Bringing Bitcoin virtual currency to proximity points of sale

Aleš Breznik[1,2], Boris Turk[1], Amor Chowdhurry[1,2]

[1]Margento R&D d.o.o., Gosposvetska cesta 84, 2000 Maribor, Slovenija
[2]Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor, Slovenija
E-mail: ales.breznik@margento.com

Keywords: *Bitcoin, POS, mobile, transaction, implementation*

Abstract:

Recent rising trends in digital currencies provided an initiative for Margento to develop a transaction system for digital currency transfers ready for use at physical points of sale. The system was designed using already established DOV technology channels and a supporting third-party server for Bitcoin wallet integration and transaction handling with on –site Margento POS terminals.

1. Introduction

Bitcoin is a peer-to-peer payment system and digital currency introduced under the name Satoshi Nakamoto in 2008 as open source software based on cryptography to control the creation and transfer of money.

Since then Bitcoin suffered a major blow in its infancy when a technical glitch in March 2013 caused a fork in the block chain resulting in two different transaction histories adding simultaneously to two different chains. Later, in February 2014 Mt. Gox, one of the largest bitcoin exchanges filed for bankruptcy due to 744,000 lost bitcoins, claiming they have been stolen some time ago. Some mainstream websites started accepting bitcoins c. 2013, including WordPress, OKCupid, Atomic Mall, TigerDirect, etc. with many more additional businesses and services joining the trend.

Users send and receive bitcoins using wallet software on a personal computer, mobile device, or a web application. For a transaction, a new bitcoin address is made on the receiving party end. The address is a special code called a public key. The public key is transmitted to the sending party. The sending party now initiates a new transaction to the public key address received earlier. The transaction is signed by another code, called the private key. This key is not transmitted but is rather used to encrypt the transaction details. The wallet, where the transaction is initiated then transmits the encrypted transaction details to the network. The transaction is now concluded for the sending and receiving parties, which now have to wait approximately 10 minutes for the transaction to be validated by the network. Until then, the bitcoins included in the transaction cannot be used by the receiving party.

It is important to note, that there is no actual bitcoin. A bitcoin is actually the entire range of addresses of all transactions made with this specific bitcoin. Every wallet is a Bitcoin client that can initiate and receive transactions.

The validation process now requires a bitcoin miner on the network. The transaction is included into a block of all transactions conducted in the previous 10 minutes. This block is further encrypted and is processed by a Bitcoin miner. The miner recalculates all verification codes to validate the validity of all transactions. If any fake signatures are found or transaction history of any bitcoin isn't as it should be, the transaction is denied. No personal codes are disclosed in the process, as the miner uses a verification algorithm where all transactions are recalculated by public keys that must match the private key signature result provided with the transaction details. The private key is only used as an encryption method and is not known by the network.

2. Bitcoin Payment

Due to its digital nature, Bitcoin transactions are out of the ordinary in the sense of transaction tracking on the point of sale itself. There is no physical currency to keep and no credit card verification and the bitcoins are available only after a certain period.

Multiple methods are available for channelling bitcoins on the point of sale from the customer to the merchant, most notable of which is the QR code scanner and terminal method.

2.1. QR Code

Currently the most popular proximity payment is based on a QR code system that requires a QR code generator, be it digital or printed form, to display the QR code to the customer for verification. The customer confirms the transaction with a processor with an integrated wallet app on the device, usually a smartphone or tablet.

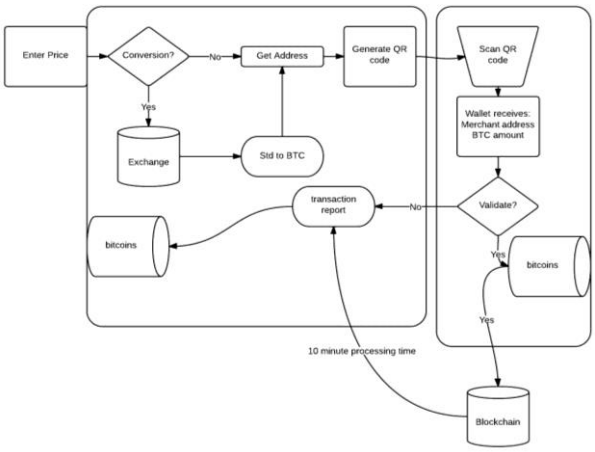

Figure 1: QR code method diagram

2.2. Data over Voice

Phones have become our everyday companions in society abroad. Their use has seen a broad expansion and wide acceptance and as such offer an excellent platform for payment integration. Smartphones have seen a steep incline in numbers recently, offering a range of functionalities and features. Despite all these, there are some basic features a phone will have regardless of its age, price or company. One of those features is a voice call. Every phone in the history of time offers this basic functionality and taping this channel for data transmission enables an even wider use for these devices.

Payment systems have already been implemented using the Data over Voice (DOV) transfer and Bitcoin would only be an extension to the already present system[8].

3. Bitcoin Payment Integration

Bitcoin currently serves primarily as digital currency focused on activity on the internet[7]. While there are retail stores already present accepting Bitcoin, they are few in number. One of the main reasons Bitcoin hasn't found its way from the digital world is a fear-of-risk factor involved in accepting such currency.

Its anonymous nature has sprung a range of illegal activities across the web and as a result contributed too much turmoil regarding the currency itself (silkroad). The Bitcoin exchange market is one of the most volatile currency exchange market on the planet, which additionally adds to Bitcoin's bad reputation as a real world currency[7].

This volatility however is not something only Bitcoin experiences. The USD soared by nearly 50% in the late 1990s, and then dropping by 30%. Similarly, in late 2008 jumped 20% in a matter of weeks and this is considering the trade-weighted dollar. Individual currency pairs can exhibit much more fluctuation. The average person however, doesn't notice these fluctuations in everyday use of the currency, since all prices are in dollars and currency value only matters with respect to another.

In the case of Bitcoin, the story has a different twist. When using the digital currency, almost all prices are valued in USD (or any other currency) and are recalculated to bitcoins, and visa versa, based on the current exchange rate. This results in almost no Bitcoin value reference independent of the Bitcoin-dollar exchange rate.

Bitcoin lacks a real anchor of goods being traded in Bitcoin, where the value of the currency could be internally based[7].

This can, however turn for a great change. Bitcoin currently has a lot of purchasing power, which is still on a steep incline. An increasing number of business venues are therefore prepared to expose their trade to the volatility of the Bitcoin market.

To avoid the exchange volatility, entrepreneurs will pay suppliers, providers, employees in the same currency they are accepting as payment. This in turn strengthens the Bitcoin market with increasing number of goods that can be purchased or sold using exclusively bitcoins[7].

With increasing purchase power of the currency, internal trade increases. For trade within a certain market, currency exchange volatility bears no importance. This will in turn stabilize the exchange due to the gross amount of goods being traded with specific value.

Until the Bitcoin market reaches broad availability however, a certain amount of risk is involved in the exchange. Both customer and merchant accept this risk when using bitcoins as a trade currency.

3.1. Building a new Hybrid channel for Bitcoin payment

Bringing Bitcoin to a retail environment requires the use of already implemented payment procedures. Margento DOV services are already widely accepted and recognized as a legitimate and secure payment method. Margento terminals already support most proximity payments[2], additionally expanding Bitcoin to other digital formats such as NFC-enabled telephones and smartcards[1].

Adding Bitcoin transactions to an already stable and affirmed procedure would increase public acceptance of virtual currency as well as establish a stand on the market and propagate Bitcoin use in a more common environment.

3.1.1. DOV service

Every DOV service incorporates transactions between three entities[5]:

- Mobile phone (customer)
- Terminal (merchant)
- Processing Center (bank)

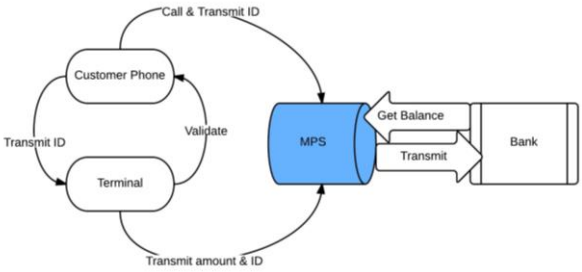

Figure 2: DOV service diagram

The customer initiates a call to the Processing Center (MPS) providing the initial transaction request and customer ID. The call is routed through the terminal that contacts the MPS independently to verify the correct customer ID[3]. The Processing center, if successful, confirms the transaction and initiates the fund transfer. Bitcoin DOV service is no different.

3.1.2. Bitcoin Transactions

While the basic Bitcoin transactions function in a two-party system, since every transaction is conducted between a sending and receiving party, critical transaction information is broadcasted to the rest of the network[9].
The transmission contains:

- Sending address
- Receiving address
- Amount

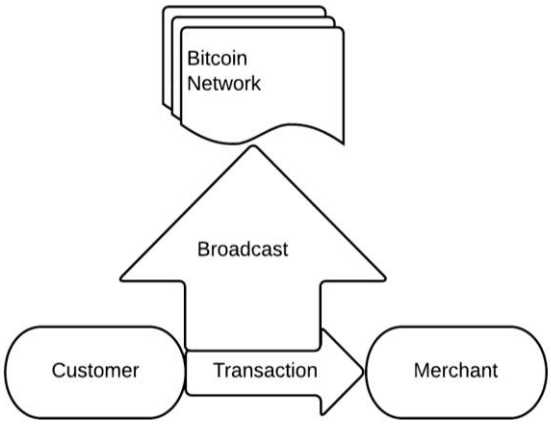

Figure 3: Bitcoin transaction diagram

In this sense, the Bitcoin network forms the third party in the transaction process that validates the transaction.

3.1.3. Complete integration to MPS

Providing a different payment link for Bitcoin is implemented by substituting standard transaction notification to a bank with the Bitcoin cloud[4].

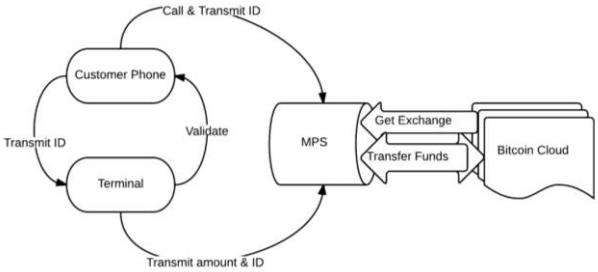

Figure 4: Hybrid system diagram

Transactions between the customer and merchant appear only as bookkeeping changes to their account balance inside the MPS[6]. There is no actual Bitcoin transaction until any of the parties withdraws bitcoins from their account on the MPS to their Bitcoin wallet.

With each purchase, a certain amount of logged Bitcoin balance is transferred from the user's account to the merchant's account in virtual currency and not as an actual Bitcoin transaction.
This eliminates any transfer fees and transfer delays and transforms the Bitcoin account into a prepaid account. Due to the nature of the service, the exchange rate is calculated on a much larger interval than it would normally be and thus offers additional security to both the merchant and the customer.

Both customer and merchant have a dedicated Bitcoin wallet for receiving and sending funds for purchases. The wallet can be managed like any other Bitcoin wallet and can be used normally, but with the perk of an additional payment channel.

3.1. Ease of Use

The DOV service offers additional advantages considering its use[4]. Calling a three digit number and tapping the phone on the terminal is all it takes to carry out the transaction.

All transactions are directed at the transitory account, where the validity of Bitcoins and parties involved is verified. The transitory account then transfers the funds to the merchant account associated either with the terminal or the entire service. This account however, does not require phone number association. The merchant can simply transfer bitcoins to other accounts in the form of a pay check, expenses, etc. or sell the bitcoins on a pre-set exchange or any other market on the internet.

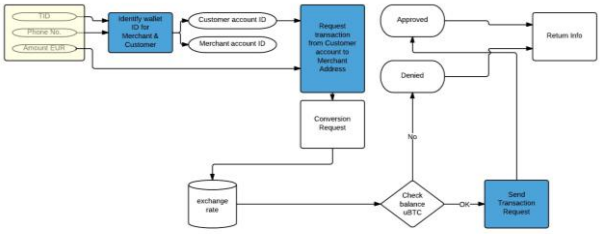

Figure 5: Transaction flowchart

The user can associate any wallet with the DOV service and immediately use their phone as a payment method[4]. The only addition is its link to a phone number, with which the customer can purchase goods in stores that receive bitcoins.

4. Conclusion

The Bitcoin has been part of much recently, experiencing a great hype, greatly increasing its price, to a market crash with bankruptcy of the biggest exchange service online and even criminalization in certain countries due to its bad reputation.

The fluctuating nature of Bitcoin values results in a certain degree of reluctance in merchants regarding Bitcoin acceptance as a valid compensational currency and renders its use in everyday life somewhat difficult.

Nevertheless bitcoin survived and has proven to be a resilient market currency. Whether it will expand into a full-fledged monetary system or remain as a border market is still to be determined, but it certainly is an interesting concept and a terrain worth exploring.

References:

[1] J. Kroflič, A. Chowdhury, B. Kotnik in R. Svečko, RFID tehnologija na področju pametnih kartic, ERK 2010, Portorož, Slovenija, 20.-22. september 2010.

[2] M. Kseneman, F. Horvat in A. Chowdhury, Modularna zasnova programske opreme plačilnega terminala – mPOS T4500, ERK 2010, Portorož, Slovenija, 20.-22. september 2010.

[3] Andrej Medved, Amor Chowdhury, Stanko Golicnik, Preizkušanje GPRS modemov ter razvoj mPOS tiskanine za vec GPRS modemov, ERK 2010, Portorož, Slovenija, 20.-22. september 2010.

[4] J. Slatenšek, Z. Mezgec, Zdenko, F. Horvat, A. Chowdhury, Vmesnik za razširitev funkcionalnosti plačilnih terminalov. V: ZAJC, Baldomir (ur.), TROST, Andrej (ur.). ERK 2009, Portorož, Slovenija. 21-23. september 2009,

[5] Z. Mezgec, M. Pec, R. Svečko, A. Chowdhury, Prenos podatkov po govornem kanalu GSM sistema. ERK 2005, Portorož, Slovenija, 26. - 28. september 2005

[6] M. Fras, Z. Mezgec, P. Žerdin, A. Chowdhury, Storitev Točka na plačilnem terminalu mPOS T4000. ERK 2009, Portorož, Slovenija, 21-23. september 2009

[7] Report on new payment methods: prepaid cards, mobile payment and internet payment services, GAFISUD-EUROPEAN UNION Project, June 2013, http://www.prestashop.com/blog/en/pros-and-cons-of-accepting-bitcoin-for-e-commerce-merchants-and-their-customers/

[8] Casascius Bitcoin POS system, https://en.bitcoin.it/wiki/Casascius_Bitcoin_POS_system

[9] Bitcoin transactions http://www.coindesk.com/information/how-do-bitcoin-transactions-work/