Skimping on Gas

Reducing Ethereum Transaction Costs in a Blockchain Electricity Market Application

Taneli **Hukkinen**[1] – Juri **Mattila**[1,2] – Kari **Smolander**[1] – Timo **Seppälä**[1,2] – Tobias **Goodden**[3]

[1] Aalto University

[2] The Research Institute of the Finnish Economy (ETLA)

[3] Fortum Oyj

HICSS 52, Hawaii, U.S.

January 11, 2019

Conclusions

- We **explored ways to analyze and improve the feasibility of an experimental distributed blockchain market application** designed for conducting microtransactions of electricity in a nanogrid environment [2]. By applying the design science research methodology by Peffers et al. [1], we managed to pinpoint inefficiencies in the design of the smart contract and to **reduce its gas consumption by 11 %**.

- We formulated **a set of general guidelines suitable for optimizing the efficiency of any Ethereum-based smart contract.**

- While the improvement achieved in efficiency was **not adequate for economic feasibility** on the public Ethereum blockchain, we established that further improvements are likely to be possible with more radical reformations to the source code, redefined market mechanics, and the use of an alternative deployment environment.

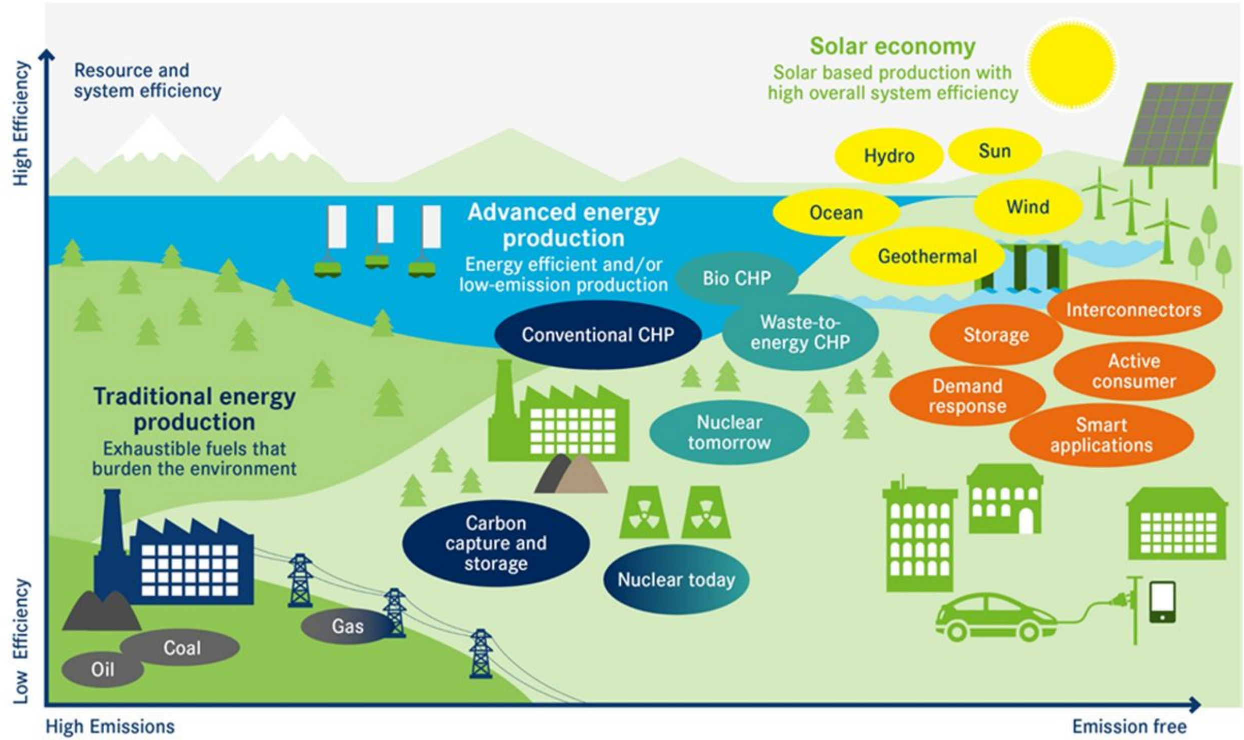
- Further research is encouraged on the recognized improvement opportunities where additional efficiency gains could be achieved. We also invite the exploration of other new ways to improve the efficiency of Ethereum-based smart contracts.

[1] K. Peffers, T. Tuunanen, M.A. Rothenberger, A Design Science Research Methodology for Information Systems Research, J. Manag. Inf. Syst. 24, 2007, pp. 45–77.
[2] T. Hukkinen, J. Mattila, J. Ilomäki, T. Seppälä, A Blockchain Application in Energy, ETLA Reports No. 71, 2017.

Research Background

Research collaboration with Fortum Oyj (*2016-2018)*

- *Use case conceptualization*
- *Proof of concept mock-up demo*
- *Smart contract application development*
- *Smart contract optimization*



Theoretical Background

ETLA

- The efficiency of information systems and business computing applications has not received wide attention in research lately. Ever since the 1980s, **IT systems have not been mainly evaluated by their operating costs**, but rather by their enhanced market access, product differentiation, strategic benefit and competitive advantage [1]. The systems have been largely perceived as investments with long-term effects and benefits [2], across their whole lifecycle [3] and most often emphasizing infrastructures, human resources and IT-enabled intangibles [4].

- Recently it has become increasingly popular to provide applications via decentralized blockchain smart contracts, governed by algorithmic incentives [5]. As the computational resources of these blockchain networks are allocated and priced according to free market mechanics [6,7], **resource-efficiency and cost-optimization are placed in the center of blockchain application development.**

[1] B. Ives, G.P. Learmonth, The information system as a competitive weapon, Commun. ACM. 27, 1984, pp. 1193–1201.
[2] P. Weill, The Relationship Between Investment in Information Technology and Firm Performance: A Study of the Valve Manufacturing Sector, Inf. Syst. Res. 3, 1992, pp. 307–333.
[3] D.G. Woodward, Life cycle costing—Theory, information acquisition and application, Int. J. Proj. Manag. 15, 1997, pp. 335–344.
[4] A.S. Bharadwaj, A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation, MIS Q. 24, 2000, pp. 169–196.
[5] G. Wood, Ethereum: A Secure Decentralised Generalised Transaction Ledger, 2013.
[6] C. Catalini, J. Gans, Some Simple Economics of the Blockchain, MIT Sloan Research Paper 5191-16, 2016.
[7] J.A. Kroll, I.C. Davey, E.W. Felten, The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries, in: Proc. WEIS, 2013: pp. 1–21.

Blockchain & Smart Contracts

- Blockchain technology enables the creation of **decentralized, distributed and replicated digital ledgers**. The technology itself consists of components such as peer-to-peer networking, public-key cryptography, digital tokens, a decentralized consensus algorithm and a tamper-resistant chain of blocks used to store database modifications [1,2].

- While cumbersome and often more expensive to operate than centralized systems, blockchain networks can be useful due to their **tamper-resistant** and **non-hierarchical** quality. Built on public open-source protocols, they can also help foster the growth of digital ecosystems with a bottom-up approach different from conventional centralized platforms.
- For this paper, we define smart contracts as digital programs that:
  - a) are written in computer code and formulated using programming languages
  - b) are collectively stored, executed and enforced by a distributed blockchain network
  - c) can receive, store, and transfer digital assets of value
  - d) can execute with varying outcome

[1] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
[2] D. Tapscott, A. Tapscott, Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world, Penguin, 2016.

Ethereum & Gas

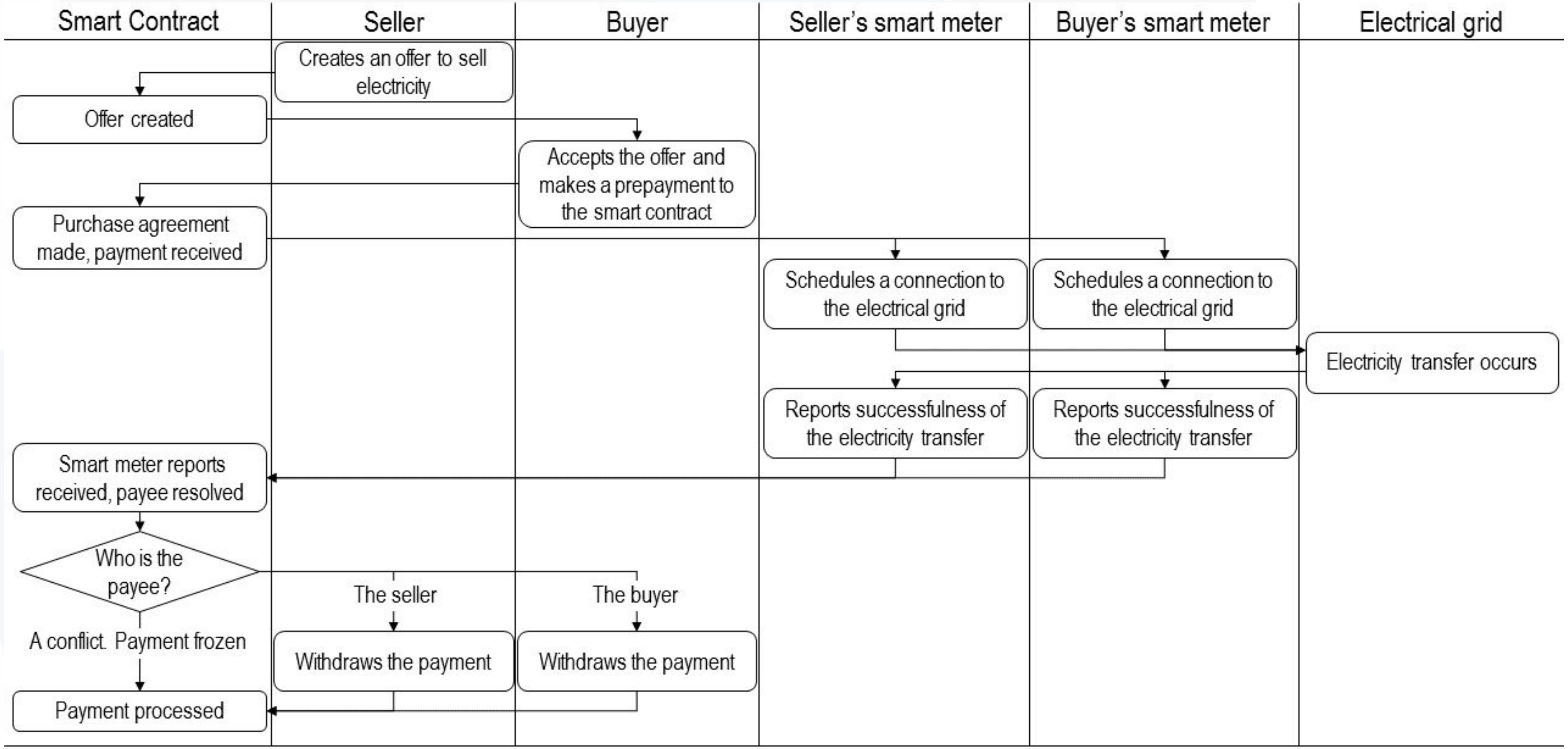
- Ethereum is a smart contract platform which offers a Turing-complete programming language for writing smart contracts and allows the deployment of smart contracts into its blockchain [1].

- Ethereum uses the concept of “gas” to quantize the finite resources of the network. Each block may only use up to *n* amount of gas (on January 11, 2019 around 8 million).

- Ethereum utilizes a transaction fee system to prevent denial-of-service attacks and to incentivize efficient smart contract deployment. A transaction fee—or gas consumption—is determined by the amount of computational work, network bandwidth and storage space the transaction consumes [1].

[1] V. Buterin, Ethereum White Paper - A Next Generation Smart Contract and Decentralized Application Platform, 2013.

Electricity Market Smart Contract



Research Problem

- In the absence of a centralized authority, blockchain networks can consume vast amounts of electricity to maintain consensus [1]. The Ethereum smart contract platform has been estimated to consume more electricity than the country of Iceland, constituting approximately 1/1000th of the world's electricity consumption in total [2].

- Advancing the understanding and **developing best practices in the optimization of blockchain-based smart contracts** is important to ensure that the maximum innovation output and utility is achieved in return for the vast energy consumption of such systems and their strain on the environment at large [3]. While some theoretical research has focused on embedded costs [4] and institutional changes [5] of blockchain, so far there has been little in the way of formal research into the optimization of blockchain-based smart contracts.

- The **blockchain electricity market application** [6] **is not economically feasible** on the public Ethereum blockchain

[1] J.A. Kroll, I.C. Davey, E.W. Felten, The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries, in: Proc. WEIS, 2013: pp. 1–21.
[2] Digiconomist, Bitcoin Energy Consumption Index, 2018.
[3] S. Murugesan, Harnessing Green IT: Principles and Practices, IT Prof. 10, 2008, pp. 24–33.
[4] D. Easley, M. O'Hara, S. Basu, From mining to markets: The evolution of bitcoin transaction fees, 2017.
[5] S. Davidson, P. De Filippi, J. Potts, Economics of blockchain, 2016.
[6] T. Hukkinen, J. Mattila, J. Ilomäki, T. Seppälä, A Blockchain Application in Energy, ETLA Reports No. 71, 2017.

Analytical Framework

- **Design science research methodology** by Peffers et al. [1] **was applied to the electricity market smart contract**. Design science is a suitable research approach when an innovative, purposeful artifact is created and evaluated for a special problem domain [2].

- The methodology consists of a process model involving six activities:
  - 1) problem identification and motivation
  - 2) defining the objectives for a solution
  - 3) design and development
  - 4) demonstration
  - 5) evaluation
  - 6) communication.

[1] K. Peffers, T. Tuunanen, M.A. Rothenberger, A Design Science Research Methodology for Information Systems Research, J. Manag. Inf. Syst. 24, 2007, pp. 45–77.
[2] A.R. Hevner, S.T. March, J. Park, S. Ram, Design Science in Information Systems Research, MIS Q. 28, 2004, pp. 75–105.

Optimization principles

1) Avoid a design pattern where many new smart contracts need to be deployed, for instance, on a per-user basis. At a cost of 32 000 gas, contract creation is the most expensive EVM operation.

2) **Keep the amount of transactions needed to interact with the smart contract low to diminish the impact of the transaction base fee of 21 000 gas. Design an interface with fewer functions that do more actions, rather than more functions that do fewer actions.**

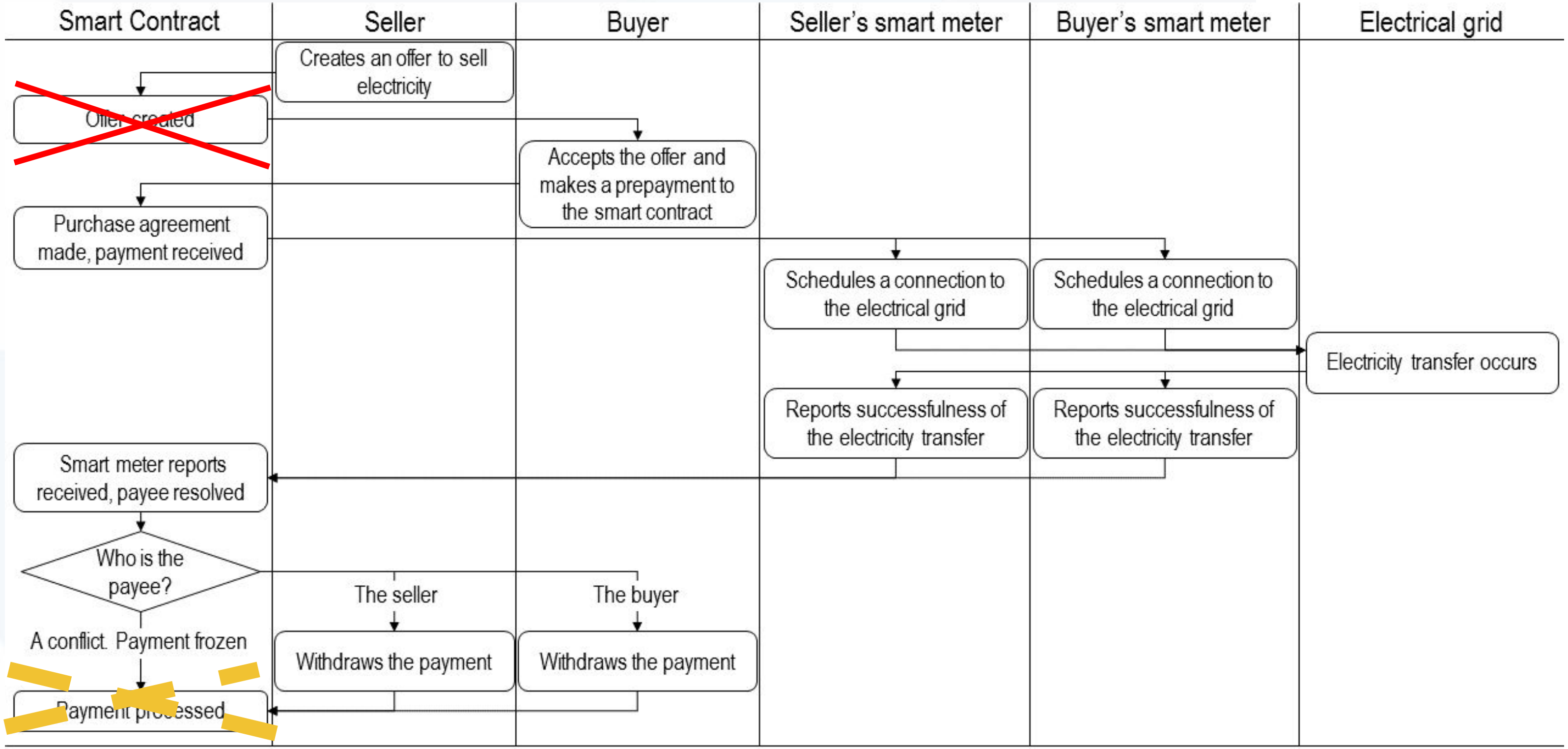
3) Optimize the smart contract's use of storage space. Whenever possible, use memory instead of persistent storage. Storing a word in persistent storage costs 20 000 gas, whereas storing a word in memory only costs 3 gas plus a memory expansion fee, whenever more memory is required. The memory expansion fee scales quadratically as more memory is needed, so memory should be used densely.

4) When the use of persistent storage is necessary, consider if the stored data could be replaced with its cryptographic hash on-chain, and the data itself could be stored off-chain.

5) Delete contracts and data stored in persistent storage that are not needed, in order to gain gas refunds.

6) **Make use of off-chain transactions, using the blockchain only as an arbiter in case disputes happen.**

Optimizations



Results

Table 2. Reference measurements from the original electricity market smart contract.

Amount of trades (n)	Gas consumed
1	400 318
2	787 210
3	1 175 676
4	1 565 716
5	1 957 330
6	2 350 518
7	2 745 280
8	3 141 616
16	6 368 968
32	13 125 496
64	27 848 152
128	62 128 792

Table 3. Measurements from Artifact 1 that has off-chain offers implemented.

Amount of trades (n)	Gas consumed	Difference to reference (%)	Difference to reference (gas)
1	379 534	-5.19	-20784
2	745 578	-5.29	-20816
3	1 113 260	-5.31	-20805
4	1 482 516	-5.31	-20800
5	1 853 346	-5.31	-20797
6	2 225 750	-5.31	-20795
7	2 599 728	-5.30	-20793
8	2 975 280	-5.29	-20792
16	6 036 168	-5.23	-20800
32	12 459 832	-5.07	-20802
64	26 517 208	-4.78	-20796
128	59 466 520	-4.29	-20799

Table 4. Measurements from Artifact 2 that implements the renewed withdraw function.

Amount of trades (n)	Gas consumed	Difference to reference (%)	Difference to reference (gas)
1	402 564	+0.56	2246
2	762 007	-3.20	-12602
3	1 123 024	-4.48	-17551
4	1 485 615	-5.12	-20025
5	1 849 780	-5.49	-21510
6	2 215 519	-5.74	-22500
7	2 582 832	-5.92	-23207
8	2 951 719	-6.04	-23737
16	5 959 480	-6.43	-25593
32	12 276 826	-6.47	-26521
64	26 121 121	-6.20	-26985
128	58 645 051	-5.61	-27217

Table 5. Measurements from Artifact 3, off-chain offers and renewed withdraw function.

Amount of trades (n)	Gas consumed	Difference to reference (%)	Difference to reference (gas)
1	381 780	-4.63	-18538
2	720 397	-8.49	-33407
3	1 060 652	-9.78	-38341
4	1 402 481	-10.43	-40809
5	1 745 884	-10.80	-42289
6	2 090 861	-11.05	-43276
7	2 437 412	-11.21	-43981
8	2 785 537	-11.33	-44510
16	5 627 010	-11.65	-46372
32	11 611 844	-11.53	-47302
64	24 791 563	-10.98	-47759
128	55 985 573	-9.89	-47994

Conclusions

- We **explored ways to analyze and improve the feasibility of an experimental distributed blockchain market application** designed for conducting microtransactions of electricity in a nanogrid environment [2]. By applying the design science research methodology by Peffers et al. [1], we managed to pinpoint inefficiencies in the design of the smart contract and to **reduce its gas consumption by 11 %**.

- We formulated **a set of general guidelines suitable for optimizing the efficiency of any Ethereum-based smart contract.**

- While the improvement achieved in efficiency was **not adequate for economic feasibility** on the public Ethereum blockchain, we established that further improvements are likely to be possible with more radical reformations to the source code, redefined market mechanics, and the use of an alternative deployment environment.

- Further research is encouraged on the recognized improvement opportunities where additional efficiency gains could be achieved. We also invite the exploration of other new ways to improve the efficiency of Ethereum-based smart contracts.

[1] K. Peffers, T. Tuunanen, M.A. Rothenberger, A Design Science Research Methodology for Information Systems Research, J. Manag. Inf. Syst. 24, 2007, pp. 45–77.
[2] T. Hukkinen, J. Mattila, J. Ilomäki, T. Seppälä, A Blockchain Application in Energy, ETLA Reports No. 71, 2017.

Questions?

Comments, remarks & discussion are welcome:

Taneli Hukkinen
hukkinen@iki.fi
+358 50 596 4990

Juri Mattila
juri.mattila@etla.fi
+358 43 825 8238