Embedding a Digital Wallet to Pay-with-a-Selfie, from Functional Requirements to Prototype

Perpetus Jacques Houngbo[1](✉), Joel T. Hounsou[1],
Ernesto Damiani[2,3], Rasool Asal[2], Stelvio Cimato[3], Fulvio Frati[3],
and Chan Yeob Yeun[2]

[1] Institut de Mathematiques et de Sciences Physiques, Avakpa, BP 613,
Porto-Novo, Benin
jacques.houngbo@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. In an effort to embed a digital wallet to the PGS, we analysed the system architecture that will be needed and the requirements drive us to opting for blockchain based architecture. We have presented the applicability of a blockchain as platform in a previous paper. The current paper is presenting the functional requirements, the platforms needed for the development as well as the prototypes of the major interfaces.

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

1 Introduction

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. It is worth to stress on the fact PGS is not intended to replace the current schemes that banks and mainly telecom operators have in place. PGS aims at completing them by going further and reaching those who were unreachable because of lack of network coverage.

Previous works have demonstrated its usage and the current version is evolving towards an accomplished product that will serve people living in remote areas where network coverage is patchy. In the meantime, efforts are being made to improve the way the PGS is expected to perform, that is the reason why it has been decide to equip

R. Zitouni and M. Agueh (Eds.): AFRICATEK 2018, LNICST 260, pp. 47–56, 2019.
https://doi.org/10.1007/978-3-030-05198-3_4

it with a digital wallet. Analyses conducted to that extend lead to the option of basing the architecture of the digital on a blockchain construction. In the wake of our works of improvement, we have presented the applicability of the blockchain based solution. This paper aims at elaborating on the functional requirements and the prototyping of the major interfaces.

The paper is organized as follows: starting by the summary of the requirements for the system architecture, Sect. 2 gives an extensive presentation of the functional requirements. Then, Sect. 3 goes further with the platforms and Sect. 4 is devoted to the prototyping the main interfaces. Finally, Sect. 5 gives our conclusions.

2 Functional Specification

2.1 Summary of Requirements

Regarding the system architecture we have defined the requirements of the PGS digital wallet as follows:

- basic operations: balance on account, payment of purchase, transfer, top up, and withdraw
- purchase of goods and services is the main functionality, but the wallet must also serve for:
  - remittances;
  - social and cultural functions: rewards for artists, dowry, collection during the mass, during any religious ceremony, assistance during grief;
- pivotal role of the "village chief", street corner shops, point of sales (POS) or broker is stressed on;
- performances measured in term of:
  - ease of use and simplicity: the system must be designed for people who are not able to juggle with complicated keyboards;
  - immediate confirmation of transactions, in matters of seconds, in less than ten seconds;
- security aspects:
  - fully-authenticated network;
  - prevent double spending;
  - *Anti-Money Laundering* and *Know Your Customer* issues are to be integrated from design.

All the requirements and properties lead to the choice of implementing the system on a private permissioned blockchain.

Figure 1 presents three groups of use cases for the PGS users, the POS and the institutions.

2.2 Numbers

PGS per se is devoted to serve large group of populations, all the population in rural and remote area with no network coverage. Its digital wallet will then serve that

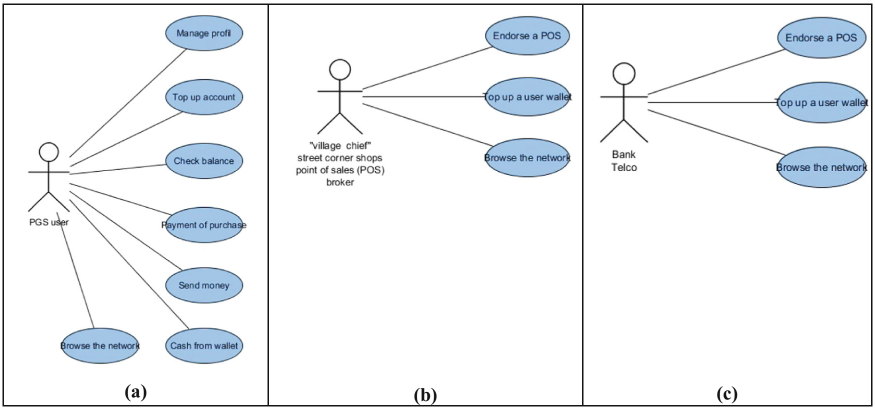


Fig. 1. PGS user use cases (a), POS use cases (b), and institutions use cases (c).

population. It has to be noted that actually every single smartphone user is targeted as they can transfer money to PGS users and vice versa.

The vision is also to plan for big players like banks and telecom operators to join the PGS network. The regulatory authorities may also come in, but they will only be granted read privileges on the ledger. The final number of user is then very large, with groups of specific needs, as shown in the illustration in Fig. 2. That illustration is showing a unit of "System administration and back end". Such unit can be surprising in a decentralized environment.

We estimate that is compulsory at least during the inception phase where there is a need for intense housekeeping at blockchain nodes in term of installing, supporting, and maintaining servers or other computer systems, and planning for and responding to service outages and other problems that may occur. Software maintenance will also be part of their responsibilities.

2.3 Existing System

Currently, in the targeted areas, the payment system is traditionally cash-based. PGS is introducing a new system, still anchored on customs that are already spreading in those areas: the use of smartphone to do selfies. Furthermore, one pivotal actor is the broker, the ambulant banker who is already trusted in the area collector of savings. The broker was introduced [1] to act as a store-and-forward transport layer (where trust in the broker plays the role of security controls [2]), pushing selfies between PGS users on one side and multiple Banks on the other side. The broker will maintain his role with PGS, and this role may eventually be strengthened by the new layer of blockchain that will guarantee the log of all savings collected and their final destinations.

2.4 Uses Case: Direct Purchase

Only one use case (depicted in Fig. 3) is presented here due to its importance in terms of need for immediate result in a peer-to-peer operation. Indeed, when buying an item

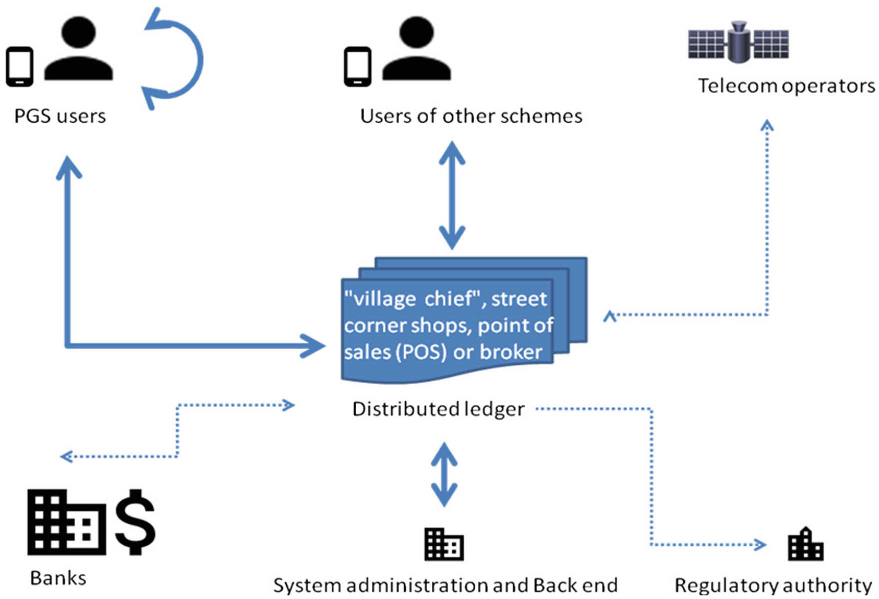

PGS users
Users of other schemes
Telecom operators
"village chief", street corner shops, point of sales (POS) or broker
Distributed ledger
Banks
System administration and Back end
Regulatory authority

Fig. 2. Overview of the users

in a local market for instance, buyer and seller are facing each other. When the deal is concluded, the merchandise and money are synchronously exchanged. This is where the peer-to-peer payment enters the scene:

- buyer and seller agree on the price;
- buyer launches her PGS on her device and logs in;
- seller launches her PGS on her device and logs in;
- buyer enters amount to pay;
- PGS on the buyer's device checks the balance and alert buyer in case of insufficient credit note;
- PGS offers a list of sellers;
- buyer selects the seller who will receive the money;
- PGS on the buyer's side sends a checking message to seller;
- seller confirms the checking message;
- buyer sends the money;
- seller confirms reception of the money;
- PGS on the seller's side prepares a transaction record to be sent later to the blockchain when a broker will pass by;
- PGS notifies buyer that seller has acknowledged receipt of money;
- PGS on the buyer's side prepares a transaction record to be sent later to the blockchain when a broker will pass by.

All these actions have been done between the two actors using only their own devices. The transaction will be saved later to the blockchain after the broker has passed by and collected the appropriate records to be transferred to the network nodes.

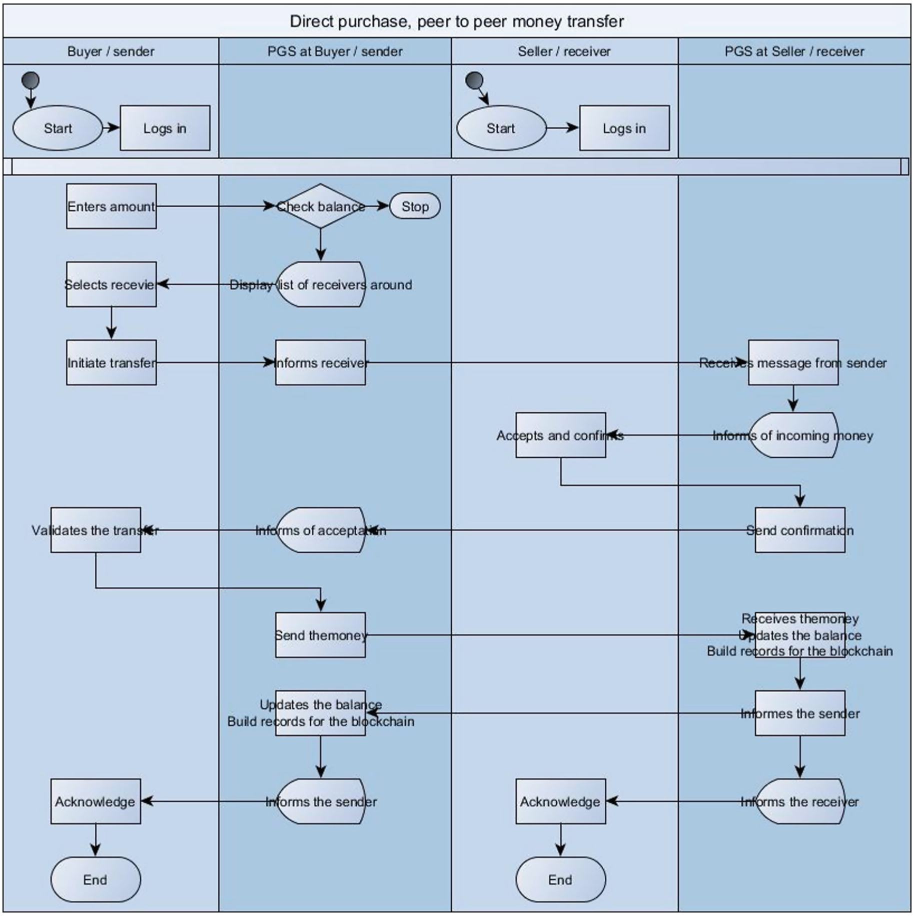


Fig. 3. Activity of direct purchase, peer-to-peer money transfer

2.5 Administration Functions - Support and Maintenance

As mentioned earlier, the system includes the role of system administration. This role is purely devoted to handling technical issues: assistance to network nodes and to final users in setting up their application. The role is totally separated from any interference in the money flowing from one actor to another. The control of all access must clearly prevent any kind of manipulation.

The business model to cover all financial issues of the system is deliberated ignored at this point and sent out of the scope of this paper. It has to be pointed out that the broker and the street corner shops are the most natural point of transfer from cash to the digital wallet. Such services to PGS users are activities that infer risks and costs. When it will be analysed, the business model will also estimate all costs related to the management of the financial transactions and to the service cost.

2.6 Security

Security considerations are an important part of any project so it is for this digital wallet for PGS. This project needs strong security measures, a range (technical and organisational) of methods and procedures implemented to make sure that all transactions are authentic and recorded, and that no record can be tampered with.

In order to prevent frauds, we designed the digital wallet to only manage genuine transactions on accounts in good standing. This means ensuring that the transaction is ordered only by a valid party, and that the party cannot subsequently deny having placed that order. All instructions shall be recorded immutably. The security measures should also include techniques to implement user identification and authentication, integrity of transactions, origin authentication, and non-repudiation of origin. The system must incorporate:

- methodologies to identify all users (devices of users, systems of corporate and institutions, etc.);
- means to verify that the user behind each device is who he/she pretends to be;
- methodologies to allow the user to perform actions he/she has privileges for.

As the system is designed mainly for non-literate people, implementation of a Pretty Good Privacy (PGP) or Public Key Infrastructure (PKI) as security method is not a practical solution and password based system are to be avoided. We have then to find ways to implement some light biometrics based tools: face recognition, voice recognition, fingerprint, etc. There are many researches on biometric [3, 4] that have explored its usability and improvement. Nowadays biometric for consumers is deployed on many devices; in [5], authors have surveyed its usage on iPhone and Android and they came to the conclusion that fingerprint is the most preferred method by users. On the other hand, it has to be noted that fingerprint is quite widely used in microfinance. Furthermore, in [6] authors noted down that deploying the biometric capture technology is expensive and creates a significant barrier to customer enrolment while not provides substantial additional security. In the meantime, some other works [7–9] salute the usage of fingerprint as best practice.

It has then been decided that the security analysis in PGS digital wallet will explore both the “Trusted face” feature of Android and fingerprint at the level of actors interacting with their mobile devices, while all other actors like corporate and institutions, as well as street corner shops and/or brokers, will have “stronger” and more appropriate security management built on a Public Key Infrastructure (PKI). PKI [10] is a system that is comprised of Certification Authority and a Registration Authority; it is managed by the mean of a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

3 Platforms

The concept of blockchain itself is still in rapid pace development and so is it for entire landscape for developing, testing, and deploying blockchain applications: it is evolving rapidly. Many architectures are available and we opted for Hyperledger. Hyperledger, one of the biggest blockchain standardization efforts, is an open-source initiative overseen by the Linux Foundation. Hyperledger's members are tech companies (Cisco, IBM, Intel, Red Hat, Samsung, VMware, etc.), banks and financial institutions (JPMorgan, Wells Fargo, etc.), blockchain start-ups, global manufacturers and device makers, etc. Hyperledger Fabric is a blockchain framework that offer implementation of permissioned private on a modular and extendable architecture [11–13].

In PGS, We plan to exploit a Hyperledger Composer Business Network Archive (BNA) file for the assets trade and deploying it on a Hyperledger Fabric. Modelling that network, we will define:

- Participants, as the actors who are the PGS users, the users of other schemes, the corporate, the institutions; they will all go through a process of registration and they will then acquire an identity (an enrolment certificate);
- Assets, as the money that move from one participant to another;
- Transactions, as the state change mechanism of the Network.

The platforms to develop this digital wallet for PGS will be comprised of at least three layers: the server, the abstraction layer composed of the applications, the user interfaces. The elements of the platforms are represented in Fig. 4.

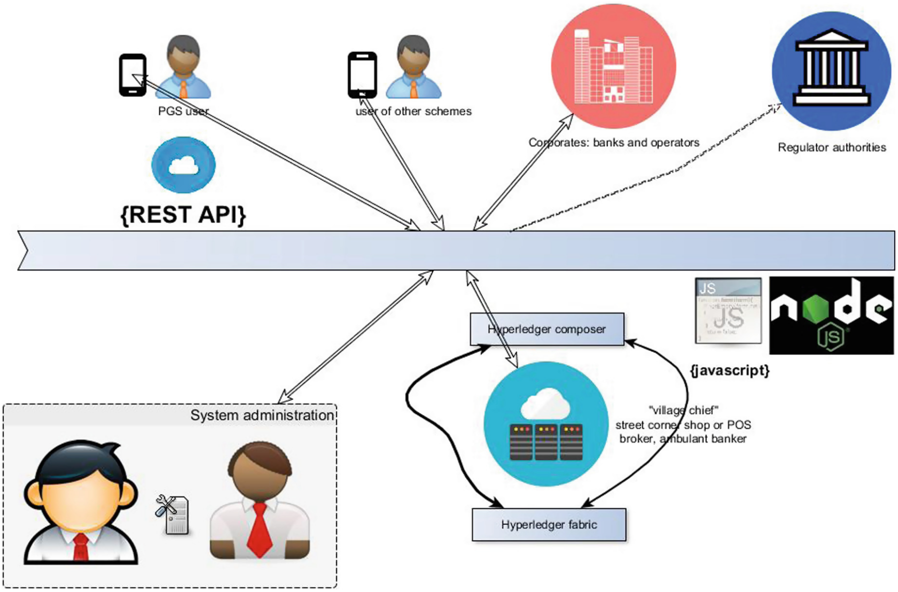


Fig. 4. Hyperledger platform actors

The server

The server must manage network and hence the communications between the client applications and the blockchain itself. The communications relate to the assets, their status, their ownership, and their movements from one participant to another. The server will be implemented in Node.js, an asynchronous event driven JavaScript runtime, designed to build scalable network applications. That server will be part of the Hyperledger Fabric components to be set up.

The abstraction layer

The abstraction layer is the framework where the interactions will take place among the participants, i.e. the network nodes, the assets, based on the transaction logic that drive state changes on the distributed ledger. This is where Hyperledger Composer comes in. It models the business network, containing the assets and the transactions related to them.

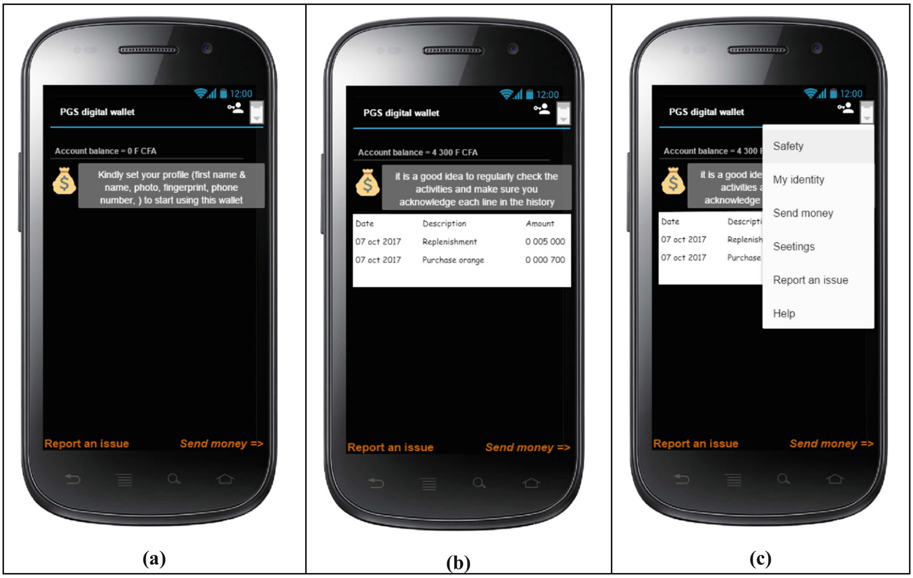
The user interfaces

The user interfaces are for all participants to the business network to interact with the distributed ledger. The user interfaces are typically developed using Javascript. As we have the large part of participants using their android device, we will develop the needed part of interfaces using REST API for Android.

4 Interfaces

The PGS user interfaces will provide means for all users to:

- manage their identities;
- check balance;



PGS digital wallet

Account balance = 0 F CFA

Kindly set your profile (first name & name, photo, fingerprint, phone number,) to start using this wallet

(a)

PGS digital wallet

Account balance = 4 300 F CFA

it is a good idea to regularly check the activities and make sure you acknowledge each line in the history

Date	Description	Amount
07 oct 2017	Replenishment	0 005 000
07 oct 2017	Purchase orange	0 000 700

(b)

PGS digital wallet

Account balance = 4 300 F

(c)

Fig. 5. Initial or empty wallet (a), wallet with some activities (b), and wallet with open menu (c)

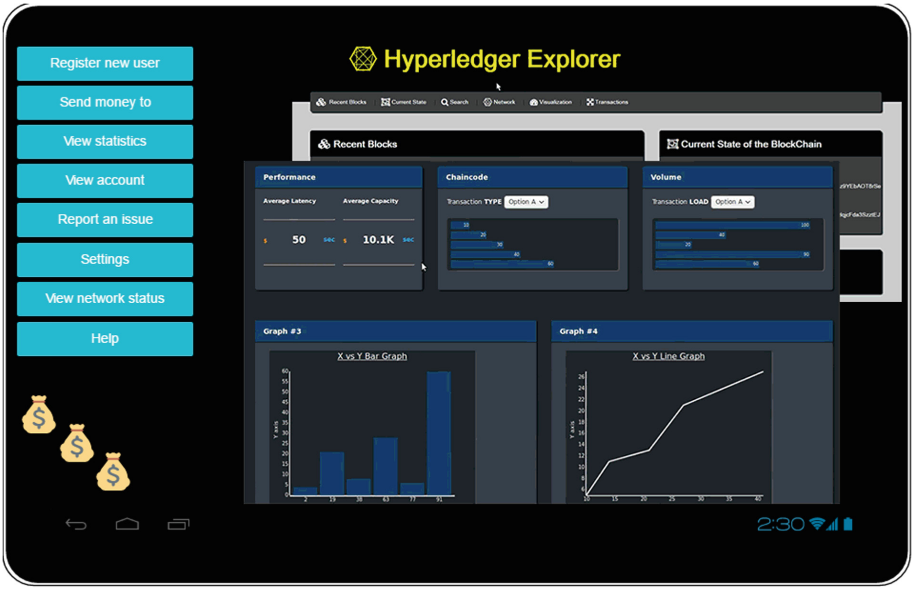


Fig. 6. Tablet at point of service

- send money;
- notify events;
- manage history of transactions.

In the backend, the user interfaces will record all transactions and send them to the blockchain whenever online or in reach of brokers' devices. As showed by the statistics Gartner presented in May 2017, the most popular OS in smartphones[1] is still Android with 86.1%, followed by iOS with 13.7%. As it has been done for the PGS itself, the digital wallet will be developed on Android. Figure 5 shows the three main presentation of the user interface: with an empty wallet, one with some activities recorded, and an interface where the menu is played.

Subsequent interfaces will be needed for every action and for the notifications of events. The elaboration of these detailed interfaces is deferred to the design specification stage. Nevertheless, one more important interface is designed above, the one that is used by actors operating in their capacities of "village chief", street corner shop or POS, or broker/ambulant banker (Fig. 6).

5 Conclusions and Future Work

With the intention to pursue the accomplishment of the Pay-with-a-Group-Selfie (PGS), the digital wallet to embed to it is now evolving a blockchain project. We are currently at an advanced phase of the research and development. The next steps will

[1] http://www.gartner.com/newsroom/id/3725117.

then mostly devoted to the coding, testing and improving. This will call on setting up an appropriate network to host the private permissioned blockchain that we have opted for.

Acknowledgement. This work has been partly funded by the Bill & Melinda Gates Foundations under the grant no. OPP1139403.

References

1. 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
2. Zarki, M.E., Mehrotra, S., Tsudik, G., Venkatasubramanian, N.: Security issues in a future vehicular network. In: Proceedings of European Wireless (EW02) (2002). https://www.ics.uci.edu/~dsm/papers/2002/sec001.pdf
3. Devi, O.R., Reddy, L., Prasad, E.: Face recognition using fused spatial patterns. Int. J. Adv. Trends Comput. Sci. Eng. **4**(2), 15–21 (2015)
4. Medran, J., Musa1, A., Gonzalez, V., Shadaram, M.: Dual stage optical label switch architecture to create an all optical network based WDM and optical CDMA. In: Proceedings of 2006 IEEE Region 5 Conference, pp. 190–195 (2006). https://doi.org/10.1109/tpsd.2006.5507431
5. Bhagavatula, C., Ur, B., Iacovino, K., Kywe, S.M., Cranor, L.F., Savvides, M.: Biometric authentication on iphone and android: usability, perceptions, and influences on adoption. In: Proceedings of Workshop on Usable Security and Privacy USEC 2015, pp. 1–10 (2015)
6. Muhammad, Z., Rahman, H.U., Makki, B.I., Jehangir, M., Rehman, S.: Branchless banking in pakistan: opportunities and challenges. NFC-IEFR J. Eng. Sci. Res (2017). https://doi.org/10.24081/nijesr.2017.1.0014
7. Buang, A., Suryandari, R.Y., Ahmad, H., Bakar, K.A., Jusoh, H.: Women and liveability – best practices of empowerment from Mozambique. Malays. J. Soc. Space **10**(7), 70–80 (2014). http://ejournal.ukm.my/gmjss/article/view/18992/6091
8. Boateng, F.G., Nortey, S., Asamanin Barnie, J., Dwumah, P., Acheampong, M., Ackom-Sampene, E.: Collapsing microfinance institutions in Ghana: an account of how four expanded and imploded in the Ashanti region. Int. J. Afr. Dev. **3**(2), 37–62 (2016)
9. Maharjan, M., Shakya, S.: Technology acceptance model: understanding local government employees intention in social cash transfer through branchless banking in Nepal. Int. J. Comput. Sci. Mob. Comput. **4**(12), 203–210 (2015)
10. Internet X.509 Public Key Infrastructure Certificate Management Protocols. RFC410 (2005). https://tools.ietf.org/html/rfc4210
11. Li, W., Sforzin, A., Fedorov, S., Karame,. G.O.: Towards scalable and private industrial blockchains. In: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts BCC17, pp. 9–14 (2017). https://doi.org/10.1145/3055518.3055531
12. Cachin, C.: Architecture of the Hyperledger Blockchain Fabric. IBM Research (2016). https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf
13. Valenta, M., Sandner, P.: Comparison of Ethereum, Hyperledger Fabric and Corda. Medium (2017). https://medium.com/@philippsandner/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6