Real-Economy Applications of Blockchain Technology

Technological requirements and potential usecases: a research blueprint

BTRI - Blockchain Technology Research Institute

Q1 2018

Abstract

This paper blueprints the framework for a research project with several objectives. The concept of Fiat-Money-Equivalent (FME) is introduced to outline challenges with volatity of digital payment systems. Also, a localizer function is introduced to overcome transparency challenges in modeling real-economy processes. Identified Research Objectives with high potential for future usecases that take unique advantage of the main pro-blockchain arguments (‘distributed’, ‘immutable’, ‘trustless’) are identified in a) integrated systems design, b) export credit and c) transportation industry applications, wheighed against their specific challenges (‘too much transparency’, ‘unwanted profit margin pressures’) and evaluated briefly to be further explored in future projects.

Contents

Introduction and Overview

This paper outlines the research project for which we seek funding. The project is conducted by a foundation (Stiftung faire Kapitalmaerkte - Foundation for Fair Capital Markets) to access resources through an innovative channel that is technologically related and to provide results to the public consequently.

Blockchain technology has had a major impact on the worldwide community. It has shown the potential of a decentralized global database with regards to accessing previously unknown resources. However, to this day we haven't seen any meaningful usecases of the technology where real-economy applications and blockchain technology are combined to "make things better". We believe this is due in large part to the extremely high volatility in crypto assets that create significant economic uncertainty for application in real-economy applications. While many large corporations have expressed interest in the technology, only a few usecases have been implemented in small scale like the Daimler-LBBW debt issue that was implemented as a blockchain solution in parallel to the conventional processes in place for a long time (LBBW 2017).

The objective of this project is to start from an overview of the status-quo in blockchain technology as a basis to list current challenges and shortcomings with regard to applications in the real-world economy.

Subsequently, we will try to blueprint a technological framework that makes the use of blockchain technology viable for real-economy applications. Depending on the available funding, we will also provide proof-of-concept for this new technology and **participants will have priority access** to our research.

This paper will also highlight future fields of possible research. Some of the research questions arising throughout our discussion will be put out as Bounty for the open-source community who will receive tokens for their contributions. Bounties highlighted in this paper will be accessible later through the website. The main cornerstones of the project headlight as follows:

Real-Economy blockchain	German engineered	Research-focused
identify prerequisites and requirements, as well as potential usecases	work towards a technological framework with user-friendly feasibility, thoroughly engineered for value	"think first, then act"-philosophy

Laying the groundwork for the further reading of this document we provide a summary of "what has happened so far" in the following section.

Cryptocurrencies and blockchain - a short history

In summary, cryptotransaction systems use the technical progress in the field of asymmetric cryptology to carry out transactions in encrypted form and to record them in a transparent, comprehensible and forgery-proof database (called blockchain or cryptoledger). Both the execution and recording of transactions in the database is carried out entirely in a (decentralized) peer-to-peer network, the algorithm of which is based on a consensus mechanism.

Cryptocurrencies are digitized tokens, also known as tokens (a Bitcoin, or a litecoin), which are also accepted online as a means of payment. Currently, the best-known representative of these technologies is the Bitcoin protocol, the first client of which was released as open source by Satoshi Nakamoto in autumn 2008 (Nakamoto 2008). The cornerstones of the digital transaction system (also known as crypto) proposed by Nakamoto (due to the asymmetric encryption of transactions used) can be summarized as follows:

- Mathematical algorithms control the processes in the entire open source software program.
- The transaction system is formed de-centrally from equal participants (peer-to-peer) who each run a Bitcoin client on their computer and connect to each other via the Internet.
- A Bitcoin is a purely digital value within this network, consisting of a digital string.
- Transactions take place at pseudonymous addresses, these Bitcoin addresses can be generated by the individual user in any number.
- All transfers are made directly between equal participating users, without involving a service provider, without delay, regardless of physical distances and national borders.
- To protect privacy and to protect against cyber attacks, the Bitcoin software provides an asymmetric encryption system for the transactions carried out.
- Using the secret/private key, each participant can prove beyond any doubt that he or she is entitled to dispose of the Bitcoin belonging to a public address.
- Each transaction is recorded in a publicly accessible and non-reversible database.
- This database is also known as blockchain/Cryptoledger due to the systematics of its structure and is completely decentralized.
- Network participants (miner) de-centrally confirm the correctness of transactions and their consistency with all previous transactions in the network.
- The blockchain is stored de-centrally with all Bitcoin nodes and is continuously updated.
- Since the blocks refer to each other, an intervention in this system would require an artificial recalculation of all transactions, which is considered technically impossible.
- The money creation process is limited to 21 million monetary units and is independent of the demand for Bitcoin.

Achievements of the technology

Double Spending of a token/ticket is solved in traditional economic systems by involving the financial systems (a third party manages and controls). In the cryptocurrency systems, the Double Spending problem is solved by creating a decentralized and forgery-proof block chain. Technically, a Bitcoin transaction is initiated in a double-spending attempt and subsequently - before the first transaction has been confirmed - a further transaction is initiated with the same Bitcoins. The trick is to get a fraudulent transaction confirmed on the Bitcoin network first, so that the first transaction is not executed (double-spend-race-attack).

Based on the open source concept, according to which every developer can copy and further develop the source code of the software, the first alternative transaction systems to the Bitcoin system appeared in 2011. By further development or modification of the Bitcoin source code, new cryptocurrency systems are created which differ in certain characteristics of Bitcoin, but leave the basic principles (mathematical algorithm replaces trust in middlemen, peer-to-peer transactions and decentralized databases) largely unchanged. These alternative currencies are also called altcoins. There are currently more than 400 alternative cryptotransaction systems of this kind in existence - with more or less success.

Decentralization and digitality of the system

One of the most important basic elements of the Bitcoin system is decentralization. The system architecture of the Bitcoin system does not have any central authority with a control or monitoring system.
The verification and validation of the transactions in the Bitcoin network is decentralized. In the Bitcoin system, decentralization is based on the implementation of the system as a peer-to-peer network. The only condition for participating in the network is the operation of a Bitcoin software client that is compatible with the Bitcoin protocol or the use of an online service provider that provides this functionality.

The creation of digital values is also carried out decentrally on the basis of this system, as is the determination of value. The value of a Bitcoin results exclusively from the supply and demand of the network participants. Money is created independently of the demand for a certain mathematical algorithm.

Decentralization brings a globally operating network, without a control center and without any central server. The creation, validation and verification of the transaction orders as well as the administration of the resulting database are carried out exclusively digitally.

Market usage

As electronic digital money and financial assets, Cryptocurrencies have become one of the most interesting Internet products in recent years. Since 2010 Cryptocurrencies have been accepted as means of payment in Japan, the United States, China and other countries. In some countries like Venezuela they have even taken a more prominent role partially replacing official payment systems as a function of local inflation rates ("Venezuela's Hyperinflation Sees Record Highs of Bitcoin Use" 2016).

There has been a wave of rapid development of financial products for trading Cryptocurrencies on the Internet. Cryptocurrency exchanges have now been constantly active and liquid since 2013, while transaction prices have also shown an explosive increase. Due to the lack of limit changes and the ability to execute 24-hour transactions, the market price of Cryptocurrencies is rising rapidly, accompanied by a substantial volatility in the price. At the same time, China quickly became cryptocurrency's largest trading nation.

The Status Quo of Money, Banking and blockchain

Building a model of a process that was observed in real-economy environment always requires an understanding of the individual functions of the process first. We observe a multi-staged process that later will be examined more closely by breaking up into production - fulfillment - payment systems. But one of the main challenges of current blockchain applications always lies with the payment system. It is the interface to the real-economy and therefore plays a crucial role. We therefore have chosen to provide in the following paragraphs some more background on money, payment systems and their interaction with blockchain technology.

To find out how money works, the following questions must be considered:

1. What are the factors that originally allowed a fair value for money and
2. What are the factors that cause changes in the "objective exchange ratio of money" or its purchasing power?

Money is a means of exchange that facilitates trade in goods and services. Wherever people went beyond the simple barter trade, they began to use their most marketable goods as barter. In primitive societies they used cattle, or measures of grain, salt or fish. In early civilizations where the division of labor extended to larger areas, gold or silver proved to be the most marketable commodity and ultimately the only means of exchange called money.

It is obvious that the chiefs, kings and heads of state have not invented the use of money. But they have often seized control of them whenever they have suffered budget deficits and have been able to obtain income from the devaluation of currencies. As a result, the money we know today is nowadays also controlled by central banks and, to a much greater extent, by commercial banks. At the end of the day, they can simply create money as long as it is considered stable in value by the population and accepted as a means of payment.

Therefore, the value of each asset is to have confidence that you can still use it tomorrow.

Value of money

From an economic point of view, in recent monetary theory, a thing or institution is called money when the following basic functions are fulfilled:

- Arithmetic function: The prices of goods are used as a measure of value and the value of goods is set in relation to each other.
- Value retention function: The storage of money allows you to store purchasing power.
- Exchange medium or payment means function: Constitutive for the essence of money is its property as a means of exchange.

This property gives money the highest liquidity ratio as factor 1, meaning that money is accepted at face value without discount.

Unbanked People

According to the Global Findex 2014, at the end of 2014 approximately 2 billion people or 38% of the world's adult population does not have a bank account (Demirgüç-Kunt et al. 2015).

The reasons are many and varied, with the main factor being probably the inefficiency of account management for financial institutions. This may depend on the underdeveloped legal framework for ownership and identification in the economically undeveloped countries.

There is neither a registration of real estate nor a company register comparable to European registration systems. Without formal proof of identity and assets, however, no credit rating, no pledging and therefore no lending can be carried out.
As a result, the world's poor lack the basis for participation in the global banking system. However, numerous studies show the direct link between poverty, lack of education and access to the global financial system.

If a population, for whatever reason, loses confidence in the state institution responsible for maintaining the country's financial system, this dysfunctionality usually has a direct impact on the country's income and wealth situation. Through the use of alternative payment methods it is possible to quickly and cheaply eliminate logistical hurdles. Furthermore, due to the non-nationality of cryptocurrencies, local restrictions to move money in and out of an economy won't apply anymore and therefore provide access to international markets at a great level of transparency.

Current Status of our Banking based Payment System

Money transfers can nowadays be handled in cash or electronically via banks. A cash transaction requires that both parties are physically in one place and complete the transaction. Once transferred, it is difficult to unilaterally reverse the transaction. This will cause the cash to be secured by the users as best as possible. (small quantities in the wallet, in case of large quantities with a cash transporter with special protection).

Ensuring this security was one of the original reasons for setting up banks. The transportation of money was very risky and reminds us today of the great stories of stagecoach raids in the Wild West.

Banks took the risk of taking money from one person to another safely. At first, physically, but relatively quickly the procedure was adopted, in which the claim to the money was first transferred, and only if a person wanted to have this paid out in money again, this was physically moved. Thus, it was possible to increase security in one place by protecting the money in expensive safes and with security precautions. First the claim to the money was recorded in books, later electronically in databases.

We know this today as bank transfer or generally as payment transactions.

Secondly, banks were and are the interface between lenders and borrowers. Just a few years ago, it was technically impossible to communicate with all people at the same time. By bundling many small money-holders, they try to enable even large borrowers to make medium-size arrangements. Legal regulations stipulate that deposit protection is a fraction of the total volume. This gives banks the power to create additional paper money, since only a fraction of the loans they grant have to be backed by deposits - this is the predominant business model of the savings banks.

However, the money transfer function can be completely taken over by new technology. Banks do it themselves, stagecoaches are no longer available nor necessary, all payment transactions are processed electronically.

Is the traditional system still needed when blockchain is available?

Banks are still used today as trusted intermediaries. In addition, the industry as a whole still has very attractive wages even for lower level employees. Why give up the one job where you don't have to do anything? Setting up a non-volatile payment system in a decentralized and trustless fashion could quickly dry up a major part of the banks' liquidity. The more people carry out their payment transactions via decentralized networks and services attached to these networks, the less the existence of our current banks is justified. One has to ask which value is supposedly created by bank payment systems that justifies the high economic cost. Would it not be economically useful to have inexpensive and direct transfers of monetary values between its users directly? This also leads to the question what economic value could be freed by using such systems? Is the value quantifiable as the total profits or costs of bank payment systems or is there additional and currently untapped economic potential? These are just some of the questions we look to address in further research.

Requirements for payment systems

In summary, we see the following points as prerequisites for functioning payment systems:

- Transaction costs should be kept as low as technically possible
- It must be ensured that there is value retention
- Transactions must be easy for everyone to perform
- Value must be protected against unauthorized access
- All transactions are treated equally and not preferentially
- No one should enrich themselves in transactions, value creation is not created by transactions
- A transaction system must provide its users and suppliers with the ability to use case law-based reversibility, trustee procedures and data protection controls.

Such a transactional system can and will continue to develop with technical progress. Irregardless of what technical basis this is taking place, it can relieve us of today's tasks and thus give people freedom.

Freedom does not consist of doing everything you want to do, but rather freedom is primarily the fulfillment of what is necessary for the earth to continue to exist with its diversity.

Modeling real-economy processes

When comparing the differences between the "classic" markets (illustrated by the horizontal strand in the figure) and the digitized version on distributed ledger models (vertical strand), there are some obvious differences.
The classic flow often struggles with complexity stemming from interfacing the main building blocks production - fulfillment - payments. It can be unsure if ordered products have been delivered, if they arrived and if so were they billed correctly and finally paid for in time. There have been numerous attempts to interlink these horizontal block like solutions brought to us by big software companies like SAP etc. We argue that while these solutions have helped to create communication between the different blocks, at the same time they have introduced two things that are generally unwanted: complexity and additional cost.

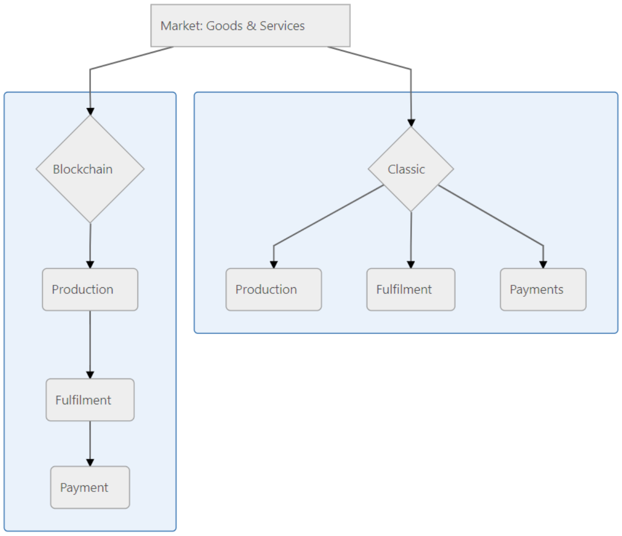


Figure 1: Current models of economic system

With distributed ledger solutions it should be possible to reach a much higher degree of integration across the blocks. Then, it quickly becomes obvious what potential lies in these solutions: **significantly reduced complexity and massively lower cost** (if not eaten up by fees of middleman who helps to implement the blockchain solution).

Let's look at figure 1 again and argue that the digitized blockchain solution basically transformed the flow from a horizontal process to a vertical one that integrates at least two of the classic block (payments and fulfillment) for physical goods and all three blocks for digital goods. The integration is powerful because it is creating a unique digital model of real-economy processes that allows for interconnection, flow of information and logical rules to be integrated within the model itself, without the need for added complexity. Obviously, such a solution can strongly lift efficiency in an economy.

Challenges in today's blockchain ecosystems

When looking at the digitized work-flow on the side of the blockchain solution it quickly becomes obvious that the fulfillment block can easily be implemented. In theory, the same goes for the payment block. But in reality, even large corporates interested in the technology would never use the payment function for several shortcomings:

- high **volatility** of cryptocurrency
- unwanted **transparency** of who holds how much cryptocurrency (takeover targets, payroll volumes, corporate liquidity)
- unwanted transparency of size differences (i.e. small supplier scared to be squeezed by big off-taker)

On the more technical side we identify some shortcomings as well:

- Requirements for higher **security standards** (multi-signature, two-factor authentication)

- User-friendly and **fast transaction confirmation** (i.e. PoW vs. PoS[1])
- **Energy footprint** of the entire system

We will discuss these challenges subsequently and offer approaches to create a user-friendly blockchain system that can find applications in the real economy.

Shortcomings of the current System

Cryptocurrencies are a digital, decentralized, anonymous currency for which no government or other legal entity is responsible. These electronic peer-to-peer payment systems were introduced in 2008. Technology foundations for Cryptocurrencies and other electronic cash systems are distributed ledgers, which are managed by a peer-to-peer network. Within the distributed ledger, transactions are organized in blocks and then linked together into a chain, the blockchain.

Cryptocurrencies are issued to competing miners connected within the Cryptocurrencies peer-to-peer network, using computers to generate solutions to problems that ensure the integrity and security of the system. The difficulty of the problem arises in such a way that Cryptocurrencies are created at a given decreasing rate, independent of the total computing power of the network, and the upper limit of cryptocurrencies is set at 21 million.

The system is partially anonymous, because no account in the system is tied to an individual, but everybody can view the history of all transactions from all accounts. In addition, each individual can create unlimited independent accounts. Cryptocurrencies transactions are irreversible, as are cash transactions.

Trustless Systems Transparency - good or bad?

Transparency is often advocated as a big bonus of distributed-ledger databases. It is designed to enable "trustless" transactions whereby each user can trust the database entry, i.e. if Alice wants to exchange goods or services for a form of payment, she can trust the blockchain entry that her counterpart Bob actually is in possession of the payment means to compensate her for the goods or services provided. When examining reasons why real-economy corporations are hesitant to use the technology, this very transparency stands out as one of the main reasons not to (next to the currently observed volatility if used as a form of payment). Let's consider two examples to clarify this point we have highlighted earlier:

1. A company assistant makes a reimbursement for travel expenses to an employee of the company. To execute the payment on a blockchain (say the company reimburses its employees in Ether) the receiver's address is required. The assistant transfers the coins and gets curious what other transfers have been made to this address and looks it up on Etherscan. it would now be possible to see any payments to and from this address. Especially transfers that occur every month on the same day could be interpreted as salary payments. These are usually kept secret and most employees contracts have a clause that demands non-disclosure of salary. This is commonly used by employers to maintain the asymmetric information structure with which employees are controlled and manipulated. Office gossip would be thriving. . . .

[1] Proof-of-Work (PoS), Proof-of-Stake(PoS)

2. On a more strategic level, let's think about a companies cash reserves. Even if multiple accounts for receivables, payables, cash etc. would be used to cloud full transparency, it would be easy to find out which accounts belong to the company. By simply adding up all transactions from the beginning of the ledger's entries, any competitor could at any time deduct the financial state of its competitor. This information could easily be used for tactical and strategical moves. Just a few examples:

- Negotiations with take-over targets that are currently low on cash (and maybe you know both current cash and monthly salary payments to be made since you scanned all accounts that receive monthly payments from the company) could be shortened with the demand of a lower price that must be met due to liquidity pressure.
- When competing for a new order, tactical information about timing and amount of payments can easily be used to put pressure on the competition and squeeze them out of any potential deal.

Any real-economy CEO would be deemed insane to create such vulnerability and exposure for the company. The obvious quick-fix for the above problems would be to use new accounts for every transaction so that trace-back difficulty rises with number of accounts. At the same time this would create new threats to security and open gates for attacks just simply because the number of possible doors to attack grows every day. Security of key management would also become a very complex matter.

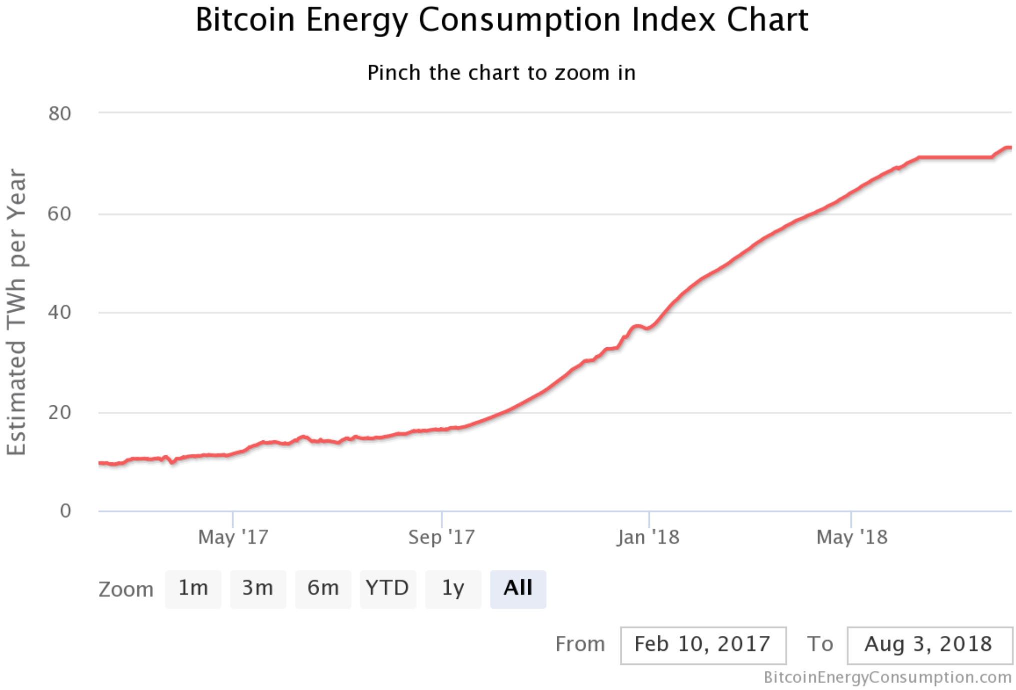
Another apprach might be to separate the pure transactional data from the header rows (illustratively speaking) so that the data alone can be publicly available while the headers (i.e. the meaning of the data) remains private information. Only with the correct key can the two components be zipped together again. This approach could possibly be one of the research approaches of the BTRI.

High resource consumption through prevalent incentives

The Achilles' heel of the proof-of-work programs is that mining capacity is growing in direct proportion to incentives. A good Bitcoin analogy can be found in a star that constantly has to merge hydrogen with helium in order to generate the necessary pressure to prevent collapsing under from its own gravity. When the price of Bitcoin first reached $1.000, mining capacity increased and with it difficulty increased, resulting in higher mining costs to keep the system balanced.
The need for a proof-of-work concept is to ensure the integrity of the blockchain and maintain the integrity of the network, which goes hand in hand with the decentralization of the network. The necessity of attack defense requires a massive amount of computing power. In the summer of 2015, a journalist in the online magazine Motherboard calculated that a single Bitcoin transaction requires as much energy as 1.7 US households per day.

In March 2016, the energy consumption of the entire mining network corresponded to 350 KW per day which is the equivalent energy consumption of about 280,000 US households. This amount has grown rapidly this first calculations were made and today is expressed in the bitcoin energy consumption index link which as of mid 2018 shows a value of around 70 TWh per year being consumed by the Bitcoin network as shown in figure **??**.

To put this amount into perspective, it is often compared with the energy used in credit card transactions. About 100,000 VISA card transactions consume as much energy as 1 Bitcoin transaction as of mid 2018. This does not seem to be a sustainable development (Vries 2018).



From Feb 10, 2017 To Aug 3, 2018

Figure 2: Bitcoin Energy Consumption

The misguiding incentive structures also im summary lead to the following observations: * Difficulty levels currently very high due to mining-craze. * Scientific Research (NASA, CERN) is already delayed as GPUs are sold out (Lamb 2018). * long confirmation times / low capacity for transactions on i.e. the Bitcoin blockchain. * High transaction cost render the use of crypto uneconomic for everyday-life purchases like coffee. * High uncertainty as to restorability of wallets at a later point and legal/tax uncertainties forbid the use of crypto for institutional investors. * High volatility of all crypto currencies prevent the use of the technology for interested industrial players who need certainty about the value of their payment-means when entering into a transaction.

The obvious problems with blockchain architecture are currently being discussed and different solutions suggested. Poon and Buterin outline in their working draft for Plasma that a fixture to slow and overloaded Ethereum Main Chain can be fixed with adding a chain tree structure with faster transactions and exit rights (strange when a large part of the fix talks about how to get out quickly?) (Poon 2017). Others, like Ethereum co-founder Gavin Wood suggest to not fix the things that don't work in previous versions of different blockchains but rather provide a new development system that can host an ecosystem of many heterogeneous blockchains that can be interlinked and therefore creating a single point of access to the best-fitting implementation. (Wood 2017) This is a nice approach for the token which it will run on as by definition this will be the most valuable token of the "blockchain-of-blockchains". However, it might not always be desirable or necessary to strive for the highest degree of public availability but rather adjust to the individual requirements of usecases at hand.

Possible Approaches for improved usability

There are a number of areas which can be improved and are potentially topics to deepen our research in the future. The following section will go through the ones we identified so far and outline possible approaches for improvement.

Security

One of the biggest problems is the security of individual accounts. How do you make sure that double-spending is not possible and that only the legitimate owner carries out transactions and that no third party has access to your computer or private keys?

Nowadays, cryptography algorithms are often not the point of attack but people themselves. By negligence or laziness, (example: the most common password on computers is: “password”) it is often easy for criminals to gain access and thus carry out data or transfers.

Many cryptocurrencies rely solely on a private key, which is used to authorize transactions. We don’t suggest to get away from this basic concept, but are of the opinion that a dynamic key based on a private key plus an Authenticator number, which is stored on a third device/app like a smartphone and protected by biometric or other mechanisms is a step to increase the security of your own key.

An ECDSA[2] provides smaller key sizes and faster operations then RSA keys for equivalent estimated security. key pair can be created with almost any random data. These key pairs consist of a private key and a public key. Only together do they give a checksum which confirms a transaction.

The public key is statically unchangeable. Everyone has access to it. Often this is also the account address. The private key is in its pure form, in which it never occurs, also static. Users enter only one encrypted private key at any time. This encryption runs dynamically as follows: A component of the key is constantly changing, consisting of a number combination that randomly changes based on an original timestamp and the current time, e. g. Google authenticator and a static key, which serves as a second component key. Only in combination of both, it is possible to decrypt and verify the master key for this period of time (compare figure 3).

Confirmation / Proofing Concepts

PoW can be good for fighting SPAM/DOS attacks where you distribute the load to the endpoint/user instead of focusing on the system. A tiny load per sender of the mail/request instead of a huge load on the shoulders of the system helps to build up an unfair race against the opponent. In Bitcoin, PoW lies on the shoulders of the system and not on the shoulders of the users and relies on a fair race between the opponent and the honest. The design error here is amazing! The safety level is directly proportional to the injustice of the race against the opponent. PoS/dPoS, etc. all suffer from the “anchor to water”problem and therefore cannot escape the AR dilemma.

An intrinsic segregation of interests between delegates and voters is the common trust problem of democracy, which cannot be solved by dPoS. They are subject to the propaganda of candidates who promise you good incentives to vote for them. Delegates have their own interests and cannot guarantee that they all have the necessary knowledge. To make things worse, voters have different

[2] Elliptic Curve Digital Signature Algorithm (ECDSA)

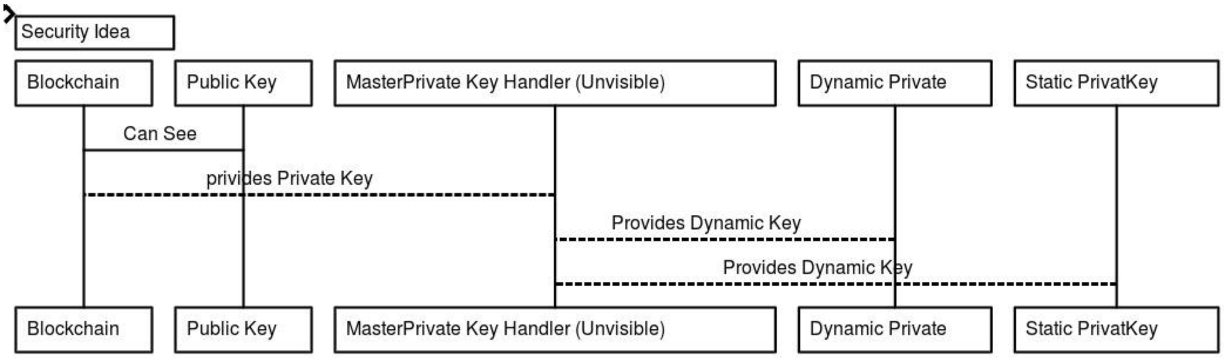


Figure 3: Little Authentication Overview

interests. Besides, you can always be deceived by a super-rational attacker. In fact, the super-rational attacker has an advantage over the honest candidate who lacks external advantages.

Asymmetric encryption provides a means for an unfathomably unfair race against the opponent. We should focus on finding a solution to the problem of double expenditure. Once we have achieved the necessary anchoring, the system will become much more effective in terms of efficiency, flexibility, security, privacy, regulation, regulation, government-population relations to the satisfaction of both sides, and so on. Such a system is absolutely destined to be future-proof, on which all other systems rely.

Proof of Stake Algorithm - Empowering Eco Friendly blockchains

If the incentive structure is changed to something like a delegated proof-of-stake system, the incentive for validators becomes building and operating a system with high availability, high security, and the bandwidth, storage, and compute resources to keep up with what could be a so-called “big blocker’s” fantasy. This would eliminate the sort of Utopian dream of “anyone can run a Bitcoin node” but that too is an idea I find highly questionable. If the validators (and things like inter-chain peg zones, auditors, and a handful of other use cases) are the only ones who need to see the fire hose, it can move much, much faster than the 4 transactions/sec Bitcoin is doing on-chain today, and the rest of the network can operate using light clients.

It also means the system can come to consensus much faster, in seconds rather than minutes, because the validators can run a traditional BFT algorithm between each other rather than Bitcoin’s consensus-by-lottery/race condition. This means clients can be much simpler than systems which use off-chain payment channel protocols, and there is no (surprising) latency to open a channel: the system can operate at a scale where transactions are confirmed on-chain at a reasonable rate to begin with.

A faster blockchain is a more expensive one to operate, but in the process should also be a more lucrative one for system operators with respect to transaction fees. Instead of investing in an arms race to do the best job wasting electricity, we could be investing in compute resources to make the system faster: a virtuous cycle instead of a vicious one. (Archieri 2018)

At the same time, we feel that technology which places a lower burden on the global environment must be preferred, keeping in mind the global energy consumption with its devastating consequences. Responsibility to future generations should at any time be a leading beacon, especially when designing technological ecosystems for future use.

Role based access control in immutable distributed ledgers

With immutability and traceability as the most prominet and important aspects blockchain / distributed-ledger technology, the question about access rights arises.

In real-economy processes, many tasks are divided into smaller projects and split on different levels - with responsibilities on global, local and team levels. There is often a clear message with a work order as well as a confirmation to the higher authority once an order has been executed. The quicker tasks and feedback can be distributed and processed, the more efficiently a company can work, as Adam Smith already recognized in 1784, but what is the best way to store and automate such feedback with appropriate authorizations?

First of all, every partner in this chain requires rights to be able to carry out a certain task. Even if only the top level process outcomes are of interest, complete traceability of all actions might still be desirable at all times. Therefore, a non-modifiable and immutable database in the form of a blockchain is of great advantage. Every entry and correction will be recorded and can be retrieved at later points in time.

Speaking in Ethereum / Smart-Contract lingo, an asset is established with a Smart Contract on the mainchain. This main contract can be imagined as the personal file of the asset, where all essential information is gathered in and can be queried from.
The main contract is assigned a unique owner. The main contract can now create subordinate contracts that have access rights and write access to the main contract for certain parameters. These can again assign lower level contracts, which are designed in the same way while access rights can be granted differently from level to level.

Through this cascading set-up which reproduces the role-based-access structure we know from conventional databases, it will be possible to control which participants sees information on each level of the sub-chain and thus keeping information like profit margins between buys and sells for traders along the value chain depicted on the blockchain and it's sub-chain secret and separated from the general public.

The advantage with defining roles through Smart-Contract properties is that they can't be altered once the contract is established. This contributes greatly to the trustless component as a database admistrator can't revoke access rights at a unilaterally.

The volatility issue

With regards to the aforementioned **volatility** issue we find that apart from fixes in the market to mitigate the cryptocurrency risk by diversifying to baskets of several tokens and overcollateralizing (i.e. Zencash (Viglione 2017)) - by the way a solution that in our view adds complexity instead of reducing it - there are additional ways to approach this.

- Going back a step and using an old-fashioned bank for payments.This can be more or less integrated. The basic solution would use existing payment systems, i.e. the token issuer would hold an account with a bank and always hold the corresponding EUR amount in cash. Alternatively, a "paypal"-like solution would issue e-money, require a license, and collateralize each token with fiat money while not being allowed to use the deposits for loan issuance. This seems to be the logical first step when aspiring to build an integrated solution.
- In a second and more advanced stage, the system could acquire a proprietary e-banking license and fully back issued tokens with fiat money while guaranteeing a fixed exchange rate at any time (i.e. 1 token = 1 EUR). Such a solution would have to be expected at a later stage as it would require more preparation, licenses and business volume to justify.

We introduce the **concept of fiat-money-equivalent (FME)** (see figure 4) to express the relation of cryptocurrency-to-fiat exchange value. With FME it will be possible to ensure the stable value of cryptographic payments as they will be hard-linked to fiat currency. Through the use of FME it will also be possible to interconnect several blockchains between buyer and seller when transferring payments. At the same time the volatility hindering the use and prohibiting the wider acceptance of blockchain based systems will automatically be overcome and one is "only" left with the security and transparency issues. To make this a functioning concept some more research not only on the technical side but also with regards to regulatory and supervision questions must be made.

In the simplest version, the operator of a blockchain would simply hold a current account at a major brand bank. The balance of that account can be made publicly visible (i.e. show it in real-time on your website) and the amount of EUR in this account would always reflect the number of tokens in circulation. Creation of new tokens would be dependent on introduction of new fiat funds in the system. This would work just as well with a different fixed exchange ratio other that 1:1. for physical goods the system would look like the lower branch of the above chart and for systems dealing with digitizable goods, the system would be able to be a model of the total value chain from product through fulfillment, logistics and payment.

The only caveat with this model would be the initial 2 days delay when using cash, but that could easily be sped up by accepting payments into the system by credit cards - the card issuer would simply take over the credit risk (and charge for it, of course). With the use of a fully backed token it would also be paramount to use a bank that would not be allowed to forward the majority of the deposits as loans to other clients. such institutes already exist and are licensed i.e. in Germany under the e-money license. The full collateralization would provide freedom from volatility and provide a sturdy calculation basis for use of digital funds.

Coming back to fiat-money-equivalent we define the term as follows: A digital currency (token, coin, e-money) has a FME of 1 when transfers between the two can be initiated from the token holder at any time and the exchange rate remains fixed in order to allow for maximum planning security. FME levels below 1 would indicate that there is some uncertainty as to either timing, value, cost or other factors that could be supplied with different weights. Further definition of the terminology, its quantification and integration in potential applications that connect real-economy and blockchain

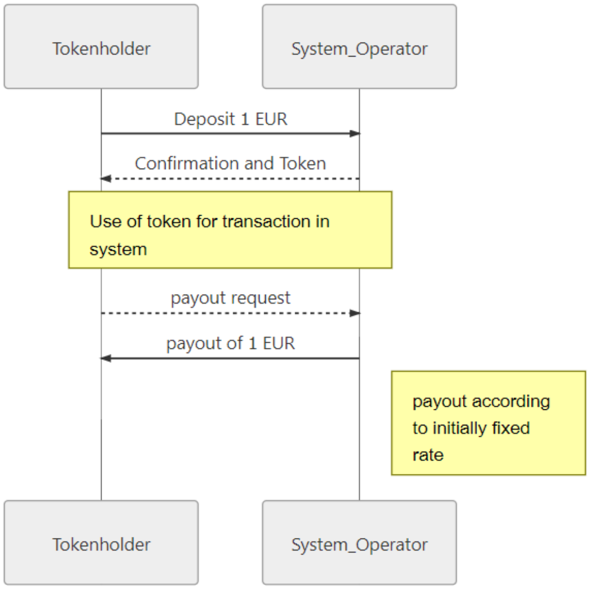


Figure 4: FME process

applications will be one of the topics of our future research. For example, in our definition an FME of one would imply a free at-the-money put right embedded in the token. This raises the question why free ATM puts would be given out and who might profit from being short ATM puts - just one of the topics to be adressed in further research.

Adressing the **transparency** issue requires a more technical approach and shall be covered in the following chapter.

The transparency issue

As discussed earlier, it is not always preferable to have transparency throughout the economic process that is being modeled on the blockchain. Just as a reminder why we need the blockchain solution in the first place when we now go about reducing transparency? Well, transparency is wanted for some parts and not for other, so why not go back to a local and off-line solution? This would not allow to fully integrate the entire economic process to be modeled in one model and therefore increase complexity again. The main technological revolution and advantage of the distributed ledger technology is that entire economic processes can be integrated and modeled thus reducing complexity and number of interfaces needed.
Some approaches that will require further research shall be illustrated here:

The “Localizer” concept

Imagine a system that would make use of transparent blockchain technology (distributed information) to make payments but at the same time anonymize sender and receiver (localized / encrypted information) as oulined in figure 5. This could be described as follows:

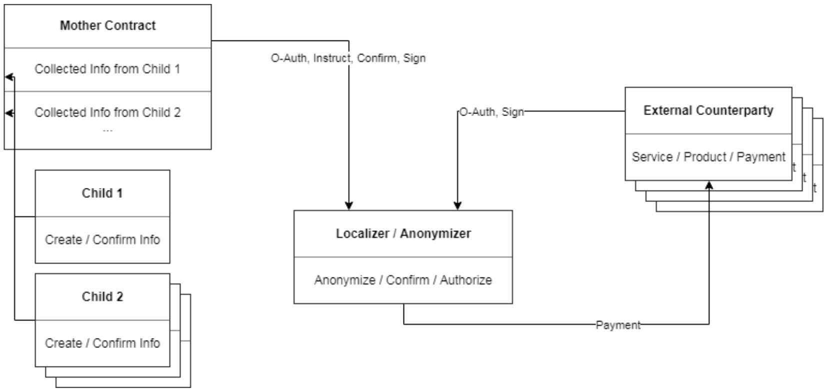
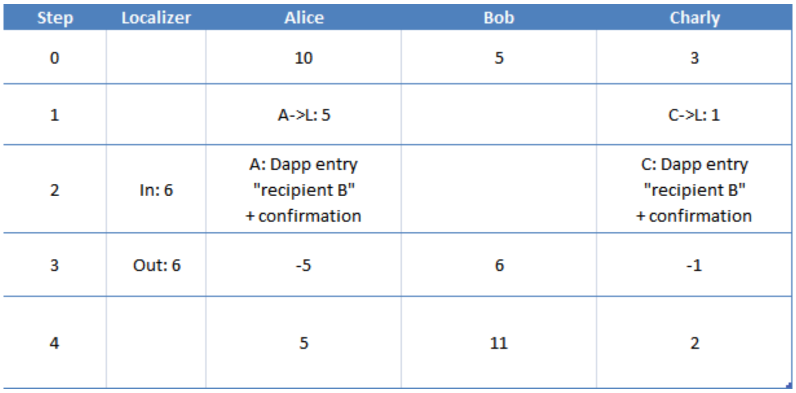

Mother Contract
Collected Info from Child 1
Collected Info from Child 2
...
Child 1
Create / Confirm Info
Child 2
Create / Confirm Info
O-Auth, Instruct, Confirm, Sign
O-Auth, Sign
External Counterparty
Service / Product / Payment
Localizer / Anonymizer
Anonymize / Confirm / Authorize
Payment

Figure 5: Interlinked Mother-Child Chains with intransparent interface



Step	Localizer	Alice	Bob	Charly
0		10	5	3
1		A->L: 5		C->L: 1
2	In: 6	A: Dapp entry "recipient B" + confirmation		C: Dapp entry "recipient B" + confirmation
3	Out: 6	-5	6	-1
4		5	11	2

Figure 6: Localized payment between 3 parties

Alice and Charly both want to make a payment to Bob (he was nice and has helped them with something) but they don't want the public to know that they did. They send their payment to a “localizer” in step 1. In the next step they log-in through a specific DApp into their localizer account and individually supply the information “receiver” in an encrypted way. At the same time the private key encryption could be used to authorize the payment. Step 3 sees the “localizer” make payments leading to new account balances in step 5. Obviously with only 3 participants this sender and receiver information could easily be figured out but not anymore if the number of participants grows. This could be even harder to re-construct when payments are not made in full but split up into different sums as is illustrated by figure 6

There are already blockchain based technologies available, both for encrypted decentralized storage like Swarm (Tron 2016) as well as for encryption of information on a blockchain, like Enigma (Zyskind 2017). It is easy to gain the impression that many projects are developed in parallel and ignorant of each other which leads to the hypothesis that great value can be unlocked by combining already available blocks of technology, especially since most projects are open source.

The “localized” information block could also be used to store large quantities of encrypted data on a blockchain while guaranteeing that remains accessible only to authorized (two-factor, multi-signature) users as illustrated in figure 7. This would also provide an entry-point to manage and grant access rights in detail without compromising the advantages of the distributed design.

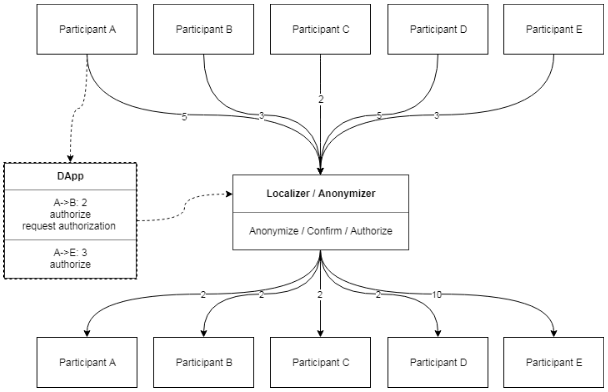


Figure 7: Localized payments between multiple parties

Research Objective general system design

It will be one of the research objectives to analyze how existing blockchain application can be combined to yield the desired result as described above.

The electronic payment market is still far from being established worldwide. In order to achieve this, several strategic challenges must be addressed by all participants in the industry. However, when comparing the adoption speeds of new technologies over the last century, it quickly becomes obvious that adoption speed has accelerated significantly. ("Technology-Adoption-by-Households-in-the-United-States" 2018) It therefore seems safe to expect adoption speed to at least remain at constant high levels. With this in mind and the number of new blockchain-based projects in the back of our heads we can safely assume that this technology will have a major impact on how business is done around the globe once the links between crypto / blockchain technology and the real economy are established (which they're currently not). The following indications for potential usecases give a rough idea of the economic scale and potential that remains untapped to this day.

Potential Usecases

Potential usecases include applications where a user-friendly setup can actually motivate real-economy players to engange in using new technology for the benefits it provides. This regards the aforementioned issues on transparency, volatility, security and so on.

As illustrated, transparency works two ways (more on one side, less on the other) but taking volatility out of the equation and providing an improved layer of security with corresponding rights and access management should play a significant role.

Tying in the payment systems functionality should round of the picture and allow for a possibility to connect real-economy applications with blockchain technology. In the following paragraphs we provide a few indications of potential usecases.

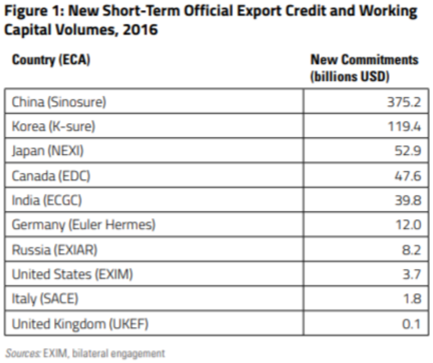


Figure 1: New Short-Term Official Export Credit and Working Capital Volumes, 2016

Country (ECA)	New Commitments (billions USD)
China (Sinosure)	375.2
Korea (K-sure)	119.4
Japan (NEXI)	52.9
Canada (EDC)	47.6
India (ECGC)	39.8
Germany (Euler Hermes)	12.0
Russia (EXIAR)	8.2
United States (EXIM)	3.7
Italy (SACE)	1.8
United Kingdom (UKEF)	0.1

Sources: EXIM, bilateral engagement

Figure 8: ECA Market Overview

Export Credit

One of the potentially interesting usecases - both because the complexity level of implementation is comparably low and the market is very large - could be Export Credit. In this market, the trust-factor plays a dominant role. This is partially due to large geographical as well as chronological distances between parties involved in a transaction. The seller only wants to send the goods when there is certainty that they will be paid for upon arrival. Likewise, the buyer wants to receive the goods as fast as possible but only transfer payment upon safe arrival.

For these cases, when funds shall only be released when the physical goods have arrived at their destination, it will be necessary to include a secure "escrow" function which grants peace of mind to both parties. This is usually a requirement in export financing. The current market accepted solution is a letter-of-credit (LOC) whereby the buyer's bank or credit agency guarantees that there is sufficient credit-worthiness to make the payment. LOCs are usually priced at around 50bps. Banks and ECAs[3] are the largest players in this market where a multi-national presence is required and therefore barriers-of-entry are higher than in comparable local businesses.

The Global ECA market is growing strongly with China in the lead. As of 2013, China had over 150bn USD outstanding ECA authorizations alone ("The Global Export Credit Dimension" 2014). This amount has grown to 375bn USD by 2016 and other countries exhibit strong growth rates as well. As indicated in figure 8, other economies also add substantially to the global market size.

ECA Usecase

The ECA usecase could encompass a simple payment system that has an escrow function built-in. The buyer's funds are blocked when goods are ordered and released to the seller upon arrival. Once again, the volatility of the payment would have to be non-existent so that the seller can be certain of the economic value he receives.

We have introduced the concept of fiat-money-equivalent (FME) to express the relation of cryptocurrency-to-fiat exchange value. Through the application of crypto payment systems with an FME of one or near one, it will also be possible to interconnect several blockchains between buyer and seller when transferring payments, like indicated in several ongoing projects like Polkadot.

[3] Export Credit Agency

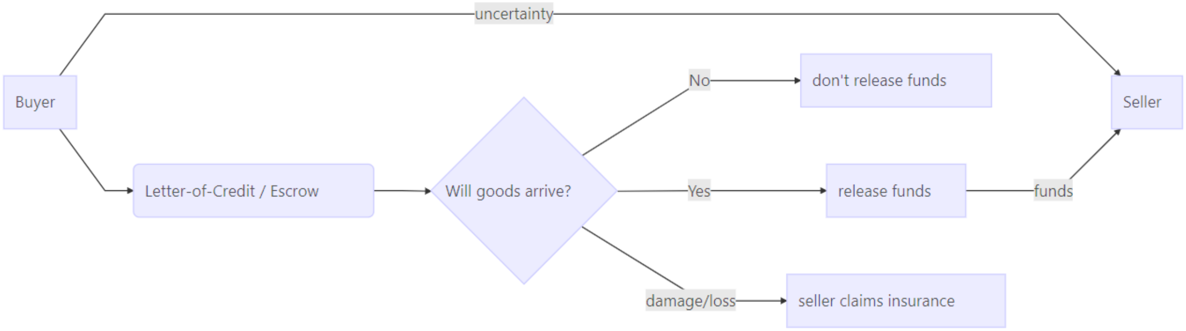


Figure 9: Possible structure for blockchain ECA System with stable FME

Figure 9 shows a possible structure for a distributed ECA chain.

Research Objective ECA

As the process is easily defined the research objective in this case can only focus on a user-friendly implementation of a stable FME payment system with an escrow or letter-of-credit function. Such a system could also be the ground layer for any stable FME usecase and the escrow functionality would be an added feature that allows for the inclusion of conditionality in the transfers. The question of how to safely implement who controls the contracts payloads remains to be solved. As an example, you wouldn't want the seller (or any third party) to be able to set the status of goods to "delivered safely" and therewith send a pull request for the payment without having a prior confirmation of the buyer that the goods have actually arrived safely. At first glance the obvious advantage of handling such a transaction through a blockchain seems to be that no third party is actually necessary. Banks or ECAs would not be needed, as the required functionality "blocking of assets" / " escrowing assets" can easily done on the blockchain. One would probably have to implement a conflict-solution instance for cases where both initial parties don't agree. Such an instance could be paid with crypto assets from the escrow in the same way the transaction was set up before.

Transportation usecase

Among many possibilities, we identify the transportation sector as potential field of application. At a first glance, this included several major sub-sectors of the fields (airline, shipping, logistics) both for goods and personal transport. Subsequently, we start with an example of the airline industry and outline potential milestones toward a decentralized system for the sub-industry.

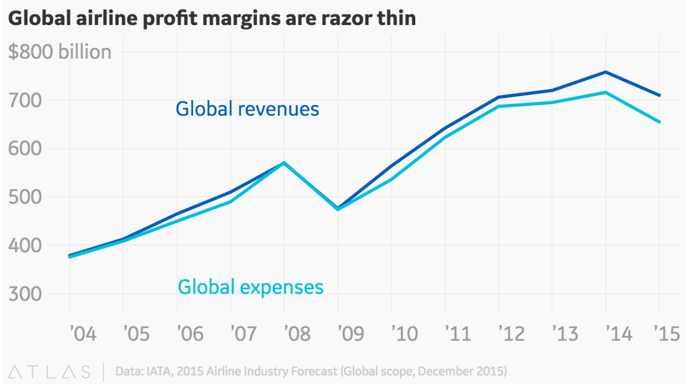


Figure 10: Thin profit margins for the airline industry

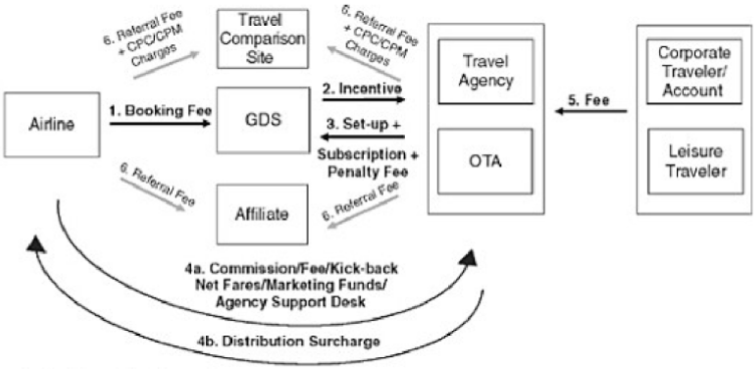

Airline
1. Booking Fee
GDS
Travel Comparison Site
Affiliate
6. Referral Fee + CPC/CPM Charges
6. Referral Fee
6. Referral Fee + CPC/CPM Charges
2. Incentive
3. Set-up + Subscription + Penalty Fee
6. Referral Fee
Travel Agency
OTA
5. Fee
Corporate Traveler/ Account
Leisure Traveler
4a. Commission/Fee/Kick-back Net Fares/Marketing Funds/ Agency Support Desk
4b. Distribution Surcharge

Figure 11: Tangled web of fees when buying an airline ticket

Aviation Market Overview

Globally, commercial airlines will generate combined revenue of around 824 billion U.S. dollars in 2018. With Airports like Atlanta handling over 100 million passengers annually, there seems to be a large market of potential users for a transparent and flexible technology that maker passenger transportation easier for all involved stakeholders (Statista 2018). While revenues in the industry reach new highs every year, so do costs as illustrated in figure 10. The resulting operating margins are small and make the industry susceptible for economic shocks.

If an enhanced ticketing systems would be able to reduce costs along the value chain between operator and passenger, there could be benefit for everyone - for operators and airlines with higher margins, for passengers with attractively priced and resellable tickets. When looking at the currently prevailing mechanism for ticket sales, the Amadeus platform is the dominating player in the market. This system was built in the last millennium and relies on booking classes for which capacities are changed by the airlines. This leads to overbooking of planes and non-transferable tickets. Many carriers have already started to counteract the high fees in the ticket-sales process by setting up direct ticketing distributions and charging extra ticket fees, but profit margins over 40% of the booking system providers still surpass those of companies like Apple, while ticket distribution cost around 12% remain a major cost factor as illustrated in figure 11 (Hanke 2016).

Within this environment a decentralized, trustless ticketing system would benefit both passengers and carriers. With current visibility of the fast changing environment, the aviation industry could be a first usecase for the technology of this research project.

Dynamic Pricing in the airline industry

Currently, ticket pricing in the industry is highly intransparent and carriers like American Airlines change around half a million prices per day (McAfee and Te Velde, n.d.). Consumers have to consider multiple factors when making a decision. This decision gets even more complicated if the destination can be reached by driving as well:

- The time involved in searching for the best deal.
- Uncertainty about whether or not you got a good deal.
- Travel time to the airport.
- The wait time at the airport.
- Uncertainty about unforeseen charges.
- Airlines overbooking strategies.

Additionally, the prices from websites oftentimes don't reflect the full package including taxes, fees etc.

A fully transparent and transferable ticket, based on blockchain technology, would make this process much easier. It could also include algorithms that help the consumer to decide to chose the most economic way for his personal travel plans.

Research Objective Aviation

The objective of the research project is to find out how a decentralized ticket booking and distribution system can be build to access the potential that is currently unused. This should take into consideration several factors like environmental impact (through energy usage), speed and capacity (given the large scale global market and the high number of passengers). Furthermore, we expect several optimization problems to arise along the way such as routing, capacity planning, catering etc.

Optimization Problem	Potential method
Routing	Graph Theory, min. spanning tree (Chinese Postman Problem)
Dynamic Pricing	Algorithms for dynamic and client-centric pricing (Bounty)
Ticket Marketplace	Possibility to trade tickets (Bounty)
Catering	Economically efficient catering based on dynamic ticket prices (Bounty)
Capacity	Economically efficient capacity management with regards to fleet, routes, schedules as a function of dynamic ticket pricing (Bounty)

Simple online store usecase

A rather simple application could be to create a digital image of the processes needed to run an online store. For illustration we chose a case that is related to the aforementioned transportation case, but with simpler products. Assume the product is a softdrink from a local brewery. It shall currently only be distributed in the region but might have received media attention so that there is assumed demand in other regions.

The blockchain approach would be to implement each product as an asset on the chain. As some information storage would be needed for this, it might be helpful to use a blockchain solution that is coupled with a database backend like Mongo DB or Rethink DB to store the data of each asset.

Where classical solutions are oriented along the processes (procurement - storage - order - packaging - shipping - billing) and have many interfaces between the IT systems that govern each or several steps of the process, the DLT solution would be able to combine the entire process chain as informational states of the assets itself.

Each asset would be created on the blockchain and simply store its state in an updateble format. PAssing on to the next step or process would then be modeled as transaction on the blockchain, in which the asset is "sold" or transferred to a new owner, namely the next step in the process. The information for when and how this happened could be stored in the asset as well. This would create the advantage that the consumer could understand and retrace each step the asset / product has gone through, even when handled by a number of different and potentially independent (i.e. running on different IT systems) service providers.

Asset contract design

BTRI is currently modeling such an approach in combination with an online store. This particular design along with advantages and sample apps shall be discussed in a separate working paper in more detail (the BeerBlock App).

SME wholesale warehousing solutions

Another interesting approach to implement a distributed ledger solution that models a trading process with slighty more complex products is currently being developed as well.

BTRI is researching the optimal design in an environment where the products are variable, i.e. priced by weight and material, not on an itemized basis. This problem is more complex as every sales process potentially goes a different route. Say the warehouse holds a piece of sheet metal in the dimensions fo 2000x2500 mm and the customer wants to buy a piece in smaller dimensions. The original piece has to be cut to the customer's requirements - but how? What is the ideal way to cut the original piece so that the rest is still sellable and the customer doesn't have to be charged for the waste.

Pricing the ordered piece is easy as we can get the weight from the dimensions and density of the product. The asset design would simply start with the original size sheet. The asset would then be "sold" to the saw and two (or more - depending on how many cuts are needed) new assets would be created and updated with new dimensions. Pieces under a certain threshold would be labeled as waste and their cost added to the ordered asset. Remaining assets can still can be sold separately would not need to be charged to the client but could reenter the warehouse (by updating an "in-warehouse" variable to TRUE) and thereby be picked up by the online shop displaying every item in the warehouse.

Likely milestones and conclusion

Given the aforementioned background we believe that research to implement a subordinated blockchain solution for the outlined usecases could encompass the following:

Milestone	Description
Structural Design	Design of subordinated blockchain with data types specific to problem
Stepwise implementation	Implementation of the subordinated / child contracts in a test environment
Proof-of-concept	live usecase implementation (i.e. with the FVL, a 100+ year history flight organization), participation of beta-tester / tokenholders
Publication	Publication of results (priority access for tokenholders)

Questions regarding a potential timeline will heavily depend on available funding (i.e. how many people we'll get working on this) so that a timeline cannot be foreseen at this stage. However, with our initial funding goal of EUR 5 Mio. we assume to be able to present first results before year-end 2018 and proof-of-concepts versions during 2019.

Questions for further expansion of the research can lie in making the technology easily accessible and therefore usable. We envision to that any potential distributed database will run on the tokens that are being given out as confirmation of your donation to the foundation.

Conclusion

In this paper we have given an overview of the current state of distributed ledger technology as well as outlined the major shortcomings that hinder the acceptance and broad application by real-economy users, especially on a larger corporate scale.
We believe that much of the required technology for a truly user-friendly application is already available but not yet connected.
Furthermore, we list a number of potential usecases of the blockchain technology within real-economy applications and outline the potential market sizes respectively to illustrate the potential disruption impact.
Namely, the main usecases are in export finance and in transportation but both applications have a two-tiered complexity build in - to actually make blockchain technology usable one has to also provide not only a solution on the information storage / content side of the problem but also on the payment-system side. At the same time, renovations in payment systems would have the highest disruptive effect on real-economy usecases. Regulators are catching on quickly and tend to err on the side of over-regulation rather. Despite already being ongoing, we define a number of research objectives that should be expanded deeper. We hint at possible solutions like child-chains and also outline potential and possible challenges in this research like issues around security, transparency and user-friendliness.

Much more research to come, thanks to your generous support!

References

Archieri, Tony. 2018. "Proof of Work Is the Worst Way to Do a Blockchain." webpage. http://www.metzdowd.com/pipermail/cryptography/2018-February/033788.html.

Demirgüç-Kunt, Asli, Leora F Klapper, Dorothe Singer, and Peter Van Oudheusden. 2015. "The Global Findex Database 2014: Measuring Financial Inclusion Around the World."

Hanke, Michael. 2016. *Airline E-Commerce.* Routledge.

Lamb, David. 2018. "Cryptocurrency Mining Is Hampering the Search for Alien Life." https://www.engadget.com/2018/02/14/cryptocurrency-mining-is-hampering-the-search-for-alien-life/.

LBBW. 2017. "Daimler Und Lbbw Setzen Erfolgreich Blockchain Bei Schuldschein Transaktion Ein." *Website LBBW.* Daimler AG. https://www.lbbw.de/de/presse/presseinformationen/presse_detail_71040.jsp.

McAfee, R Preston, and Vera Te Velde. n.d. "Dynamic Pricing in the Airline Industry."

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System."

Poon, Vitalik, Joseph; Buterin. 2017. "Plasma: Scalable Autonomous Smart Contracts." *Plasma.io.*

Statista. 2018. "Revenue of Commercial Airlines Worldwide from 2003 to 2018Revenue of Commercial Airlines Worldwide from 2003 to 2018." Statista. https://www.statista.com/statistics/278372/revenue-of-commercial-airlines-worldwide/.

"Technology-Adoption-by-Households-in-the-United-States." 2018. https://ourworldindata.org/grapher/technology-adoption-by-households-in-the-united-states.

"The Global Export Credit Dimension." 2014. NAM National association of manufacturers. http://www.nam.org/Issues/Global-Export-Credit-Dimension-Web/.

Tron, Aron;Nagy, Victor;Fischer. 2016. "Swap, Swear and Swindle: Incentive System for Swarm." whitepaper. http://swarm-gateways.net/bzz:/theswarm.eth/.

"Venezuela's Hyperinflation Sees Record Highs of Bitcoin Use." 2016. CNN. https://www.ccn.com/venezuelas-hyperinflation-sees-record-highs-bitcoin-use/.

Viglione, Rolf;Yabut, Robert;Versluis. 2017. "Zen White Paper." whitepaper. https://bravenewcoin.com/assets/Whitepapers/Zen-White-Paper.pdf.

Vries, Alex de. 2018. "Bitcoin's Growing Energy Problem." *Joule* 2 (5): 801–5. https://doi.org/10.1016/j.joule.2018.04.016.

Wood, Dr. Gavin. 2017. "Polkadot: Vision for a Heterogenous Mulit-Chain." Whitepaper.

Zyskind, Nathan;Pentland, Gui;Oz. 2017. "Enigma: Decentralized Computation Platform with Guaranteed Privacy." whitepaper. https://enigma.co/.