"For centuries, global trade has been the single greatest creator of wealth in human history and market friction the greatest obstacle to wealth."

"…those banks with the most hands-on experience in blockchain technology, scan the horizon, they see something different than other banks – a wall of disruption heading toward them.

"It's moving, my friends, it will be there sooner or later…"

ABSTRACT

Bitcoin is the world's first decentralized digital currency, allowing the easy storage and transfer of cryptographic tokens. It uses a peer-to-peer network to carry information, hashing as a synchronization signal to prevent double-spending, and a powerful scripting system to determine ownership of the tokens. There is a growing technology and business infrastructure supporting it [1].

Paysfer is a centralized marketplace with a decentralized settlement system, one that is based on Ethereum smart contracts that represent units of fiat currencies. As of today, the users of Ethereum pay $0.84 for a transaction [2].

TRANSACTIONS

[Today], many business transactions remain inefficient, expensive and vulnerable [3]. Over the past forty years, individual steps of the workflow of financial transactions have been computerized; the business process remained unchanged, as if processing continued to be manual. Delivery and settlement of transaction is batch based and occurs with a time delay of two and more days and does not happen at the time of the trade. Every bank has its own bookkeeping system and is an island from an audit point of view, where verification of trades is cumbersome and prone to errors. This regime contributes to a high degree of fragmentation and uncertainty in the market, multiplication of risk factors, high transaction costs for financial assets and lack of liquidity and transparency in financial markets [4]. These costs are of course ultimately bared by the customers.

Lengthy settlement periods – often 20 days or more – are tying up capital and hamper corporate liquidity. Smart contracts on blockchains have the potential to dramatically reduce the time to settlement [5]. Overall, we believe that the transition to blockchain technologies is inevitable and those who will be prepared to embrace the change will prosper.

Any transaction requires a universal unit of value. Both, fiat and cryptocurrencies are ill-suited for this role in the blockchain-based economies of the future. In what follows we propose a solution.

CRYPTOCURRENCIES AND FIAT CURRENCIES

In its conventional sense the currency is distinguished as serving three major functions: it is a store of value, medium of exchange and a unit of account. Bitcoin and other cryptocurrencies also match these characteristics, however, lack convenience of fiat currencies as a unit of account and their stability as a medium of exchange. Further, the technical complexity involved in using cryptocurrencies is far beyond the level of comprehension of an average person. Notwithstanding these issues, they represent a lucrative investment opportunity (this shall not concern us in this report) and possess several other characteristics that distinguish them favorably from the traditional fiat currencies and that are directly relevant to our topic. The list of benefits and disadvantages of fiat currencies (and transfers of value using them) and their crypto counterparts can be found in the table below.

	Fiat Currencies and transactions thereof	Cryptocurrencies and transactions thereof
Advantages	+ Relatively low volatility + Conventional unit of account + CB commitment behind price stability	+ Broad transferability + Low transaction costs + Short transaction times + Trustless ownership and exchange + Transparency and auditability + Cryptographically secure
Disadvantages	- Limited transferability hampered further by cross-border capital transfer restrictions - High transaction fees - Low transaction times - Vulnerability to theft - Low degree of transparency and auditability	- Inconvenience as a unit of account - High volatility[1] - High complexity from the public viewpoint

Table 1: benefits and disadvantages of fiat and cryptocurrencies

As it is evident from the table above, the list of disadvantages of fiat currencies mirrors (with the opposite sign) the list of benefits of cryptocurrencies. The same applies to the drawbacks of

[1] Both, ECB and EBA as well as other authorities refer to the volatility of cryptocurrencies as one of the major impediments precluding the use of it as a means of payment.

cryptocurrencies. The issue we are determined to resolve is the creation of a hybrid currency, one that would inherit only the best from both words.

THE HYBRID CURRENCY AND THE PAYSFER

The idea of creating a hybrid currency is not new in the community [1]. There have been multiple papers and attempts of actually issuing a hybrid currency that would take the best of both worlds (see e.g. [1], [6], [4]). As we shall illustrate below, however, neither of these attempts can be called flawless.

We propose a public blockchain-based payment system suited for users' everyday convenience that will utilize 1:1 fiat backed crypto tokens and that will be characterized with:

1. Low transaction fees,
2. Short settlement times[2],
3. Cryptographically secured ledger,
4. Trustless ownership and transfer,
5. Transparency and auditability,
6. Ease of use and integration,
7. Absence of liquidity constraints,
8. Decentralized (hence, without a single point of failure),
9. Fiat-like price-volatility and
10. That would allow for a conventional denomination of goods and services that can be bought or sold.

As it is evident, some of the aforementioned qualities are normally associated with cryptocurrencies, while others qualities characterize their fiat counterparts. In general there are three major ways to achieve such a synthesis:

1. One is to use Bitcoin blockchain in the manner Tether does: via the Omni-Layer protocol [6]. This has a disadvantage: Tether is not a truly decentralized system; it serves as a custodian of the

[2] For example, "Let's Talk Payments" reports that recently ATB has successfully transferred CA$1,000 (EUR 667) to ReiseBank using a network built on SAP technology and Ripple's network of enterprise blockchain solutions. The payment, which would typically have taken between two to six business days to process because of requirements such as settling with the counterparty bank and reconciling accounts, was completed in around 20 seconds.

real assets that back the USDT in circulation and is, thus, susceptible to all the treats that the Distributed Ledger Technology (DLT) can solve.

2. Second method is to color coins: the colored coins represent issuer-backed securities on the Bitcoin Blockchain (see e.g. [4]). This approach as it appears to us is far superior to the first one, however, is not without flaws as well. The two major ones of them are that:
    a. Bitcoin while being the first and the most popular cryptocurrency is not as flexible as for example Ethereum in terms of contract design: it requires additional protocols to expand its functional.
    b. The Blockchain used is that of Bitcoin, which notwithstanding strong benefits (such as massive processing power) over other cryptocurrencies, suffers from the limited block size and minimum transaction processing time. Overall, while building a separate coin on the basis of Bitcoin has its benefits.
3. Finally, as yet a different solution, it is possible to create a smart contract on the basis of Ethereum that will represent a digital claim on a dollar bill deposited on the account of the holder. This is quite similar to the colored coin solution discussed above; however, it is based on Ethereum blockchain and has several major advantages. Unlike Bitcoin Colored Coins that are literally stored in the Bitcoin addresses, Ethereum tokens are just records in a single variable of an Ethereum smart contract [4]. Ultimately a standard token contract on Ethereum blockchain is both, a coin holder's ledger and an interface (set of rules and functions) that allows updating internal contract ledger records in a proper way.

Smart Contracts:

In 1996, Nick Szabo described a smart contract as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."

Smart contracts are computer protocols that facilitate, verify, or enforce the negotiation or performance of a contract, or that make a contractual clause unnecessary. Smart contracts involve objectively verifiable performances, or performances that can be automated such as cash flows.

The humble vending machine is the original form of a smart contract. At its core, a vending machine is a security mechanism: the amount in the till should be less than the cost of breaching the till. Additionally, the machinery reflects the nature of the deal: it computes and dispenses change as well as the customer's choice of product [5].

From the discussion above, it is clear why we opt for the Ethereum-based solution: it is more flexible and avoids major inconveniences that come with the use of Bitcoin and its blockchain as a foundation for a new digital currency.

The Ethereum smart contract that is a foundation of our system has the following basic features:

1. The client can deposit the fiat funds with the reference bank and instantly receive an equivalent amount of Paysfer tokens (basic smart contracts) on one's wallet.
2. The client can withdraw his fiat funds whereby the Paysfer tokens are destroyed while the client's bank account is credit with the equivalent amount of fiat currency.
3. Any transfer of Paysfer tokens from one wallet to another has to be signed by both parties to the transaction and Paysfer. This feature utilizes the multisignature functional.

In our design we opt for a conservative approach and are, thus, guided by the considerations of minimal risk, transparency and simplicity.

Paysfer does not take possession of either fiat currency backing the token, or the token itself and simply matches the buyers and sellers settling the transactions on the common public blockchain: a centralized marketplace with the decentralized settlement. In this manner, Paysfer's clients do not need to trust it in order to be confident that their funds are safe from fraud.

However, there are two concerns that might arise irrespective of the aforementioned:

1. Paysfer might not provide its clients with the best prices of goods and services that are listed on the marketplace.
2. There needs to be a trust in the Token itself, meaning that a selling party to a trade must be confident that a buyer possess sufficient amount of fiat currency on his or her account in order to actually be able to pay for a purchase.

We are confident that the first problem can be easily resolved by the most basic comparison with other sources where a similar product is offered while the second one will be solved by designing the smart contract in a way where the Paysfer tokens are issue if and only if an amount is transferred to a custodian bank, thus requiring any user to hold 1:1 collateral against their Token balances. This ensures that at any moment in time every token in circulation is backed with exactly one unit of the respective fiat currency, thus inheriting its value. This process of 'digitalizing' the fiat currency, thus creating a fiat-crypto hybrid, generates a unit of account that synthesizing all the benefits of cryptocurrencies and fiat currencies without inheriting any of their flaws[3].

[3] We realize that the value of the Paysfer token will always have a discrepancy with that of the fiat currency backing it representing the credit risk of the depository institution safeguarding the fiat balances. We, however, believe that by depositing the funds with several large reputable depository institutions we will be able to diversify away any credit risk, thereby minimizing the discrepancy.

At the same time, by opting for such design Paysfer effectively does not take possession over the fiat currencies in the form of deposits. Instead, Paysfer acts as a marketplace and a payment system that allows for a direct and quick transfer of tokens between the parties wishing to participate in a transaction. This greatly reduces the regulatory burden and the associated compliance costs while at the same time enhancing the customer value.

According to our vision, in the future the actual exchange between the Tokens and fiat currency will not be necessary. We, thus, view the fiat currency to be the equivalent of gold in an era of gold standard, just backing the value of Paysfer tokens.

PARTIES INVOLVED

There are multiple parties that are involved:

1. Paysfer's clients purchase the Paysfer Tokens, each of which represents an IOU on one unit of fiat currency. This insures that the value of each and every Token that was issued by Paysfer mirrors 1:1 the value of the currency that has been deposited. The clients need to be registered with Paysfer in order to establish a basic level of trust and fulfill the KYC and AML requirements. Every token can always be exchanged back to the respective number of fiat currency units.
2. Vendors registered with Paysfer provide access to their goods and services that can be traded for Paysfer Tokens. The goods and services are listed on the platform in a convenient and user-oriented manner and any client with an appropriate amount of Paysfer Tokens can purchase any good that suits one's preferences. Any transaction between a client and a vendor is being matched using the Paysfer's matching mechanism and once confirmed is settled on the Ethereum blockchain.
3. In principle any vendor can be a client and vice versa: any form of B2C, C2B, C2C or B2B type of transactions is possible.

Once a client opts for a particular product listed under the name of a vendor, his or her Token balance is verified. Once there is a sufficient amount of Tokens, the presence of the good is verified along with its availability and other particularities. Once both are confirmed, the necessary amount of Tokens is sent to Paysfer and the order is placed. The payment requirements will vary from vendor to vendor and from country to country, however, the basic arrangement is as follows:

1. The order is placed and the goods are being sent to the client,

2. The Tokens that have been transferred to Paysfer are being held as a collateral for both parties, the vendor and the client:
    a. If the goods do not arrive or arrive late, etc. the balance is being transferred back to the client and the transaction is not settled on the blockchain.
    b. If the goods arrive according to the terms and conditions agreed upon by the client and the vendor, the vendor receives the Tokens and the transaction is settled on the blockchain[4].

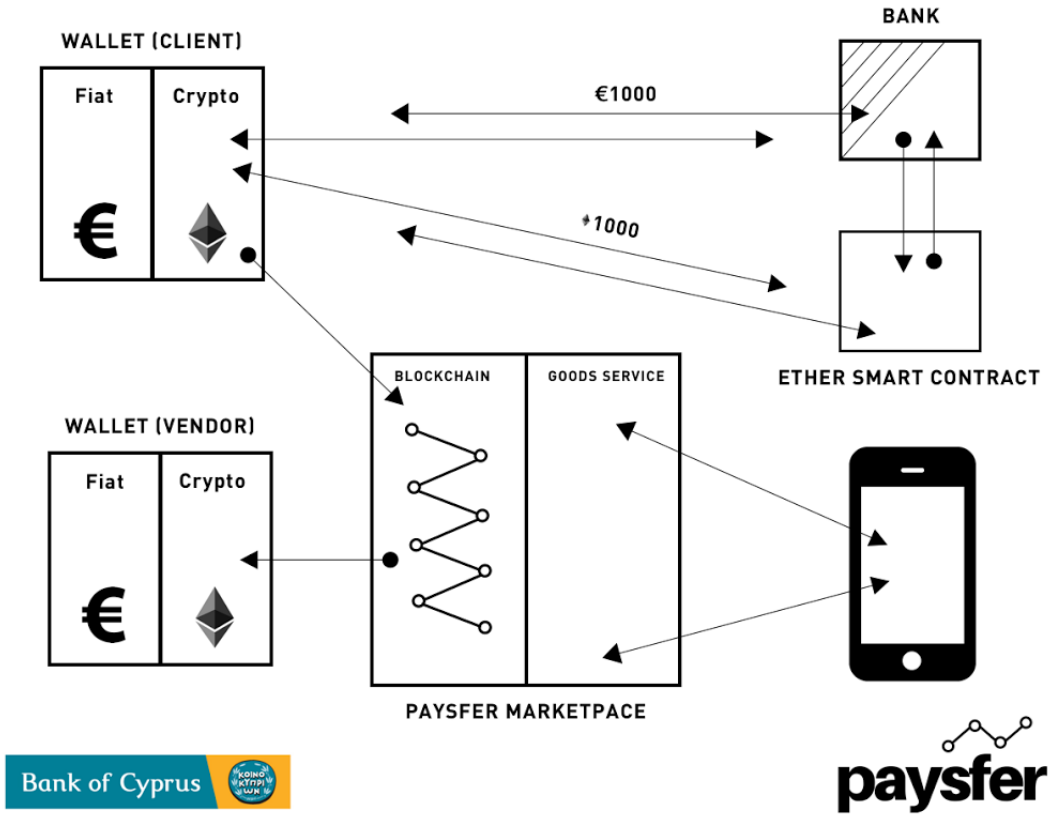


Figure 1: the Paysfer concept

The variety of product and services that can be bought or sold via Paysfer is basically unlimited. Any transaction that represents a transfer of value for cash ranging from the purchase of a pizza in a nearby store to bulk order of industrial materials can be made using Paysfer's tokens.

[4] Obviously, such arrangement favors the client. Industry-, product- and country-specific arrangements can be made in order to tailor the terms to the needs of various groups of clients and vendors.

The flexibility of the Ethereum as a Smart contract platform combined with a convenience of a fiat currency represented by the means of a Token on the Ethereum blockchain allows for a virtually unlimited freedom in designing the contracts. For example, instead of paying for goods, a client of course can simply transfer the funds from his or her account to that of a friend or a family member. All the benefits of Paysfer's hybrid currency apply here as well.

TRUST

"In business, trust is incredibly hard to engineer and impossible to guarantee. Until now, we've relied on instruments and institutions to be surrogates for our trust. With blockchains, trust can be embodied in the transaction itself. A far greater assurance of trust is now possible. As this heightened sense of trust pervades the ecosystem, third parties that were once necessary to broker trust will be disintermediated. Smart contracts, certifications and digital compliance on blockchain networks will codify trust at the level of the individual transaction. This codification of trust can optimize transactional relationships, making business interactions across ecosystems far more efficient."

There are multiple problems related to trust that are present in real world transactions as we know them today that require the presence of a trusted 3-rd party. As we shall illustrate in what follows, the design of Paysfer allows for eliminating all of them except for one. The exposure to the latter, however, can be mitigated to a large extent.

In its nature, Paysfer is a semi-decentralized payment system: it does not take possession of the Tokens being transferred from one counterparty of a trade to the other; however, these Tokens are backed by the real money balances held with Paysfer's trusted bank acting as escrow. Any withdrawals or deposits to this account can only be made with the use of Paysfer's wallet:

1. A client with fiat money balance can transfer it to the bank receiving newly issued Paysfer Coins in exchange,
2. A client with Paysfer Coins can opt to claim back the fiat money if one wishes to do so; in this case the Paysfer coins will be automatically destroyed and one's fiat account credited accordingly.

This implies that the bank serves as a custodian for the deposited funds and, thus, has to be trusted. A large regulated financial institution shall suffice in this role. Furthermore, as it was mentioned above, it is possible to diversify away the credit by using accounts of multiple banks.

Other trust concerns and the ways in which Paysfer is planning to resolve them are as follows:

1. Concern: In simple terms, in order to be able to pay via Paysfer, a client needs to deposit one's funds. Thus, a client has to entrust Paysfer his or her coins (the wallet) and is therefore susceptible to malicious intent on the side of Paysfer itself or in case of a security breach on the side of hackers or other wrongdoers. Is it? As we shall see, depositing coins does not imply trusting them.

   Resolve: To our best knowledge, one of the most inventive, convenient and elegant solutions are multisignature wallets. Basically, in order for any transaction via Paysfer to be executed, at least two private keys have to sign the transaction: one on the side of Paysfer, one on the side of the wallet owner (obviously, this implies one wallet for the buyer and another one for the seller). This ensures that Paysfer cannot spend client's coins without his or her consent. In simple terms, if you explicitly make it harder or impossible for yourself to do certain things, then others will be more likely to trust you and engage in interactions with you, as they are confident that those things are less likely to happen to them. At the same time a client cannot transfer the coins outside of Paysfer without Paysfer's consent. One also cannot spend his or her coins on for example illegal goods and services.

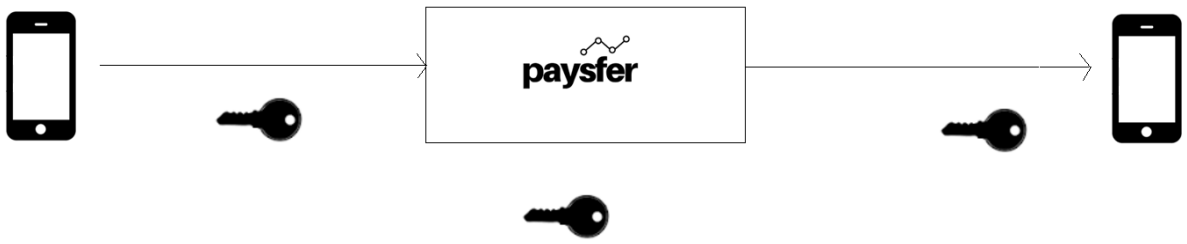


Figure 2: Multisignature Wallets

2. Concern: the private keys to client's wallets can be destroyed or stolen from Paysfer due to, for example, hackers attack or other similar unfortunate event. Does this imply that client's wallets will be frozen?

   Resolve: there are two layers of defense against such event: firstly, the Ethereum Smart contracts that underlie Paysfer Tokens once on the wallet, can be readily exchanged back to dollars. Mechanically, the dollars are transferred back to the client's debit or credit card and once there is a confirmation (recall that client's card is attached to the wallet), the token are automatically destroyed. Such mechanism ensures that while the tokens cannot be transferred outside of Paysfer, the fiat money is always readily available to all the clients that have Paysfer tokens on their wallets. In case of a malfunctioning of this mechanism, Paysfer offers an offchain refund. Further, as it is evident from the preceding paragraph, Paysfer never actually takes possession of

the clients' tokens. This ensures that there will be not too many incentives for any attacker to hack Paysfer: the most that one can achieve from doing this successfully is to take possession of the collateral that will be deposited in Paysfer in that given time instance. In order to limit this treat Paysfer will cold store the collateral worth more than a pre-defined threshold. This means that the damage done to the exchange in an event of a hacker attack is extremely limited.

3. Concern: the goods actually delivered can be of poorer quality than those advertised on Paysfer's platform or can be delivered late or even not delivered at all.
   Resolve: in order to resolve this issue, Paysfer has two layers of defense against vendors' wrongful behavior. Firstly, once the coins are transferred to the Paysfer platform (once the transaction is initiated by the two parties and the buying side along with Paysfer confirms the transaction by using their private keys) these coins actually temporarily reside with Paysfer. Only once, the payee confirms that the good is of expected quality and that it was delivered on time, the transaction is being settled on the blockchain. In this vein, the tokens being held by Paysfer serve as collateral for the transaction. Therefore, to the same extent as they protect the buyer form seller's wrongdoing, they protect the seller from the malicious intent on the side of the buyer. Additionally, in order to have its products listed on Paysfer, any company will have to be accredited by the relevant authorities.
4. Concern: unlimited issuance of coins.
   Resolve: not possible due to the nature of the smart contract underlying the issuance of Paysfer Tokens.

In this section we will discuss the benefits that each of the parties discussed above will enjoy by using the Paysfer.

Clients:

> *"There is a clear opportunity to create a better customer value proposition by offering real-time financial transaction status tracking, better visibility on financial institutions' fees to and from participating partners, more accurate recovery of fee revenue, and faster resolution of disputed billing transactions," Judd Holroyde, Head of Global Product Management at Wells Fargo*

1. Dramatically increased speed and transparency of transactions;
2. Increased transparency of fees;
3. Reduced transaction costs;
4. Improved security;
5. Real-time tracking of orders;

6. Reduction in counterparty risk;
7. Access to new markets, goods and services

Banks:

> *"[Banks] see a significant wall of disruption heading their way. They expect five out of nine core business areas to experience significant disruption and are investing in each one .... Across the industry, all banks are investing in international payments, other cash management, corporate lending, consumer lending, mortgages and deposit taking."*
>
> *"First mover advantages for this group include the ability to influence and set the business standards by which others will operate. Moreover, as start-ups take aim at incumbents and new business models expand beyond industry boundaries, first-mover banks will be well situated to get ahead of the consequent disruption."*
>
> *"Costly and time-consuming reconciliations are all but eliminated and an instantaneously verifiable superior platform for up to-the-minute analytics. Because reference data is integral to all of a bank's activities and isn't bound by the complex regulations found in other areas of banking, it's proving a good place to start."*

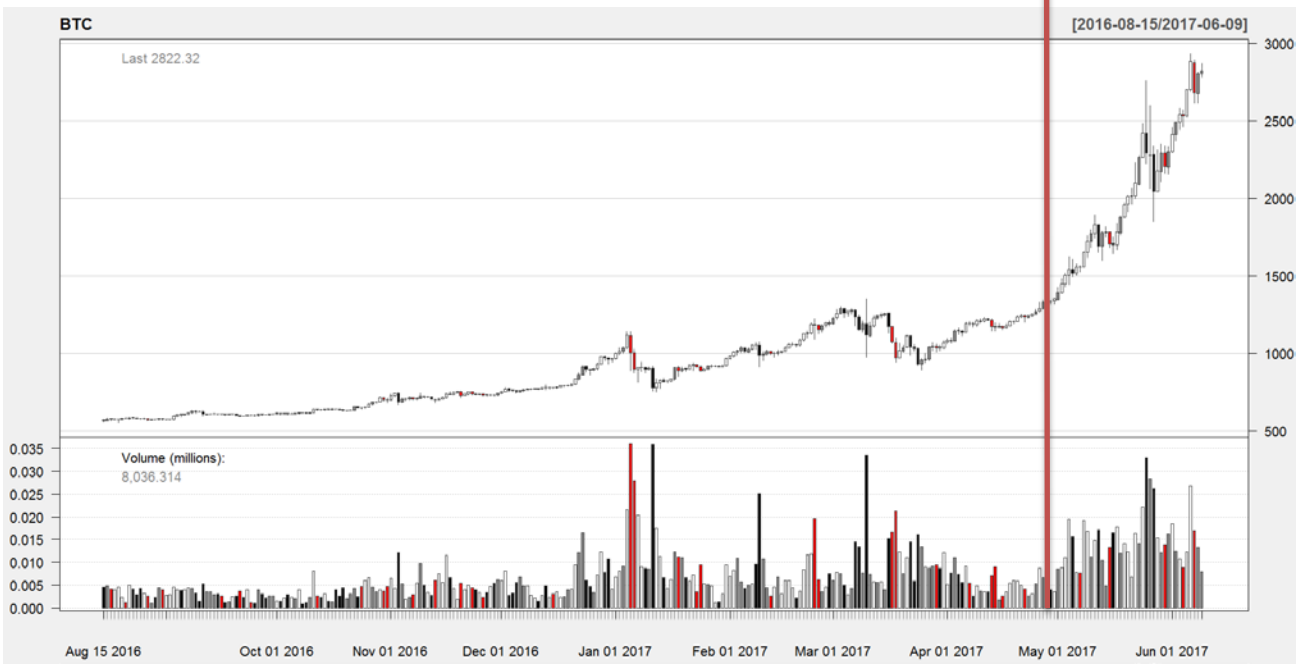
In broad terms, by integrating the Paysfer's blockchain, a bank will leverage the following benefits:

1. Cutting the middleman: the fees for transactions are now collected by the bank;
2. Increased customer value, satisfaction and, thus, retention;
3. Higher payment transparency, for both banks and customers;
4. Reduction in the number of reconciliation activities and investigations;
5. Reduced overheads and costs related to maintaining the idle IT infrastructure;
6. Reduced operational risk and possibly a significant reduction in capital requirements;
7. A superior platform for real time data analytics, enhanced data integrity and accuracy;
8. Reduced time and effort required for reconciliation, reduced costs of human errors;
9. Access to previously inaccessible data and, thus, superior analytical power;
10. Better KYC;
11. Superior scalability: the expansion will come at zero marginal cost.

CONCLUSION

We do not just promise you the improved ERP, we promise the revolution.

#BLOCKCHAIN #REVOLUTION



REFERENCES

[1] https://bitcoil.co.il/BitcoinX.pdf

[2] https://bitinfocharts.com/comparison/ethereum-transactionfees.html

[3] https://www-01.ibm.com/events/wwe/grp/grp308.nsf/vLookupPDFs/blockchain%20archtage/$file/blockchain%20archtage.pdf

[4] https://www.lykke.com/Whitepaper_LykkeExchange.pdf

[5] http://www.the-blockchain.com/docs/Smart%20Contracts%20-%2012%20Use%20Cases%20for%20Business%20and%20Beyond%20-%20Chamber%20of%20Digital%20Commerce.pdf

[6] HTTPS://BRAVENEWCOIN.COM/ASSETS/WHITEPAPERS/TETHER-WHITE-PAPER.PDF