype was deployed only on a local test chain. We expect deployment on the "real" Ethereum blockchain to be straightforward, even under the concomitant increased latency and cost.

4 Findings

So what have we learned from our implementation of the §42 process? First of all: *it is possible*. It was, at the outset, not obvious that confidentiality requirements could be met, nor that the complex mechanics of appeals and process rollbacks could be (easily) implemented; nor was it obvious that the formalisation of process execution rules in a smart contract would be helpful.

Pros. The implementation realises both the main envisioned benefits of (1) process transparency and verifiability by citizens and Appeals Board alike; and (2) that process execution is guaranteed to follows the steps set out in the law. This

[3] It is an interesting question whether government institutions ought to process cases *anonymously*, and how that might be arranged. We leave this for future work

key benefit was identified both by our municipal government partner and, implicitly, by the Appeals Board [1]. Moreover, (3) the implementation allows the Appeals Board to impose directions directly on the process rather than relying on a possibly intransigent municipal government to act against its own convictions. Finally, (4) assuming a generally accepted blockchain based currency accessible to the smart contract, direct payout from the contract may significantly decrease the municipal governments banking costs.

Cons. In societies like the Scandinavian countries, where government motivation (but perhaps not ability) is generally trusted by the public, correct process execution (2) could just as well be enforced by an ordinary (non-blockchain) computer system, operated by some central government authority.

Moreover, several additional concerns are apparent or were raised by our municipal government partner in the final evaluation. (A) On the blockchain, immutability cuts both ways [10,11]: once deployed, there is no mechanism for the municipal government to alter or fix a smart contract; and there is similarly no mechanism for the municipal government to fix its own (non-decision) processual mistakes. This point is especially acute if the contract has access to municipal government funds, and may disburse these independently. Moreover, (B) transaction latency and (C) transaction cost remain considerable concerns [21].

It is the estimation of our municipal government partner that because there is public trust in government institutions, (2) does not apply, and it is sufficient to implement better traditional IT systems; that savings from on-chain payouts are not realisable in the foreseeable future (4); and that latency costs (B) and transaction costs (C) already outweigh the remaining benefits of verifiability (1) and direct Appeals Board interventions (3).

Moreover, the loss of control of the parts of the process *for which it has responsibility* implicit in (A) is completely unacceptable. While concerns regarding latency and transaction costs can be addressed by permissioned blockchains [20], such blockchains also place control of the processes firmly back in the governments hands, obviating any reduction in trust. In addition, challenges regarding the updateability of running processes would remain. These challenges are general to the application of blockchain technologies in government: government institutions are in general responsible for both administering particular laws, and organising transitions when the law changes.

Thus we conclude this paper with a challenge to the community: It seems smart contract implementations of government processes needs on the one hand to be immutable and outside the governments control when running; however, they also need to be updatable when laws change, and have an "out" for the rare case when errors in the contract implementation result in unlawful behaviour. We propose these conflicting requirements as a foundational research challenge for blockchain to be applicable to governmental processes.

Acknowledgments We are indebted to Syddjurs Municipality, Denmark, for volunteering time and information without which this paper would not be. We are particularly grateful to Nicklas Pape Healy and Sofie Lykke Sørensen.

References

1. Ankestyrelsens praksisundersøgelse om tabt arbejdsfortjeneste efter servicelovens § 42. Investigation 978-87-7811-322-0, Ankestyrelsen (Jun 2017)
2. Borre, L.H., Krogsbøll, M.: Prototype implementation, `https://github.com/magkr/Smart-Contracts-for-Government-Processes-Implementation`
3. Buterin, V., et al.: A next-generation smart contract and decentralized application platform. white paper (2014)
4. García-Bañuelos, L., Ponomarev, A., Dumas, M., Weber, I.: Optimized execution of business processes on blockchain. In: Carmona, J., Engels, G., Kumar, A. (eds.) Business Process Management. pp. 130–146. Springer, Cham (2017)
5. Hou, H.: The application of blockchain technology in e-government in China. In: ICCCN '17. pp. 1–4 (July 2017)
6. Jun, M.: Blockchain government - a next form of infrastructure for the twenty-first century. Journal of Open Innovation: Technology, Market, and Complexity **4**(1), 7 (Feb 2018)
7. Bekendtgørelse af lov om social service (Aug 2017), Børne- og Socialministeriet
8. López-Pintado, O., García-Bañuelos, L., Dumas, M., Weber, I.: Caterpillar: A Blockchain-Based Business Process Management System. In: BPM Demo Track and BPM Dissertation Award, BPM 2017, September 13, 2017. (2017)
9. Madsen, M.F., Gaub, M., Høgnason, T., Kirkbro, M.E., Slaats, T., Debois, S.: Collaboration among adversaries: distributed workflow execution on a blockchain. In: 2018 Symposium on Foundations and Applications of Blockchain (2018)
10. Mavridou, A., Laszka, A.: Designing secure ethereum smart contracts: A finite state machine based approach. arXiv preprint arXiv:1711.09327 (2017)
11. Mavridou, A., Laszka, A., Stachtiari, E., Dubey, A.: Verisolid: Correct-by-design smart contracts for ethereum. arXiv preprint arXiv:1901.01292 (2019)
12. Mendling, J., Weber, I., Aalst, W.V.D., et. al.: Blockchains for business process management - challenges and opportunities. ACM Trans. Manage. Inf. Syst. **9**(1), 4:1–4:16 (Feb 2018)
13. MetaMask, `https://metamask.io/`
14. Nakamoto, S., et al.: Bitcoin: A peer-to-peer electronic cash system (2008)
15. Ølnes, S.: Beyond bitcoin enabling smart government using blockchain technology. In: Electronic Government. pp. 253–264. Springer International Publishing, Cham (2016)
16. React - A JavaScript library for building user interfaces, `https://reactjs.org/index.html`
17. Swan, M.: Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc." (2015)
18. Szabo, N.: Formalizing and securing relationships on public networks. First Monday **2**(9) (1997)
19. Truffle Suite | Sweet Tools for Smart Contracts, `https://truffleframework.com/`
20. Wüst, K., Gervais, A.: Do you need a blockchain? In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). pp. 45–54. IEEE (2018)
21. Wüst, K., Kostiainen, K., Capkun, V., Capkun, S.: Prcash: Fast, private and regulated transactions for digital currencies. In: International Conference on Financial Cryptography and Data Security (2019)
22. Zyskind, G., Nathan, O., et al.: Decentralizing privacy: Using blockchain to protect personal data. In: Security and Privacy Workshops. pp. 180–184. IEEE (2015)
23. Ølnes, S., Ubacht, J., Janssen, M.: Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Government Information Quarterly **34**(3), 355 – 364 (2017)