

Objectives

In recent years, blockchain's utility is being recognised through smart contracts - potentially a vital building block to realising open and transparent government activities. Employ the concept of smart contracts to government tendering activities.

- The proposed scheme is based on smart contracts, enabling a fair, transparent and independently verifiable (auditable) government tendering scheme.
- The scheme is then implemented on the Ethereum platform to evaluate the performance and financial cost implications, along with an evaluation of the potential security and auditability challenges.

Introduction

As society's values have shifted, so have expectations of government from the traditional model to something commonly referred to as 'open governance'. For the success of open governance initiatives, there are some technologies, such as the internet, that are crucial.

These technologies enable access to both the data and to engagement activities between citizens and government. There are also other technologies, like blockchain and smart contracts, which could be utilised to assist open governance.

A sound starting point would be moving from a system where information is tediously released by a government, on an 'as they please' basis, to an infrastructure where critical actions are captured with strong integrity, non-repudiation, and evidential guarantees.

An added dimension is the facilitation of these action records being made accessible to public scrutiny in near real-time.

In recent years, blockchain's utility is being recognised through smart contracts - potentially a vital building block to realising open and transparent government activities.

Smart Contract Tendering

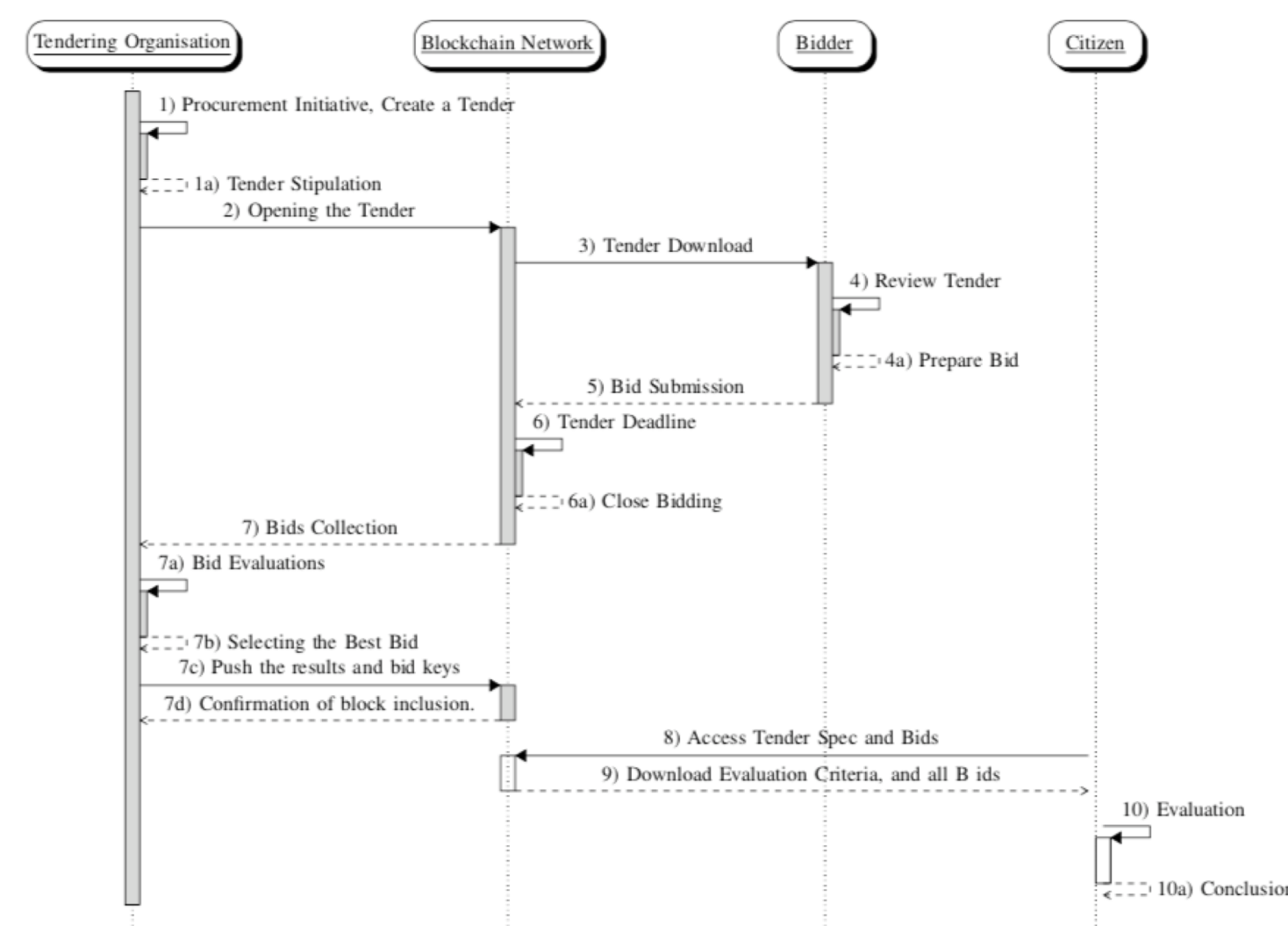


Fig. 1: Smart Contract Based Tendering Architecture

Implementation Results (Full Track Scheme)

Contract	Time (secs)	Cost (gas)
1	198.57	892160
2	88.86	892160
3	124.34	892160
4	96.52	892160
5	103.65	892160
6	174.69	892160
7	166.33	892160
8	137.11	892160
9	133.56	892160
10	253.98	892160
Average	147.761	892160

TABLE I: Full Track Scheme: Contract Deployment

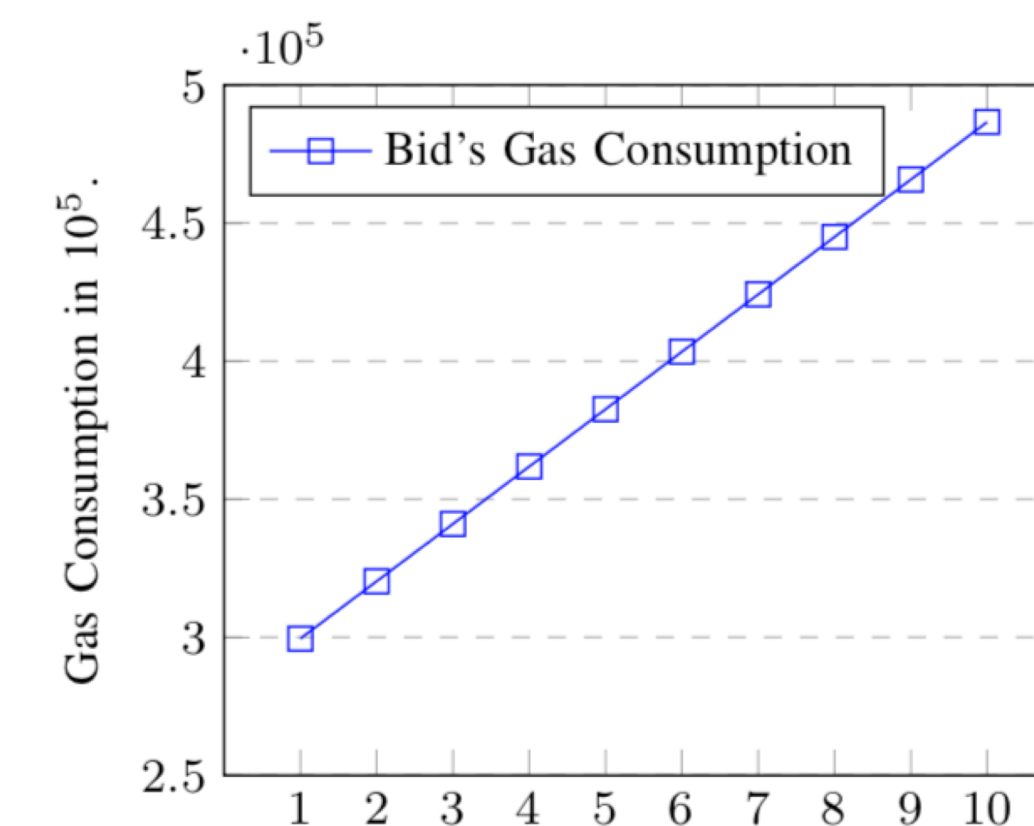


Fig. 2: Individual Bid's GAS usage (x 10⁵) for Full Track Scheme

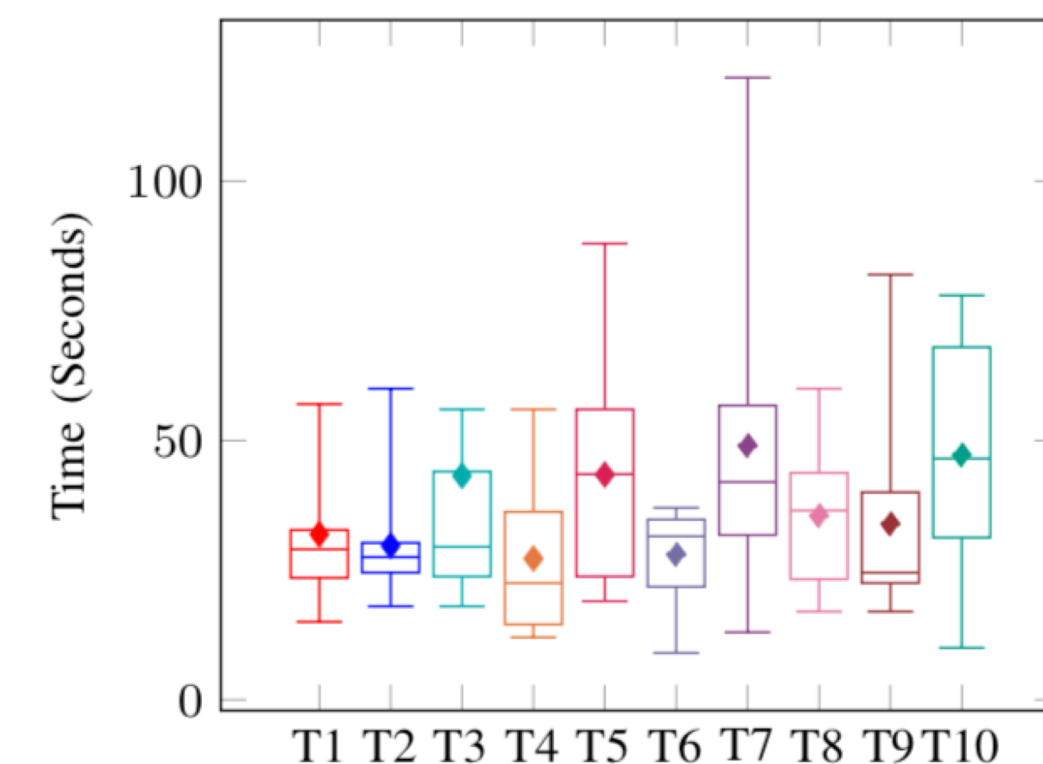


Fig. 3: Contract timing for Full Track Scheme Over Ten Trial Tenders

Important Contribution

Propose an secure and efficient blockchain and smart contracts based open governance framework that can facilitate citizens oversight on government functions that is easy to carry out with no associated financial costs.

Implementation Variants

Implemented three variants of the scheme:

- Full Track Scheme:
- Protected Scheme:
- Stateless Scheme:

Algorithm 1 Initiating A Tender

```

1: procedure REQFORTENDER(_length, _pubk, _limit)
2:   biddingEnd ← TimeNow() + _length
3:   limit ← _limit
4:   pubk ← _pubk

```

Algorithm 2 Placing A Bid (Full Track Scheme)

```

1: procedure PLACEBID(id, data, msgHashed, v, r, s,)
2:   bidValidity ← ValidBid(id, msgHashed, v, r, s)
3:   if bidValidity then
4:     bidCount[id] += 1
5:   bid ← new Bid(id, data, bidValidity, bidsPlaced, biddingEnd)
6:   bidsPlaced.add(bid)
7:   return bid
8: procedure VALIDBID(id, msgHashed, v, r, s,)
9:   validHash ← verify(msgHash, v, r, s)

```

Algorithm 2 Placing A Bid (Full Track Scheme)

```

10: validTime ← timeNow() < biddingEnd
11: allowedBid ← bidCount[id] < limit
12: return validHash and validTime and allowedBid
13: procedure BID(_id, _data, _validity, _bidsPlaced, _biddingEnd)
14:   id ← _id
15:   data ← _data
16:   validity ← _validity
17:   bidsPlaced ← _bidsPlaced
18:   biddingEnds ← _biddingEnd

```

Algorithm 3 Evaluating All Bids

```

1: procedure MAKEREQUEST(_length, _pubk, _limit) ▷ Running on the local machine
2:   listOfBids ← ReqBids()
3:   for bids in listOfBids do
4:     validBid ← bids.getValidity()
5:     if validBid then
6:       listValidBidDataAdresses.add(validBid.getDataAddress())
7: procedure REQBIDS(_length, _pubk, _limit) ▷ Running in the blockchain
8:   afterAuction ← timeNow() > biddingEnd
9:   if afterAuction then
10:    return bidsPlaced

```

Conclusion

With the increasing adoption of e-government and open government initiatives, public opinion is in favour of developing innovative solutions that can increase openness and transparency in government activities with minimum cost to citizens. For citizens to be involved in monitoring the governance activities, they need efficient tools and intuitive assessment that gives clear results. To build such an environment, blockchain and smart contracts show great potential. In this paper, the government tendering process is implemented in the blockchain environment to provide an open and fair tendering scheme. Based on the proposed architecture, we put forward three variants that were then implemented on Ethereum to show their applicability, Gas cost, and computational performance. The main objective of the paper was to show that the tendering scheme can be made fully open, autonomous, fair, and transparent using smart contracts. To this end, it was successful.

Contact Information

- Web: <https://scc.rhul.ac.uk/>
- Email: Freya.SheerHardwick.2016@live.rhul.ac.uk