



Embedding a Digital Wallet to Pay-with-a-Selfie, Defining the System Architecture as Blockchain Based

Perpetus Jacques Hougbo^{1(✉)}, Joel T. Hounsou¹,
Ernesto Damiani^{2,3}, Rasool Asal², Stelvio Cimato³, Fulvio Frati³,
and Chan Yeob Yeun²

¹ Institut de Mathematiques et de Sciences Physiques,
Avakpa, BP 613, Porto-Novo, Benin
jacques.hougbo@auriane-etudes.com,
joelhoun@gmail.com

² EBTIC-Khalifa University,

Abu Dhabi Campus, PO Box 127788, Abu Dhabi, UAE

{ernesto.damiani, rasool.asal, cyeun}@kustar.ac.ae

³ Università degli Studi di Milano, via Bramante 65, 26013 Crema, CR, Italy
{stelvio.cimato, fulvio.frati}@unimi.it

Abstract. The Pay-with-a-Group-Selfie (PGS) project, funded by the Melinda & Bill Gates Foundation, has developed a micro-payment system that supports everyday small transactions by extending the reach of, rather than substituting, existing payment frameworks. PGS is designed to work with devices with limited computational power and when connectivity is patchy or not always available. Once the concept of PGS has been accepted as demonstrated by the experimentation, we move to integrating elements and tools intended to ease federation or incorporation of the large spectrum of stakeholders. Embedding a digital wallet is one step in that vision. We analysed the system architecture that will be needed and the requirements drive us to opting for blockchain based architecture. We are then presenting the applicability of a blockchain as platform.

Keywords: Digital wallet · Mobile payment systems · Visual cryptography
Trust · Blockchain · Distributed ledger

1 Introduction

Nowadays, mobile devices are everywhere around the world, and many users have them in their pockets or in their purses instead of a regular wallet, and use their own devices to make payments or transfer money to each other. In the last 15 years, many apps (such as Google Wallet, or Samsung Pay) and technologies (like NFC) have become available supporting smartphone users in their payment needs.

In developing economies, the number of people with access to mobile phones is high and increasing from year to year, but the availability of the overall technological infrastructures and the usage habits are very different from those of the western world.

The availability of financial, health-care, agricultural, and educational services via mobile terminals is changing traditional relationships inside previously remote local communities, and it is bringing increasing economic opportunities. For example, many people living in rural areas of Africa and Asia have started using SMS services to find out daily prices of agricultural goods, to improve their bargaining position in local markets, and to select markets that offer the maximum income [1].

There are research works that focus on finding appropriate ways for illiterate people in rural areas to benefit from the development and expansion of the digital world [2]. The *Pay with a (Group) Selfie (PGS)* System is designed with the same ambition. In fact, the PGS [3] is an innovative payment system that uses a *group selfie* to collect all information items behind a purchase: the seller, the buyer, the service/product and the agreed price. The need for such system in rural areas where network coverage is patchy clearly moderates the enthusiasm created by the mobile boom earlier in the 2010 [4].

This paper is an attempt to present the research and development steps of the extension of the PGS by embedding a digital wallet in it. Its overall aim is to show the achievability of that extension and the technical viability of the proposed solution to be based on distributed ledger. Blockchain is a hot topic that keeps coming in every talk. Although many seem to just be “buzzword compliant with the latest and greatest”, blockchain is unquestionably among the hottest technologies in the enterprise security, data storage and file-sharing arenas. Blockchain is an emerging and strategic trend, Gartner¹ ranks it 6 out of 10 in its “*Top 10 Strategic Technology Trends for 2017*”. The interest of blockchain for this work resides in its properties of trust-free, tamper-proof and resilience. A blockchain system is:

- a peer-to-peer (P2P) distributed system that:
 - is used for storing a single sequence of events;
 - admits only appending new events;
 - enforces a fixed or user-defined protocol (contract) for appending;
 - does not require trusted parties;
- a distributed ledger with no single trusted/privileged guardian.

The paper is organized as follows: Sect. 2 presents a light introduction to blockchain. As blockchain is an important part in the design of the solution, it is worth presenting that introduction before gearing towards the design of the solution. Section 3 briefly recalls the status of PGS and its experimentation. Upon analysis of the need for digital wallet for PGS, Sect. 4 presents the state of the art in designing digital wallet. Section 5 elaborates on the system architecture, from the requirements analysis up to the system design. That section basically explains the rationale of relying on a blockchain platform to scaffold that system architecture. In that layout, the paper presents the initial steps of research and development: research solutions, requirements analysis, and system design. The further steps from functional specification up to the design of first prototype are out of the scope of this paper. Finally, Sect. 6 draws our conclusions.

¹ <https://www.gartner.com/doc/3471559/top-strategic-technology-trends>.

2 Blockchain

The innovation of blockchain is so breakthrough that currently there are numerous research and publications related to it. After that Nakamoto [5] has opened the path to crypto currencies, many institutions performed adaptation on them. Blockchain operates as a shared ledger recording the history of electronic business transactions that take place among participants in the P2P network. The participants then need a consensus mechanism, a collaborative process that they use to agree that a transaction is valid and to keep the ledger consistently synchronized. Participants agree to the transaction and validate it before it is permanently recorded in the ledger. The great value of the consensus mechanism is that it lowers the risk of fraudulent transactions, because tampering with transactions added to the ledger would have to occur across many places at the same time. Blockchain platforms use a range of consensus models [6]. From the original form of Proof of Work initiated by Bitcoin [5] and the Practical Byzantine Fault Tolerance algorithm (PBFT) implemented as modular consensus protocol to be plugged into Hyperledger [7, 8], other models have been proposed, such as Proof-of-Stake (PoS) and Proof-of-elapsed-Time (PoeT) and Proof-of-Activity (PoA).

One of the key properties of blockchain is information security, King [9] elaborates on how blockchain can help in combating a large spectrum of issues in the cyber threats landscape. The immutability of the blockchain records resides on the common shared ledger whose state is collectively maintained by the network in a decentralized fashion [10–13]. This is a consensus protocol [14] that ensures a common, unambiguous ordering of transactions and blocks and guarantees the integrity and consistency of the blockchain.

The World Economic Forum [14] elaborates on the governance challenges and multi-stakeholders cooperation opportunities that arise from the blockchain development. The same way as other authors did [15], Crosby et al. [16] insisted on the difference between bitcoin and a blockchain. The core technology of blockchain is abundantly explained [17, 18]. As a means to navigate through the multiple platforms and architectures offered, Xu et al. [19] have proposed a taxonomy to classify and compare blockchains and blockchain-based systems while Ellervee, Matulevicius, and Mayer [20] attempted to overcome lacks of standardization and uniform understanding. Because of the ubiquity of the phenomena of blockchain, the temptation is high to serve it almost any way. Xu et al., Ellervee, Matulevicius, and Mayer [19, 20] and most importantly Wüst and Gervais [21] offer frameworks to determine whether a blockchain is the appropriate technical solution.

3 Status of PGS

PGS development was carried out by three teams: one in charge of the client-side back end (that generates shares [22] at the seller's device), one in charge of the point-of-service back-end (reconstruction of the original selfie from the shares, validation of the purchase and interface with external payment systems), and one in charge of the user interface on the mobile devices.

3.1 Development Environment

Android was selected as the execution environment at the client side. According to Gartner² report for August 2016, as of Q2 2016, Android represents over 86% of market share and dominates the market together with iOS that counts for 13%. Also, it is by far the preferred choice in Africa and particularly in the Republic of Benin, where PGS has been experimented.

The PGS is currently designed in the form of four modules playing distinct roles. The Seller module triggers the process by taking the photo. Then, it compresses the photo, computes the shares using visual cryptography, and sends appropriate files to the Buyer module. The Buyer module receives the files and can later send them to the Broker one. Finally, the Broker module receives files from both the Seller and the Buyer and transfers them to the Bank module.

3.2 Experimentation

The experimentation phase has defined the following objectives:

- assessment of the viability of PGS design;
- functional testing and experimentation;
- user acceptance;
- checking of unexpected results.

It is a great satisfaction to notice that the concept of PGS has been quite widely accepted. Almost 80% of those who came across the two teams have clearly accepted the idea and many of them have also expressed the will to get more information about it.

Observations at the level of the software are also element of great satisfaction. The numerous challenges that the lab tests have help fix turn to be advantageous for the current version. From the captcha to the taking of the selfie, from transferring files from Seller to Buyer, and exchanging files with the Broker, the software modules performed as expected. The functionalities previously validated during of lab experimentation have been confirmed. The option of relying on Bluetooth as main channel of communication has been proved to be efficient.

One of the objectives of this experimentation was to observe unpredicted or unexpected results. This experimentation went through with almost no unpredicted or unexpected results, apart from the surprise about the type of telephones in use, to be discussed in the next section.

With the continuously increasing offer of Android applications due to the predominance of Android devices in Africa, this experimentation was expecting to confirm the omnipresence of Android devices in the suburb of Porto-Novo. Mainly the common belief was that Samsung (mostly fake Samsung) as a brand is dominating the market. It was really a surprise to see from the figures that the most common mobile phones in use are not the Samsung like as it was previously thought. Nobody from the

² <http://www.gartner.com/newsroom/id/3415117>.

team was expecting that it would be, but Nokia and ITEL are on the top, ahead of the Samsung only ranked as third.

The current design of the PGS software requires the user to be at a certain level of literacy. The experimentation has been run by people who can be perceived as smartphone savvy as they very easily master the entire process. Nevertheless, that full process requires several steps to complete:

- seven taps on buttons from the Seller:
 1. take the selfie;
 2. take the photo;
 3. confirm the photo;
 4. validate to continue at the end of encryption;
 5. send the share to the buyer;
 6. find the buyer device in the list;
 7. select the buyer's device in the list;
- data entry for item purchased and price from the Buyer
- four taps on buttons from the Buyer;
- four taps on buttons from the Broker;
- identification of the name of the receiver device in a list of available Bluetooth devices.

While some studies confirm importance of “ease of use” in mobile-payment services adoption [23], other studies demonstrate that “*ease of use had no significant effect on perceived usefulness and intention to use*” [24]. Nevertheless, we consider enhancing the current stage of ease of use of PGS. All these steps may need to be simplified for the PGS to come to be usable by people who are less smartphone savvy, as it may be expected in remote rural areas.

The design around the introduction of the Broker has proved to be efficient in terms of assuring the shares reach the bank asynchronously, without disrupting the system. Even though the current design relies on human action to trigger the file exchange, it is conceivable that this data transfer can be performed automatically whenever the broker's device comes close to a seller's or a buyer's device.

3.3 Conclusion of the Experimentation

The experimentation meets expectations: it showed that the PGS concept is accepted, the software performed well and the experimentation gave clues on the level of smartphone literacy level the software currently requires. The experimentation then shows path for improvement of the software in terms of need for more automation for devices to actively operate in machine to machine interface. Finally, the experimentation highlighted the need for a further study of the actual devices in use in the remote rural areas.

4 Digital Wallet for PGS, State of the Art of Digital Wallets

PGS completely integrates the prediction of transforming “*the mobile phone from a pure person-to-person communication device to an electronic wallet*” [25]. While the current version of PGS only simulates the transfer of money from one account to another, the product cannot be complete without a practical way of handling those transactions.

Simply put, a digital wallet is an application running on an electronic device that allows an individual to make electronic transactions. With the user’s payment information and credentials stored in it, the digital wallet, also known as an *e-wallet*, can be used with mobile payment systems that allow consumers to pay for purchases with a smartphone equipped with the proper application and a near-field-communication (NFC) microchip or with the capabilities of scanning a QR (Quick Response) at a Point-Of-Sale (POS) terminal. This is also referred as a contactless payment.

In a previous work, we have attempted to clarify the numerous terms and concepts that run around virtual currencies, e-money, digital wallets, crypto currencies [22]. This paper starts from the assumption that a digital wallet is not limited to crypto currencies, but it is supposed to adapt to store any kind of currency. PGS is designed with the clear intention to offer mobile payment for any kind of currency, including cryptocurrencies. But that vision will be implemented later. As for now, PGS offers its services on the base of the currency currently in use. In that framework, the digital wallet facilitates transactions by allowing users and merchants to transfer the currency among themselves, making sure that the right parties are credited and charged. In a research to identify the security challenges that mobile payment faces, [26] have depicted the layers pertaining to traditional card payment process and those added by mobile payment process. They then divide mobile payment systems into five categories: mobile payment at the point of sale, mobile payment as the point of sale, mobile payment platform, independent mobile payment system, and direct carrier billing.

Mobile Payment at the Point of Sale

In the category “mobile payment at the point of sale”, the customer uploads his traditional credit card data into the mobile device and then performs transactions by presenting her mobile device to the terminal at the merchant. All big players like Android Pay³, Apple Pay⁴, Microsoft Wallet⁵ and Samsung Pay⁶ offer this type of specific digital wallet⁷. Their main property is that they allow user to add credit cards to mobile device by taking a photo or entering account information. Users can do the same for loyalty cards, digital coupons and gifts card. When making a purchase at a

³ <https://www.android.com/pay/>.

⁴ <http://www.apple.com/apple-pay/>.

⁵ <https://www.microsoft.com/en-us/payments>.

⁶ <http://www.samsung.com/us/samsung-pay/>.

⁷ MasterCard’s new MasterPass program is an attempt to simplify further: it is a partnership with the major big players. That unifying approach may solve the issue of fragmentation in the marketplace. While consumers will operate one single account, merchants will access one single Application Programming Interface (API) to process transactions.

store, the user places the mobile device over the card reader, selects the appropriate card for payment and approves the payment via fingerprint or password.

Mobile Payment as the Point of Sale

In the case of “mobile payment as the point of sale”, the merchant transforms his mobile device into a point of sale by installing appropriate applications. This trend comes as a must for merchants as they are stressed to upgrade their POS terminals to better protect the customer’s financial information. Unfortunately, there is no single standard solution for the POS terminals. In the meantime, the option of deploying multiple solutions will be complex and expensive, and merchants should opt for installing a digital wallet on their mobile device. This allows them to stay away from a lot of hassle while benefiting from numerous advantages.

Mobile Payment Platform (Can Be “Independent Mobile Payment System”)

The mobile payment platform option integrates many features. By the mean of an application, the consumer uses her mobile device to access several payments services like the pure digital wallet, cardless (and contactless) ATM cash withdrawals or mobile airtime top up for instance. When the system is dedicated to a specific company, it is termed as “independent mobile payment system”.

Direct Carrier Billing

The category of direct carrier billing defines the cases where the cost of purchase is charged on the mobile subscriber’s account at the operator. This system does not require a credit or debit card.

Of special note is the case of the Peer-to-Peer (P2P) Payment systems championed these days by Venmo⁸. This type of payment enables consumers to send, receive, or request a payment to or from another person and are most frequently used for sharing the cost of a restaurant bill, sending a cash gift, or paying a babysitter. Such peer-to-peer payment is the one that suits most the digital wallet PGS will embed but unfortunately, the traditional design backs it on credit cards and bank accounts. For PGS to be able to implement that scheme, it has to find way around bank accounts.

One of the main drawbacks of these digital wallets described above is that it is not obvious how the user adds money (cash) to his wallet. The different cards have their direct link to the issuer bank, but moving cash directly to the wallet is mostly silenced, the operation must be from a credit card or a bank account.

Overall, digital wallet offers some tangible advantages directly appreciated by the consumer: transaction fees are lessened, more flexibility with the possibility to pay in a combination of credit, points and coupons, fast checkout at stores. The reduction of monetary and environmental costs of physical cards and receipts that can be digitized, and the improvement in security are two other significant advantages to be noted. It is therefore wise to predict that the development of digital wallets will only improve in the future and PGS must enter that development by embedding its own version of digital wallet.

⁸ <https://venmo.com/>.

5 System Architecture

This section aims at answering the question of what is needed for implementing a digital wallet, through the analysis of several types of requirements. Numerous frameworks are available to conduct such analysis, going from some light and almost linear steps like offered by [27] up to more complex roadmap similar to the Checklist-Oriented Requirements Analysis (CORA) framework presented by [28]. At this stage, we took the option to proceed by using a slightly adapted model of requirements analysis that is comprise of customer requirements, functional requirements, performance requirements, design requirements.

5.1 Customer Requirements

The customer requirements in this paragraph derive from the overall ambition of the PGS itself. Based on the objective of opening digital opportunities for people living in rural areas with no network coverage, PGS must embed a digital wallet that will cover all financial parts of transactions in such areas. One can think of the basic checkout of purchase of goods and services. But many other needs are to be covered as well, and remittances are one of them. Beyond the traditional conditions where the digital wallet uses to serve, there are some social and cultural functions in which it will get involved: rewards for artists, dowry, collection during the mass and any religious ceremony, assistance during grief, etc.

Rewards for Artists

It is quite common that any ceremony, baptism, initiation rites, bridal, wedding, or grief and funeral, turns to be an opportunity for performances of bands, artists, orchestras. Apart from the cachet the artist got for performing, they essentially receive rewards and gratuities during their show. The principle is the more people come and give money, the better. Giving many times a small amount of money, instead of donating a big amount at a time makes much more impact.

Dowry

The dowry of the bride is key element during the African bridal ceremony. It has to comply with numerous characteristics, one of them being the quality of banknotes; they have to be quite new. Whatever the amount being donated, the dowry is giving in bank notes. The digital wallet has to incorporate the function of making the dowry the same way as the rewards for artists, because the most important thing in those cases is the number of brand-new banknotes (big notes) that are displayed to the receiver.

Collection During the Mass, During any Religious Ceremony

Christianity has spread in several remote areas and numerous churches are active. Collection during the mass and other ceremonies holds many significations for all the faithful of the churches and thus is very important.

Assistance During Grief

Money plays an important role in terms of assistance to someone during grief. Even though the assistance is also common for happy events like baptism, in several places, it has reached a very specific extend when it comes to funerals. This is probably due to the fact that people have usually enough time to get prepared to happy events, whereas deaths often arrive unexpectedly. The social organization and the management of death

practically occupy a central place in traditions, thus the importance of financial assistance during mourning. Funerals in such places are events where people invest lot of money, but also a lot of energy and a lot of time.

It is not expected that the digital wallet of PGS performs the same for all the social and cultural events evoked above. While some of them perfectly suit the secrecy of transaction, others on the other hand are really rooted in the exposure and hype made around them. As people go around in all those places with their devices, the digital wallet embedded within the PGS can offer its services even though the core concept of taking a selfie for the PGS may not apply in some of the cases.

The digital wallet of PGS will mainly enter the scene when the transaction is coming to the settlement, when the money is supposed to move from one actor to the other. In terms of performance, this operation implies some data entry from the buyer. Voice recognition to enter the amount and/or image analysis from the original selfie can ease the process. The same can apply for the selection of the recipient of the money. Operating systems offer variety of such tools, and many have been ported to mobile [29–31]. Improvements in PGS will benefit from those tools that are available.

5.2 Functional Requirements

As PGS is mainly intended to unbanked customers, the digital wallet that it will embed cannot rely on any form of credit or debit card. A mechanism to replenish users' accounts is then compulsory. From the many mechanisms to top up digital wallet account that can be implemented, PGS will not research in integrating credit or debit cards. However, street corner shops or point of sales are a must, as well as peer to peer money transfers. In [32], we have stressed the role and importance of a specific intermediary in PGS: it is the broker. Being it point-of-service, “village chief”, street corner shops, point of sales or broker, this actor operates as a trusted third party whose main mission is to discourage users' malicious behaviour in the long term. It can then perform and adequately record replenishment actions of the digital wallet. The same actor is then one of the most important actors in the chain as we will describe it below in the next sections.

Basic operations on the digital wallet of PGS will include balance on account, payment of purchase, transfer, top up, and withdraw.

5.3 Performance Requirements

The main constraint in all cases is that PGS and its digital wallet should be operating for users who can be not computer savvy, even not-literate at all; it is then compulsory to minimize at the extreme any need of text typing. This brings the importance of ease of use and simplicity in a sense that the entire system is designed for people who are not able to juggle with complicated keyboards. Ease of use and simplicity are of paramount importance for PGS.

Another aspect in terms of performance is that all status information must be displayed at the device immediately at any change so that users are alerted about the final status of their account after the operation has been concluded. It is of paramount importance that that information will arrive in less than ten seconds. This performance

requirement is of great importance in an environment where there is no network coverage to perform any online transaction with any central authority.

5.4 Operational Constraints and Security Issues

One of the constraints imposed to a digital wallet for PGS is that it must comply with two of the main constraints of today's financial world: *Anti-Money Laundering* and *Know Your Customer*. It may not seem accurate to impose those constraints in areas where the expected amount of transactions are known to be very low but we have opted to fully integrate them from the beginning in order to be able to deploy the system with very few roadblocks in the future. These constraints impose then the PGS network to rely on a fully-authenticated network. The system must then incorporate enhanced security.

Beyond the challenge of authentication, the digital wallet that PGS will embed will also have to pay attention to the issue of double spending. *Stricto sensu*, double spending is the case to use the same quantity of money in two different purchases. In the digital wallet of PGS, that scenario has very probability to happen since all spending are requested to immediately reflect on the balance. And the accuracy of the balance is then more valuable. Nevertheless, even if the scenario of insufficient credit note can be programmatically controlled, the case of double spending needs specific solution. When analyzing innovations in payments systems, authors in [33] have presented the security issues as well as some solutions. This issue is of high importance in the case of PGS as the system will operate mainly out of the control of banks. Because the target customers are located in areas with scarcity of modern infrastructures and services like bank or mobile coverage, PGS is built without relying on any bank account or credit card. This implies that appropriate solution must be in place to prevent customer to spend more than they have in their balance. The solution is presented below in Sect. 5.7.

5.5 PGS Network

As described above, in the traditional way, a digital wallet is designed by merchant offering e-services to its customers. PGS is connected to a central authority, a bank where some specific actors plays their respective roles. In our case, the main actors are as follow:

- user/consumer: the one who owns the device and who uses it for transactions as payer or payee;
- street corner shop: this is the first point of replenishment of the digital wallet, the place where money is moved from cash unto the digital wallet.

The system might be able to operate fully working only with those two basic actors, but it is foreseen that banks and telco operators will join when they will appreciate the extend of the PGS and regulators⁹ will more than probably also enter in the game. The complete system will then resemble to the illustration in Fig. 1 - Illustration of the actors of PGS.

⁹ Regulator and supervisor of financial institutions, law enforcement, national security, etc.

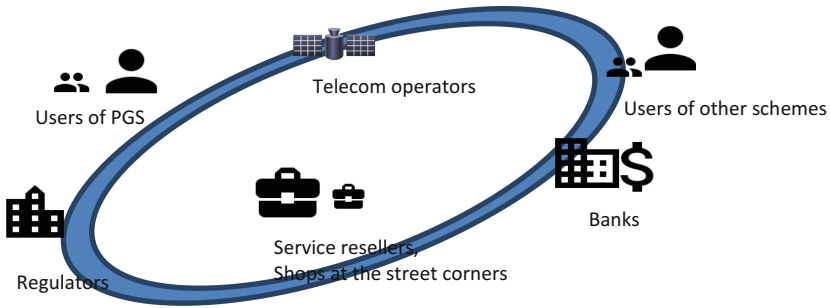





Fig. 1. Illustration of the actors of PGS

This illustration shows a network of participants transferring money among themselves, some of them being restricted to the level of observers: they are not active participants actually transferring money. The users of other schemes have been included in the network as they may also be willing to use their current scheme as payers or payees. The appropriate interface must be added in the future for them to be fully integrated, even if this implies solutions, to be analyzed separately, for interoperability. The properties of that network are:

- actors are numerous, but also clearly known and identified when boarding;
- actors are very demanding on security, and they only trust information their own device displays to them;
- actors have diverse read and write needs, regulators can only read, banks may only read, payers and payees will read and write to the specific transaction they are involved in;
- “always online” is not an option, while whenever internet connection is available it must be used;
- status storing is a must, the network will have the responsibility to provide accurate balance of any wallet;
- scalability is of high importance, because most transactions are performed offline, whenever network coverage is available, fast replications will take place;
- throughput should be pushed to “high”;
- network latency should be pushed to “fast”, ten seconds is a maximum of delay between the order to pay and the confirmation message displayed on the payee’s device.
- Linking the actors together is achievable by the mean of:
 - common [distributed] ledger with privacy service to determine who can see what;
 - consensus, who validate or approve transactions;
 - provenance, audit trail or complete record of who own what asset throughout its life cycle;
 - immutability, one block linked with the next block, impossible to tamper.

Every actor is doing its business (or is performing) by using a specific interface to manage its transactions and all the transactions are recorded by the core operating system that is the blockchain platform. The complete network is represented in Fig. 2 - Illustration of the full network. In that configuration, the network operates in three layers:

Symbols of the rings (layers)	Description of the rings
	Business network
	User interface [java-based module or android based module] to manage transactions handled either over message broker
	Core operating system: platform for decentralized applications where smart contracts get executed to process transaction messages

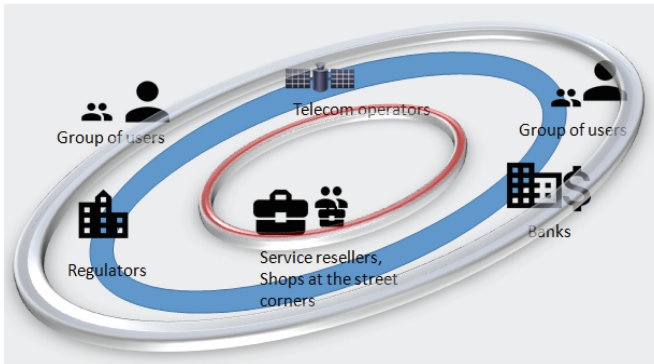


Fig. 2. Illustration of the full network

5.6 PGS Blockchain

The properties beforehand enumerated have paved the way for the blockchain-based digital wallet PGS will embed. Some of those properties are: number of actors, importance of trust-less network where permissions to read and write the data are distributed among all the users connected to the network and no user is given any special privileges, high need for security, storage of state, immutability of records. To be sure, we have also confronted this option with the flow chart designed by [21] to determine whether a blockchain is the appropriate technical solution. As shown in Fig. 3 - Flow chart to determine whether a blockchain is the appropriate technical solution, that framework confirms our option. As indicated by the blue arrows, the process led to the selection of **private permissioned blockchain**:

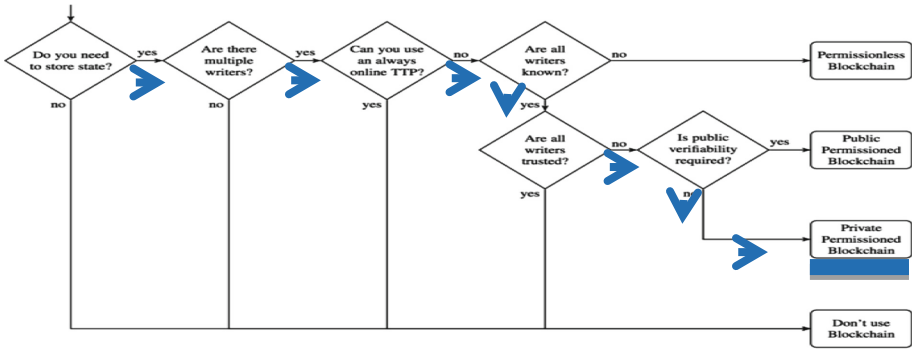


Fig. 3. Flow chart to determine whether a blockchain is the appropriate technical solution

- Do you need to store state? → Yes
- Are there multiple writers? → Yes
- Can you use an always online trusted third party (TTP)? → No
- Are all writers known? → Yes
- Are all writers trusted? → No
- Is public verifiability required? → No

5.7 Solutions to Specific Security Issues

The option of basing the system architecture on blockchain offers also a solution to the specific security issue of preventing double spending. As the system will then be decentralized, copies of the ledger are shared among participants, with appropriate consensus model in order to validate transactions. The next question is then about the implementation of the consensus.

It is obvious that we do not opt for the Proof of Work as pioneered by the Bitcoin blockchain: it requires a massive expenditure of energy. Alternatives include Tendermint¹⁰. Tendermint consists of two chief technical components: a blockchain consensus engine and a generic application interface. The consensus engine, called Tendermint Core, ensures that the same transactions are recorded on every machine in the same order. The application interface, called the Application Blockchain Interface (ABCI), enables the transactions to be processed in any programming language. For this issue of consensus, we are also considering the approach that Microsoft has taken in developing the Coco Framework¹¹. The approach consists in implementing a trusted network of physical nodes without requiring the actors that control those nodes to trust one another. In that configuration, it is then possible to control what code is run and guarantee the correctness of its output — thereby simplifying consensus and reducing duplicative validation. The network nodes operate distributed key value store with

¹⁰ <https://tendermint.com/>.

¹¹ <https://azure.microsoft.com/en-us/blog/announcing-microsoft-s-coco-framework-for-enterprise-blockchain-networks/>.

RAFT consensus [6]. Moreover, the Microsoft Coco Framework presents other advantages in term of scalability, confidentiality and consortium governance.

6 Conclusions and Future Work

We have presented the practical potential of the concept of embedding a digital wallet to PGS and basing that digital wallet on a private permissioned blockchain. The next steps start with the functional specification and cover software requirements documentation, modelling, first prototype, platform support and integration. There is still a long way to that integration, and we are confident the blockchain based solution will deliver promises in security and immutability; other design options will provide ease of use and simplicity.

Acknowledgement. This work has been partly funded by the Bill & Melinda Gates Foundations under the grant n. OPP1139403.

References

1. Kochi, E.: How The Future of Mobile Lies in the Developing World. TechCrunch (2012). <https://techcrunch.com/2012/05/27/mobile-developing-world/>
2. Duncombe, R., Boateng, R.: Mobile phones and financial services in developing countries: a review of concepts, methods, issues, evidence and future research directions. *Third World Q.* **30**(7), 1237–1258 (2009). <https://doi.org/10.1080/01436590903134882>
3. Cimato, S., Damiani, E., Frati, F., Hounsou, J.T., Tandjiékpon, J.: Paying with a selfie: a hybrid micro-payment framework based on visual cryptography. In: Glitho, R., Zennaro, M., Belqasmi, F., Agueh, M. (eds.) AFRICOMM 2015. LNICST, vol. 171, pp. 136–141. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-43696-8_15
4. Kizza, J.M.: Mobile money technology and the fast disappearing African digital divide. *Afr. J. Sci. Technol. Innov. Dev.* **5**(5), 373–378 (2013). <https://doi.org/10.1080/20421338.2013.829298>
5. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008). <https://bitcoin.org/bitcoin.pdf>
6. Baliga, A.: Understanding blockchain consensus models. Technical report, Persistent Systems Ltd. (2017). <https://www.persistent.com/wp-content/uploads/2018/02/wp-understanding-blockchain-consensus-models.pdf>
7. Castro, M., Liskov, B.: Practical Byzantine fault tolerance and proactive recovery. *ACM Trans. Comput. Syst. TOCS* **20**(4), 398–461 (2002). <https://doi.org/10.1145/571637.571640>
8. Gramoli, V.: From blockchain consensus back to Byzantine consensus. *Future Gener. Comput. Syst.* (2017). <https://doi.org/10.1016/j.future.2017.09.023>
9. King, C.: Ensuring secure enterprise blockchain networks: a look at IBM blockchain and LinuxONE. Pund-IT whitepaper (2017). <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSW03359USEN>
10. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: architecture, consensus, and future trends. In: Proceedings of 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564. (2017). <https://doi.org/10.1109/bigdatacongress.2017.85>

11. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., Wang, H.: Blockchain challenges and opportunities: a survey. *Int. J. Web Grid Serv.* **14**(4), 352–375 (2017). https://www.henrylab.net/pubs/ijwgs_blockchain_survey.pdf
12. Poon, J., Buterin, V.: Plasma: scalable autonomous smart contracts. White Paper (2017). <https://plasma.io/plasma.pdf>
13. Debus, J.: Consensus methods in blockchain systems. Frankfurt School Blockchain Center (2017). <https://medium.com/@fsblockchain/consensus-methods-in-blockchain-systems-d2eae18b99b7>
14. Ongaro, D., Ousterhout, J.K.: In search of an understandable consensus algorithm. In: Proceedings of the 2014 USENIX Conference, pp. 305–320 (2014). <https://web.stanford.edu/~ouster/cgi-bin/papers/raft-atc14>
15. Tapscott, D., Tapscott, A.: Realizing the potential of blockchain: a multistakeholder approach to the stewardship of blockchain and cryptocurrencies. World Economic Forum White Paper (2017). <https://www.weforum.org/whitepapers/realizing-the-potential-of-blockchain>
16. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V.: Blockchain technology: beyond bitcoin. *Appl. Innov. Rev.* **2**, 6–10 (2016). <https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf>
17. Beck, R., Czepluch, J.S., Lollike, N., Malone, S.: Blockchain-the gateway to trust-free cryptographic transactions. In: Proceedings of European Conference in Information Systems ECIS 2016, Research Paper 153 (2016). https://aisel.aisnet.org/ecis2016_rp/153
18. Gupta, M.: Blockchain For Dummies, IBM Limited Edition. Wiley, Hoboken (2017)
19. Xu, X., et al.: A taxonomy of blockchain-based systems for architecture design. In: Proceedings of 2017 IEEE International Conference on Software Architecture, pp. 243–252 (2017). <https://doi.org/10.1109/icsa.2017.33>
20. Ellervee, A., Matulevicius, R., Mayer, N.: A comprehensive reference model for blockchain-based distributed ledger technology. In: Proceedings of 2017 in ER Forum/Demos (2017). <http://ceur-ws.org/Vol-1979/paper-09.pdf>
21. Wüst, K., Gervais, A.: Do you need a Blockchain? IACR Cryptology ePrint Archive (2017). <https://eprint.iacr.org/2017/375.pdf>
22. Damiani, E., et al.: Porting the pay with a (group) selfie (PGS) payment system to crypto currency. In: Belqasmi, F., Harroud, H., Agueh, M., Dssouli, R., Kamoun, F. (eds.) AFRICATEK 2017. LNICST, vol. 206, pp. 159–168. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-67837-5_15
23. Keramati, A., Taeb, R., Larijani, A.M., Mojir, N.: A combinative model of behavioural and technical factors affecting ‘Mobile’-payment services adoption: an empirical study. *Serv. Ind. J.* **32**(9), 1489–1504 (2012). <https://doi.org/10.1080/02642069.2011.552716>
24. Koenig-Lewis, N., Marquet, M., Palmer, A., Zhao, A.L.: Enjoyment and social influence: predicting mobile payment adoption. *Serv. Ind. J.* **35**(10), 537–554 (2015). <https://doi.org/10.1080/02642069.2015.1043278>
25. Srivastava, L.: Mobile phones and the evolution of social behaviour. *Behav. Inf. Technol.* **24**(2), 111–129 (2005). <https://doi.org/10.1080/01449290512331321910>
26. Wang, Y., Hahn, C., Sutrave, K.: Mobile payment security, threats, and challenges. In: Proceedings of 2016 Second International Conference on Mobile and Secure Services, pp. 1–5 (2016). <https://doi.org/10.1109/mobisecserv.2016.7440226>
27. O’Driscoll, K.: The agile data modelling and design thinking approach to information system requirements analysis. *J. Decis. Syst.* **25**, 632–638 (2016). <https://doi.org/10.1080/12460125.2016.1189643>
28. Brace, W., Cheutet, V.: A framework to support requirements analysis in engineering design. *J. Eng. Des.* **23**(12), 876–904 (2012). <https://doi.org/10.1080/09544828.2011.636735>

29. Mittal, P., Singh, N.: Speech based command and control system for mobile phones: issues and challenges. In: Proceedings of 2016 Second International Conference on Computational Intelligence and Communication Technology, pp. 729–732 (2016). <https://doi.org/10.1109/cict.2016.150>
30. Kam, A.C.S., Sung, J.K.K., Lee, T., Wong, T.K.C., van Hasselt, A.: Improving mobile phone speech recognition by personalized amplification: application in people with normal hearing and mild-to-moderate hearing loss. *Ear Hear.* **38**(2), e85–e92 (2017). <https://doi.org/10.1097/aud.0000000000000371>
31. Fouzan, A.: Voice Recognition Anatomy, Processing, Uses and Application in C#. SSRN (2017). <https://doi.org/10.2139/ssrn.2968335>
32. Damiani, E., et al.: Pay-with-a-Selfie, a human-centred digital payment system. arXiv Prepr [arXiv:1706.07187](https://arxiv.org/abs/1706.07187) (2017). <https://arxiv.org/abs/1706.07187>
33. Ali, R., Barrdear, J., Clews, R., Southgate, J.: Innovations in payment technologies and the emergence of digital currencies. *Bank Engl. Q. Bull.* **54**(3), 262–275 (2014). <https://EconPapers.repec.org/RePEc:boe:qbullt:0147>