Global marketplace on blockchain

A white paper

Executive Summary

Lykke is a new company that will take advantage of breakthroughs in crypto-technology to build a global Internet exchange with immediate settlement for all asset classes and types of financial instruments.

The banking architecture is outdated and needs to be replaced. Crypto specialists have pioneered a new technology called distributed ledger technology (DLT) that makes a redesign feasible. DLT is an Internet based notary service that maintains a log of all financial transactions and keeps track of ownership. We propose an Internet exchange that uses DLT to trade all types of financial instruments. The benefits of DLT are immediate settlement, low transaction fees, the absence of a single point of failure, and strategic independence. Immediate settlement and highly competitive pricing will lead to rapid volume growth and establish the exchange as the Internet marketplace. This document provides an overview of the Lykke high-level software architecture, an analysis of the power of open systems, a risk assessment, and an evaluation of the legal context.

Table of content

Introduction

Today

The financial system architecture has grown organically. Over the past forty years, individual steps of the workflow of financial transactions have been computerized; the business process remained unchanged, as if processing continued to be manual. Delivery and settlement of transaction is batch based and occurs with a time delay of two and more days and does not happen at the time of the trade. The outcome is a convoluted banking architecture, a pile of spaghetti. Every bank has its own bookkeeping system and is an island from an audit point of view, where verification of trades is cumbersome and prone to errors. This regime contributes to a high degree of fragmentation and uncertainty in the market, multiplication of risk factors, high transaction costs for financial assets and lack of liquidity and transparency in financial markets.

Vision of the Future

There will be one global Internet exchange, where all financial instruments are traded and exchanged against each other, whatever their asset class or the size of transaction. Every financial instrument will be a listed security in the form of a digital token (a so-called colored coins[1]) and all transactions will be logged in a universally accessible distributed ledger, a decentralized notary service that ensures immediate global consensus about completed transactions and asset ownership. Like the Internet itself, the ledger is not controlled by a single entity, but an emergent phenomenon consisting of its participants. Trades will be settled and validated immediately; processing will be digital and transaction costs will be minuscule. The ledger includes a deposit box service, so that every owner of a digital coin has his own private key protecting his ownership. There will be an intraday interest rate market and yield curve. Market participants will be able to buy and sell colored coins of different issuers and change counterparty risk at any time. The number of traded financial instruments will grow exponentially, transaction volumes will skyrocket and liquidity will be ample.

Lykke aims to become the global marketplace and establish itself as the backbone of a new and highly sophisticated banking architecture that is not plagued by the deficiencies of the present system.

[1] Colored coins is a software protocol to specify terms and conditions attached to a particular Bitcoin or smaller Bitcoin increment. In analogy to financial securities issued as paper certificates, Bitcoin or a small increment is used as a kind of paper to specify additional terms and conditions. For example the ECB could issue a colored coins in the same way as it prints paper money; it would buy a fraction of a Bitcoin and then insert the ‚I_Owe_You' statement of the ECB, very much like a regular bank note but in digital format. The same mechanism can be used for any financial claim.

Distributed Ledger Technology

“A stroke of genius.” - David Andolfatto[2]

This chapter provides an overview over what DLT can and cannot do in comparison to a traditional software architecture. It also compares different variants of distributed ledger technology and compares them to Bitcoin, which is the oldest and most popular implementation.

What DLT does

In abstract terms, DLT is a way to find a consensus among a multitude of servers in the absence of mutual trust. Most DLT variants follow a proof-of-work protocol, which provides strong economic incentives for contributing to the network security (mining). The largest distributed ledger currently in operation is the Bitcoin blockchain. The hardware cost to match the computing power that currently secures the Bitcoin blockchain is likely in the triple-digit millions, if not higher.

How DLT works

A distributed ledger is fundamentally based on publicly announcing every transaction, thus allowing anyone listening to verify and track the balances of every other network participant. Whenever Alice wants to transfer 3 Bitcoins (or whatever currency that ledger supports) to Bob, she creates an according transaction, signs it and publicly announces it. From now on, everyone knows that Alice has 3 Bitcoins less and Bob has 3 Bitcoins more.
This is all there is to it. All other complications such as mining stem from the problem of ensuring the existence of a reliable public transaction archive and that everyone agrees on which transactions have actually happened in what order.

Traditional alternatives

As soon as the involved parties can be trusted, there are usually more efficient solutions than a distributed ledger. When the main issue is unreliable hardware that can otherwise be trusted, the Paxos algorithm is typically used. This is what Google does in order to provide reliable services with commodity hardware. Then, there are a number of database solutions that can be the most efficient in principle but require highly reliable hardware and also complete trust in the operator. Decentralization comes at a cost.

Proof-of-work

Bitcoin itself and most Bitcoin clones rely on proof-of-work to secure their blockchain. The idea behind proof-of-work is to increase the cost of an attack by letting the majority of the computing power in the network build the blockchain. A sustained brute-force attack would require a majority of computing power in the Bitcoin network. As proof-of-work comes with an immense amount of “wasted” computing power, “proof-of-stake” has been proposed as an alternative.

---

[2] David Andolfatto, Vice President of the Federal Reserve Bank of St. Louis, http://static.nzz.ch/files/8/4/1/Bitcoin-3-31-14_1.18303841.pdf

However, some argue that this approach is fundamentally flawed and so far, attempts at creating proof-of-stake based ledgers have had mixed success.

When to use DLT

A distributed ledger is a great platform to build other services on top, as it is an independent technology without any vendor lock-in or other entity behind it that might abuse it one day to further their strategic agenda. Examples of other such decentralized technologies that serve as a platform for others to build on are Linux, Email, or the Internet. A distributed ledger should be the technology of choice for projects that benefit from high inter-operability and versatility in use.

The most secure distributed ledger

When measuring security as the USD-cost of an attack, the most secure distributed ledger currently in existence is the Bitcoin blockchain. There are alternative cryptocurrencies that add security in principle thanks to certain tweaks. Litecoin, for example, uses a hashing algorithm that makes it harder to create specialized mining chips. Ethereum follows similar plans to discourage a professionalization in mining. But the sheer amount of computing power securing the Bitcoin blockchain dwarfs the effect of those tweaks. One cannot rule out that other cryptocurrencies succeed at taking the lead security-wise in the medium term future, but for now, the Bitcoin blockchain remains the most secure platform to build on.

The Power of the Bitcoin Platform

“Bitcoin may be the TCP/IP of money.” - Paul Buchheit [3]

Open platform technologies can unleash enormous powers, that would not materialize in a centralized setup. The classic example is the Internet, which thrives thanks to its open architecture and which has quickly outrun all alternative approaches (e.g. the French Minitel). Another example is Linux, which serves as an operating system for the majority of servers in the Internet. It main advantage is the fact that a company can commit to using it without becoming dependent on a potential competitor. A third example is the email protocol, which is being used to send billions of messages every day. Email would never have flourished to the same extent if it was directly controlled by a company. Similarly, Bitcoin is often seen as a platform for finance. The power of open technologies with open communities manifests itself in various ways. For example, there are dozens of websites visualizing Bitcoin transaction and market data, there are multiple vendors of Bitcoin ATMs, dozens of exchanges, and various merchant solution providers.

Community

Originally, Bitcoin was most popular among cypherpunks and crypto-anarchists. To this day, Bitcoin has significant number of proponents from that background, who love Bitcoin for its libertarian philosophy and who cherish it as digital gold. Driven by a vast inflow of venture capital,

[3] Paul Buchheit, Creator of Gmail, https://twitter.com/paultoo/status/328969714283995136

Bitcoin is of gaining broader traction among early adopters whose enthusiasm stems more from Bitcoin's usefulness and versatility than from its technical brilliance. Countless memes around Bitcoin have emerged, illustrating the creative dynamics of a large and diverse community of users. Figure 1 shows an artwork inspired by a recent 30'000 Bitcoin sell order posted by a wealthy seller on the exchange bitstamp. It managed to push the price down to exactly 300 USD for multiple hours, but was eventually eaten by hundreds of smaller bids, leading to a rebound towards 400 USD soon thereafter. This event is known as "the slaying of the bearwhale" (owners of large amounts of Bitcoin are commonly referred to as whales, whereas Bitcoin bulls are often pictured as Spartans).

Figure 1: The Slaying of the Bearwhale - Matt Habel 2014

Venture Capital

In 2014, Bitcoin saw unprecedented inflows of venture capital. Prominent firms such as Andreessen Horowitz, Draper Fisher Jurvetson, and Winklevoss Capital are examples, each of which having invested amounts in the double-millions into Bitcoin. Coinbase estimates 2013 venture capital investments to be more than 100 million, and projects them to reach 300 million in 2014.[4] The highest reported valuation of a Bitcoin startup is Coinbase with 400 million.[5] It is one of a number of a growing startups that have each raised venture capital in the double digit millions. While most Bitcoin startups are profit driven with a clear plan for generating revenue, blockstream which recently raised 21 million is a remarkable exception. Unlike other Bitcoin startups, blockstream aims at improving the Bitcoin infrastructure itself - without obvious financial benefit. Its investors argue that there is huge value in being able to help shaping the future of the Bitcoin protocol and being at the forefront of Bitcoin development.

[4] http://www.coindesk.com/will-bitcoin-venture-capital-investment-reach-300m-2014/

[5] http://recode.net/2014/11/14/ bitcoin-company-coinbase-raising-new-investment-at-400-million-valuation/

Bitcoin Statistics

The most important metrics for Bitcoin traction is the number of transactions per day, which is currently approaching 225'000, as illustrated in figure 2.[6] Another interesting metric is the amount of computing power supporting the network, which currently approaches 750 petahash/s (see figure 3). It would probably cost several 100 million USD in hardware to acquire enough computing power to dominate the Bitcoin network. The Bitcoin exchange rate peaked in autumn 2013 somewhat above 1000 USD, and now meanders between 300 USD and 400 USD. As currently 3600 new Bitcoins are mined daily, an inflow of more than 1 million USD per day is necessary just to hold the price at its current level, which is high, but obviously not unrealistic.

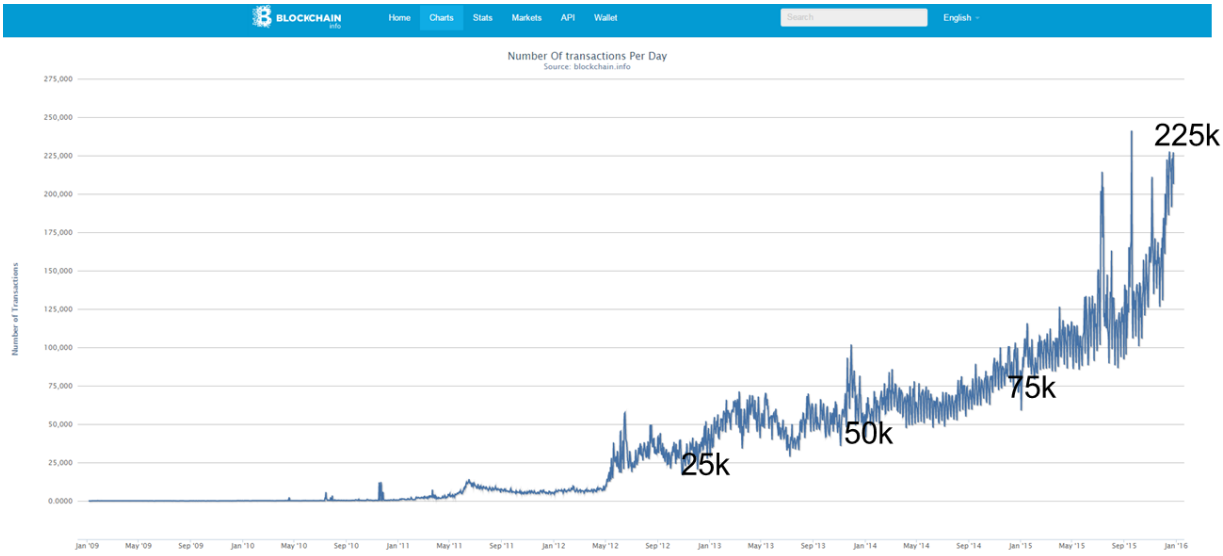

Figure 2: Transactions per Day

[6] https://blockchain.info/charts/n-transactions?timespan=all&daysAverageString=30

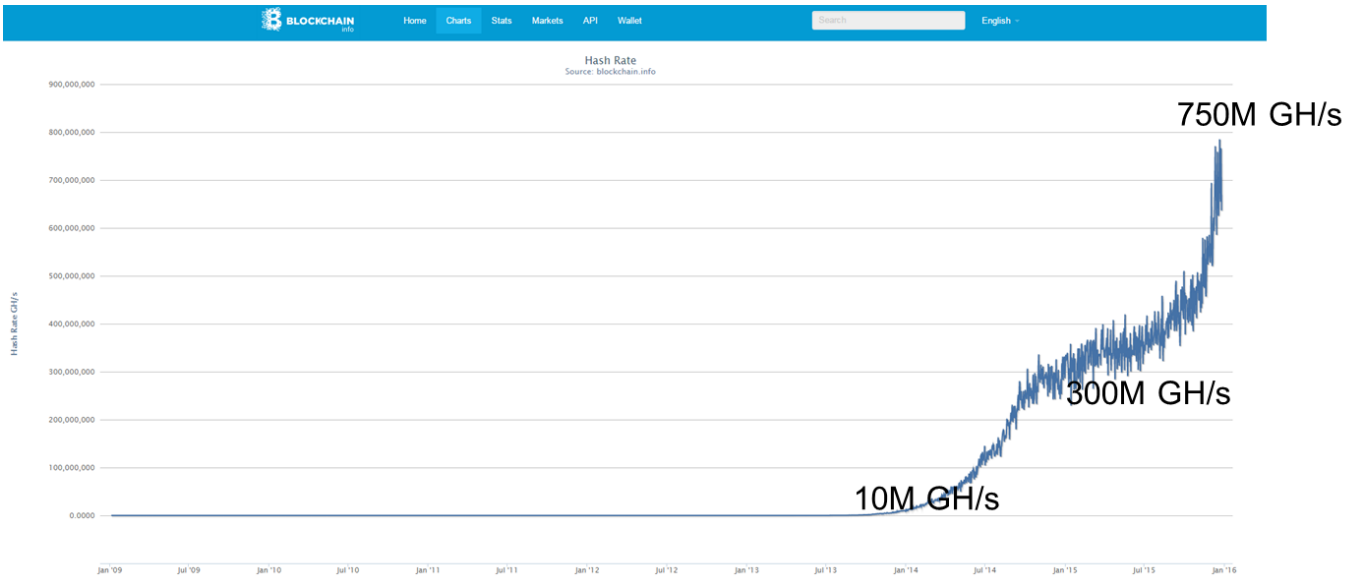

Figure 3: Computing Power Supporting the Bitcoin Ledger
(an average PC has about 0.01 GH/s, a specialized chip up to 1 GH/s)[7]

Initially, enthusiasts and hobbyists with desktop PCs and later graphics cards equipped with parallelized chip architecture did Bitcoin mining. Today, Bitcoin mining has become a professional endeavor, with custom-designed chips and a value chain of specialized services. Hardware manufacturers such as KNC[8] or Butterfly Labs[9] design and manufacture specialized hardware, which they sell to miners all over the world. The miners operate the hardware - typically in locations with low electricity costs (see figure 3). The miners sell the generated computing power to mining pools, who in turn create blocks for the Bitcoin blockchain and redistribute the freshly minted coins and earned transaction fees back to the miners.

[7] https://en.bitcoin.it/wiki/Mining_hardware_comparison
[8] https://www.kncminer.com/
[9] http://www.butterflylabs.com/

Figure 4: A Bitcoin Mine

The Winner Takes It All

Bitcoin is valued more than 7 times as high as the second most highly valued crypto currency, thereby clearly taking the lead (table 1).

The value of a currency strongly depends on the number of participants,[10] which in turn attracts more participants, leading to a network effect. Typically, communication technologies such as the telephone or WhatsApp and social networks such as Facebook share this network effect, which makes competing with the number one an uphill battle. Thus, Bitcoin has a significant first-mover-advantage, which plays out threefold:

- The more users there are, the more useful Bitcoin becomes, as there are more places to spend Bitcoin and counterparties to exchange Bitcoin with, attracting even more users.
- Currencies require trust, but trust can only be built over time, thus - everything else equal - giving the oldest currency a natural edge over its competitors.
- The more volume there is, the more transaction fees there are, attracting more miners and making the network more secure, which in turn again attracts additional users and volume.

With currencies that serve as a store of wealth, there is an additional lock-in insofar as it is takes effort to transfer that wealth into other currencies. Thus, there are multiple effects in place that make it very hard to dethrone Bitcoin. At this point in time, Bitcoin is the safest bet among crypto currencies.

[10] This effect is often referred to as Metcalfe's Law: http://en.wikipedia.org/wiki/Metcalfe%27s_law

#	Icon	Cryptocurrency	Market Capitalization in USD
1		Bitcoin	6,513,441,253
2		Ethereum	895,814,174
3		Ripple	268,451,213
4		Litecoin	147,322,748
5		MaidSafeCoin	44,534,778
6		Dash	42,628,125
7		Dogecoin	22,375,043
8		Monero	16,260,330
9		BitShares	15,138,043
10		Factom	14,921,525

Table 1: Cryptocurrencies by Market Capitalization[11]

Conclusion

Bitcoin is one of those technologies in which people see the potential to disrupt the world. It illustrates the power that open platforms can unfold. There are various competitors and clones, but none of them comes close to the popularity and success of Bitcoin. The many unsuccessful attempts of creating competing coins show that one should, whenever feasible, ride the wave and build on top of Bitcoin instead of creating one's own proprietary ledger. By building on top of Bitcoin, one can leverage the power if its blockchain, which has been continuously running for over five years and amassed computing power worth hundreds of millions, thereby enabling a lean business model, that stands on the shoulders of a giant.

[11] The total value of all coins in circulation at current prices is often referred to as market capitalization. Updated as of 28/03/2016. Source: http://coinmarketcap.com/

Colored Coins Exchange

We present the architecture of an exchange for colored coins (issuer-backed securities on the Bitcoin blockchain). Orders are collected and matched by a semi-trusted exchange. Matched orders are settled on the Bitcoin blockchain, where each successful trade between k parties appears as a set of k+1 transactions. Unfilled and expired orders are discarded. The exchange does not take possession of the traded coins, but needs to be trusted to match trades correctly. Assuming a basic level of trust in the trader - which could for example be established by providing collateral - trading can take place as fast as the communication between trader and exchange permits, with a subsequent settlement on the blockchain.

Introduction

Exchanges for crypto-currencies can be organized with a different degree of centralization. Typically, centralized exchanges are much more efficient, whereas decentralized exchanges are more secure as they require less trust in the exchange. Due to their higher efficiency and simplicity, most volume is currently traded on centralized exchanges such as BTC China, Bitstamp or Bitfinex.[12] A trader on such an exchange must entrust all assets in his trading account to the exchange. History shows that this is not without risk, with the most famous examples being the collapse of MtGox (more than 600'000 Bitcoins disappeared) and the hacking of Bitcoinica (43'000 stolen Bitcoins). Exchanges such as Bitcoin.de and LocalBitcoins are more decentralized and restrict themselves to organize trades and offer escrow services, but let the traders execute the actual trade bilaterally, whereas traders on LocalBitcoins often even meet physically. This naturally limits the achievable speed of trading to the speed of the underlying payment system (e.g. SEPA or moving bank notes). These exchanges can achieve a much higher trading frequency without having to resort to client deposits by restricting themselves to crypto-currencies that can be exchanged instantly. Examples of such exchanges or whole crypto-currency systems that include built-in decentralized exchanges are OpenTransactions, Ripple, Nextcoin, and BitsharesX - none of which achieved the same commercial success yet as the aforementioned centralized exchanges. These exchanges frequently try to even decentralize the matching of trades, which is problematic as it is fundamentally hard to enforce rules in a decentralized system, especially when timing is crucial. For the design of our exchange, we opt for a system with centralized matching of trades, but with direct bilateral exchange of assets, trying to combine the best of both worlds. One should also note that, when trading a particular colored coins or any other issuer-backed asset, there is exposure to a centralized point of failure anyway, namely the issuer.

Design Considerations

We follow the design principles of simplicity and minimal risk. Thus, we prefer proven systems with known shortcomings that are good enough for our purposes over theoretically better systems. The best validated distributed ledger technology is clearly Bitcoin, with a blockchain spanning back more than five years. Unfortunately, the Bitcoin network only supports one asset,

[12] Market Overview, bitcoincharts.com

the Bitcoin. One way to overcome this, would be to create an adapted version and to operate a separate blockchain that runs that adapted protocol. With a separate blockchain, one cannot benefit from all the computing power securing the Bitcoin network, calling for further adaptions, such as abandoning proof-of-work (majority of computing power says which transactions settle) for proof-of-stake (majority of coin wealth says which transactions settle) or something entirely different. The path of building a custom ledger has been chosen by a number of crypto-currencies, such as Nextcoin or Ethereum. This leads to the risks of over-engineering and stepping into uncharted territories, which are both hard to control.
Thus, instead of creating yet another distributed ledger, we decided to make use of the Colored coins approach, which builds on top of the Bitcoin blockchain. As the name suggests, colored coins follow the idea of “coloring” a specific Bitcoin, with an issuers guaranteeing to hand out the underlying assets to whoever returns that colored Bitcoins (or a fraction thereof). Thus, such colored coins are always linked to Bitcoins - like physical coins being bound to a few grams of a metal that also has a value in itself and is independent of the currency value. Further limitations are discussed in the scalability section.
The proposed exchange is positioned in between completely decentralized proposals (such as Counterparty) and completely centralized ones (such as Bitstamp). Decentralized approaches tend to come with significant overhead, for example by creating an entry on the blockchain for every issued order. Centralized exchanges are much more efficient, but require the exchange to take possession over the assets of the traders as deposits, which in many jurisdictions comes with certain regulatory duties (e.g. requiring a banking license). Our approach finds a middle ground between those two. Only completed trades enter the blockchain, while unfilled orders are discarded. At the same time, assets can be traded ad hoc and are directly transferred between the trading parties, thereby letting the exchange act as a mere broker without clients’ deposits.

Involved Parties

There are three involved parties:

- Issuers issue IOUs as colored coins. These coins can represent currencies, stocks, or any other transferable asset. An exchange can demand from the issuer to file a formal application for his coins to be listed, but there is no technical necessity to do so. In principle, any colored coins could be traded on an exchange - even without the consent of the issuer. The role of the issuers is passive, all they can do is observing completed trades as they settle on the blockchain.
- Traders possess Bitcoins or colored coins and desire to trade them for other assets. Traders typically need to be registered with the exchange in order to establish a basic level of trust (e.g. legally or by providing a collateral). To initiate trades, they send orders to an exchange of their choice. The traded assets must reside on a Bitcoin address associated with the trader’s account on the exchange. Traders primarily communicate directly with the exchange, but should also observe the blockchain to verify the correct settlement of their trades.
- Exchanges wait for traders to send them orders and collect them in an order book. The usual order types are supported (bid, ask, limit, etc). Matched trades are settled on the

blockchain. In principle, any asset pair can be traded, but in practice market forces will probably let a dominating currency emerge (similar to the USD in classical foreign exchange). There could be various competing exchanges.

High-Level Description

Traders create an order by creating and signing a transaction to send x coins to the exchange, whereas x is the amount and type of coins they intend to sell. Unlike usual transactions, this transaction is not sent to the Bitcoin network, but to the exchange instead, along with additional information about the order (type, asset to buy, limit, etc.). As soon as the exchange receives a matching order containing a second transaction, the exchange creates a third transaction that sends the exchanged amounts to the two traders. These three transactions together form a trade and are sent to the Bitcoin network for execution. The third transaction is also sent to the two traders, so they can immediately reuse the proceeds for subsequent transactions. Unfilled or cancelled orders are simply discarded.

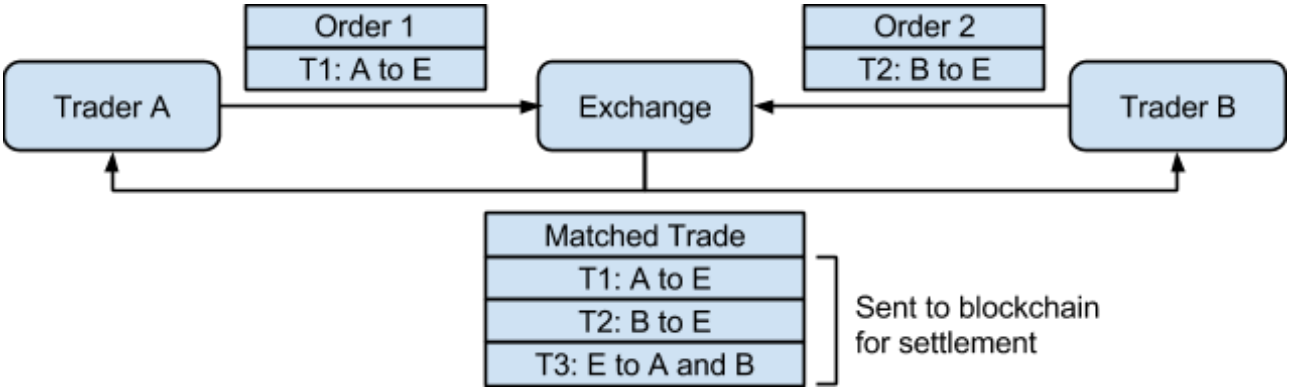

Figure 5: Transaction Matching: Each trader sends an order including a pre-signed transaction to the exchange. In case the exchange can match two orders, it creates a third transaction for the trade itself and sends them all to the blockchain for settlement. In case an order expires, it is simply dropped.

Alternative Approach

Depending on the desired properties of the exchange, one could also follow the alternative approach of having one transaction per trade that is signed by all involved traders. Its main advantages are guaranteed atomicity, and no risk of the exchange taking possession of the traded coins. Its disadvantage is that the orders are not enforceable: in order to execute a trade, both traders must sign a settling transaction after the orders have been matched. Thus, traders must be permanently online as long as they have pending trades. If one of them happens to be unavailable at the time of trading, the trade is delayed or fails, making execution less reliable and reducing achievable trading frequency to the speed of the party on the other side of the trade. We do not further describe this alternative approach inhere, but - depending on design priorities - it remains a valid option. In theory, one could even create an exchange that supports both types of orders and match trades across order types.

Matching

The employed order matching algorithm can be freely chosen by the exchange. For example, an exchange could allow for different order types: immediate orders that are matched as soon as possible, and fixing orders that are matched at the next fixing point. Thanks to the high transparency provided by the blockchain, these fixings are good candidates as official exchange rates.

Atomicity

Normally, all the three transactions that comprise a trade between two traders should make it into the same block, leading to atomic settlement of the trade. However, this cannot be guaranteed. A miner could embed the first two transactions without embedding the third transaction into the blockchain - for example because there is not enough space left in the current block. Since it is not possible to settle the third transaction without both of the others, the worst this can lead to is that the assets temporarily reside with the exchange until the third transaction settles.
In case of a large order that is matched with k smaller orders at once, all of the resulting trades can be executed in k+1 transactions.

Partial Trades

Most of the time, one of the involved orders will only be partially filled. The remaining funds are immediately returned to the sender for resubmission of the remaining trade. For example, if trader Toni issues an order to sell 100 USD for EUR and his order is immediately matched with 80 USD worth of counter-orders, the remaining 20 USD are sent back to Toni along with the acquired EUR. Toni's trading software then automatically creates and signs a new order to sell the remaining 20 USD.

Scalability

Generally, all received coins can immediately be reused in a new trade. Thus, trading can be as fast as the connection between trader and exchange permits (normally in the range of 10ms - 100ms). Temporarily, the number of trades can exceed the limits given by the Bitcoin blockchain, as this just leads to a delayed settlement. Note that the size of the collateral (or amount of trust in the trader) should cover the potential net gain of the trader when unwinding the unsettled transactions. Thus, the exchange should measure that potential net gain and block further trading in case it approaches the size of the collateral.
Today, Bitcoin has a limit of about 500'000 transactions per day.[13] Today, the network processes about 80'000 transactions per day.[14] The limit was set by Satoshi Nakamoto in 2009 with the aim of making sure that a typical home PC can archive and process every transaction in real time. As soon as the number of issued transactions hits the limit, miners will start to drop the ones with the lowest fees. As every dropped transaction means a loss of potential revenue, they will likely push for an increase of the limit in such a scenario. Also note that our exchange can probably afford to

[13] Depends on transaction, see also Maximum Transaction Rate on Bitcoin Wiki
[14] Blockchain.info, Number of transactions per day. https://blockchain.info/charts/n-transactions

pay higher transaction fees than the average user (e.g. 10 cents per transaction instead of just 5 cents as currently recommended), thus letting others suffer from dropped transactions first. The actual technical limit according to core developer Gavin Andresen is in the range of hundreds of millions of transactions per day.[15]

Another issue is that verifying the ownership of colored coins is computationally more expensive than necessary because the Bitcoin blockchain is unaware of their existence: instead of just verifying one transaction, the recipient of colored coins must verify the whole chain of transactions since the issuance of that coin. This verification is no problem for a normal PC, but could be for a light-weight client (e.g. a mobile phone). One could alleviate the problem by allowing the issuer to offer a reissuance service. Similar to a central bank that replaces worn bank notes with freshly printed ones, the issuer could renew often traded colored coins every now and then, thereby collapsing their transfer history and ensuring efficient verification. Another alternative would be to convince a majority of the miners to reject invalid colored coins transactions, which is politically hard - if not impossible - to achieve.

Attacks

Malicious traders could prevent the settlement of a trade by issuing a competing transaction that sends the offered coins elsewhere. Doing this is trivial as long as the order is pending and thus no transaction published - but assuming that the exchange provides an option to cancel pending orders, there is no motivation to do so as both result in the same, namely the cancellation of the order.

A malicious trader might also regret an order after it was matched and sent to the network, thus wanting to disrupt settlement. As transactions spread quickly through the Bitcoin network, successfully issuing a competing transaction to prevent that regretted trade would require collusion with the miner who happens to mine the next block - something a large mining pool probably would not want to risk its reputation for as such cheating attempts are perfectly detectable. The easy detectability also allows to automatically trigger counter-measures such as freezing the collateral of the trader or banning the trader.

A related attack is based on transaction malleability. Transaction malleability is a weakness in the Bitcoin protocol that allows anyone to slightly alter a transaction in ways that cause the transaction to change its id (hash). Should the altered transaction enter the blockchain instead of the original one, already issued follow-up transactions will be orphaned and fail as they use the original id to refer to their predecessor. The necessary adaptations to the Bitcoin protocol to fix this are known, but not implemented yet.[16]

Another attack on the system could be performed by the exchange itself. If hacked or run by a malicious operator, whoever controls the exchange could potentially take possession of all assets in all currently pending orders. This is already much better than the risk of traditional exchanges like MtGox to misappropriate all their clients accounts, but is still a significant risk that needs to be addressed through according security and regulatory measures. Theoretically, one

[15] Gavin https://gist.github.com/gavinandresen/e20c3b5a1d4b97f79ac2

[16] BIP 0062, Dealing with Malleability, https://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki

could improve the situation by adding order metadata to the transactions and convincing a majority of the miners to verify transactions and to refuse the settlement of invalid trades (for example, trades that does not respect the limit specified in the order). In practice, this might not be feasible due to the strong political resistance against any kind of major change to the Bitcoin protocol.

All the aforementioned risks pale in comparison to the counterparty risk inherent in colored coins. Regardless of how securely the exchange is organized, an issuer of colored coins could default or misappropriate the underlying assets. An exchange can help to alleviate this risk by only allowing the trade of coins from verified issuers with quantifiable counterparty risk. This risk can be mitigated by diversifying coins across multiple issuers and by swapping to coins that are deemed less risky if necessary.

Leveraged Trading

In order to provide leveraged trading, an intermediary service such as a bank willing to provide credit is necessary. This is basically the same as traditional leveraged trading.

Instead of directly trading on the exchange with their own wallets, traders will transfer their assets to a managed wallet. Such a managed wallet resembles a bank account, with the bank managing the wallet having full control over the contained assets. Like in classical banking, orders issued by the traders go to the bank first, where they are verified, and then sent to the exchange. The bank can then offer credit to the trader, which is added to the managed account. But as soon as the account is not sufficiently covered any more, the margin call is issued, the assets liquidated, and outstanding credit returned to the bank.

Competing Exchanges

At a later stage, it would also be nice to support competing exchanges. To do so, a protocol to discover the best trades needs to be introduced. Before issuing a trade, a trader takes a peek at the order book of various exchanges and then sends the order to whatever exchange he prefers. Assuming that all exchanges understand the same protocol and thanks to the fact that the traders does not need to have accounts with them, switching between exchanges on a per-trade bases is not problem. There could even be “best-execution” services to perform that work for the customer.

Integration

Colored coins will have an ISIN code, see www.isin.org. The code will be used to map the new instruments into existing risk management and bookkeeping systems of banks and other financial institutions. It is thus straightforward for the financial industry to embrace the new technology and move to immediate settlement.

Conclusion

Building a secure, high-performance exchange for colored coins is technically feasible. There are a number of trade-offs between performance and security. In a trusted environment, the highest performance is reached, whereas a completely secure setup comes at a price of slower

transactions. Both approaches can be mixed depending on requirements. Distributed ledger technology allows to run such a crypto-exchange in a fully transparent and open way, potentially allowing for anyone to trade on it with minimal trust requirements and providing a platform for other crypto-services to build on. Such an exchange could be an integral part of the growing ecosystem of crypto currencies.

Software Architecture

"Swift could someday send transactions in bitcoin as a currency if banks offer accounts in bitcoin" - Gottfried Leibbrandt, CEO of SWIFT[17]

Basics

Essentially, there are three major components:

- The DLT core library, which connects to the ledger
- The Colored coins extension
- Trading component

This section shortly describes them. Figure 6 illustrates how these three components are connected. When it comes to Bitcoin, there are hundreds of open-source projects in various programming languages that all could potentially help in getting a head-start as one does not have to reinvent the wheel.

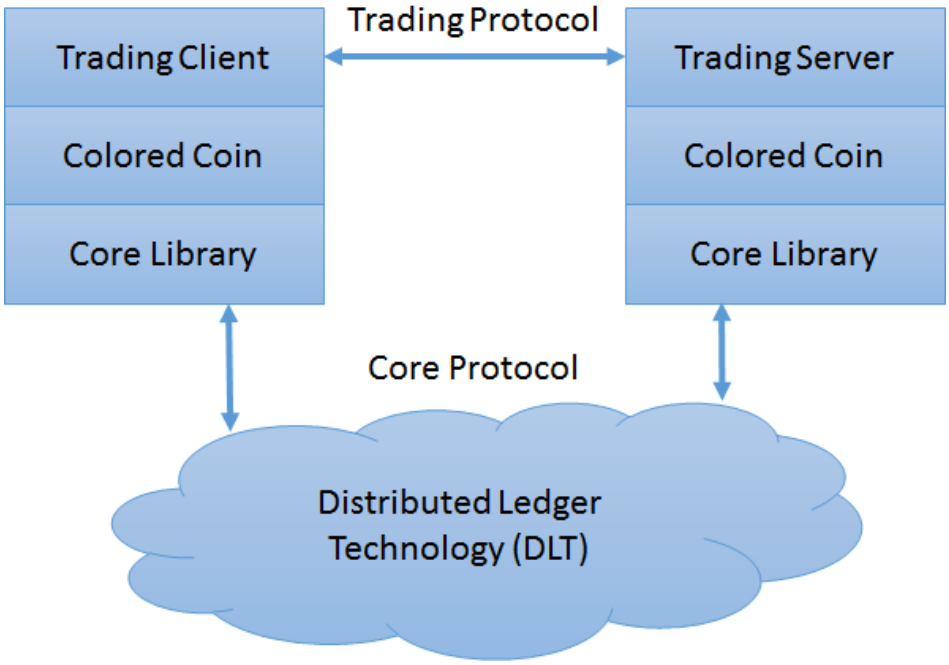

Figure 6: Software Architecture Basics

Core Library

This is the Bitcoin (or alternative DLT) core library. In the case of Bitcoin, the most major version is the main client, which is written in C++.[18] This is what most network participants run. There is also a Java[19] and a Go version[20] of the core library. However, they are not as well-tested as the C++

[17] http://bitcoinquotations.com/
[18] https://github.com/bitcoin/bitcoin
[19] https://code.google.com/p/bitcoinj/

version, which can pose a risk. For example MtGox repeatedly run into difficulties with their own custom-built PHP version of the Bitcoin protocol.
The core library connects to the Bitcoin network. If it is running as full node, it collects and verifies every single transaction that occurs. In SPV (simplified protocol version) mode, it only listens to those transactions that are relevant to the user. The C++ version of the Bitcoin core can either be directly embedded into other software, or interacted with through a JSON RPC interface.

Colored coins Extension

Building upon the core library, an extension to support colored coins is necessary. It scans relevant transactions for colored coins and maintains a database of balances by account.

Trading Component

The trading component sits on top of the colored coins extension and comes in two variants: one for the exchange and one for the trader. A custom protocol is used to interact between client and exchange, allowing issuing and canceling orders.

Potential Simplification

In principle, it would be possible to further simplify the trading client, by only letting it communicate with the exchange and not connecting to the distributed ledger. This slightly reduces the risk of attacks, as there is one less communication channel to the outside. But the trader would have to rely completely on the data it gets from the exchange and would not be able to independently verify transactions any more.

Extended View

Figure 7 illustrates how the basic architecture integrates in a wider context. On the trading side, there is the necessity for administrative tools as well as integration into existing trading desks via an appropriate choice of protocol (e.g. the popular FIX protocol). The administrative tools enable the monitoring of individual traders as well as the specification of limits and other restrictions. Figure 7 also depicts the role of the issuer. In practice, issuers will often also be traders and vice versa, but in principle, these are two distinct roles. Issuers issue new coins, which they can either do through their own distribution channels, or sell on the exchange. There is no necessity for a direct connection between issuer and trader, even though it might make sense to implement such a connection when enabling traders to quickly convert positions in traditional accounts into positions held in the form of colored coins.

[20] https://github.com/conformal/btcd

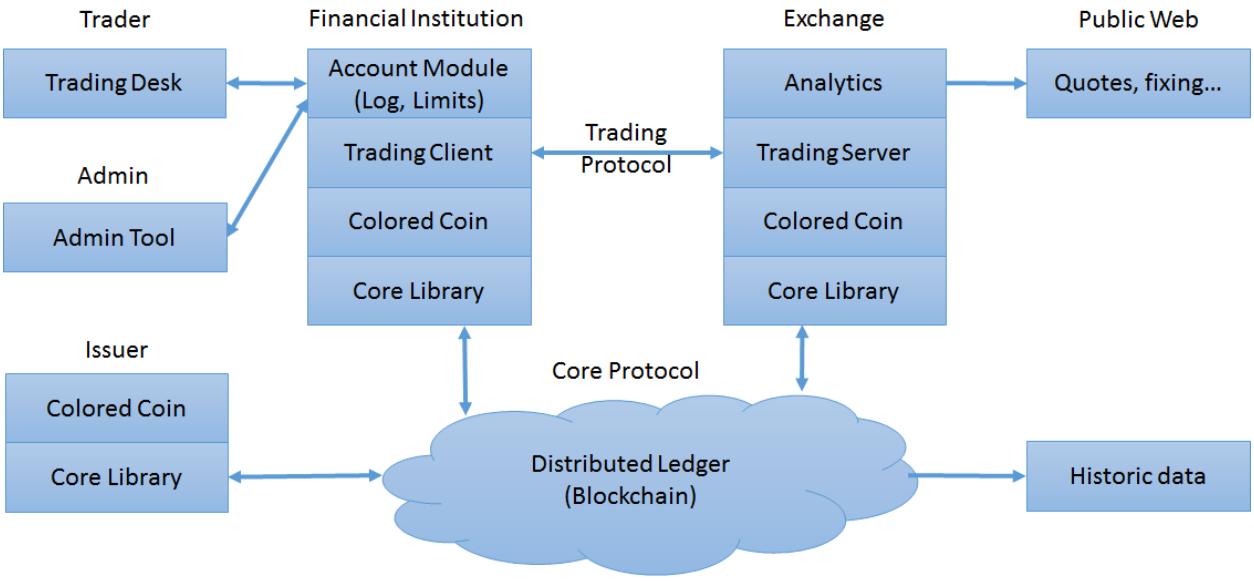

Figure 7: Software Architecture

Since every successful trade is recorded in the public ledger, the public ledger becomes a valuable source of trading data. While it is not possible to identify the traders, any observer can deduct quantity and exchange rates as well as fees paid from the public data visible in the ledger. While the data in the ledger already provides transparency, it can also serve as a valuable source for research. The data collected by the exchange goes much further. The exchange can identify traders and knows about all issued orders, not only those that lead to trades. Thus, the exchange can provide additional information services, such as data about the order book or hourly fixings, which can be made public on the website or via open APIs. In the Bitcoin ecosystem, there are dozens of services that read such data provided by exchanges and visualize it. Figure 8 shows one such service.

Figure 8: Bitcoin Wisdom, a market data visualization service [21]

[21] https://bitcoinwisdom.com/markets/bitfinex/btcusd

Secure Coin Storage

Secure coin storage is primarily relevant to traders and issuers of coins. They need to make sure that their coins are properly backed up and protected from theft.

Risk of Theft and Loss

Not unlike physical coins, colored coins are tokens that represent value. Consequently, there is a risk of those tokens getting lost or being stolen. For example, Christian Decker[22], a PhD student at the department of Computer Science of ETH, lost 9222 Bitcoins due to a successful intrusion by Russian hackers into his mining server.[23] Today, those Bitcoins would be worth multiple millions. Another known loss is that of Stefan Thomas, who lost 7000 Bitcoins due to an inaccessible backup.[24] He still has the private key to unlock those coins on a highly-secure memory card, but cannot access it as he forgot its password and the card is constructed in such a way that it self-destructs after five unsuccessful attempts. These two examples show that the responsibility for properly storing crypto currencies lies with the user. If a key gets lost, the coins are irrevocably lost. In case of a theft, there is a slim chance of identifying the thief and getting the coins back by use of legal force, but unlike in other financial systems, there is no way to undo transactions. This calls for services that professionally store cryptocurrencies on the users behalf - just like banks do with traditional currencies.

Backups

The most popular measure against loss is to create backups of the used private keys. The more backups there are, the higher the likelihood that at least one of them is still accessible when the funds are needed. As a private key has a length of only a few dozen Bytes, a widespread backup method is to print it onto physical paper and store that paper in a safe place (a so-called paper wallet). One can also encrypt the key with a password or other key before printing, in order to reduce the risk of theft.

Cold Storage

The aforementioned paper wallets do not only provide a secure backup, but are also immune to electronic attacks through viruses or other malware. Thus, Bitcoin companies often move larger amounts to cold offline wallets and only keep as much as necessary for daily operations online in hot wallets, which are exposed to such attacks. Moving coins to cold wallets is as effortless as sending coins to any other address, and thus can be fully automated. Only when moving the coins back from a cold to a hot wallet, a manual intervention is necessary. Depending on the type of cold storage, one might have to manually type in a code from a piece of paper, scan a QR code, connect a memory card that stores the private keys, or do whatever else is necessary to feed the keys into the computer.

---

[22] http://www.disco.ethz.ch/members/cdecker.html

[23] http://www.handelszeitung.ch/unternehmen/ hacker-stahlen-eth-doktoranden-bitcoin-fuer-9-millionen-536971

[24] http://www.spiegel.de/spiegel/print/d-91871156.html (story not accurate)

Multisignature Addresses

Bitcoin supports multi-signature addresses. Multiple private keys must sign any transaction moving coins away from such addresses. For example, one could specify that three out of five signatures must be present. In particular in larger organizations, this makes it possible to distribute the responsibility for highly secure processes such as the issuance of new coins across multiple persons and locations. For example, one could entrust five keys to five different directors in five different locations. When issuing new coins, an appropriate transaction is created and passed around. As soon as three directors have added their signatures, the transaction is released to the network, thereby issuing the new coins. Never during this whole process are the used keys in the same place and no one ever has access to more than one key at a time, making the process highly secure.

Securing the Market Participants

Securing the Exchange

In its most simple variant, the role of the exchange is that of a broker that matches orders, but never actually takes possession of the exchanged assets. Instead, the traded assets are directly transferred between the involved traders, all of whom have to sign the transaction that represents the trade. The way, the only value a successful attacker could ever steal from the exchange are the transaction fees. And those can be regularly transferred to cold storage, such that the worst-case damage done by a hacker is extremely limited by design.

Securing the Traders

Trading must be secured against attacks not only from the outside, but also the inside. Traders often do not trade with their own money, but are hired to do so in the name of a larger organization or a third party. Thus, there is an incentive to traders to misappropriate some of the entrusted coins.

This problem can be most easily tackled by using multi-signature addresses, such that each trade does not only need to be signed by the trader itself, but also a second person or service who monitors the trades. Such a monitoring service could be programmed to only allow trades that are within predefined limits or fulfill other freely specifiable criteria.

Alternatively, a server running within the trader's organization could sign the trades. Each entered order would first go through the organization's usual checks and filters, and only those reaching the server would actually be issued to the exchange. This second variant is probably easier to integrate into existing trading systems.

Securing Coin Issuance

Having access to the keys necessary to issue new coins is comparable to having access to the national banks printing press: one could issue arbitrary amounts of new coins to anyone. Thus, it is paramount to properly secure these keys and to follow a secure issuance process. Again, one option could be to use a multi-signature address as described in section "Multisignature Addresses".

Conclusion

The broad software architecture for operating the exchange as well as for the connected market participants is straightforward and does not yield any surprises. There are still many open questions when going into further detail, for example how to exactly integrate the service into existing trading environments, but we do not expect fundamental obstacles that would prevent us from realizing the architecture as described.

Risk Assessment and Mitigation

"While these types of innovations may pose risks related to law enforcement and supervisory matters, there are also areas in which they may hold long-term promise, particularly if the innovations promote a faster, more secure and more efficient payment system." - Ben Bernanke[25]

This chapter focuses on business, reputational, legal and broad technology risks. More specific technical risks are discussed in chapter "Colored coins Exchange White Paper" as well as chapter "Software Architecture", sections "Secure Coin Storage" and "Securing the Market Participants".

The business plan assumes that Lykke builds its technology on top of Bitcoin DLT. The public perception of Bitcoin is mixed due to a number of incidents in the recent past. We need to understand the risk history of Bitcoin and the risks of cryptocurrencies in general.

Bitcoin Risk History

Price Volatility

Bitcoin exchange rates have suffered from extraordinary, but decreasing, volatility in the past. As Bitcoins are not backed by any real value, no one knows what they are really worth, leading to significant price swings largely driven by greed and fear. Fortunately, more and more professional investors enter the market, which leads us to expect volatility to decrease further. Also, colored Coins have value independently of the value of Bitcoins and are thus unaffected by Bitcoins volatility, just like the value of bank notes is unaffected by volatile paper prices. Some exposure to Bitcoin volatility stems from the fact that transaction fees in the Bitcoin network have to be paid in Bitcoin, requiring the exchange to keep some limited liquidity in Bitcoins.

MtGox Default

MtGox used to be the largest and most popular Bitcoin exchange. Even though it repeatedly suffered from technical and other problems, it remained popular as there were only few alternatives. In January 2014, MtGox revealed that they lost half a billion worth of customer deposits in Bitcoin. It is still unclear what exactly happened. A likely explanation is sheer dilettantism and the funds were already lost or stolen much earlier without anyone noticing. This was not the first Bitcoin exchange to collapse and probably won't be the last one. However, the frequency of such issues seems to decelerate with newer and more professionally organized exchanges taking over.

[25] http://online.wsj.com/public/resources/documents/VCurrenty111813.pdf

Silk Road

Some abuse Bitcoin for illicit activities such as gambling or selling illegal goods and services. The most famous market place for such goods was Silk Road, which was closed by the FBI in 2013. In the meantime, imitations have appeared that are still online. Figure 12 shows a screenshot of the original Silk Road. Such markets tarnish the reputation of Bitcoin, and thus pose a reputation risk to everyone associated with Bitcoin.

Figure 12: Black Market “Silk Road” in 2012, before shutdown through FBI

It is unfortunate the Bitcoin the distributed ledger and Bitcoin the currency both have the same name, which makes it harder to distance one’s use of the Bitcoin technology from platforms such as Silk Road. However, we expect - similar to the development of the early Internet - that the Bitcoin ecosystem will become more and more professional with questionable market players gradually stepping into the background and being overshadowed by the growing number of positive use-cases, for example in micro-payments or remittance, and as a technology platform in general.

Legal Risks

There is legal uncertainty regarding Bitcoin and even more so colored Coins. In the medium run, law-makers might decide to address this uncertainty by creating new laws. These laws could for example regulate the issuance of colored coins in more detail or provide a regulatory framework for exchanges. Lykke needs to be prepared to quickly react to changing legal environments and to observe any relevant developments. For more details, see also chapter “Legal And Regulatory Environment”.

Risk of Abuse

Due to the versatility, colored coins could in principle also be used for illicit transactions such as money laundering. As colored coins can be transferred without the involvement of the issuer, the issuer can generally not veto suspicious transactions. Provisions in the issuance contract can mitigate this risk - in extreme cases one can even declare an issued coin worthless under some circumstances, for example when it is sent to a blacklisted account. Generally, the best points of intervention are the issuance and redemption of colored coins. Here, the issuer can demand arbitrary checks and additional information from the client - for example proofs of proper tax declaration. Thanks to all transactions being public it is possible to verify the plausibility of such information and to refuse the redemption if necessary. This risk is further limited by addressing the professional forex market with reputable participants that cannot afford to be involved in illicit activity. More details regarding the concern of money laundering can be found in the chapter “Legal Considerations”.

DLT Risk: 51% Attack

Distributed ledgers do not have a central authority by definition. The ledger is an emergent phenomenon consisting of its participants. Some form of majority vote reaches consensus - in the case of Bitcoin voting weight is determined by computing power. Thus, a group of people that succeeds at amassing 51% of the voting power in the network gains the ability to perform certain manipulations - a so-called 51% attack. Vitalik Buterin, founder of Ethereum, a competing DLT, fears that this could allow successful attackers to arbitrarily add Bitcoins to their accounts, thereby enriching themselves.[26] However, as long as there are other parties keeping a record of all transactions, this can be trivially detected and countermeasures taken. In fact, all of the major merchant payment processing services are already doing so and would simply refuse to accept Bitcoins obtained without adhering to the agreed protocol, rendering them worthless. This limits the 51%-attack to less harmful manipulations such as censoring transactions or undoing recently processed ones. Fortunately, the economics of Bitcoin would make a rational attacker use that computing power to support the network, thereby earning freshly minted Bitcoins and transaction fees, rather than attacking Bitcoin and thereby diminishing the worth of his own infrastructure.

[26] https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf

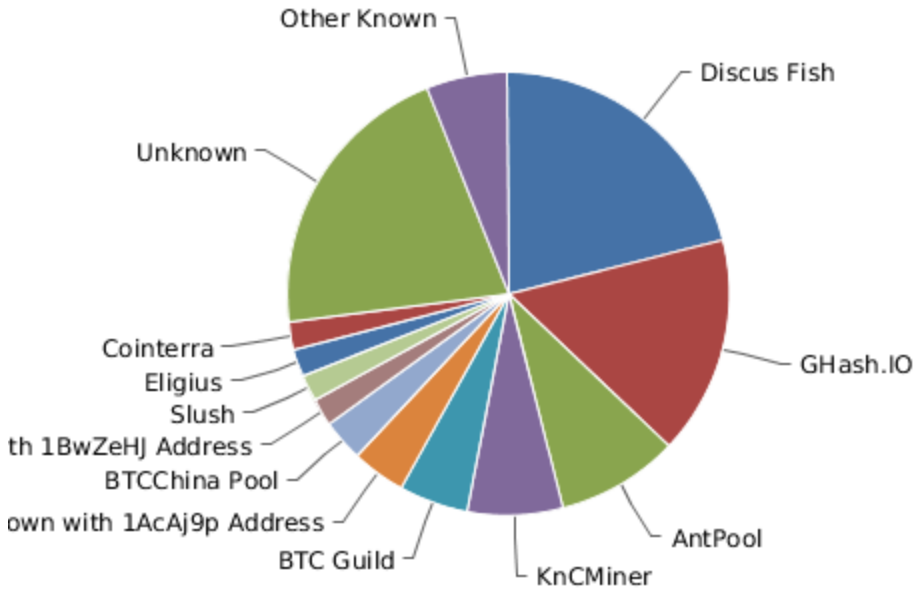

Figure 13: Computing Power by Mining Pool

Still, this remains Bitcoin's major weakness and often gives rise to discussion, as one cannot completely rule out the scenario of a malicious, irrational attacker with vast resources. Given today's computing power in the Bitcoin network, the cost of such a brute force attack would be in the triple-digit millions - far more than with any other cryptocurrency. Furthermore, such an attack will only have a lasting impact if the computing power is sustained, making the attacker susceptible to detection and prosecution (or other real-world countermeasures). Thus, it is very likely that any goal such an attacker pursues can be achieved more cheaply in alternative ways (e.g. through bribes, social engineering or other more traditional means).
A cheaper and more subtle variant of this attack is to gain control over a major mining pool and to then manipulate very few select transactions in collaboration with the issuer of the transaction before the transactions got confirmed (i.e. within about 10 minutes). This is usually averted by waiting for transactions to be confirmed before they are accepted. But if one does not want to await the 10 minutes confirmation time, other measures need to be taken, as described in the "Attacks" section of the white paper chapter.
As a general measure to mitigate such attacks, it is recommended that any major participant in the Bitcoin ecosystem runs a full node, i.e. logging and archiving all transactions, which would amount to a few terabytes of data per year at a rate of thousand transactions per second. Furthermore, one could reach agreements with mining pools or run a mining pool themselves. This gives more direct control over computing power and comes with potential benefits such as prioritizing own transactions.

Business Risks

We are early, but we are not the only ones working on a Colored Coin exchange. There is a risk that others are faster and better, which makes it important to be agile and to quickly adapt to

changed circumstances. We believe that the market we address first - namely professional foreign exchange - will bring us a natural edge over competitors that start in the retail market, as we will face fewer compliance challenges and be able to gain volume much faster. Bitcoin today as a daily trading volume of about 10 million USD, a drop in the bucket in comparison to the 5 trillion daily volume of worldwide Forex.

Every startup is a risky endeavor by definition and the prospect of high returns on investment comes at high risk.

Financial Risks

Lykke is subject to the spectrum of financial risks, including credit risk, market risk, liquidity risks and operational risks. The risk management framework will be developed to transfer and price the risks. Aggregated risk matrix is provided below:

Risk	Low	Medium	High	Mitigation
Bitcoin price volatility	X		`	Bitcoin not used as an asset. Small increment is colored (0.000006 BTC). Small fee is paid for processing (0.0001-0.0005 BTC).
Crypto-currency breaches	X			Blockchain is safeguarded by cutting edge technology.
KYC/AML		X		Regulatory standards will be applied. Only green nodes are allowed. Direct transfers of funds disabled.
Legal and regulatory risks		X		All blockchain obligations will be replicated in terms and conditions (legal contracts).
Risk of abuse	X			Safe settlement in the compromised environment. Green-node network (KYC). Strong market surveillance
Operational risk		X		KRIs, health check, capital allocation, best industry practices.
Credit risk		X		High rating institutions, reliable and regulated partners. Limit management system.
Market risk		X		Clearing and settlement of trades following market risk policy.
Liquidity risk		X		Treasury policy. Liquidity management system.

Table 2: Colored coins exchange financial risk profile

Legal and Regulatory Environment

"Despite a number of clearly identified risks resulting from its volatility, its anonymity and its lack of legal guarantee, the bitcoin offers multiple opportunities for the future, both as a payment system and, above all, as a decentralized validation protocol. Public authorities should work on a well-balanced regulatory framework, in order to prevent abuses while preserving the capacity of innovation. To that effect, the use of existing legal categories seems like the most relevant solution for now, for the definition of both virtual currencies and associated services."
- Commission des Finances, Sénat, Republique Francaise[27]

Crypto currencies are novel. Thus, it is not immediately clear how they map to existing legal concepts. The general consensus among lawmakers in different countries is that no new laws are necessary for now and that it suffices to properly apply the existing laws. This is also the conclusion of the Swiss Federal Council.[28] This section provides a short overview over what this means for the legal situation in Switzerland, according to various experts we have met and discussed the matter with.

Law Firms

We have met with lawyers from MME Partners (Martin Eckert, Luka Müller, and Gabriela Spühler), which are well-known for their competence in digital currencies in relation to Swiss money laundering regulation. They were the first to establish rules for online gambling in close collaboration with Finma and they are the law firm of choice by the DFCA (Digital Finance Compliance Association). We furthermore discussed the idea of a colored coin exchange with Martin Hess from Wenger & Vieli, who is one of the few experts familiar with the current state of the planned financial market infrastructure act (Finanzmarktinfrastrukturgesetz),[29] which aims to regulate marketplaces and other financial market actors in more detail and is likely to be discussed in parliament in 2015. We also discussed our ideas with Harald Bertschi[30] and Christian Meisser[31] from Lenz & Stähli at a legal conference, as well as with Prof. Seraina Grünewald[32], all of which are about to publish papers on cryptocurrencies and could be valuable future sources of relevant expertise. Furthermore, we have discussed our ideas with Yann Wermeille from Finma.

[27] http://www.senat.fr/rap/r13-767/r13-767-syn-en.pdf
[28] http://www.news.admin.ch/NSBSubscriber/message/attachments/35355.pdf
[29] http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20140061
[30] http://www.lenzstaehelin.com/en/people/attorneys/mode/detail/employee/baertschi.html
[31] http://www.lenzstaehelin.com/en/people/attorneys/mode/detail/employee/meisser.html
[32] http://www.rwi.uzh.ch/lehreforschung/alphabetisch/gruenewald/person.html

Relevant Laws

In our context, any law concerning financial market actors is potentially relevant. This is in particular the Geldwäschereigesetz (moneylaundering act), the Kollektivanlagegesetz (act on collective investments), and the Börsengesetz (exchange act). Furthermore, the upcoming Finanzmarktinfrastrukturgesetz (financial markets infrastructure act) will be of relevance once it is enacted. Furthermore, the Bundesgesetz über die elektronische Signatur (federal act on electronic signatures) might be of relevance should we ever decide to sign transactions with signatures that fall under this law, which comes with certain legal benefits (e.g. ensuring that each market participant can be identified).

Bitcoin

For Bitcoins itself, the legal situations is clear in general thanks to a report by the federal council[33] and additional clarifications by DFCA[34] in collaboration with Finma. Bitcoins are recognized as a form of wealth and as a means of payment. As a consequence, they are most likely VAT exempt.[35] Since there is no issuer and they are not backed by anything, they are not a security. Of all the existing financial instruments, they mostly resemble foreign currencies, but differ insofar as there is no country that recognizes them as legal tender. Legally, Bitcoins are very similar to private money issued by the WIR bank or also the Taiwanese dollar, which is issued by an entity which is not recognized as a country by the Swiss government.

Finma applies money laundering laws (GwG) to Bitcoin and other crypto-currencies in the same way as it applies them to traditional currencies. What is unclear as of now is how Bitcoin mining is treated; the most reasonable and likely approach is that miners are not financial intermediaries, but simply sellers of computing power in exchange for cryptocurrencies.

Finma requires a banking license to operate Bitcoin exchanges in Switzerland, as they host client deposits (Kundeneinlagen). This poses a high barrier of entry and is probably the reason why no Bitcoin exchange has yet been established in Switzerland. The Lykke design of the exchange with colored coins does not involve any client deposits.

Colored Coins

Colored coins are a novel concept and have not widely used. Colored coins are different in nature to crypto currencies, because they have a specific issuer and are backed by a financial asset. The legal status of colored coins depends on the kind of asset they are backed with, as well as the exact terms and conditions of issuance and redemption. Traditionally, financial securities have been issued as a physical paper certificate, digital colored coins might well fall

---

[33] http://www.admin.ch/aktuell/00089/?lang=en&msg-id=53513

[34] Digital Finance Compliance Association, http://dfca.ch/

[35] A tax ruling initiated by Bitcoin Association Switzerland with the federal tax office (ESTV) regarding this question is pending. However, the wording of the federal council report does not leave much room for a different conclusion than recognizing Bitcoin as means of payment, which do not underlie VAT when bought or sold.

into legally uncharted territory, which may be a blessing in disguise or represent an additional a risk factor.

The biggest risk is that the issuer of colored coins will be viewed as taking client deposits requiring him to have a banking license. If the issuer is a bank, then this is a non-issue. Lykke will initially target the professional market, which has all the legal wrappers and the necessary regulatory licenses.

As part of the execution plan, the details of issuance and redemption (with potential expiration) of colored coins, be it directly or through a distributor, will be specified.

Due to the unknown exact legal status of colored coins, it is unclear at which points KYC rules apply, if at all. A reasonable application of the law would require KYC checks whenever colored coins are issued and redeemed.
Furthermore, the sale of colored coins might be restricted to professional market participants such as Finma-licensed traders (Effektenhändler), which would inhibit the access of retail-traders to our platform and could therefore pose a risk to business-expansion beyond the professional market. There are no precedents. The only way to gain certainty regarding these issues is to approach Finma and discuss the open issues with the regulator.

Colored Coins Exchange

According to a forthcoming paper by Prof. Seraina Grünewald, colored coin exchanges fall outside the scope of existing regulation as long as they are limited to match-making, i.e. matching buyers and sellers and initiating the trade, without ever taking control of the coins to be exchanged. This is good news as it would allow Lykke to start as an exchange in its most simple and secure mode without any special license or permit.
However, with the previously described high-performance trading, which requires Lykke to temporarily take possession of traded coins, it is necessary to be regulated as a Multilateral Trading Facility (MTF) as specified in the new financial market infrastructure act.

Objectives of Regulators

In response to the 2008 financial crisis the regulators have tried to reform the banking architecture. Progress has been modest and very little of substance has been achieved. The Lykke proposal promises a leap forward: it is possible to introduce real time settlement in a seamless fashion - every market participant can get immediate settlement by using Lykke; no heavy handed regulatory enforcement is necessary. There are other advantages as well. The trading of colored coins is an elegant way to price counterparty risk between different issuers.

We have been in contact with Yann Wermeille of the Finma to discuss the proposal of creating a modern Internet exchange; the feedback was very positive. Likewise, we have met up with members of the Fed, FSA and Bank of England and again, they were very supportive.

We have also met with the parliamentary group for digital sustainability,[36] which consists of digitally interested members of all major parties and which is very supportive of any developments that could help to preserve the competitiveness of Switzerland's financial sector. In 2013, they wrote a postulate that suggested to legally treat Bitcoin like any other currency, e.g. the euro.

[36] http://www.digitale-nachhaltigkeit.ch/

Conclusion

The distributed ledger technology will revolutionize business processes and have a profound impact on the financial industry; there is no way backwards, the innovation has been made and cannot be sidestepped. Similar to the Internet itself that has penetrated the most distant places on earth, the DLT will do likewise. The development of the distributed ledger technology is a major innovation that will disrupt the financial industry.

Lykke will build an exchange to trade financial assets as colored coins using the Bitcoin blockchain. Initially, we will focus on the professional forex market, in which we see the most potential due to high volumes and the highest potential for gaining market share rapidly. Lykke matches buyers and sellers; trades are directly settled on the distributed ledger. Thanks to cryptographic property guarantees, this provides every trader with an unprecedented level of control over his assets. We have opted for the Bitcoin blockchain, because it offers the highest level of security compared to other DLTs, has enormous momentum with large inflows of venture capital, has the longest track record of robustness and is known for its enthusiastic grassroots community.

Lykke users will be able to switch counterparties in a matter of minutes and will not be hostage to counterparty risk with two-day delivery, as is standard business practice for other venues. The operational efficiency of the exchange will translate into low ticket fees and the matching engine with price-spread-time queuing will provide for efficient price discovery. The combined effect of these features will attract a lot of volume, initially from the price sensitive trader community that focuses on short-term trading. In recent years, a number of new marketplaces have started from scratch and succeeded to establish themselves side-by-side to established exchanges. They provide evidence that market participants are ready to move to new trading venues.

The mission of Lykke is to become the global marketplace and establish the exchange as the backbone of a new and highly sophisticated banking architecture that is not plagued by the deficiencies of the present system.

Literature and Resources

This chapter lists the most important resources and further literature. It does not repeat all the sources already cited elsewhere in the report.

Technical Resources

Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008.
Satoshi presents his invention in this famous paper and publishes a first prototype a few months later. bitcoin.org/bitcoin.pdf
Bitcoin source code: github.com/bitcoin/bitcoin
Bitcoin protocol specification: en.bitcoin.it/wiki/Protocol_specification

Yoni Assia et al, “Colored Coins - BitcoinX”, the technical specification and ongoing discussion on colored coins,
2014,docs.google.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE/edit#heading=h.v3px1rgmf10o

List of BIPs (Bitcoin Improvement Proposals): en.bitcoin.it/wiki/Category:BIP
Coinprism: a web-based wallet for colored coins. www.coinprism.com
Chromawallet: an application based wallet for colored coins. chromawallet.com
Ethereum: ethereum.com
Ethereum white paper: ethereum.org/pdfs/EthereumWhitePaper.pdf

Financial Reports on Bitcoin and DLT

UBS, “Bitcoins and Banks, Problematic currency, interesting payment system”, 2014. No public link.

Bank of England, “Innovations in payment technologies and the emergence of digital currencies”, 2014.
www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf

ECB, “Virtual Currency Schemes”, 2012.
http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

JP Morgan, “The Audacity of Bitcoin”, 2014. ultra-coin.com/images/Coins/206481948-JPM-the-Audacity-of-Bitcoin.pdf

Goldman Sachs, “All About Bitcoin”, 2014.
www.paymentlawadvisor.com/files/2014/01/GoldmanSachs-Bit-Coin.pdf

Bank of America, “Bitcoin: a first assessment”, 2013. ciphrex.com/archive/bofa-bitcoin.pdf

Wells Fargo, “Bitcoin 101: A Primer”, 2014. No public link.
Federal Reserve Bank of St. Louis, “Bitcoin and Beyond: The Possibilities and Pitfalls of Virtual Currencies”, 2014. static.nzz.ch/files/8/4/1/Bitcoin-3-31-14_1.18303841.pdf

Fitch Ratings, “Sizing up Bitcoin”, 2014. thewhyforum.com/articles/sizing-up-bitcoin

The Economist, “The great chain of being sure about things”, 2015. www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

Community Resources

BitcoinTalk: the most popular online forum on Bitcoin, bitcointalk.org
Bitcoin Reddit: a popular Bitcoin news aggregator: www.reddit.com/r/bitcoin
Bitcoin Foundation: an US organization to support Bitcoins: bitcoinfoundation.org
Bitcoin Association Switzerland:bitcoinassociation.ch
Global Bitcoin Alliance: global-bitcoin-alliance.org

Government Reports and Legal Resources

Swiss Federal Council report on Bitcoin: www.news.admin.ch/NSBSubscriber/message/attachments/35355.pdf

Comments by parliamentary group for digital sustainability: www.digitale-nachhaltigkeit.ch/2013/12/bitcoin/ and www.digitale-nachhaltigkeit.ch/2014/07/bundesrat-beantwortet-bitcoin-postulat

Digital Finance Compliance Association: dfca.ch

European Banking Authority, “Opinion on Virtual Currencies”, 2014. http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

BitLegal: Legal status of Bitcoin around the world. www.bitlegal.io

Wall Street Journal, reporting on Bitcoin senate hearing, “Authorities See Worth of Bitcoin”, online.wsj.com/articles/SB10001424052702304439804579205740125297358
Finance Commission of the French Senate, “Public Authorities and the Development of Virtual Currencies”, 2014. http://www.senat.fr/rap/r13-767/r13-767-syn-en.pdf

Committee on Finance, US Senate, “Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Tax Compliance Risks”, 2013. www.gao.gov/assets/660/654620.pdf