PayCoupons

A high-liquidity cryptocurrency solution for economic exchange.

Matthias Ansorg, Daniel Ansorg
2018-06-14

Contents

1. Summary

Current economies suffer from economic deadlocks and extreme disadvantages for entrepreneurs based on the market dominance of established companies. Both issues are connected to design properties of state currencies (interest, compound interest, and centrally controlled scarcity to manage the value). We have set out to solve that with a completely new mode of economic exchange.

For that, we are creating PayCoupons, an exchange platform where participants pay each other with self-issued value coupons. Everyone issues their own coupons and accepts payments in their own coupons only. To get newly issued coupons to those who want to use them for payments, a network barter algorithm calculates multilateral barter trades where every participant receives coupons they want in exchange for coupons they issue. (This is our core innovation.)

On a system level, this yields a stable economy where every small business and startup gets its chance in the market. Our coupons use well-known state currencies (Euro, U.S. Dollars etc.) only as a unit of value, so including coupons into business accounting is trivial but no state currency is needed to obtain coupons.

PayCoupons is a cryptocurrency system: below, we introduce cryptographically secure, irreversible offline payments for all coupons. Since these payments can be done offline and are never recorded on a blockchain, they cannot be traced online.

The PayCoupons also requires a platform for multi-party exchanges, which is provided as a mature, centralized online platform.[1] While there are clear benefits in a decentralized alternative, state-of-the art blockchain technology cannot provide this yet while also maintaining user privacy. For that, blockchains must fist support efficient and secure multi-party computation and atomic transactions with thousands of participants; both are severe challenges which, at this stage, no single party can promise to solve. However, we lay out a clear roadmap for future steps towards a decentralized exchange system if and when the cryptocurrency technology matures.

In contrast to traditional cryptocurrencies which are are volatile and deflationary, we designed a system that is great at facilitating economic exchange: actually more so than money, and in our estimation also more than any existing cryptocurrency solution. We estimate that, even in its current centralized nature, our system for economic exchange can replace fiat money currencies in many applications.[2]

For payments of usage fees on the PayCoupons exchange platform (as a commission of issued coupon value), we introduce a cryptocurrency token on the Stellar blockchain. Together with various ways to obtain or earn these coupons in distribution events, this provides a suitable workaround for all users who cannot easily make small international online payments with money. As of 2018, this still includes large parts of developing countries where credit card companies either do not or cannot provide regular credit cards, and where online payment services like PayPal do not exist.

Details of our token distribution strategy are discussed in chapter "Token Distribution".

---

[1] Open for productive use at https://pay.coupons/

[2] The exception is for spontaneous purchases outside of established business relationships, where traditional currencies perform better compared to any one type of coupons, due to their wide acceptance.

2. Our Economy is Broken (in so many ways)

Since the demise of communist command economies, nearly all national economies and the whole international economies are governed by a mixture of price and regulation. Due to economies of scale, large-scale companies have advantages in both creating cheap products and meeting (or circumventing) regulatory requirements. Over time, this lets established market actors outcompete small and new companies in all sectors of the economy. Only new economic sectors provide some companies with a chance for long-term success, before they mature and shut off this market to newcomers – this is exactly what happened with the Internet, now dominated by a few large players. And due to the advanced state of automation (and pre-existing inequality), there is not enough economic demand for all that can be produced, leaving a large section of the populace in economic precarity. This is how market economies create permanent inequality, to the permanent disadvantage of small and medium businesses.

Inequality, combined with permanent underemployment, is a situation where “the disadvantaged” have resources but can't use them to provide for their own living because the economic system, on average, does not let them start a new business. Among these resources is the working time of the unemployed. This situation is a deadlock, a situation of circular dependencies where “everyone is waiting for everyone else”, blocking any progress. In this case, the disadvantaged wait for jobs so they can fulfill latent demands, which would provide jobs to others. In fact, it is worse than a deadlock: providing the poor with money does not create jobs for the poor in return, but only additional demands of the more competitive products of established market actors.

To solve this issue, a new economic exchange system must provide (1) a way to break the deadlock and (2) a way to isolate the demands and offers of the disadvantaged into its own closed economy, so they do not immediately have to compete with established producers.

National economies have a (limited) way of breaking deadlocks by Keynesian “countercyclical” spending of the state. However, without meeting the other requirement this does not help the permanently disadvantaged members of an economy, only against the ups and downs of regular economic cycles. "Quantitative easing" and other countercyclical spending also helps the wealthy more than the poor because the money is received by banks and big industry first – and only some levels down some of it becomes wages of ordinary workers. And only in this role, the money helps an economy to recover because the marginal propensity to consume of low- and middle-income consumers is higher than that of high net worth individuals. In other words, an increase in the spending capacity of a poor individual has a higher effect (via Keynesian multiplier) than a similar increase for a wealthy one. So countercyclical spending can solve deadlocks, but is wasteful, and may even exacerbate inequality. In addition, increased sovereign debt after the 2008 financial crisis does not leave much room for using countercyclical spending for most European national economies. As a result, to fix the economy we cannot rely on anything that is at the mercy of state actors, or supranational actors like the EU.

Theoretically, economically disadvantaged persons can create a closed economy. However, beyond the level of communes and monasteries, this requires tools for large-scale collaboration. And right now, money is the only major tool to organize large-scale collaboration, and the poor have no money. A new tool is necessary, and it has to be inherently available to everyone.

3. Solution

In the following sections, we outline our proposed new system for economic exchange, which has been the focus of our research and development work since 2013.

3.1. We Need Solutions

It goes without saying that economic inequality is bad in many ways – foremost for those suffering economic depravity, but also for society as a whole. Among others, inequality is a risk factor for ecological collapse[3], associated with higher levels of mental illness, and politically dangerous. Regarding its political dangers, it can fuel political violence of the oppressed, if not defused in time by sensible policies (see Peter Turchin's "secular cycles").

We are also potentially close to a new economic crisis, which will arguably be more severe than the Financial Crisis of 2007–2008 and the economic crisis following it. The severely limited economic activity in such crisis times is an exacerbated version of the economic deadlocks that exist permanently in the economic system. An economic crisis affects the poor disproportionately, so we better have a solution ready when it hits.

As we don't want to see ecological collapse, societal collapse or political violence, it is apparent that we need a solution for inequality. We can continue to treat symptoms, or we can treat the root cause; but from the the last chapter it is also apparent that the root of inequality cannot be solved within the framework of market economies built around state-controlled fiat money and state-sanctioned big business. This framework – our system for economic exchange – is the root cause of inequality.

To reduce inequalities, economic growth has to happen at the right spot. Incomes should grow at the bottom of the income distribution and shrink at the top. This way, low consumption at the top will offset the ecological impact of economic growth at the bottom.

3.2. Exchange Model

When it comes to alternatives to money, the idea of complementary currencies to provide additional, "self-made" liquidity has been around for a long time. However, those of them that are backed by state currencies or precious metals do not solve the issue of economic deadlocks: to solve a deadlock, additional liquidity has to be created *on demand*. And while those complementary currencies that are based on a mutual credit system do solve this issue, they can only do so for a small local group. This is because accepting the currency implies trust in its user community that they will accept it back when one wants to spend it. This "collective trust" is a problem as none of the users are under any obligation to keep accepting the currency.[4] The only way out is knowing enough of them personally to be able to trust them, which limits the group size to around Dunbar's number (120-300).

To address these shortcomings, we use a system in which every user issues their own type of value coupons, denominated in "traditional" currency values. Conceptually, this makes every type of these

[3] For a particularly telling study, see the HANDY model of collapse.

[4] In our "three-signature model" of payments, as discussed in section "Payment Model", this is interpreted as insufficient backing: the whole user community, or at least a trustable and large enough subset, has to sign off payments to guarantee the currency hold value, but this is not done in mutual credit currencies.

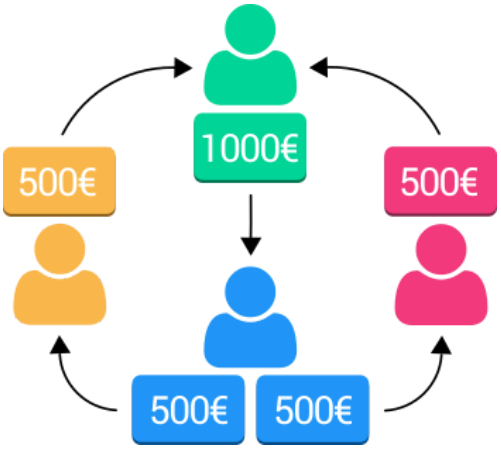
self-issued coupons to be its own type of currency, only accepted by one party (its issuer). This setup solves the issue of having to trust the whole group – instead a coupon holder only has to trust that the coupon issuer will redeem their coupons when asked. But it has its own issue: these “single purpose currencies” can no longer fulfill the main purpose of money, which is to be “the universal product”: something that is readily accepted by a multitude of users in exchange for all products and services they offer, and in this way facilitates economic exchange.

Our solution here is what we call “network barter”, our core innovation. It is a new way to facilitate economic exchange and works without a universal product, that is, without money. In this context, network barter is a token exchange / currency exchange mechanism based on multilateral barter with many (potentially thousands) of participants in each barter trade. All participants obtain coupons they want in exchange for the same value of own coupons they issue.

Network barter is a major evolution of direct barter, which refers to simultaneous barter of products or services between two agents. Direct barter is a severely limited exchange mechanism due to the “coincidence of wants” issue: it requires that each participant offers what the other needs, at the same time. In today’s economy with a highly diversified range of products, this is an improbable case. This issue is solved by our multilateral, network shaped barter trades that can connect the offers and wants of more than two agents.

Network barter also solves economic deadlocks. It does so in the same way as direct barter does, achieving liquidity without money. A network barter trade constitutes a set of conditional promises of the form “I will buy *n* of your coupons if somebody buys *n* of mine” that mutually fulfill each other, so they can be executed as one single transaction. And network bartering performs well in resolving economic deadlocks: according to our agent-based simulations, network bartering in a network of ≥25 users (with one coupon offer and two coupon orders per user) can resolve about 75% of all orders that can be resolved in principle on a per-user basis. For example, for a user ordering coupons for 150 EUR and having incoming orders for 200 EUR, 150 EUR is the maximum order volume that can be resolved by paying for orders with offers, and network bartering would on average resolve 75% of that. More users and a higher network density will only increase that performance. The performance is consistently 25-30% better than the turnover that can be realized by executing circular barter loops in random order until no more loops can be found. (In practice, it may not always be advisable to clear the order book as much as possible, as the network structure may take longer to recover and cannot integrate new incoming orders into trades for some time. But that is another issue.)

To better understand network barter, consider the simplest possible network barter trade:

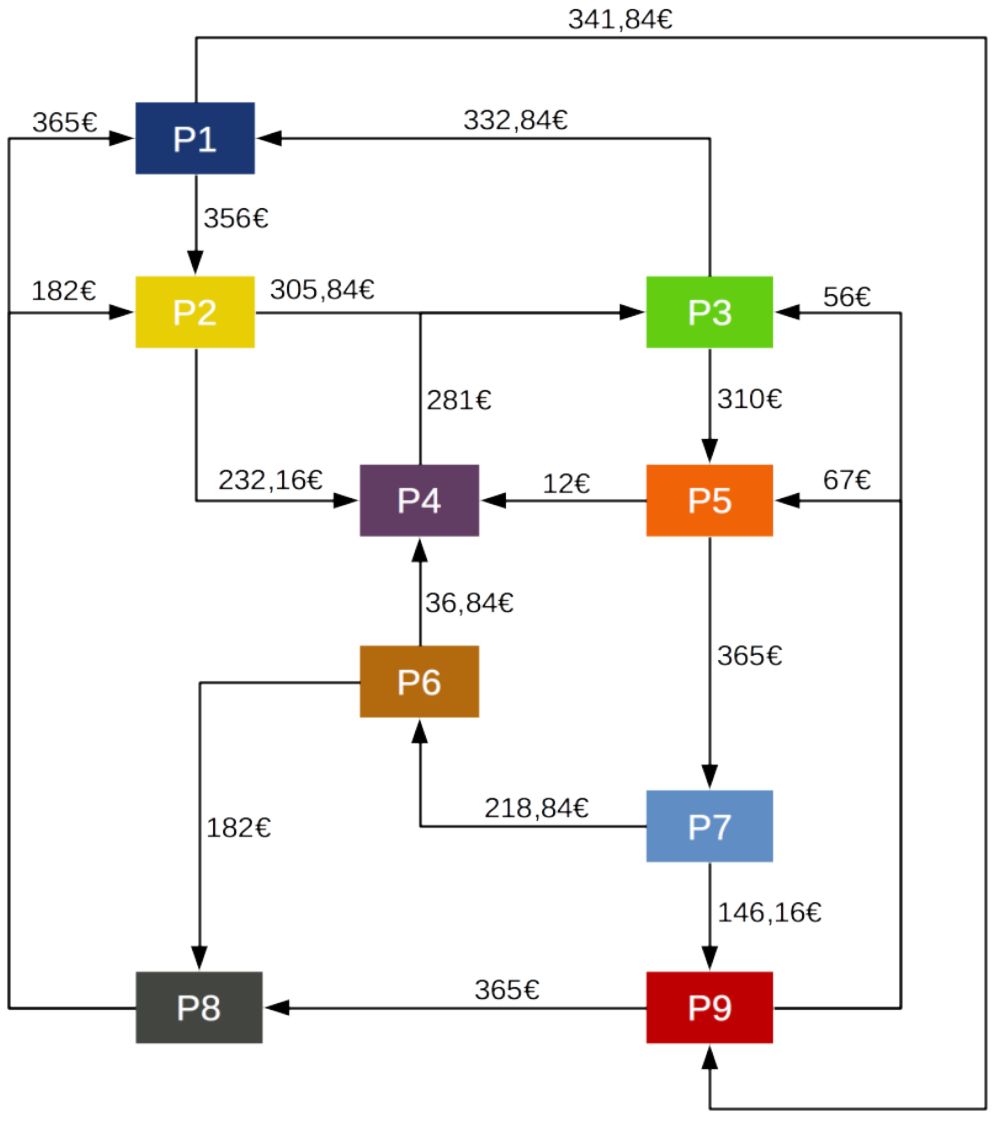


Blocks represent coupons, issued by different users as represented by their colors. In this minimal scenario, all users obtain as much value in desired coupons as they give away in newly issued own coupons. This is the invariant that must hold true in every network barter trade:

- "orange" **gives 500** EUR in coupons (to "green"), **gets 500** EUR (from "blue")
- "green" **gives 1000** EUR in coupons (to "blue"), **gets 1000** EUR (from "orange" and "red")
- "blue" **gives 1000** EUR in coupons (to "orange" and "red"), **gets 1000** EUR (from "green")
- "red" **gives 500** EUR in coupons (to "green"), **gets 500** EUR (from "blue")

Now after understanding the principle, let us look at a bit larger network barter trade, closer to a real-world scenario. For that, compare the diagram on the following page. In this example, the same invariant applies: everyone gets as much value as they give, so everyone is happy.

Note that this diagram shows a network barter trade, which is the subset of the order network that could be resolved by the algorithm. There will still be orders that could not be executed, and these are not shown in the diagram. They might be executed in one of the subsequent network barter trades.



3.3. Payment Model

In the PayCoupons system, three conditions allow us to create a unique, efficient consensus algorithm that even makes offline payments with coupons possible:

1. **Pre-existing trust.** Both ordering and owning somebody's coupons imply that you trust them "to stay true to their word" (in this case, to their promise of redeeming their coupons for products and services). This works well, as PayCoupons is meant to enhance the relations of long-term business partners, who know each other well enough (personally or by business reputation) to be able to trust. In a general cryptocurrency use case, this condition does not apply.
2. **Pre-existing reputation.** The system is based around real-world trust between businesses, which account holders want to keep up (their "business reputation"). This results in a strong motivation for coupon issuers to accept coupon payments with the coupons they issued.
3. **Local consensus.** Since every participant issues their own independent currency, and coupon holders generally obtain their ordered coupons directly from the issuer, only a consensus between coupon issuer and coupon holder has to be achieved. In contrast to the global consensus required for transactions in traditional cryptocurrencies, this enables more efficient storage and also offline payments.

This chapter will explain the theoretical basis how true offline payments are possible in the PayCoupons cryptocurrency system. Note that this only applies to paying with coupons, not to network bartering them, for which we will still need an online based, centralized mechanism as discussed later. We start with a general model of what constitutes a successful payment:

The three-signature (“3-sig”) model of payments. A successful payment is a transfer of balance between accounts in an accounting system that (1) is atomic (“happens in full or not at all”) and (2) cannot be plausibly denied or hidden by one party from the other affected parties involved in this transfer of balance. The second condition protects against double-spending of the same balance. For a payment to be successful, the following three parties have to consciously, willingly and verifiably agree (“sign off”) that the payment should happen, in the following order:

1. **sender:** one or more agents from which the payment originates
2. **receiver:** one or more agents to which the payment is directed; can be omitted if refusing a payment is not an intended feature, as discussed below
3. **backer:** one or more agents promising to accept the same balance from the receiving agent in a subsequent payment, in exchange for real-world products or services

All agents are identified by account addresses. We introduce a formal notation for payments as follows: a payment of 100 units by sender S to receiver R, backed by backer B is written as:

$$S \overset{100\,B}{\rightarrow} R$$

Where applicable, B is the name of the currency used, as this identifies the backer. By requiring the signature of the receiver for a valid payment, the receiver’s consent becomes mandatory for receiving a payment. Depending on the application, this is a useful albeit not essential property – it is for example not used in bank transfers or Bitcoin. It is however useful to avoid the legal hassle of being accountable for incoming erroneous or malicious value transfers, for example connected to money laundering activities. If not a desirable feature, the recipient’s signature can be required only on request by the

sender, or made optional (then also allowed after the backer's signature), or omitted altogether. Where that signature is provided, it can serve the sender as proof of receipt for business accounting purposes. Where not provided, a business can still issue a manually signed receipt for a payment, as is established business practice for cash payments.

The signature of the backer means "I promise that, on request of the receiver, I will redeem the balance transferred in this payment for products and services or another currency I offer." That promise protects the receiving user against a potential double-spending attack by the sender, because it is not conditional on the absence of such an attack. This also implies that it is the responsibility of the backer to check for double-spending attacks before making this promise – that is, before signing the transaction. And this in turn implies that the backer always has to sign last, because that finalizes and executes the payment as an atomic transaction.

If not signing last, the backer would not be aware of which payments are being finalized and executed after giving her signature, and which ones are never finalized. And in such a situation, the backer would not be able to decide whether a new payment request for spending the same balance is a double-spending attack or not. So to be able to protect herself against double-spending attacks of her currency, the backer always must sign last, and in all other cases the transaction is considered invalid by the protocol.

Depending on the currency and use case, the backer can be obliged to redeem the balance against products and services by legal obligation (tax authorities), contractual obligation (companies), or voluntarily (blockchain cryptocurrencies, mutual credit currencies). But in all cases, the sender and receiver have to know with sufficient precision who the backers are, as that is the value proposition of a currency.

The following table illustrates our three-signature model for two well-known currency systems, and for PayCoupons, with explanations in the text below:

currency	sender	backer	receiver
state currencies	A	central bank	B
Bitcoin	A	Bitcoin users	B
PayCoupons: B coupons ("A pays with B coupons")	A	B	B
PayCoupons: coupons of A ("A issues A coupons")	A	A	B

State currencies in the three-signature model. For state-issued currencies, the state government (represented by the central bank) is the "backer of last resort", guaranteeing to accept the currency as settlement for tax debt. So theoretically, the state government would have to observe and sign every payment to be sure nobody double-spends a balance to settle tax debt. However, since that is impractical, a complex system is set up to delegate that task, including state-sanctioned banks and forge-resistant cash currency.

Bitcoin in the three-signature model. For blockchain-based cryptocurrencies like Bitcoin, the backer is the whole user community, as together they constitute "everyone who would accept these tokens in the future". So essentially, every Bitcoin user would have to sign off every Bitcoin transaction. Since that is practically impossible, the innovation of the blockchain is to automatically select a subset of users who are trustable enough to sign off on behalf of all users. In Bitcoin, this is done by letting two or more different miners[5] sign off the transactions (implicitly, through block mining). The Bitcoin protocol makes sure these miners are trustable enough, as they have to invest a lot of effort ("mining") to be able to do the signing. This incentivizes them to sign truthfully, as they would lose the mining reward and all their effort if their block is not accepted by the majority of the other miners who probably follow the incentive to mine truthfully.[6]

PayCoupons in the three-signature model. The interesting systemic property of PayCoupons is that, both for coupon redemption payments $A \xrightarrow{B} B$ and coupon issuing payments $A \xrightarrow{A} B$, two of the three parties required to sign the payment are identical. Because: A is the only backer of A coupons, and B the only backer of B coupons. So practically, two signatures are enough for a payment, and no complex delegation mechanism (like the banking system) or global consensus mechanism (like the blockchain) has to be employed.

How PayCoupons enable offline payments. With only two signatures required, and both required parties A and B present at a point of sale, true offline payments are possible in the PayCoupons cryptocurrency system. To exchange the two digital signatures, the parties can simply communicate device-to-device, without the need for a network. This communication can even be unidirectional if the protocol does not require the receiver's signature to make a payment valid. Unidirectional communication allows very comfortable offline payments, using for example a single QR code scan between two smartphones instead of two or three scans or a NFC or Bluetooth connection:

- For a coupon payment transaction $A \xrightarrow{B} B$, the sender A lets the receiver B obtain a transaction record stating the new balance of B, signed by A as the sender.
- For a coupon issuing transaction $A \xrightarrow{A} B$, the sender A lets the receiver B obtain a transaction record stating the new balance of B, signed by A as both the sender and backer.

Side effects of offline payments. As a side effect, the receiver has no ability to reject a payment, but that seems to be the less important feature. Another side effect is that offline coupon redemption payments $A \xrightarrow{B} B$ are deniable: A signs a record stating the new balance and transfers the signed record to B by letting her scan a QR code. B also has to sign but does prove that to A when "one scan" unidirectional offline communication is used. So A will record the new lower balance locally without a cryptographic confirmation by B. Practical confirmation is given when B hands over the goods or services A paid for, which will usually be enough for small offline payments. A will then trust that B won't complain about a missing payment later based on the existing trustable business relationship, and even when a complaint happens (e.g. if B really lost the record of payment), it is only a nuisance as the payment can be confirmed again without loss for any party by agreeing on the current balance. This is possible, as any payment record is not worth something by itself, but simply a statement of the current balance of one type of coupons, and that can be re-calculated from the last transaction record both

[5] Bitcoin is said to require six blocks for confirmation, but these may come from just two miners each sharing 50% of mining power, the maximum before the network becomes dysfunctional due to the "51% attack".

[6] The mechanism how this happens: the truthful miners create a longer chain based on an alternative truthful block, and the longest chain is automatically considered the authoritative version by all Bitcoin clients.

parties have stored and the business interactions that happened since then. For higher-value offline payments, bidirectional “two scans” offline communication would be used, by which A obtains a record signed by B as proof that the payment happened. Alternatively, B could issue a manually signed paper receipt that the payment happened, as is current business practice for cash payments.

Opportunities for offline payments. The offline payment ability in PayCoupons creates interesting new applications for cryptocurrencies. For example, coupons can be spent very similar to “cash”, independent of the availability of an Internet connection and independent of state-sanctioned infrastructure for electronic payments. This makes them suitable for low-infrastructure regions where, so far, cash far outperforms electronic monies. Also, offline payments are more resilient and need less infrastructure than SMS banking applications (M-Pesa etc., a current success story of “banking for the unbanked”). Offline payments can happen device-to-device via Bluetooth, wifi, NFC or by scanning QR codes from another phone’s screen. This way, payments can be made in shops without having to struggle with Internet downtime and with spotty indoor network availability in low-infrastructure areas.

And since the network bartering mechanism of PayCoupons solves economic deadlocks, using a widespread tool to access PayCoupons could result in an economic revival of urban and rural communities, both in developing and developed countries. And the most widespread tool is the mobile phone, esp. when not requiring permanent Internet access. This is especially encouraging since it revives the local production and service economy, due to the algorithmic detection of local economic cycles in network barter trades. These properties may also make it a new favourite tool for organizations dedicated to help regions in their economic development.

Transferring third-party coupons. In the PayCoupons system, payments $A \overset{C}{\rightarrow} B$ (by A to B using C coupons) are also possible. The three-signature model requires C to sign such a transaction. This requirement also implements the additional requirement in PayCoupons that a coupon issuer can control who holds their coupons (and thus, who they agree to do business with). But, as three distinct parties have to sign off the payment, this can’t be a true P2P offline payment. To preserve the unique ability of true offline payments in the PayCoupons system, we will not support $A \overset{C}{\rightarrow} B$ payments offline. We will however need this type of transaction to transfer coupons to and from the PayCoupons exchange, which implements network bartering. See on “check-in” and “check-out” payments below for details. In these cases, $A \overset{C}{\rightarrow} B$ payments do not create usability issues: interacting with an exchange implies having to communicate online with a third party anyway, so these payments naturally require an online connection already.

3.4. Real-world Use Case

Large-scale network barter transactions with more than 200 participants each are the mode of economic exchange in PayCoupons, as implemented on our existing centralized exchange platform pay.coupons. Each network barter trade resolves an economic cycle (which is a deadlock where liquidity is low).

To understand better how network barter works in practice, here are the typical steps for a group of small and medium businesses:

1. **Get an account.** Small and medium businesses sign up for user accounts on the pay.coupons exchange platform.
2. **Make connections.** They find the PayCoupons user accounts for their existing, trusted business contacts (and others they might want to get to know as future business partners), and use the

PayCoupons “connect” feature. The benefit of “having a connection” is that it allows users to order each other’s coupons.

3. **Order coupons.** Users now order certain amounts of coupons from other users, with order volumes depending on the expected volume of doing business with them. When users order coupons from others it follows that many users also receive incoming orders for their coupons.
4. **Find the network barter trade.** A trade finder algorithm will now crunch the numbers and find the network of users with the largest subset of coupon orders that balances every user in this network. A user is balanced if, in the proposed trade, the sum of the user’s incoming coupon orders equals the sum of the user’s outgoing coupon orders. This means that in a network barter trade, each user “pays” for all their coupon orders with own coupons they issue to others.
5. **Execute the network barter trade.** This network barter trade is executed in an indivisible transaction and recorded in the pay.coupons database. All users are then notified of the coupons they got and the amount of own coupons they issued in return.
6. **Pay with coupons.** Users can now use any of the coupons they hold to pay for all products and services offered by the respective coupon issuer. For example when purchasing something in the coupon issuer’s shop, they can use the PayCoupons smartphone application to pay with coupons. Paying with coupons is spontaneously possible – only obtaining them requires to wait for the network barter algorithm to do its work.

3.5. Properties of Coupons

The following coupon properties follow from the design of PayCoupons as a system of self-issued value tokens:

- **Legal.** While Bitcoin and other “fiat cryptocurrencies” reside in a legal gray area in several jurisdictions, or are even forbidden to use, this is not the case for coupons in the PayCoupons system. Legally, they are just coupons, which have a long-established use in commerce in pretty much every country. For example, companies often hand out vouchers when a customer returns a purchased article.
- **Stable value.** All coupons provide a stable value as they use the same unit of account as a mainstream fiat currency (Euros, U.S. Dollars etc.). This is a necessity for a tool designed to support the goods and services economy. Otherwise, business accounting would be severely disturbed as stored value meant to purchase goods or services can fluctuate wildly, and the new currency would not find mainstream acceptance for business use due to this. As it happened to all cryptocurrencies with free-floating valuation, and none of them provides a useful alternative to state currencies in the goods-and-services economy at this point.
- **Easy to use.** Using coupons feels like using “regular” money, as coupons use the same unit of account as the money a user is accustomed to. So business is done as usual, just without money.
- **Secure.** With cryptocurrency infrastructure, checked-out coupons are under the full control of the user, just like tokens of a blockchain-based cryptocurrency. Users may opt to put their coupons into hosted online wallets, but there is no need for that as there will be a self-hosted offline wallet software made available by PayCoupons. (Online wallets may be more comfortable though, esp. because they do not require installing software.)
- **Trustable.** Trust in PayCoupons is a network of trusted relationships. To participate in the PayCoupons economy, you do not need to trust a central authority or “the system” as a whole, but simply to trust the issuers of the coupons you are ordering or holding. Specifically, trust

means to expect that the issuer accepts their coupons back in exchange for products and services in the future, because that promise is what makes coupons valuable in the first place.

- **No systemic collapse.** When users lose trust in a currency, as it happens with complementary currencies and sometimes with state-issued currencies, the whole currency collapses, for example through hyperinflation. In the PayCoupons system however, all trust is tied to individual business partners, so breaches of trust are local and have no systemic effect. (Each user's coupons are technically a separate currency, and its demise does not affect any other currency.)
- **No need for government enforcement of contracts.** By specifying in the terms and conditions that coupons are not enforceable with government help, the PayCoupons credit network would function very similar to certain historical credit networks (9th century Indian Ocean Muslim trading cities, or Medieval Europe). These flourished despite states refusing to step in if a client refused to pay, solely based on merchant reputation (and caution on the side of creditors). Similarly, coupon holders would be cautious in a PayCoupons economy and require a spotless history of redeeming their coupons from a coupon issuer before ordering from them, while coupons issuers would lay priority on maintaining such a spotless reputation.
- **No credit bubbles.** The PayCoupons system is composed of peer-to-peer credits, but there are no incentives that could inflate credit volume so much that the stability of the whole system is at stake. First, these credits come at zero interest, so creditors will only hold as much in coupons as they plan to spend in the next months in order to not lose out due to inflation adjustments of the issuer's products and service prices. Second, coupon credits may not be enforceable with government help (see above), and even if they are they can only be redeemed for products and services, not for money, due to the terms and conditions of the PayCoupons platform.

  From a game-theoretical point of view, this disposes of moral hazard. Moral hazard happens only when the creditor (coupon holder) is motivated to increase credits by the prospect of profit (interest), and when the creditor knows that someone (ultimately the government) will enforce or repay the credit no matter what. That situation incentivizes reckless lending, as creditors can never lose their money. A major example were the "too big to fail" lenders in the 2008 U.S. mortgage crisis.
- **No winner-takes-it-all competition.** In the monetary economy, price and quality are the only decision criteria. So in the longer term, markets tend to create an oligopoly of big business as large companies can create the same product at a lower price. Obviously this makes it next to impossible for new businesses to get a foothold in established markets. With the PayCoupons system on the other hand, existence of an economic cycle in a network barter transaction is a third requirement. It allows market players who can't compete on price to stay in business by trading with each other. And it forces big business to order from less competitive suppliers if they do not get enough orders otherwise.
- **Contributes to social cohesion.** According to David Graeber's "Debt: The first 5000 Years" , the web of small credits in a credit-based society never quite cancels out. Everyone owes small amounts to everyone else all the time. This was still observable in some traditional African societies in the 20th century. Graeber's radical idea is that society *is* this web of credits. Owing to each other other means we cannot walk away from each other. These credits are a driver of social cohesion, because after all you want people who owe you money to prosper, because your own prosperity depends on theirs. This does no longer apply when laws enable debt: credits that are transferable to other creditors without the consent of the debitor. This replaces the interest in the fate of the debitor with interest in maximizing profit. In PayCoupons however, credits are not debt, so coupons are expected to contribute to social cohesion.
- **Breaks the deadlock.** We invented the network barter protocol as a way to facilitate economic exchange without deadlocks, and without the systemic risks and interest costs of transferable

debt. In every network barter transaction, users “pay with what they have” for coupons they ordered – namely, they pay with their own coupons, which are self-issued, interest free value tokens.

Breaking economic deadlocks is important because it allows to jumpstart economic exchange at any time, without liquidity reserves, in any group beyond a certain minimum size. This applies to plain everyone, and even under economic recession and depression.

The properties of deadlock resolution and ingrained limited competition (instead of all-out winner-takes-it-all scenarios) let PayCoupons contribute to solving economic inequality. Money as we know it does the opposite. Due to these properties, we see a significant opportunity that our technology can become the next big disruption in financial technology, based on voluntary adoption and not government monopoly.

4. Technical System Description

4.1. System Overview

The PayCoupons cryptocurrency system consists of:

- **Exchange platform.** The current pay.coupons platform. It includes the network barter algorithm to enable coupons trading between users without money.
- **Internet infrastructure.** An Internet connection is a requirement. Technically, exchange platforms similar to pay.coupons can also be run in disjunct smaller networks, but at this time we do not plan to do so.
- **Stellar network.** The token for paying platform fees is a token on the Stellar blockchain.[7]
- **Identity infrastructure.** Allows to connect a real-world identity to one’s PayCoupons account for trust building. Given the importance of reputation in the PayCoupons economy, this is critical. We intend to use one of the existing identity service providers, or ideally one of the emergent ones providing this service on the blockchain in order to let users keep their coupon reputation independently of the existence of the pay.coupons platform.

The PayCoupons ecosystem contains the following major data structures:

- **Coupons.** Each PayCoupons account is associated with one public and one private cryptographic key, which enable the account holder to issue, transfer and accept their own type of coupons. Coupons are digital tokens recording a credit relationship between two PayCoupons account holders.
- **Order graph.** Information about who orders what amount of coupons from whom, and who offers what amounts of coupons of which type.
- **PayCoupons token.** Not a coupon but a widely accepted token that is used to pay the PayCoupons platform fees. Available to account holders in exchange for various other currencies and assets.
- **Stellar blockchain.** Records payments of platform fees with the PayCoupons token (PCT).
- **Identity proofs.** Signing with the private key of a registered electronic identity document will be taken as an (optional) proof of identity.

The following sections explain these data structures and the operations possible with them in detail.

[7] See: https://www.stellar.org/

4.2. Coupons

Coupons in the PayCoupons system are self-issued value tokens, embodying the right to products and services as offered and priced by the coupon issuer. Coupons of different issuers are not equivalent, as they encode the rights to different products and services. They do however use the same unit of account, which makes them exchangeable by means of network bartering with a constant one-to-one rate.

The unit of account for coupons is that of the country's regularly used fiat currency. This enables seamless integration into business accounting. Still, this denomination does not imply any need for state issued currency since coupons do not include the right to be redeemed for currency.

Both traditional trade bills and coupons in the PayCoupons system are self-issued credit notes, but coupons differ in several ways: they come by default with immediate maturity, their transfer to a third party requires the agreement of the issuer to do business with this third party, and they can only be exchanged for products and services of the issuer and not for money. While trade bills only increase monetary liquidity through deferred payment, coupons replace the need for monetary liquidity.

This also shows how coupons are different from debt. While coupons have a credit value measured in a monetary unit, they do not constitute debt because (1) they cannot be transferred to another creditor without the agreement of the debitor, (3) they do not entitle to interest and (2) the creditor can only require settlement in products and services, not in money. By not being debt, they remain simpler to handle in a legally compliant way, as debt-related laws for financial institutions, consumer protection etc. do not apply.

In total, coupons are modeled like a complementary currency with only one acceptance point (the issuer), and as such are not likely to attract regulatory action as both value coupons and (small) complementary currencies are legal in most jurisdictions. The exchange of coupons is modeled like barter, which again is legal in most jurisdictions (usually coming with a requirement to document it with invoices for both parts of the transaction, each for the same value, expressed in legal tender currency).

4.3. Accounts, Wallet

CAS. As discussed in chapter "Payment Model", due to favorable design constraints coupons can be spent offline, outside of any blockchain mechanism.[8] In the following, this offline subsystem to hold coupons in a digital wallet and pay with them is called the CAS ("coupon accounting system"). This part of the PayCoupons system will be released as open source software.

Addresses and accounts. An address is a unique identifier of a payment endpoint for coupons. One or more addresses that are proven to be controlled by the same agent are said to belong to the same "account" or "identity". So far, an account always corresponds to a user account on the pay.coupons exchange platform.

Address format. The PayCoupons address format will be similar to the "long random-looking sequence" format known from Bitcoin and other cryptocurrencies. The reason is that this allows permission-free, decentralized, offline address creation: a user simply uses the CAS client software to create a public and a private key, and then the address as a partial hash of the public key with an added

[8] However, exchanging coupons by means of network bartering can only be done online in a centralized platform, as detailed in following chapters.

checksum.[9] Also this way, coupon accounts exist fully independent of the network barter exchange platform pay.coupons. This makes it inherently possible for third parties to implement independent coupon exchange platforms that operate in different ways. (In the medium-term future, some might enable decentralized coupon exchange on the blockchain.) Still, all of them will be compatible with the same basic CAS account infrastructure where everyone can hold everyone else's coupons.

Coupon wallet function. An offline application that stores the coupons a user holds in a digital wallet is a precondition for offline payments. For that, the CAS application stores coupons in the form of cryptographically signed and countersigned records by which a coupon issuer and coupon holder agree on the balance of the held coupons. These records can be the result of earlier offline payments with coupons or of checking in newly issued coupons from a network barter trade made on the pay.coupons platform. Both of these cases are detailed below. The CAS is the basis to "have" coupons and pay with them.

Implementation technology. The following is a preliminary, non-committal analysis. The CAS is a relatively compact software, and we will implementing it as a standalone application that can run comfortably even on entry-level smartphones. We may or may not use GNU Taler[10] to base the CAS application on. GNU Taler implements the concept of three-signature transaction discussed above, including all required cryptographic functions. In the case of PayCoupons, a GNU Taler "exchange" and "merchant" will always be on the same device since as a coupon issuer has both functions. So with some modifications, offline usage will become possible with GNU Taler. We will not use any blockchain technology to implement the CAS, as that would conflict with the requirement to allow offline transactions.

4.4. Check-in and Check-out Transactions

Coupon check-in transactions. As indicated, network bartering of coupons cannot be done offline but needs a dedicated exchange mechanism (described in following sections). After a network barter trade happened, new account balances are not immediately available in the CAS, so they are not immediately spendable offline. They are however already spendable online in the pay.coupons platform. This is also more convenient for most users, esp. those starting off from a hosted account on a marketplace platform, so we will not force them to do a check-in to their CAS offline wallet before they can spend the balance.

However, when a user wants to transfer coupon balances to the CAS, the following check-in mechanism is used. It is equivalent to a payment $A \xrightarrow{B} A$ between two accounts of A (online and offline), so only requires the signature of A. B has to be notified before being able to spend the balance offline, but does not have to sign the transaction as there is no change in ownership or amount.

Note that check-in transactions need to be stored in a central database. In the current scenario, this will be the pay.coupons platform's database. Technically, this can also be a blockchain. However since network bartering requires centralized exchange platforms so far and there is only one of these, there is no benefit at all to recording it on the blockchain, but the severe drawback of limited privacy when recording the transaction records publicly on the blockchain. Still, it makes sense to store the check-in /

[9] Checksums are a relevant feature, as can be seen from the "hack" used in Ethereum to add them later [see]. Also, checksums help to make the address format different from that of other cryptocurrencies. An example address from a prefix, 162 bit pubkey hash and 24 bit checksum, all in RFC 4648 Base64 (6 bpc) and with "_" as separator: `PC_JhgFw9Mn/yG+6gFGfswPlkM8G4H_hgQ7`

[10] See https://taler.net/en/developers.html

check-out transaction data in a tamper proof way, and for that we may employ hash chains,[11] or for convenience, store hashes of the transaction records on the Stellar blockchain while sharing the actual cleartext of these transaction records only with the transaction participants.

Specifically, a network barter trade consists of a set of two-party coupon transactions between coupon issuer and recipient, and for check-in transactions, the following process is followed for each:

1. **Transaction from online to offline account.** To send coupons to their offline wallet account, a user creates this transaction on the PayCoupons platform. Only the user's own signature is required for this. The offline account is a normal PayCoupons account, just that it requires two signatures to move balance out of it again.
2. **Notify the issuer.** The issuer has to be aware of the new balance in the offline wallet account so it is available offline when the coupon holder intends to pay offline next time. This might happen in multiple ways:
    - **If the issuer can be assumed to be online permanently:** he / she will be able to check the platform's database on demand when a payment is coming in. In this case, which applies especially for webshops, there is no need to notify the issuer actively.
    - **If the issuer is regularly online:** he / she receives an immediate update about the new state of the platform database when a check-in transaction is made. The coupon issuer's CAS client software automatically reacts to this update by confirming to the coupon holder that her coupon balance is now available for offline spending. After that, no further action is required.
    - **If the issuer is regularly offline:** The coupon holder's CAS client saves the relevant record of the platform database and transfers it to the issuer when they meet offline. The issuer will require a confirmation that this record conforms to the record stored in the platform database, and this confirmation can be made by one or more of their connected PayCoupons business partners using ordinary asymmetric key cryptography.
3. **Confirm the offline balance in CAS (optional).** When the issuer has been notified, they have all the information to allow an offline transaction. To make really sure issuer and holder agree on the available offline balance, any party can request a normal 3-sig request to agree on that balance. It will include a reference to the record that contains the check-out payment, to say that "it settles the balance up to and including everything that happened in that record".

Now normal offline payments can happen, as discussed in the section "Payments" below. This results in a modified balance that is available offline, recorded by both coupon holder and issuer, and proven by a cryptographically signed record for each new agreed-on balance.

Coupon check-out transactions. When the coupon holder wants to check their remaining offline balance out of their offline wallet and back into the PayCoupons online platform (for example for re-trading via network bartering), they can execute a check-out transaction as follows:

1. **Transaction from offline to online account.** This is a multi-signature transaction on the PayCoupons exchange platform. It sends the remaining offline balance of coupons to the user's normal online account, and the balance corresponding to the coupons spent offline to the online account of their issuer (which simply records online what happened offline). Then both the coupon holder and coupon issuer sign this, after confirming the balance is correct from the offline transaction records stored in the CAS. Since this is a multi-signature account and confirmation

[11] See https://en.wikipedia.org/wiki/Hash_chain

from both parties are required to execute it, there is no danger of double-spending for the coupon issuer.

2. **Confirm the offline balance in CAS (optional).** This is optional, as due to the multi-signature transaction described above, both parties are necessarily aware of the new balance already. However to formalize this, both can update it using a normal 3-sig CAS transaction that encodes an agreement about its new balance, with a reference to the transaction record that contains the multi-signature transaction that was just executed.

4.5. Payments

Payments with coupons in the PayCoupons system come with the following properties:

Offline payments. Offline payment is a completely new feature for cryptocurrencies. It requires device-to-device communication but no network to contact any third-party server. This is different from off-chain payments, for example in the Lightning Network. In the Lightning protocol, all participants in off-chain payment channels still need to constantly observe the blockchain for potential fraud by the other payment channel participants, so that they can prevent the success of the fraud via the revocation keys held by them. This requires a dependable Internet connection. In PayCoupons offline payments, *no* Internet connection is required at all to spend or receive coupons (only to trade them on the pay.coupons exchange platform).

Step by step, this is how offline payments work:

1. **Finding the balance.** The process starts from looking up the account balance in the coupon wallets of both the coupon holder and coupon issuer. They will find the same last record establishing the last balance, resulting from the last coupon transaction in the CAS (check-in or check-out).
2. **Confirming the balance.** Now, both issuer and holder confirm that the cryptographic signatures on that record are their own, and finding they are, communicate to each other that they agree on the current balance.
3. **Payment request.** The coupon holder creates an equivalent record about the balance after the payment has happened. This record contains a transaction number, counting coupon transactions between this holder and issuer only. It is set one higher for every new record to be agreed on, establishing a sequence of records in lieu of an agreement about the current time or a blockchain block height. The agreed-on record with the highest transaction number is always considered the current balance.
4. **Agreeing that the payment happened.** A payment is the process of agreeing that the new record describes the new current balance. The coupon holder signs the new balance record with their account's private key, and sends the record to the coupon issuer. The issuer confirms that the contained signature is valid, with the help of the public key of the holder's account. The issuer also confirms that the new balance is correct considering the old balance and the payment to receive for their product or service. The issuer then counter signs the record, and stores that version.
5. **Confirming that the payment happened.** Usually, the coupon issuer will send the countersigned payment record back to the coupon holder, which is a receipt of successful payment for the coupon holder (payer). However, in many cases such as a purchase in a shop, handing over the purchased item is an acceptable surrogate for that receipt, and if the payer is content with that it makes a more comfortable payment process possible. In this process, an

offline payment only requires an unidirectional data transfer. The payer can simply encode a signed transaction record in a QR code, and the coupon issuer can scan it off the payer's phone.

This is all that is required for a payment in with coupons. Contrary to other cryptocurrency technologies, there is no need for a shared global ledger ("blockchain"). This is achieved because each type of coupons is a very limited "currency", only accepted by its issuer according to the protocol. When accepting their own coupons, the issuer can detect double spending attempts by looking up the holder's remaining coupon balance in the issuer's own CAS wallet. Coupons simply cannot be paid to just anyone, so there is no need to know and check anyone's account balances via a global ledger to confirm that the to-be-received coupon balance has not already been paid to somebody else.

So instead of one currency with universal acceptance, we have many currencies with one acceptance point each. Economic exchange is no longer achieved via the widespread acceptance of a double-spending resistant single currency, but via a dedicated exchange mechanism. That exchange mechanism may or may not require a double-spending resistant shared currency[12] or a shared ledger. In any case, outside of the exchange system we have only simple IOUs that can be spent offline by cryptographic signing.

No need to store the history of transactions. In blockchain based cryptocurrencies, the full transaction history of accounts is kept because storing transactions into a chain of blocks connected via checksums into a chain prevents attackers from forging the transaction history due to the sheer amount of calculations involved. So, no "checkpoint blocks" are used as they would effectively start a new chain. In the CAS however, each payment transaction is like a "checkpoint block": it mentions the new current balance, not the change of balance due to the payment. For that reason, no value is lost when deleting all except the last payment record. This makes the storage requirements trivial. (Businesses may still opt to keep more of the transaction history to fulfill legal requirements of business accounting.)

No fees for the payment function. Due to the offline nature of paying with coupons, no fees are leveraged in the PayCoupons system in these transactions. From the platform's point of view, these payments are both invisible and effortless, so there is neither a way nor a justification to raise a fee.

Using coupon payments online. Of course, the payment procedure outlined above can be automated, with the sender and / or the receiver being a program instance. For example, to allow payments to a webshop, the receiving user's software would be permanently active and online. It would check the signatures of incoming payment records, and when the payments are found valid, it would change the payment status of the associated webshop orders to "paid". Since the recipient's signature is not required to receive a valid payment, this software does not need to know the recipient's private key (which enhances security against theft). It is only important to not lose these records, but even if that happens the sender can prove with their copy that the payment happened.

Offline coupon issuing. Issuing new, own coupons outside of network barter trades[13] is the second type of coupon payment that is possible offline. The process is exactly the same as for payments of coupons to their issuer, just that the account holder's new balance as agreed through that process is higher afterwards, not lower. Also, the process is initiated by the coupon issuer. At its end, the issuer paid the holder in newly issued coupons. Just like the non-digital counterpart technique of "chalking up", this technique would already be sufficient to power small-scale economies in villages. However, network

[12] In most cryptocurrency exchanges, USD or USDT takes on this function as the "universal product" to exchange between currencies, while with the network barter algorithm we use, no "universal product" is needed at all.
[13] As implemented on https://pay.coupons in the "Send coupon" feature, available from the account menu.

bartering greatly improves the amount of economic exchange compared to what can be achieved with this tool alone.

4.6. Order Graph

Coupon offers and orders of the PayCoupons user base form a directed graph with users as nodes, coupon orders as edges, and the value of coupon orders as attributes of theses edges, indicating the desired value flow. For example: if user B orders 100 units worth of the coupons of user A, it will appear in the order graph as:

A full (but still small) example of an order graph may look as follows:

Now the task of the trade finder algorithm is to work on this data structure and find the subset of the order graph with the highest aggregate turnover so that the inflow and outflow of value is balanced for each node. This subset, as found by our network barter algorithm, generally has the shape of a network, composed of multiple overlapping loops.

Each loop represents a circular multi-lateral barter trade. All other implementations of multi-lateral barter that we are aware of find such loops and execute them independently, for example as done in OpenBarter.[14] However, this strategy does not lead to the maximum possible turnover, as executing the loop with the highest turnover probably destroys the option to execute a whole network – a collection of loops – with an even higher combined turnover. This is done by the network barter algorithm, our core innovation, resulting in improved liquidity for multi-lateral barter.

Coupon re-trading. In PayCoupons, there is also the option to transfer held coupons to a third party as part of network bartering, if that third party is also an accepted trade partner of the coupon issuer.[15] This allows to exchange coupons of a type that a user does not need at the moment for coupons she wants. This process is different from paying with coupons (which means a transfer back to the issuer), and increases the turnover of network barter trades. When allowing for coupon re-trading, the structure of the order graph changes: a second node type representing pools of coupons available for distribution is introduced. There will be an edge from an issuing user to pool of their own coupon type to represent issuing of coupons, with the option to add a limit on coupon issuing here.

4.7. PayCoupons Token

The PayCoupons cryptocurrency system comes with its own token PCT (“PayCoupons Token”) that is being introduced during the PayCoupons token distribution events. It is a purpose-specific blockchain token that will be offered as an additional means of payment for usage fees on the PayCoupons exchange platform, pay.coupons. The token is launched on the Stellar blockchain.[16]

Fee and reward payments. There are multiple functions in the PayCoupons system where the PCT token plays a role, both for fee payments and as rewards. The following is a non-exhaustive and non-committal list of payments made with the PCT token:

- network barter trade finding (with the fee as a commission on turnover)
- P2P identity verification of users (using ID card)

[14] See: https://github.com/olivierch/openBarter
[15] Available in the current pay.coupons platform in the “My Coupons” area, under “Offer this coupon”.
[16] See: https://www.stellar.org/

- account ownership on the pay.coupons platform (provided for a monthly membership fee, but probably for free)
- successful referral of a new user

Discounts for paying in PCT. As an incentive for the uptake of PCT, a 50% discount will be applied to all platform fees when paid with PCT instead of money.

Proof-of-stake discounts. Further discounts may be applied for payments with PCT when a user proves (via proof-of-stake on the Stellar blockchain) that they hold a certain amount of PCT for a certain time.[17] This will make financial sense for users with certain regular turnover, and together with the growth of the user base creates market demand for purchasing and keeping PCT, stabilizing its market price.

Proof-of-stake for order prioritizing. The PayCoupons algorithms allows to prioritize orders in cases where order loops are mutually exclusive but result in a similar overall volume of a network barter exchange. A useful mechanism to prioritize orders is staking with the user's associated PCT account: by holding a certain sum of PCT for a certain time, a user demonstrates she's invested in the system and a "serious" user interested in timely execution of her orders. At the same time, staking stabilizes the PCT market price. The higher the stake, the more priority a user's orders would have, but this priority would also be distributed over the whole current order volume of a user.

Only required for coupon exchange. The blockchain-based PCT token is only required for the exchange / network barter part of the PayCoupons system, while the CAS system to hold and spend coupons can fully run on client devices, without even an Internet connection, and consequently it does not incur or allow any PCT fees.

Dynamic fee pricing. The blockchain based, fixed supply design of the PCT token implies some limitations of its own, but they do not hurt the intended use. For one, these tokens will have the typical volatility of cryptocurrencies. This does not hurt its use for paying infrastructure services, as the amount to pay will be calculated as a percentage of the transacted amount of coupons. That value is measured in the unit of account of fiat currencies, so the fee to pay will also be in that unit, with conversion to PCT units based on the current exchange rate of PCT to fiat. Example: a 1% fee for the transfer of 1000 EUR of coupons is 10 EUR, which is always the actual amount a user has to pay. At an exchange rate of 1 PCT/EUR it converts to paying 10 PCT, while at another time with an exchange rate of 0.2 PCT/EUR it converts to paying 2 PCT.

A second limitation is that PCT tokens are scarce digital assets, and the scarcity of an asset generally limits its use value for economic exchange, for example because a deflationary trend can easily establish in currencies with a capped supply. However, the dynamic pricing based on the PCT-to-fiat exchange rate guarantees that PCT currency deflation will not make it more expensive for users to pay their fees, as measured in fiat currency. And that is what matters, given most users will be businesses with some access to fiat currencies and will exchange fiat to PCT shortly before making their fee payments. In addition, PCT scarcity only affects the reward payments required for economic exchange, so only a tiny fraction of the actual values exchanged through network bartering. Scarcity in a resource scarcely needed for economic exchange is an acceptable compromise.

[17] In the sense of "signing something with the private key of their cryptocurrency token account". Does not require that cryptocurrency to use a proof-of-stake consensus algorithm. To prevent gaming this system with hypothetical "PCT short-term lending services", it could be a combined proof-of-stake and proof-of-age (referring to coin holding time).

4.8. Exchange Platform

A PayCoupons exchange platform is a website that facilitates exchanging different types of coupons for each other. The exchange platforms is the only place to register one's offers and orders of coupons.

Until the remaining challenges of implementing network bartering with blockchain technology are solved, network bartering of coupons can only happen *within* an exchange platform, not between multiple exchange platforms. Technically, multiple exchange platforms can co-exist and users can participate in multiple ones in parallel, even move coupons they hold between them with check-in and check-out transactions. However, multiple parallel exchanges partition the network, which is certainly bad for the chances of creating network barter trades. For this reason, we will only operate a single "official" PayCoupons exchange, and it already exists on the pay.coupons website. (PayCoupons is an open system, so third parties are welcome to create own exchange platforms. However, the proper solution is to solve the blockchain implementation issues for network bartering and only then create multiple, interconnected exchange platforms.)

They also provide functions to hold coupons (wallet) and to pay with coupons, but users can also choose to use their own self-hosted client application for that (more secure as the private key will not be online, but users have to manage their own backups; also, offline payments with smartphones become possible then).

The platform can allow users to issue their coupons using any state currency as a unit. It makes sense that every user issues their own coupons in the currency they use for pricing their products and services, since they are implicitly at ease with the value fluctuations of that currency – either by not caring, or by adjusting prices regularly. Most users will use the national currency at their location of residence for pricing (and hence for coupons), they can however also choose to issue coupons in other currencies to limit currency exchange rate risks when they primarily trade with users using other currencies for coupon pricing. To make handling different currencies of coupons comfortable for users, they will see all their coupon orders in the currency they use for their own coupons, automatically converted at current market rates, while the value in the coupon's original currency value is also provided as a note.

When creating a network barter trade, the exchange platform needs to compare coupon order values in a single internal unit of account. For that, it will convert all currencies into a common currency at current market rates, and calculate a network barter deal after that conversion.

4.9. Network Barter Mechanism

Unlike traditional currencies, every user's type of coupons is technically its own currency, only accepted by this one user for products and services. So to allow economic exchange, we require a mechanism to exchange "coupons I have" (including my own, self-issued coupons) for "coupons I want". This is provided by the network barter algorithm, our core innovation, and forms the core of the PayCoupons exchange platform. The principle of network bartering is explained in chapter "Exchange Model". We are in possession of a well-performing full implementation of the network barter algorithm.

There are two major ways to integrate an exchange with a cryptocurrency system: centralized or distributed. In a centralized exchange, users transfer funds to an account of the exchange, which manages trading according to their instructions. In a decentralized exchange, users trade directly with their trade partners from their own accounts, and there is only one protocol-level mechanism that

connects all users instead of several proprietary mechanisms managed by one organization each. Technically, the two alternatives differ in the mechanism used to establish (1) consensus about the latest state of offers, orders and trades and (2) privacy protection. In centralized exchanges, a single central authority “dictates” the consensus and a central database with fine-grained access rights protects user privacy. In decentralized exchanges, a blockchain protocol establishes consensus and encryption and / or pseudonymous accounts protect user privacy.

Unfortunately, the decentralized mechanisms to protect privacy are not sufficient for network barter exchanges, which use an exchange mechanism very different from the usual limit order book algorithm. In network bartering, use of multiple pseudonymous accounts is not possible as all trading businesses connect based on their single “real world” identity, and homomorphic encryption or distributed computation that would also protect the processing stage of finding a network barter deal is not yet available in production-grade solutions.

So for now, network bartering exchanges can only be centralized – the model also used by the majority of current cryptocurrency exchanges. The following paragraphs explain its properties in more detail.

A single database under the full control of one trustable party (the “exchange operator”) is a simple way to establish data integrity for network bartering. It is not “trustless” and surely not decentralized, but also not “worse” than existing exchanges in the cryptocurrency ecosystem. This exchange can have multiple parallel interfaces created by third parties (“marketplace platforms”, each specialized on a certain part of the market). The centralized exchange will calculate and execute a network barter deal, and all users (or marketplace platforms on their behalf) are then able to transfer the resulting balances to their CAS offline wallets.

A centralized exchange for network bartering is much less of an issue than a centralized exchange for exchanging cryptocurrencies for state currencies and other cryptocurrencies. Because:

- **Server availability** is not (much of) an issue as this central database only needs to create one trade per day (at most), or even only one trade per week. It hurts the total turnover of network barter exchange when doing trades too often, as executing small loops will break later loops that would come up had one let the order graph evolve more.
- **Network availability** is not an issue, as in case of Internet bisection (after disasters, in case of Internet blackouts, in case of censorship etc.) a new "single central database" can be set up in the remaining local network. It also does not hurt committing orders to multiple such databases, as long as the user is ok with all of these orders being executed. So it's not really a central system, but a multi-central system. Any group of people can agree to use a certain host as their trade-finding center. For example there could be a Raspberry Pi in a village without Internet and without intranet, to which people connect when passing the public place where it sits. It would also facilitate the exchange of the triple-signing messages, and once that is done, users have the coupons on their phones and can use them to pay offline in P2P manner (via Bluetooth, OCR on screen etc.).
- **Confidentiality** is not a worse issue than with any existing platform that has to keep database content private.
- **Security** against tampering with data is not an issue as this database does not contain any wallets but creates only one transaction, and the results of this transaction have to be confirmed by both issuer and holder via triple-signing to become spendable in the CAS. A user will not sign that their coupons go to a person who was not allowed to order them in the first place. So "stealing" coupons by bending orders in a network barter trade is not even possible.

- **Data integrity** (regarding accidental changes and data losses) is not an issue, as each record of a network barter transaction can be deleted as soon as all results have been taken over into wallets by triple-signing transactions of all involved parties. (Parties would signal that to the central database, and the central database will then indeed delete the records, or at least know nothing bad will happen if it deletes them.) Also, all orders and offers will be registered at the trade finder server anew for the next cycle, so it does not have to protect its integrity long-term either.

From this argument it appears that there is no urgent need in practice to create decentralized network bartering, and our exchange pay.coupons will continue to be of the centralized type. However, decentralized network bartering of course has advantages for the trustability, reliability and resilience of a global network barter economy, so it will keep a topic of research.

4.10. Identity and Reputation

For each type of coupons, its value comes from the trustability of its issuer. To be able to trust the issuer, it is essential to know them. For that, the system will offer multiple tools:

- Companies in an established, trustable business relation will tell each other their PayCoupons usernames or addresses. This means that users only have to reveal the real-world identity behind their PayCoupons account to those they know and trust.
- Companies which are trustable by being well-known brands simply can publish their PayCoupons username or address on a publication they control (read, their SSL encrypted website).
- As a more comfortable alternative to the previous option, companies can choose to associate their real-world identity with their PayCoupons account so it becomes findable in PayCoupons software. The first mechanism we will support for this is (probably) the Estonian E-Residency scheme,[18] which allows online identification with a so-called E-ID smartcard, provided to anyone taking part in the scheme. smartcards provided to “e-residents”. This is possible, as Estonia provides a fully open source software stack to interface with their E-ID smartcards.[19]
- As a final alternative, users can choose not to reveal their real-world identity. In this case, they build up trust by reputation on the platform, derived from reviews by users who redeemed their coupons in the past. This is a slower process but also provides the most privacy.

A reputation mechanism will be provided for all types of coupons resp. their associated user accounts, recording the experiences of users when redeeming coupons for actual products and services.

Also, the outstanding account balance is part of the reputation, included as a metric that is publicly shown. Obtaining this metric is somewhat complex, since coupons can be redeemed offline with the CAS mechanism. However, the following process solves it:

1. The exchange already has transaction records were coupons were issued online, via network bartering.
2. The coupon issuer’s CAS application contributes transaction records were coupons were redeemed back to the exchange, as the issuer is interested in reducing the number of coupons shown to be in circulation.
3. The coupon holders’ CAS applications contribute the transaction records where coupons were issued offline.

[18] See: https://e-resident.gov.ee/
[19] See: https://github.com/open-eid

4. Issued and redeemed coupons are then subtracted from one another to obtain the required metric.

4.11. Other Aspects

Role of hosted exchange platforms. For mainstream acceptance by businesses, it is essential to provide a zero-effort signup experience. After experiencing the benefits of the tool and upon deciding to do more business through it, users may invest more time to understand the concepts behind and secure their usage of the tool, but not before. For that reason, we currently provide (and will keep providing) the exchange platform pay.coupons,[20] including an online wallet functionality. This platform allows newly signed up users to issue, exchange and redeem coupons, without exposing them to the CAS system to store their coupons and pay with them offline. However once users become serious about their use of the PayCoupons system and manage larger amounts of value in their account, they will want to take full control of the coupons they hold. For that, they can use a "coupons takeout" feature at any time to transfer their coupons to a wallet software – this will usually be the CAS offline wallet software, but can also be a third-party online wallet with client-side encryption, or a self-hosted open source wallet application.

Coupons as well-defined contracts. Use of coupons in business requires that businesses know their rights and obligations when using coupons. For that, ordering, holding and redeeming coupons will be mapped to well-defined, legally binding contracts, adjusted for specific jurisdictions where required.

Arbitration mechanism. To resolve disputes around the redemption of coupons for products and services, the PayCoupons template contract defining the relationship between coupon issuer and coupon holders may include a clause that requires private arbitration in the PayCoupons system before taking an issue to court. As typically done, both parties of the conflict would designate an arbiter (among PayCoupons users), the two chosen choose a third, and the three discuss and decide the case. All of this would be provided by dedicated software features, and integrated with the reputation system (in case parties do not follow an arbitration ruling, it affects their reputation). Arbiters will be paid in PCT tokens for their services. An arbitration mechanism helps to simplify international business relations by disentangling conflict resolution from national legislation. At this time, we do not promise if and when PayCoupons will have arbitration capabilities, as we will make this dependent on the need for this observed in practical use.

Open system. To be a serious candidate for a worldwide economic exchange system, the PayCoupons cryptocurrency system will be an open system, in order to grow through an ecosystem of third-party solutions and their associated user communities. The PayCoupons protocol specification will be publicly available under an open content licence and collaboration on the protocol will be available to the public. Also, all parts of the PayCoupons cryptocurrency system will be equally open to be provided by independently created applications that adhere to the protocol. We will provide a free and open source reference implementation of the PayCoupons client application "CAS". We may or may not release our other software, such as the trade finder server, as free and open source software. But as said, all functions in the PayCoupons cryptocurrency system will have publicly available specifications in the protocol, and third parties can set up their own exchange platforms or develop their own wallet software applications. Third party exchange platforms will typically offer fee payments in PCT as well, given that all existing PayCoupons account holders will have some PCT; this is however not a technological requirement.

[20] See https://pay.coupons/

Integrations. Comfortable integration with third-party software is essential for the success of a new payment option such as ours. This ranges from modules for third-party webshop software providing a PayCoupons payment option to integration with invoicing and accounting systems. We will encourage the development of these integrations as part of our token distribution programs, and make sure they are provided as free and open source software wherever legally possible.

5. Token Distribution

The PayCoupons token PCT will *not* be made available through an ICO ("Initial Coin Offering"). Instead, we will use airdrops ("free token handouts") and other distribution methods to bring PCT tokens into widespread circulation and encourage their use on the PayCoupons platform. That said, we may auction off small amounts of PCT tokens in mini-ICOs later, if the market and legal environment allows it. It will never be our main distribution method, though.

What. PCT, the PayCoupons Tokens. A newly minted type of tokens issued on the Stellar blockchain. Used as the only utility token of the PayCoupons exchange platform pay.coupons.

When. Starting from 2018-06-15 (15 June 2018) until all distributable PCT tokens are distributed. We expect to run campaigns for a minimum duration of 10 years, but no promises are made.

How. Multiple time-limited token distribution programs, partially in parallel. The type and exact conditions of each program are only decided when starting the campaign and depend on the current growth state of the PayCoupons user community and ecosystems, and its various needs for infrastructure, users, economic activity in various areas, and so on. Our official information about current, ongoing token distribution programs is always provided at https://pay.coupons/pct. Distribution programs may include, but are not limited to, the following:

- **Airdrops.** Free handouts of PCT tokens to members of the public, with no conditions whatsoever and no strings attached.
- **Bonus programs.** PCT tokens as rewards for existing PayCoupons users if they contribute to the growth of the PayCoupons ecosystem, for example by referring a new user.
- **Funds.** Larger amounts of PCT tokens, handed over to other organizations to distribute them according to an agreement made on a case-by-case basis.
- **Grants.** Larger amounts of PCT tokens, handed out to organizations that promote the use of PayCoupons, or do other work that the board of the PayCoupons GmbH wants to support.
- **Bounty programs.** Rewards for campaigns that seek input from the public, such as for finding security issues, software bugs, contributing success stories, or similar. Participation may be subject to conditions (for example, of being legally able to invoice for the contribution made).
- **Purchases.** Payment with PCT tokens for products and services purchased by the PayCoupons GmbH company.
- **Sales on the open market.** Sale at current market rates on exchange platforms. We have incentives to not disturb the market price through these sales, as we want to maximize the sales value of the remaining PCT holdings of PayCoupons GmbH. So we will keep these sales at appropriate, low volumes.
- **Mini-ICO sale events.** These differ from the sale on the open market by potentially selling at below-market prices, whether using auction formats or fixed offer prices. To not disturb market prices, we voluntarily limit the amounts of PCT tokens we may distribute this way to 5% per

calendar year, measured as a fraction of the already distributed PCT at the beginning of that year.

- **Sale to investors.** We may decide on a case-by-case basis, and subject to regulatory approval where needed, to sell PCT tokens to a few individual or institutional investors, particularly in the early stages of the ecosystem development. To limit the influence of major investors ("whales"), this distribution program will cover 20% or less of distributable tokens.

Apart from airdrops, at this time we do not commit to any of the distribution methods mentioned above. Each distribution program may be subject to regulatory conditions and / or approval, and depending on the exact conditions, we may choose at any time to halt or omit any distribution method, especially if it conflicts with the ability to legally airdrop the PCT token.

How much. The distributable PCT tokens amount to forty million tokens (40,000,000 PCT), all of which will be distributed in the various programs. This amount equates to 80% of the total supply of fifty million tokens (50,000,000 PCT) that will ever exist, all of which have been issued on 2018-04-14. The remaining amount of ten million tokens (10,000,000 PCT) is the founders' share, equating to 20% of the total supply. Using a Stellar blockchain explorer, you can confirm the amount of total supply and that no new tokens can be created in the future: examine the PCT tokens issued by account GCVF4SNEQ4MI745ZADWDCKE7HD2JVYUOQ7YYA3U33ICZT2G2E6OJOAH4,[21] and confirm that (1) the account has issued 50 million PCT and (2) the only signer of the account was removed after that, prohibiting future issuing of this token.

Usage of proceeds. All proceeds of the token distribution will be used, at the sole discretion of PayCoupons GmbH, for the purpose of creating the technology of the PayCoupons cryptocurrency system, and towards establishing the PayCoupons cryptocurrency system as a fair, major or dominant, next-generation payment system in the global goods and services economy. PayCoupons GmbH will pursue this purpose in an economical, law-abiding and socially and ecologically fair and sustainable way. This purpose determines the use of funds on a best-effort basis, but in no way whatsoever implies any guarantee about achieving this purpose in full or in part, or of undertaking or omitting any specific action.

6. Development Status and Plan

We have developed the idea of network bartering in early 2013 and found the mathematical solution for calculating network barter trades in late 2013. Since then, we have invested a total of at least 6000 person hours of development efforts into technology development. Our marketplace platform has gone through at least five major iterations until we found what (we believe) is the "sweet spot" for network bartering, both regarding its target group and its presentation through a simple user interface. We settled for small to medium companies (esp. service companies) as the target group, and for a user interface that around the concept of "coupons" with values shown in well-known currencies. We now intentionally position PayCoupons as a kind of "Internet payment provider", not integrating a marketplace into its exchange platform pay.coupons; that allows the most generic use of PayCoupons as an alternative for state currencies, as it can be taken up by any third party webshop, brick-and-mortar shops and so on.

It was especially challenging to hide all the technological complexity of network bartering behind the user interface – as a result, our users will not even see the word "barter" anywhere. Another challenge was to select the "right" features out of the pandora box of possible features opened by our invention of network

[21] See: https://stellar.expert/explorer/public/account/GCVF4SNEQ4MI745ZADWDCKE7HD2JVYUOQ7YYA3U33ICZT2G2E6OJOAH4

barter. We still have about 600 pages detailing the possible features, developed in endless exploratory discussions, and selected only a few features in the end.

The result of that development work is the current PayCoupons platform, fully functional, mature and ready to use at https://pay.coupons/.

We have received the Social Innovation Award of the European Union[22] in 2013 for the potential of our network bartering invention to create jobs, esp. for European youth.[23] In fact, the conditions of high youth unemployment in Europe after the 2007-2012 Great Recession was our pain point. (It's absurd, right? Millions of young, energetic, well educated people, all with skills and needs and time to work, and no "economy" to connect them.) This inspired us to look for alternative solutions and eventually invent network bartering.

In late 2017, PayCoupons was outgrowing its organizational form as a joint-venture project of three European companies, so we incorporated as PayCoupons GmbH, a limited liability, privately owned company seated in Berlin, Germany.

While the idea is innovative and the PayCoupons platform concept and feature set is mature, we now require more significant funding to achieve a scale for real-world usage and impact, realizing the highly disruptive potential of the idea for the functioning of the goods and services economy. At the same time, to have an impact at scale we have to grow the PayCoupons ecosystem from a single platform into a payment ecosystem with multiple independent platforms, a framework for legal compliance, and integrations for business processes worldwide. This includes, among others, payment method integrations for major e-commerce platforms and payment modules for major open source webshop solutions.

So as the next major step, we are extending PayCoupons into an open cryptocurrency ecosystem, as outlined above.

A rough timeline for feature releases looks as follows. Features and target dates are only indicative, as they also depend on requirement changes emerging from practical use, technological challenges and available funding.

- **Q2 2018: PCT fee payment.** PCT tokens will be accepted as a payment method on the PayCoupons exchange platform, pay.coupons.
- **Q3 2018: Payment API.** Making it possible for webshops and other external actors to request a user to pay with coupons. Implemented on the existing pay.coupons exchange platform, but platform-agnostic and with an open specification so that it can be implemented by third-party marketplace and exchange platforms in the future.
- **Q3 2018: Webshop integrations.** Payment modules for several open source webshop systems that provide "PayCoupons" as a payment method, using the payment API of the pay.coupons platform.
- **Q4 2018: Smartphone wallet app, takeout feature.** The CAS offline wallet software for PayCoupons is released as an open source smartphone app for Android. It includes offline

[22] See: http://ec.europa.eu/growth/industry/innovation/policy/social/competition_en

[23] We participated under the name "Economy App". See: http://ec.europa.eu/growth/content/best-social-innovation-ideas-new-ways-create-new-jobs-and-businesses-0_en

payment functionality that can be used in shops. A takeout feature on the pay.coupons marketplace platform allows to transfer coupons to the smartphone wallet app.

- **Q1 2019: Security audit.** After this audit, the PayCoupons exchange platform and CAS application can be considered ready for productive use with large values of coupons.
- **Q2-Q4 2019: Remaining Features.** We will implement integrations with point-of-sale terminal systems, integrations with business accounting applications, and other features for which the need will emerge.

Throughout this time, we will work towards full market uptake of the PayCoupons system, starting with several pilot markets. Naturally, market seeding activities have to include incentives to offer and use coupons before a market is large enough to make the benefits self-evident. This is funded through the token distribution programs.

7. Company Information

The legal entity developing the PayCoupons cryptocurrency system, operating the pay.coupons exchange and distributing the PCT token is PayCoupons GmbH, a regular limited liability company registered in Germany:

PayCoupons GmbH
Pappelallee 78/79
10437 Berlin
Germany

Website: https://pay.coupons/
E-mail address: mail@pay.coupons
Other contact options: see https://pay.coupons/imprint/en

Registration authority: Amtsgericht Berlin (Charlottenburg), Germany
Registration number: HRB 191524

The founders and current shareholders of PayCoupons GmbH are:

- **Daniel Ansorg**, co-founder and CEO
- **Matthias Ansorg**, co-founder

Anyone may confirm the correctness of the information supplied above, using the online service of the official company registration portal of Germany, https://www.handelsregister.de/. Go to their “Normal Search” page[24] and search with: “Type of register: HRB”, “Register number: 191524”, “Register court: Berlin (Charlottenburg)”.

8. Disclaimer

No offer, no sale. None of this document, and none of the other communications of PayCoupons GmbH, constitutes an offer for sale of PCT tokens, or an investment advice to purchase PCT tokens, or a promise of any properties or rights or warranties of PCT tokens. At this time we (PayCoupons GmbH)

[24] See: https://www.handelsregister.de/rp_web/mask.do

do not sell any PCT tokens. So far, you can only obtain PCT tokens as a free gift from PayCoupons GmbH, and by accepting PCT tokens as a gift you agree that you cannot and will not hold PayCoupons GmbH legally accountable for any suspected or actual damage or loss in connection with PCT tokens.

No guaranteed use or property. The PayCoupons tokens PCT have no inherent or guaranteed rights, uses, attributes, features or functionalities, and especially have no guaranteed monetary or financial value. We (PayCoupons GmbH), and also anyone else for that matter, may *choose* to accept PCT tokens as settlement for debt with anyone or everyone, but this remains a free and voluntary choice without any legally enforceable right or guarantee given to anyone. Especially, PayCoupons GmbH does not guarantee to accept PayCoupons tokens (PCT) as a means of payment. We *intend* to do so, on a best effort basis, but may be forced or advised to change this at any time depending on changes in laws and regulations and other external or internal changes.

Disclaimer of warranty. Both the PayCoupons tokens (PCT) and all PayCoupons software are supplied *as they are* and come without any warranty, to the extent permitted by applicable law. They come without warranty of any kind, either expressed or implied, including (but not limited to), the implied warranties of merchantability and fitness for a particular purpose. The entire risk of use of the PayCoupons tokens (PCT) and PayCoupons software is with the user.

Disclaimer of liability. In no event (unless required by applicable law) will PayCoupons GmbH or any or its shareholders, board members, employees, collaborators or associates of any kind, be liable to you for damages arising out of the properties, use or inability to use of the PayCoupons tokens (PCT) or PayCoupons software. This includes any general, special, incidental or consequential damages, including but not limited to loss of data or money or funds or trust or reputation, and even if PayCoupons GmbH or another party has been warned about the possibility of such damages.