Porting the Pay with a (Group) Selfie (PGS) Payment System to Crypto Currency

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

[1] EBTIC-Khalifa University, UAE Campus, PO Box 127788, Abu Dhabi, UAE
{ernesto.damiani,rasool.asal,dina.shehada,cyeun}@kustar.ac.ae
[2] Dipartimento di Informatica, Università degli Studi di Milano,
via Bramante 65, 26013 Crema, CR, Italy
{stelvio.cimato,fulvio.frati}@unimi.it
[3] Institut de Mathematique et Science Physique Quartier Avakpa, BP 613, Porto-Novo, Bénin
jacques.houngbo@auriane-etudes.com, joelhoun@gmail.com

Abstract. *Pay with a (Group) Selfie* (PGS) is a novel payment system developed at Khalifa University in the UAE, and currently under test at the *Institut de Mathématiques et Science Physique* (IMSP) in Benin. The PGS system uses a *group selfie* to gather all information items needed to encode a purchase: the seller, the buyer, the service/product and the agreed price. Using Visual Cryptography (VC), the photo is then "digitally ripped" into two shares, one for the buyer and one for the seller. In the current version of PGS, these shares are eventually and independently sent to a Bank that cooperates to offer the digital payment service to population living in rural areas. When the purchases of a buyer at a given seller pass a pre-set threshold, the Bank executes a traditional fund transfer between the two. This way, PGS spreads the Bank's transfer fee over multiple purchases, decreasing the financial cost of each purchase. This paper discusses the challenges of *transparently coupling* the PGS payment system with digital wallets holding a crypto currency, bringing the financial cost of each purchase to zero.

Keywords: Payment metaphors, mobile payment systems · Visual Cryptography · Trust · Crypto currency

1 Introduction

Pay with a (Group) Selfie (PGS) [1] 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. Using Visual Cryptography (VC), the selfie is "digitally ripped" into two shares, one transmitted to the buyer's phone and the other kept on the seller's one. In the current version of PGS, these shares are eventually and independently sent to a Bank who accepted to cooperate to offer the PGS service to population living in rural areas. When the purchases of a buyer at a given seller's shop pass a pre-set

F. Belqasmi et al. (Eds.): AFRICATEK 2017, LNICST 206, pp. 159–168, 2018.
https://doi.org/10.1007/978-3-319-67837-5_15

threshold, the bank executes a traditional fund transfer transaction[1]. While PGS provides an entirely new metaphor for delayed payments (the ripped banknote), its innovation in the back-end consists in splitting the cost of a traditional fund transfer across multiple purchases. In this paper, we discuss backing our PGS payment system with *digital wallets* integrating a crypto currency. We believe that this idea can overcome a number of societal challenges connected with payments in emerging economies. However, here we shall focus on technical challenges only. We start by describing the PGS payment system in Sect. 2. Section 3 will discuss the rationale for putting a virtual currency behind PGS while Sect. 4 will offer a concise overview on digital wallets and crypto-currencies. Among available crypto currencies, Sect. 5 will discuss our choice for the implementation of the next version of the PGS payment system. In Sect. 6 we will discuss the different challenges and ways to overcome them. Finally, Sect. 7 will present the way forward.

2 Pay with a (Group) Selfie Payment System

PGS is a payment system that provides a *virtually costless micro-payment* system suitable for open-air markets in emerging economies. It is based on a powerful, easy-to-understand metaphor and does not require "always on" connectivity: PGS works well in environments where network connectivity is patchy. PGS is based on three key design principles: (*i*) embedding in a simple digital object (a selfie) all information about a purchase: the actors (buyer and seller), the product or service being sold, and the price agreed upon between the parties; (*ii*) producing secure shares of the original selfie, so that each single share has no value, but their combination using the human visual system can reconstruct the original image and provide proof of the purchase; (*iii*) integrating the validation of the selfie with mobile money transfer facilities, or via innovative systems exploiting virtual currencies. In its original design, PGS was *not* intended to replace existing mobile payment infrastructures, but to extend their reach wherever data connections are not guaranteed due to patchy network coverage, cost concerns or usage habits. PGS distributes the cost of a financial transaction (the fund transfer) across arbitrarily many selfie-encoded purchases. The idea of using a selfie as proof of purchase is inspired to the traditional way in which business is conducted in open-air markets. The human visual system has been used for countless years to establish the context of each sale: the purchaser, the supplier, the purchased goods or services, the price to be paid, as well as the time and location of the purchase. PGS's proof of purchase is self-validating, just like a banknote, and like a banknote ripped in two it can be held jointly by the two parties until the money transfer can be finalized. Behind the scenes, PGS uses Visual Cryptography (VC) to split the selfie, generating two random-looking shares. VC provides unconditional security [2]: owning a single share gives no possibility to reconstruct the original image, and tampering with it makes the reconstruction impossible. PGS fully supports the metaphor of putting back together the two parts of a ripped banknote. Indeed, the reconstruction of the selfie could be even performed without a

[1] The Bank alerts the sellers if the buyer's funds become insufficient for the eventual transfer. Each seller can decide whether to block or allow further purchases.

computer, simply by stacking the shares printed on two transparencies. In the current implementation, reconstruction is performed by a desktop application that stacks the shares provided by the parties, using the mobile applications (Fig. 1), to validate the transaction.

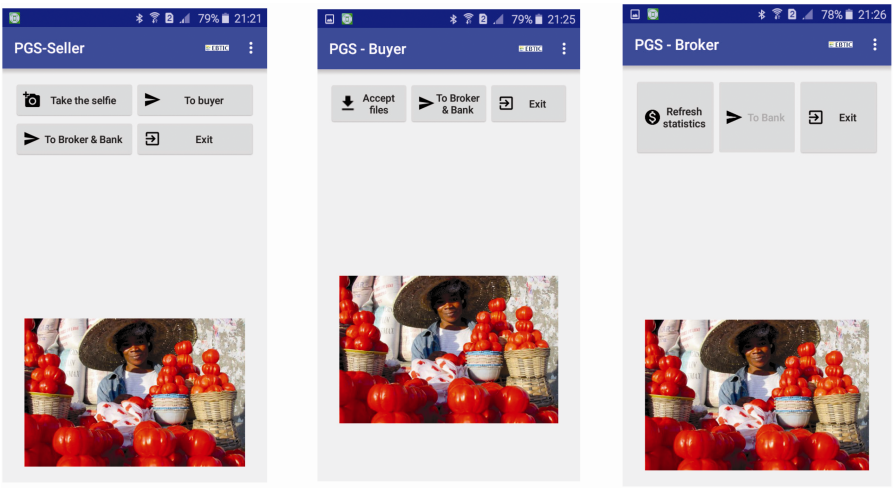

Fig. 1. The interfaces of the three components of PGS. The pictures of the modules are identical on purpose to let users feel the same environment.

Another important aspect of PGS design is that no "always on" assumption is made: when no network coverage is available, money exchange is deferred until shares have been independently and securely delivered to a payment service provider, who will stack them and validate the transaction.

3 Rationale for a Virtual Currency Behind PGS

As mentioned above, PGS original design relied on (*i*) a single Bank to accept selfie shares as proofs of the buyer's obligation to pay the seller, and (*ii*) mobile telco operators' network services to deliver the shares to the Bank. This design is distinct from (though related to) the design of so-called *mobile money* systems, which are bound to a specific mobile telecommunication operator who plays also the role of the Bank. All mobile money users are required to hold accounts with the same operator to be able to transfer their mobile money (often, in the form of minutes of conversation) between each other. In the case of PGS, any mobile telco provider can be used to deliver the selfie shares to the Bank, but all PGS users (sellers and buyers alike) are supposed to hold accounts at the same Bank, as it is the latter that executes fund transfer[2]. A first attempt to alleviate this constraint is adding a "Broker" module. The PGS design will then operate as

[2] Of course, inter-bank arrangements could be made to support account holders from other banks. This would however increase the financial cost of the transactions.

described in Fig. 2. This solution relies on the trusted Broker to act as a store-and-forward transport layer (where trust in the broker plays the role of security controls [3]), pushing selfies between PGS users on one side and multiple Banks on the other side.

The PGS implementation being tested in Benin is based on this design [1]. In this paper, we discuss how to dispense with the Banks entirely, by integrating PGS and *digital currencies* in a fully transparent way. Users will see cash transfers, possibly unaware that a virtual currency is used behind the scenes. This way, PGS will get close to catching the so-called "*mobile money unicorn*": an electronic purchase whose cost is the communication one only. The coming section aims at presenting a summary of the concepts related to virtual currency and it will then open way to the selection of one of them for implementation.

4 Crypto Currencies and Digital Wallets

Virtual currencies, e-money, digital wallets, crypto currencies, payment technology, distributed ledger and block chain are terms that often popup in conversations, many people using them loosely. This section will present some clarifications so that the rest of this work can accurately use these terms when and where needed. *Electronic money*, or *e-money*, is a fund balance expressed in a traditional currency but recorded electronically, e.g. on a stored-value pre-paid card. To generate e-money, the real currency (e.g., in form of cash) is handed over to banks and financial institutions who, in turn, load the corresponding e-money balance into microprocessors embedded in the cards. *Digital currency* has been proposed as an Internet-based form of currency. Any amount denominated in a digital currency is called *digital money*. The same way traditional physical money, such as banknotes and coins, is used in transactions, digital money can be used for digital transactions. Digital currency has its own generation and distribution mechanisms that prevent double-spending and inflation of digital money. Financial institutions worldwide tend to stress on the difference between digital currency/money and e-money. In 2012, the European Central Bank (ECB) has defined digital currency as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community" [4]. Digital currency is a digital representation of value. Even though it functions as a medium of exchange, as a unit of account and as a store of value, it does not have legal tender status [5]. The Committee on Payments and Market Infrastructures (CPMI) of the Bank for International Settlements (BIS), a financial entity cooperatively owned by the world's Central Banks, asked a working group to draft a report on digital currencies. That report, published in November 2015, defines digital currency as an *asset represented in digital form and having some monetary characteristics* [6, p. 5]. Unlike today's traditional currencies, which are managed by Central Banks[3], a digital currency can be centralized or decentralized. When centralized, the virtual currency has a single administrating authority that controls the system. That authority issues the currency, establishes the rules for its use, maintains a central registry of ownership,

[3] This was however not always the case. Some traditional currencies managed by multiple authorities have survived until the late 1800 s.

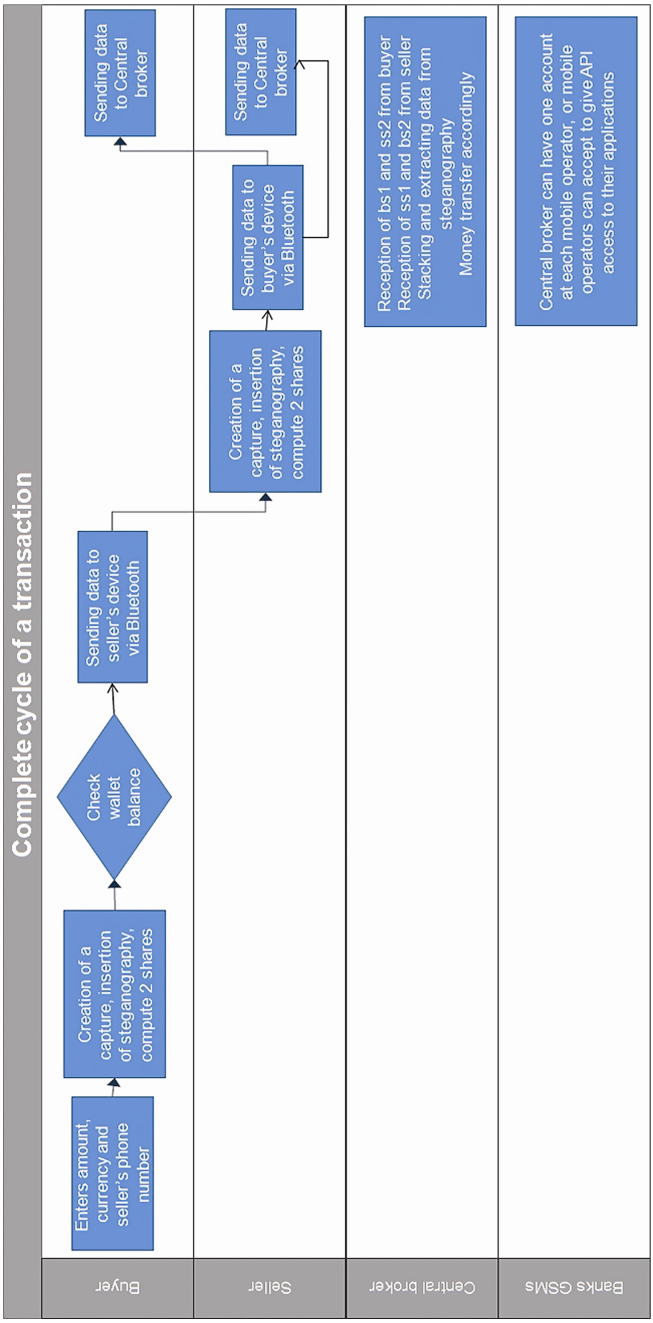

Fig. 2. PGS transaction cycle including a Central Broker, where bs1: share 1 created at buyer's side, ss2 share 2 created at buyer's side, ss1: share 1 created at seller's side

maintains a central payment ledger, and has authority to redeem the currency (i.e., withdraw it from circulation). A decentralized virtual currency is distributed, open-source and peer-to-peer. It has no central administrating authority, and no central monitoring or oversight. *Crypto-currencies* are good examples of decentralized digital currencies. A cryptocurrency is a digital currency that relies on cryptography to *(i)* to regulate the generation of currency units *(ii)* verify the transfer of funds, and *(iii)* secure payment transactions. The first fully functional cryptocurrency is called Bitcoin. It was initially proposed by an unknown group or individual writing under the pseudonym of Satoshi Nakamoto [7]. A virtual- (or crypto)-currency wallet is a system (again, encryption-based) for holding, storing and transferring virtual currency units. A *wallet provider* is an entity that provides a digital currency wallet. The wallet provider facilitates participation in a digital currency system by allowing users and merchants to transfer the digital currency among themselves, making sure (e.g., via digital signatures) that the right parties are credited and charged. The wallet provider maintains each customer's virtual currency balance, ensures transaction security, and performs backup/cold storage.

5 A Digital Currency for PGS

In the last few years, digital currencies have attracted strong interest and even Central Banks are considering creating their own, or at least are keeping a close eye on them. We claim that PGS is a natural front-end for crypto-currency transactions, as it is itself based on visual cryptography. Many works[4] [8, 9] have presented comparison of crypto-currencies, most of them based on, or derived from, Bitcoin. Those cryptocurrencies can be split into three groups, based on the way the crypto-currency is generated and distributed. One group uses *proof-of-work* and the second group uses *zero-knowledge proofs* [10]. The third group is kind of a residual group, including only two currencies that use central distribution: Ripple (https://ripple.com/) and MaidSafeCoin (https://maidsafe.net/safecoin.html). The Proof-of-Work (POW) approach allows (volunteer) currency generation points (often called *Miners*) to generate new, valid currency units each time they solve a problem that requires huge computational effort (for example, "finding a number x whose image $h(x)$ via a non-invertible hash function $h()$ has two leading zeros"). Handling a currency system based on POW requires Miners to hold powerful computational resources which we cannot expect to have among the devices targeted by PGS. So, the one of the viable solutions for integrating PGS with a POW crypto-currency is to use Bitcoin, where the generation and distribution of currency units are already handled by the existing Bitcoin infrastructure, and bitcoin transfers can be used as a service at virtually no cost. This choice and its implications in terms of risk will be discussed in Sect. 5.1. A *zero-knowledge proof* or *zero-knowledge protocol* is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true [10]. Some crypto-currencies use computationally light generation techniques for the currency units and then rely on zero-knowledge proofs for proving each unit's uniqueness and single ownership at transaction time. Albeit at a

[4] https://en.bitcoin.it/wiki/Comparison_of_cryptocurrencies.

different time with respect to POW, managing this type of currencies also requires huge computational resources that mobile devices cannot currently afford. For the sake of conciseness, in this paper we shall not elaborate further on this group of currencies. Both Ripple and MaidSafeCoin belong to the residual group of digital currencies that use central distribution. Ripple's solution is built around an open, neutral protocol (Interledger Protocol or ILP) while MaidSafeCoin is issued to the users of the decentralized Internet called the SAFE (Secure Access for Everyone). These special users, appropriately called *Farmers*, make their unused computing resources available to perform many of the protocols of collective interest (e.g., the Domain Name System) for running the Internet. In our opinion, farming looks a very interesting idea, as it envisions to use proof-of-availability to share unused resources (i.e., proof of setting aside resources for *potential* work) as a value generation mechanism rather than Bitcoin's *real* work, computing a difficult problem. Also, we find it attractive to couple PGS with a digital currency whose generation and distribution functionalities can require limited computational effort, and therefore can be entirely handled by standard mobile devices looks attractive. We shall discuss this idea in Sect. 5.2.

5.1 Integrating PGS with Bitcoin

Let us first consider a scenario where some *trusted third party* (in our case, the PGS back-end server) holds digital wallets for both PGS buyers and sellers. We assume the organization running the PGS back-end has collected cash advance payments from PGS buyers (or, alternatively, has obtained an initial cash pool from a donor organization). The advance money/cash pool is used to purchase bitcoins, which are stored in the buyers' digital wallets. Whenever the proof of a PGS purchase (i.e., the two VC shares of the group selfie containing item, parties and agreed-upon price) reaches the PGS back-end, the corresponding bitcoin transfer is triggered between the buyer's and the server's digital wallets. Periodically, PGS sellers can request to withdraw money from their digital wallets. The PGS back-end handles these requests by exchanging bitcoins held in the sellers' wallets into cash. We claim that, although very simple, this scenario has many interesting features. First of all, it is transparent: buyers and sellers incur into little additional costs with regard to traditional cash transactions[5] and may even not be aware of the digital currency used by the PGS back-end. Secondly, the ecosystem includes no financial institution but the digital currency community, so there will be no intermediation costs. Let us now consider the PGS back-end's profit model as if the back-end was a fund manager trading in and out the digital currency on behalf of investors. In the simplest case, we consider a single purchase. The PGS back-end receives the advance money from the buyer and invests it into bitcoins. Later it cashes out bitcoins to pay the purchase amount out in cash to the seller. Neglecting the cost of running the back-end in terms of hardware and bandwidth, and assuming no financial costs for the users[6], the

[5] Here, we neglect both the cost – for the buyer – of having/carrying a mobile terminal and the saving – for the seller – due to not having to handle cash.

[6] Ideally, the only costs PGS users will have are the ICT ones, coming close to the "digital unicorn" of no-financial-cost payments.

profit (or loss) of the PGS back-end will depend on the difference in the bitcoin-to-cash exchange rate at the moment when the cash was advanced by the buyer and at the moment when it was withdrawn by the seller. Due to the absence of transaction costs, it is difficult to make general statements about bitcoin exchange rate's statistical properties [11]. However, a general remark can be made. The Proof-of-Work bitcoin Miners must provide in order to obtain a currency unit is monotonically increasing, due to a built in mechanism that cuts the POW-to-reward ratio [7]. This suggests a long-term appreciation trend of Bitcoin with regard to traditional currencies. Looking at available empirical evidence, [12] discusses volatility of bitcoin exchange rate against six major currencies. Using raw annualized and adjusted data over a four year period from 2010 to 2014, the authors found that bitcoin had the highest annualized volatility in daily exchange rates. However, after accounting for the (low) volume of Bitcoin trades, the bitcoin exchange rate looks much more stable. Using data for the period 2010–2013, [13] showed that "Bitcoin investment exhibits very high volatility but also very high returns. In addition, for holders of well diversified portfolios, high risk is compensated by low correlations with other assets". So, depending on the actual timings of buyers' cash-ins and sellers' cash-outs, the notion of the PGS back-end as an intermediary for investing in bitcoin may provide a sensible business model. We plan to verify this experimentally.

5.2 Implementing a Digital Currency for PGS

Of course, we can also envision setting up a digital currency system specifically designed for PGS, including currency generation and distribution functionalities. Due to the context of the PGS application (payments in open air markets in developing countries) we need to dispense with approaches based on proof-of-work or zero-knowledge proofs. Luckily, other notions are available. Dimitris Chatzopoulos et al. have suggested that the computational hardness of the proof of ownership be replaced with "*the social hardness of ensuring that all witnesses to a transaction are colluders (users assisting the malicious user to double spend)*" [9]. They have then suggested LocalCoin, "*an alternative cryptocurrency that requires minimal computational resources, produces low data traffic and works with off-the-shelf mobile devices*".

LocalCoin perfectly suits the environment of mobile devices, it is a nice candidate for *PGS credits* as its generation mechanisms is based on the notion of proof of availability to do something useful [8] introduced by Stefan Dziembowski. We focus on the design presented by Dominic Wörner and Thomas von Bomhard [14]. They suggests that people can earn digital currency by making their devices available to share data of public interest, including early warnings of severe droughts and rains, products prices on local markets, traffic information, providing evidence to support credibility checks of scoops in social media, as part of the fight against gossip, rumor and hoax. We can assume our community will coincide with PGS buyers and sellers. Our proposed system is hybrid: "normal" buyers will buy credits in exchange of cash, as discussed in Sect. 5.1. Some special buyers, called *Sharers*, will get PGS credits by provably making their devices (or themselves) available for some *pro bono* activity. Once a seller holds PGS credits in her digital wallet, she can either cash them out or take advantage of the Sharers' resource pool. As far as implementation is concerned, we remark that creating

a crypto-currency is no longer a big deal, as every crypto-currency on the market today is based on the open source bases like Lite-coin, available on GitHub (https://github.com/bitcoin). The main features to customize are:

- Creating blocks corresponding to new currency units based on Proof of Sharing Obligation (POSH) rather than Proof of Work (POW), or by implementing a hybrid version.
- How many credits Sharers receive when they submit a POSH block (*sharing reward*);
- The hashing algorithm to be used when creating the POSH blocks;
- The time duration between POSHs creation;
- The rate at which the sharing reward cuts in half (this is needed to ensure the appreciation trend w.r.t. traditional currencies, see Sect. 5.1).

6 Challenges

Many of the challenges that PGS-plus-digital-currency system will face are societal in nature: building a community to use the new crypto-currency, setting up a robust and capable team to handle development and bug fixing, marketing the new cryptocurrency for Sharers to keep adding value and other users to reinforce trust, bringing merchants onboard so that users can have a place where they spend their PGS credits, educating the community on the promises of the new tool and on the risks it bears so that users will have what they need to secure their wealth. The challenges this work wants to focus on are basically the technical ones. As PGS is already available on mobile devices using Android, we need to show the feasibility of a crypto-currency back-end, including (*i*) the POSH notion and (*ii*) a single wallet for PGS and Bitcoin currencies.

7 Conclusions

Traditional purchase of goods and services online are dominated by credit and debit cards, or PayPal. PGS provides a much simpler alternative to these systems which is based on a powerful metaphor (ripping a banknote in two) and requires virtually no technology training. Also, PGS allows to spread the cost of a fund transfer over multiple purchases. Field experience in Benin [1] has shown that PGS is suitable for low value purchases typical of open-air market in developing countries. As the relative cost of processing low value transactions is much greater for traditional payment methods than for digital money, the latter looks an ideal companion for PGS, further increasing its competitive advantage [15]. We discussed direct interfacing between PGS as Bitcoin, as well as the design of a LocalCoin-style digital currency based on the notion of Proofs of Sharing obligations (POSH). Implementation of the PGS Back-end is currently underway.

Acknowledgements. This work has been partly funded by the Bill & Melinda Gates Foundation under the grant n. APP198273.

References

1. 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. LNICSSITE, vol. 171, pp. 136–141. Springer, Cham (2016). doi:10.1007/978-3-319-43696-8_15
2. Naor, M., Shamir, A.: Visual cryptography. In: Workshop on the Theory and Application of Cryptographic Techniques, 1–12 (1994)
3. El Zarki, M., Mehrotra, S., Tsudik, G., Venkatasubramanian, N.: Security issues in a future vehicular network. Eur. Wirel. **2**, 270–274 (2002)
4. European Central Bank: Virtual currency schemes. European Central Bank Internal report, Frankfurt-on-Main (2012)
5. Financial Action Task Force (FATF). Virtual currencies key definitions and potential AML/CFT Risks (2014)
6. Bank für Internationalen Zahlungsausgleich and Committee on Payments and Market Infrastructures: Digital currencies (2015)
7. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf (2009)
8. Dziembowski, S.: Introduction to cryptocurrencies. In: 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 1700–1701 (2015)
9. Chatzopoulos, D., Gujar, S., Faltings, B., Hui, P.: LocalCoin: an ad-hoc payment scheme for areas with high connectivity. In: 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 365–366 (2016)
10. Krantz, S.G.: Zero knowledge proofs. Expeditions in Mathematics, 249–260 (2011)
11. Chu, J., Nadarajah, S., Chan, S.: Statistical analysis of the exchange rate of bitcoin. PLoS One **10**(7), e0133678 (2015)
12. Sapuric, S., Kokkinaki, A.: Bitcoin Is Volatile! Isn't that Right? Lecture Notes Bus. Inf. Process. **183**, 255–265 (2014)
13. Brière, M., Oosterlinck, K., Szafarz, A.: Virtual currency, tangible return: portfolio diversification with bitcoin. J. Asset Manag. **16**(6), 365–373 (2015)
14. Wörner, D., von Bomhard, T.: When your sensor earns money: exchanging data for cash with Bitcoin. In: 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, pp. 295–298 (2014)
15. Grinberg, R.: Bitcoin: an innovative alternative digital currency. Hast. Sci. Technol. Law J. **4**, 160–207 (2011)