

Energy Online

J. Shah, M. Jordi, M. Stemmle, S. Oeschger, S. Zemljic

March 6, 2018

Contents

1	Introduction	1
1.1	Context	1
1.2	Background	1
1.3	Problem Statement	3
2	Literature Review	4
3	Conceptual Model	5
3.1	Overview	5
3.2	Decentralized Autonomous Organization DAO	7
3.3	Characteristics and functionalities of our proposed DAO	10
3.3.1	Energy Management	10
3.3.2	Trading at the energy market	10
3.3.3	Profit distribution	11
3.3.4	Energy Token	11
3.4	Initialization of the Concept	12
3.5	Disruption Potential	12
3.6	Evaluation	13
3.7	Uncertainties, disadvantages and risks	13
4	Solution Design	14
4.1	Idea	15
4.2	Our Model Implementation	15
4.2.1	Wallet	15
4.3	Model Scenario	16
4.4	Problems and Possible Solutions	16
5	Conclusion/Outlook - Michael S. - around 600 words	17

1 Introduction

1.1 Context

The BIOTS program exists to push education for innovative new technologies into universities to help Switzerland to become one of the leading hubs in Blockchain and "internet of things" (IoT) space.¹

Since 2016, every year the BIOTS program offers three major verticals for the students to build their ideas and use-cases. In 2018, the focus was on sustainability issues, which are currently on the agenda of the UN or hot topics in industry. Challenges from the sponsors Elektrizitätswerk der Stadt Zürich (EWZ), UBS Group AG (UBS), the European founded project FuturICT 2.0 (<https://futuraict2.eu>) across the following verticals were presented and solved in the program:



Figure 1: Major verticals of BIOTS 2018, <http://biots.org/the-bioticsphere/>

This report was created as a result of the challenge 3 "virtual energy storage" from EWZ.

1.2 Background

In a cantonal vote 2017 it has been decided, that EWZ needs to sell all its holding in the nuclear sites of Gösgen and Leibstadt until 2034. In addition, EWZ will not be allowed to obtain nuclear energy anymore as well.²

¹<http://biots.org/about/>

²<https://www.nzz.ch/zuerich/aktuell/abstimmungssonntag-zuerich-atomausstieg-zuerich-ld.130738>

In 2016 32.8% of the electricity in Switzerland is provided by nuclear power plants.³ To be able to cover those losses, massive investments into renewable energy are needed. Large power plants alone will not be enough to cover the demands, thus small-scale energy production, like private PV's will play a huge role.

Currently, the entry barriers for the installation of PV are high, battery storage for surplus energy is expensive and overall incentives are missing. For example, energy surplus from private power plants (mainly PV) can only be sold to local energy provider for a very low price of 8.50 Rp./kWh (high tariff) or 4.45 Rp./kWh (low tariff).⁴ To encourage the installation of PV, promotional money is lacking.⁵

To reach the goal of 0% nuclear energy it is important to make private power plants more lucrative. Therefore, the challenge 3 of EWZ deals with the topic "Virtual Energy Storage". Virtual Energy Storage allows private household to store their surplus energy virtually and withdraw it later when needed.

This concept has been already adapted Companies like eOn or SENEK already offer services like this to their customers:

eOn (<https://www.eon-solar.de/eon-solarcloud>)

- Service Name: E.ON SolarCloud
- Value Proposition: Genießen Sie jetzt Ihre Sonnenenergie 365 Tage, und Nächte
- Value Chain: E.ON -> End customer
- Revenue Model: Monthly Fee
- Customer Segment: Private Households with PV installations

Senec-ies (<https://www.senec-ies.com/tarife-services/senec-cloud/>)

- Service Name: SENEK.Cloud 2.0
- Value Proposition: Strom im Sommer einfrieren und im Winter wieder auftauen.

³Source: Schweizerische Elektrizitätsstatistik 2016, p. 5: http://www.bfe.admin.ch/php/modules/publikationen/stream.php?extlang=de&name=de_306571764.pdf

⁴Source: <https://www.ewz.ch/content/dam/ewz/services/dokumentencenter/energie-produzieren/dokumente/verguetung-stromruecklieferung-zh-2016-18.pdf>

⁵<https://www.srf.ch/news/schweiz/abstellgleis-solarenergie-wer-foerdergelder-will-muss-jahre-warten>

- Value Chain: SENEK -> End customer
- Revenue Model: Monthly Fee
- Customer Segment: Private Households with PV installations

Due to the companies and customers are trusted parties in those two services offerings, the necessity of the blockchain technology is not given. According to Karl Wüst and Arthur Gervais, “Blockchain is being praised as a technological innovation which allows to revolutionize how society trades and interacts. This reputation is in particular attributable to its properties of allowing mutually mistrusting entities to exchange financial value and interact without relying on a trusted third party. A blockchain moreover provides an integrity protected data storage and allows to provide process transparency.”⁶

1.3 Problem Statement

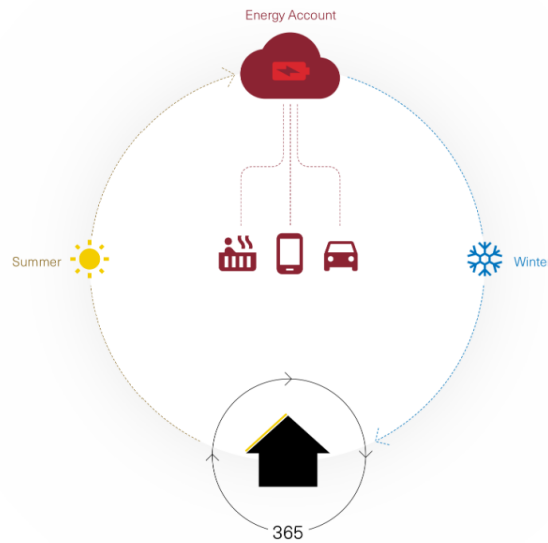


Figure 2: EWZ Challenge 3 - "Virtual Energy Storage", Source: BIOTS_ewz_challenges.pdf

The problem statement given by the EWZ Challenge 3 "Virtual Energy Storage" is: "How might the blockchain technology help to develop a reliable and highly efficient

⁶ "Do you need a Blockchain?", Karl Wüst, Arthur Gervais, <https://eprint.iacr.org/2017/375.pdf>

virtual energy solution that gives anyone the possibility to produce, store and use his/her own energy anywhere and anytime? ”⁷

2 Literature Review

The term ‘Blockchain technology’ refers to distributed databases with consensus algorithms that contain cryptographically concatenated data structure on which applications are built. The disruptive element is the ability to maintain a database that is shared in which everyone has access to all of the data however no one party has the ability to take over total control or perform modifications. Blockchain is essential when trust needs to be established without a central authority and value needs to be transferred between stakeholders.

We find that for EWZ, being the central authority, which establishes trust, having a blockchain is not essential for storing virtual energy from users that produce sustainable energy. EWZ should use a business model like the one used by eon to store solar/wind energy produced by charging the producers a fixed rate and sell the energy for a profit. However, we see that blockchain has a potential application in the heavily regulated power industry (eg. certificates) when both utilities and consumers will produce and sell electricity. Blockchain could in that case offer a reliable, low-cost way for financial or operational transactions to be recorded and validated across a distributed network with no central point of authority.

Since sustainability has been ranking higher than ever before on the global agenda of companies and governments alike, there have been considerable research and development on renewable sources of energy. The energy system will become more decentralized and versatile wind turbine parks and household solar panels are a growing trend in the generation of electricity and primary energy in general. This transition towards renewable energy means that energy production will become unpredictable and intermittent due to weather dependency associated with solar and wind energy, and hence requires long/short term demand-supply balancing.

The idea is that by creating a distributed marketplace powered by employing a blockchain consensus Blockchain technology could offer a solution by providing a neutral ground where all the parties can operate on a shared platform, on completely equal

⁷ “BIOTS_ewz_challenges.pdf”

footing. Instead of the platform provider like EWZ, BKW being the dominant player to the power of whom all others must submit, blockchain technology could enable all the participants to produce a platform together in a distributed manner, without having to trust each other in almost any capacity. Some earlier use case concepts have been drafted which focus on allocating distributed renewable energy resources between neighboring households using blockchain technology. For example, in New York state, neighbors are testing their ability to sell solar energy to one another using blockchain technology (Brooklyn-microgrid). In Austria, the country's largest utility conglomerate, Wien Energie, is taking part in a blockchain trial focused on energy trading with two other utilities. Meanwhile in Germany, the power company Innogy is running a pilot to see if blockchain technology can authenticate and manage the billing process for autonomous electric-vehicle charging stations. Another example is PriWatt, which is a token based energy trading system that allows to trade energy in a peer-to-peer network without a central price signal. The prosumer uses photo-voltaic panels harvests solar energy and makes profit by selling the generated energy surplus to the other smartgrid consumers. In a conventional power grid, energy prices are determined by a central authority like EWZ, BKW. In a smartgrid, agents are allowed to negotiate energy prices, hence creating a dynamic market of energy trade. Such a market-based energy trade decreases dependency of agents on a central energy provider, as energy supply and demand are matched directly between individual agents, resulting in a more decentralized and competitive environment. PriWatt satisfies this requirement and enables peers to anonymously negotiate energy price and securely perform trading transaction.

In our opinion although we might think that blockchain may at first appear to be a form of technological disruption that the power industry should avoid, it could prove to be the solution that is required to keep up with evolving demand for electricity. Established utilities like EWZ are best placed to evaluate and make strategic bets on blockchain technology's potential applications. If EWZ can seize the moment, they may turn out to be the true disruptors, and usher in a new era of decentralized power.

3 Conceptual Model

3.1 Overview

Our approach to the EWZ Challenge 3 "Virtual Energy Storage" is to create a Decentralized Autonomous Organization (DAO).

The DAO is not a potential future business model applicable for EWZ but demonstrates how the blockchain is in position to change the energy sector and illustrates the disruptive power due to the emerging areas of blockchain applications. However, our approach provides a "Virtual Energy Storage" of the participants of the DAO. In addition, we further address with the DAO an alternative for owners of real estate to the modest of governmental incentives to become a producer of renewable energy. With implementing such or a similar alternative blockchain based approach, it could be a way out of a potential electricity shortage due to the governmental regulation regarding the end of the production of electricity from nuclear sources in Switzerland by 2034. In this respect, the following DAO can be described as a catalyst of renewables.

In the real world exists initiatives such as Brooklyn Microgrid that enables residents of the Park Slope area of Brooklyn, NY to sell power generated from rooftop solar panels via a microgrid enabled by a blockchain ledger that records every transaction made with a local utility.⁸ The DAO brings such an initiative a step further.

The DAO's behaviour is completely controlled by smart contracts and it fulfils functions similar to the ones of an energy provider today:

- Energy Management: The DAO makes sure that there is sufficient energy available for all the participants of the systems and enables all parties to trade energy freely by using the energy token.
- Trading at the energy market: The DAO sells surplus energy and buys energy if there is a shortage in the network on the traditional energy market.
- Profit distribution: The DAO uses profits realized by trading to subsidize others to install renewable energy production possibilities and participate in the system. This enlarges the current system and creates additional surplus.

Within the DAO, energy is traded freely amongst all participants by using energy tokens. Energy tokens represent the right to obtain energy from a participant of the system.

For other energy providers, the DAO can act as a virtual power plant which generates renewable energy. Due to the energy would be generated within Switzerland, the cost and lost of transportation would be lower compared to the purchase of energy abroad.

⁸www.brooklynmicrogrid.com

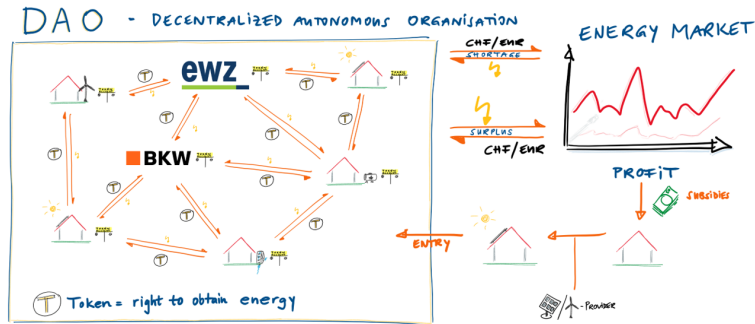


Figure 3: Conceptual Design, Source: this report

With this concept, the monopolistic Swiss energy market could be disrupted massively. Electricity could be freely traded peer to peer. The limitations through cantonal borders, would fall away, even trade across national borders could be possible at a later point. Current energy providers would take the role of a hardware provider, ensuring the maintenance of the energy grid and maybe the smart meters financed through fees for the usage of the infrastructure.

3.2 Decentralized Autonomous Organization DAO

According to CHOCHAN, a DAO, is an organization that is run through rules encoded as computer programs called “smart contracts”. A DAO’s financial transaction record and programmed rules are maintained on a blockchain, which ostensibly increases transparency dramatically at the expense of security.⁹

A DAO is, according to SWAN, a potential progression to increasingly complex and automated smart contracts that become more like self-contained entity, conducting pre-programmed and eventually self-programmed operations linked to a blockchain.¹⁰

VITALIK BUTERIN, the visionary founder of Ethereum¹¹ sees three major categories where decentralized autonomous organizations may provide genuine value to society. First, when there are natural monopolies. Second, when there are services that violate government laws and regulations (e.g. the use of decentralized file-sharing networks for copyright infringement) and, finally, there are those cases where a decentralized network

⁹“The Decentralized Autonomous Organization and Governance Issues”, Usman W. Chohan, December 4, 2017.

¹⁰“Blockchain – Blueprint for a New Economy”, Melanie Swan, 2015, O’Reilly Media, Inc.

¹¹<https://www.ethereum.org/>

can simply maintain itself more efficiently and provides better services than any centralized alternative (i.e. peer-to-peer network).¹² The DAO, according to BUTERIN, human managerial interactivity, provided the smart contracts were supported by a Turing complete platform.¹³

In essence a DAO is a system of hard coded rules that define which actions an organization will take, so the organization may run without managerial supervision or, if the platform provided sufficient rules and flexibility, completely autonomous. All rules upon which the company functions are enforced digitally.¹⁴ "Other decisions are made by shareholders who control a certain amount of the tokens, or smart contracts, who can vote for decisions. Preprogrammed rules describe what can happen in the system. Certain rules are hard-coded into the company like the amount of dividend payouts or determining a certain event in the company. Other things like, determining which project will receive money is decided by letting all token holders cast their vote."¹⁵

There exist real world DAO projects such as for example, "Dash", "The DAO", "Digix.global", "Steemit". So far, DAOs can be found mainly in the FinTech sector, where they can benefit from a sophisticated organizational structure and the resulting rapid decision-making processes in a volatile and fast-moving market.

A DAO must be able to make decisions, be liquid and communicate with internal and external bodies. After all, money must get into the organization, employees and service providers must be remunerated and interaction with the rest of the world must be possible. As a result, several components are required which are essential for a DAO:¹⁶¹⁷

- Autonomy:

Once deployed the entity is independent of its creators and cannot be influenced

¹²"Bootstrapping a Decentralized Autonomous Corporation", Vitalik Buterin, September 24, 2013.

¹³Decentralized autonomous organization, https://en.wikipedia.org/wiki/Decentralized_autonomous_organization, retrieved February 25, 2018.

¹⁴Decentralized autonomous organization - What is a DAO company?, <https://medium.com/universablockchain/decentralized-autonomous-organization-what-is-a-dao-company-eb99e472f23e>, retrieved February 25, 2018.

¹⁵Decentralized autonomous organization - What is a DAO company?, <https://medium.com/universablockchain/decentralized-autonomous-organization-what-is-a-dao-company-eb99e472f23e>, retrieved February 25, 2018.

¹⁶What is a DAO?, <https://blockchainhub.net/dao-decentralized-autonomous-organization>, retrieved February 25, 2018.

¹⁷Decentralized Autonomous Organization – Organisationen auf der Blockchain, Jonas Verhoelen, <https://blog.codecentric.de/2017/08/decentralized-autonomous-organization-blockchain>, retrieved February 25, 2018.

by outside forces. DAOs are open source, thus transparent and incorruptible. A DAO's financial transaction record and program rules are maintained on a blockchain. This approach eliminates the need to involve a bilaterally accepted trusted third party in a financial transaction.

- Currency / Tokens:

In order not to bind the organization to a central currency, the DAO's ecosystem should have its own currency, also known as "tokens". This is used for payment, external investments and finally the accumulation of wealth within the organization. As a result, the DAO is at least internally liquid. Of course, financial interactions with the outside world take place via a change point. An indirect point of contact with traditional centralized Fiat money such as the dollar or the euro thus seems to be unavoidable so far.

- Contractors:

Members of the organization can have an influence on the development of the organization and can also be involved in the implementation of the adopted proposals. However, a DAO cannot build a product, write code or develop hardware. It needs a contractor or external service providers to accomplish its goals. Such Contractors get appointed via voting of token holders and payment can be made either in the own currency or by partial liquidation in Fiat currencies.

- Proposals and Voting:

Decisions about the future of the organization must be made before it can develop further. Proposals are the primary way for making decisions in a DAO. Proposals may be raised by any member of the organization (or a specific role in the organization). To avoid people overloading the network with proposals, a DAO could require a monetary deposit to prevent people from spamming the network. After submitting a proposal, voting takes place.

- Consensus:

In order to withdraw or move funds from a DAO, a majority of its stakeholders (this percentage could be specified in the code of the DAO) must agree on the decision. Even if bugs are found in the code, they could not be corrected until a voting procedure has taken place and the majority of voters agreed on it, which could leave known security holes open to exploitation.

- Transparency:

All processes and mechanisms must be fully transparent to members of the orga-

nization. Everyone should be able to participate and work together. By recording all aspects and processes on the blockchain, this is also possible and manipulation is made theoretically impossible.

3.3 Characteristics and functionalities of our proposed DAO

3.3.1 Energy Management

As a precondition to be part of the system, every participant in the DAO is a user or a provider of renewable energy via wind, solar or hydropower. Such a participant is called "prosumer". The different participants such as real estate owners with solar panels or power suppliers such as EWZ with access to renewable energy provide electricity that flows into the system's grid. Electricity consumers are the producing or other households or companies of the area of the DAO. The DAO interconnects prosumers and/or provide a direct link between energy suppliers and energy consumers.

All electricity produced and consumed by a household is tracked by a smart electric meter that is connected to a virtual energy balance sheet. A Household may use its electricity produced by its own energy production facility or feed the power to the system, if it has a surplus. The household receives Tokens for a certain amount of electricity produced and it gives Tokens, if it does not produce enough own electricity, when it receives power of another energy provider's surplus. In case a household has consumed all its Tokens (e.g. uses more energy during night then it can produce during the day) and the virtual balance sheet shows a negative balance, it may buy energy Tokens from the DAO or a system participant with Fiat currency.

If the DAO's energy system provides an energy surplus the surplus may be traded on the energy market or in case of the system's energy shortage additional energy is purchased.

3.3.2 Trading at the energy market

The DAO's financial transaction, how energy surplus is traded and how energy shortfall is covered, is predefined in programmed rules and defined by smart contracts. This approach eliminates the need to involve a bilaterally accepted trusted third party in the financial transaction. In addition, the DOA acts fully rational and is not biased by external conditions.

If the DAO may sell its electricity surplus, e.g. when during sunny daytime the member's solar PV panels produce an electricity excess, the DAO may achieve high prices, since during daytime also electricity prices are highest.

Because the electricity exchange will not accept the tokens of the system, all financial transactions by or with the DAO are made with Fiat money (e.g. CHF, EUR).

3.3.3 Profit distribution

If the system's energy surplus is bigger than the energy bought during an electricity shortage and the DAO's smart contracts are well established so that it sells the green energy to the highest prices possible, the DAO's trading activity will produce a profit. With the profit made from trading, the DAO pays subsidies to more households, companies or other renewable energy projects to build renewable power plants and thus enlarging its network.

All processes and mechanisms must be fully transparent to members of the organization. According to the DAO's governance structure and the underlying smart contracts, the DAO's members or specific roles in the organization may vote how the profit is spent. Also other important developments of the DAO need to be voted about or created consensus among the members with voting power. The members of the organization may have an influence in e.g. what share of the profit is hold reserved for electricity shortage or which share of the profit should be allocated in the form of subsidies to which type of projects (e. g. wind, water, solar energy, etc.) to make the network and its independence even stronger. A balanced network of energy suppliers (e. g. solar, water and wind power plants) can bridge the shortfall of electricity at night or in winter, which must be taken into account in investment projects in order to be as autonomous as possible and generate maximum profit.

3.3.4 Energy Token

The DAO's ecosystem issues its own currency in form of Tokens. A Token holder has the right to obtain specified energy from the system in return of a specified number of Tokens or the receives Tokens in exchange of providing energy to the grid. Depending on the day or night tariff, the "electricity price" paid in tokens also changes within the DAO network.

Therefore, insofar as an electricity producer has the opportunity to regulate the amount of electricity that can be supplied to the system (e. g. electricity production by hydroelectric power plants at peak times or in times of little sunshine), an incentive arises to build such adaptive power plants and/or produce electricity, when prices are highest and the most Tokens can be generated.

3.4 Initialization of the Concept

At the beginning, there will be an "Initial Coin Offering" (ICO), to get the initial funds for the DAO and to distribute the Tokens. This process would give the DAO its starting capital to start investing in renewable energy, and then trade on the energy stock market. A major part of the Tokens will be sold to investors and given to energy producers. A smaller part could be distributed for example to core developers or held back as reserves. Only producers of renewable energy are allowed to participate in the ICO.

3.5 Disruption Potential

The underlying transaction model of the blockchain technology lead to a decentralized system, where energy producer and end customers or energy companies can directly start to trade. Third party intermediaries are no longer needed, if the transaction may be carried out peer-to-peer, regardless of territorial borders such as cantonal or municipal boundaries and (unless regulated) also in circumvention of a sovereign monopoly. This ensures that existing power generation capacity is utilized optimally, whilst energy is made available at the best price. And since the system's tasks are carried out automatically through smart contracts, this cuts costs and speeds up processes. The role of prosumers is strengthened considerably under such a model.¹⁸

Due to the rational acting and maximal efficiency the DAO acts as a very efficient self-growing system. In addition, based on the smart electric meter and the virtual energy balance sheet of every prosumer and the prosumers ability to consume the positive balance of the green electricity produced during low performance of the own power facility, the DAO acts as a virtual power plant and as virtual energy storage.

EWZ and other power plant owner's role in a Decentralized Autonomous Organization will change dramatically. EWZ will not be a monopolist in its territory, but a participant

¹⁸ "Blockchain – an opportunity for energy producers and consumers?", PwC, 2015.

and provider of renewable energy. And since EWZ will be the provider and owner of the grid in its territory, EWZ will be paid via a certain fee or tax levy for the constant maintenance of the grid and the DAO's use of the grid. The payments could potentially be done with Tokens. The affiliate company of EWZ selling and installing PV facilities could act as one of many providers of all physical installations such as for example solar panels, network control systems, converters, and smart electric meters. In other words, in the present presentation of this DAO system, EWZ will only be a market participant, supplier and operator of the electricity grid. Power suppliers, such as EWZ, lose their monopolistic positions.

Therefore, the potential use cases of blockchain technology in the energy sector show a lot of promise and have the potential to radically change the energy market.

3.6 Evaluation

Although the blockchain technology is very promising, first successful projects such as BrooklynMicrogrid are emerging and a DAO seems to work in theory, the implementation and introduction of a DAO in the Zurich or Swiss electricity market is associated with many hurdles. Furthermore, the experience with the blockchain technology is limited to only a few years.

As a result, virtual energy storage should be built up step-by-step in order to gain initial experience with its underlying business model and the new blockchain technology and to reduce internal and external resistance. With this experience, EWZ, together with other electricity producers and strategic partners, can develop a sophisticated concept and system around and for a DAO that integrates consumers, prosumers and electricity producers appropriately.

As a bootstrapping procedure, the following three phases could be established by EWZ:

3.7 Uncertainties, disadvantages and risks

Blockchain as a technology and its applications and extensions in the form of a DAO require or overwhelm most people. Not only because there is a need for in-depth technical understanding, but also because the disruptive upheaval is so significant that comparisons with what is known and the application of existing laws and regulations are almost impossible. Difficulties arise, for example, with the division into groups, what kind of a

legal construct a DAO is, whether a "head office" of a DAO is possible at all due to the decentralized structure, how the system is taxed, whether and how transactions within the network have to be settled, what kind of liabilities exist for a physically non-existing construct owned by nobody, and so on.

Another controversial point is trust. Blockchains are supposed to build trust, so DAOs are organizations of trust, because every participant trusts that the system has been implemented fairly and is constantly improved. For example, because the system is implemented by smart contracts that are nothing more than distributed code, the entire organization is entrusted to one program. Programs continue to be developed by people who can make mistakes. Weak points in the respective blockchain software and the smart contracts executed on it are therefore a major risk. The DAO showed that a small mistake can bring down the house of cards. When it collapses, there is no saving authority or legal barrier that can help shareholders. All trust is in the code.¹⁹

4 Solution Design

If we draw attention to the code behind our idea we can divide it into two parts: backend (solidity) and frontend (html, javascript, metamask). The purpose of the frontend is to give a simple but hopefully not less secure interface to the user so he can easily access the blockchain. The backend consists of the wallet contract (managing the tokens) and an example implementation of how some of the transfers could work. It is still not fully realistic because the complexity would increase heavily if you make the model more realistic. The focus of the following chapter is on the backend part because the frontend is quite simple. Frontend is just about letting MetaMask call some prepared functions of certain contracts on the blockchain, and about listening to events of the contracts (and showing these in a stylish and simple way to the user).

We will start with the abstract model of what we tried to build. Then the main part is about the implementation (in solidity) and it's difficulties. The last part of the solution design will be about some problems with this implementation.

¹⁹Decentralized Autonomous Organization - Organisationen auf der Blockchain, Jonas Verhoelen, <https://blog.codecentric.de/2017/08/decentralized-autonomous-organization-blockchain>, retrieved February 25, 2018.

4.1 Idea

The main target of our implementation is, that it has to be secure. So we try to do it as simple as possible (then there are less sources of errors). Every user should be able to get a wallet where his tokens will be stored. Nobody else should have the right to take tokens out of that 'bag'. But there should be some automation for the transactions (e.g when a user produces for or buys energy from the connecting network at his home).

To create the connection between the real world and the blockchain we use the concept of SmartMeters. Any organization that got the trust of people in its environment could offer this service. SmartMeters should measure the produced and consumed energy of users and report it to the blockchain, where SmartContracts between the user and the connecting network will transfer tokens dependant on the individual implementation of these SmartContracts.

4.2 Our Model Implementation

4.2.1 Wallet

This contract is responsible for the ICO and it holds the balances of tokens. Therefore it should be really really simple. If there is a bug that can be exploited in this contract the whole concept could not work. We explain shortly the functions of this contract:

- When the wallet is constructed it will initialize the amount of coins on the market to $1e20$. We did spend a lot research in how much this should be, so this could be changed. The owner is the creator of this contract. The owners address will get all the Ether that is given to this contract (the ether from the ICO).
- 'transfer' transfers an amount of tokens from the callers account to a destination account. It's quite simple. It only works if there are enough tokens on the callers account and if the transaction happened it will fire an event, there is no need for overflow check because there are not enough tokens initialized to create an overflow. Frontend programs can listen on the fired events. In the ethereum blockchain there is an extra section where fired events are listed, so everyone could check or listen to them.
- 'buyTokens' is the only payable function of this contract. It's used for the ICO. For simplicity it just does a normal transfer of tokens from the wallets account to the callers account. The amount of tokens is equal to the amount of wei paid.

Obviously the transaction gets cancelled if there are not enough tokens on the wallets account.

4.3 Model Scenario

The Wallet is the only part that will be the same for all transactions in different regions with different producers and consumers. The other three contracts just show a possible scenario how SmartContracts could do the transactions automatically.

SmartMeterBackend contains functions that can be called by the real (hardware) SmartMeter that measures electricity in and outflow of a producer/consumer. In our implementation it has just one function that reports energy production to the network operator.

The OperatorBackend will need some more explanation. There are functions (that are called by the owner, as example EWZ) that set the price for electricity from this network and the reward for feeding energy into it. Aside from that there is a list of trusted SmartMeterBackends. Only trusted SmartMeterBackends will be able to trigger a payout of tokens to the producer (they can call the rewardProduction function). Now, if a user wants to buy energy, he can call the function buyEnergy with a callback that sends tokens to the operator if and only if the operator fires the event that reports the transaction as Event.

The User is an example contract of how a producer/consumer could implement his contracts. There is a function to ‘pay for energy’ and a function to transfer tokens to other users (as example if Bob wants to sell produced electricity to Alice). The energy supply will be done by the operators of the networks but if both operators (the one of Bob and the one of Alice) allow to pay for energy with tokens, it will be as if Bob sold his energy to Alice. The ‘pay for energy’ function calls the ‘buyEnergy’ function of the linked operator and sets up all required variables and functions for the transaction (it sends the callback function and sets the price, that the callback function will expect).

4.4 Problems and Possible Solutions

One problem could be the privacy. There may be users that don’t want, that everyone could know how much energy they consume and produce. This is a hard to solve problem because one of the main features of the blockchain is transparency. An approach for a solution could be, that the operator and user handle the transaction between them

outside the blockchain (this requires trust from the user side). Still some transactions would be visible on the blockchain.

Another issue is, that in the implementation of the scenario (not in the implementation of the wallet) are still features, that could be exploited by the operator or the user. As example the operator could not trust the SmartMeter. Then the token transfer would not get triggered even if the consumer produces energy. This case is not that much a problem because all actions get logged in the blockchain and the trust in the operator would decrease much, if such things happen.

Another possible weakness of the system could be the SmartMeter itself. A user could cheat if he manages to ‘hack’ the SmartMeter. A possible solution for this would be a SmartMeter that has some features that prevent hacking (as example it destroys its private key, when it notifies an attempt).

5 Conclusion/Outlook

A very important part are reliable measurements of energy production and consumption. It would be ideal, if smart meters could provide the data directly to the network. But it’s highly possible that this does not work yet. As the trust in ewz is very high, and they already check energy consumption manually, this is a service EWZ might provide.

Another problem might be on the legal front. The DAO is still a young concept with no laws existing yet. There is also the question, of how the certificates are handled in such a system.