Bitcoin Payment Gateway

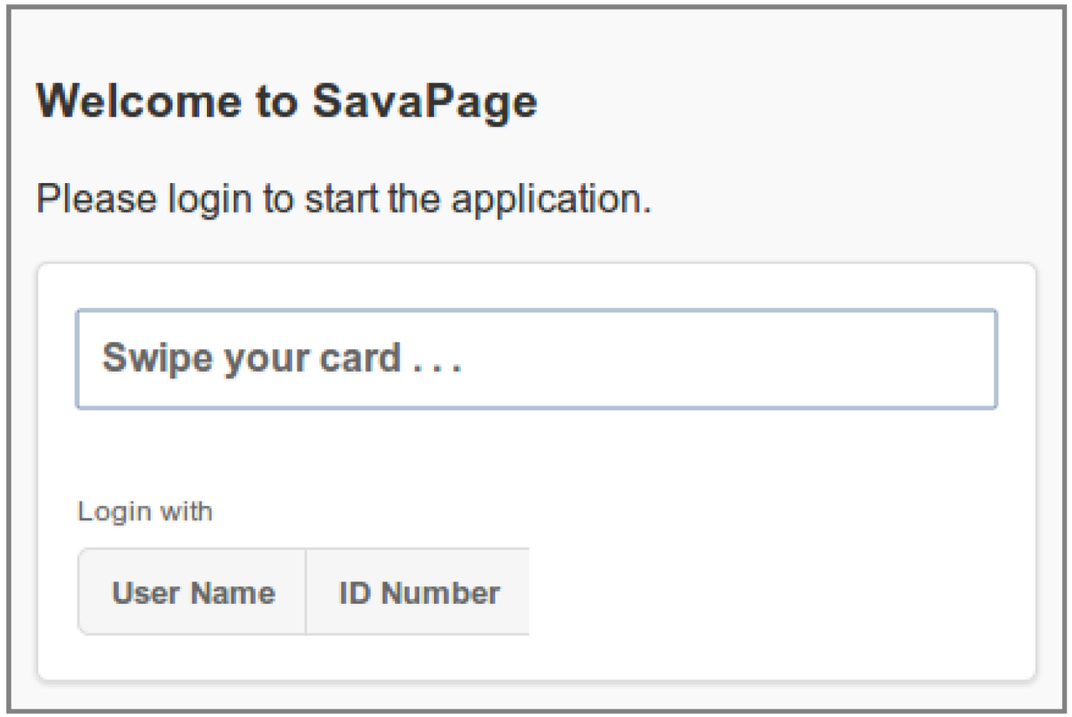
Introducing Pay-per-Print with Bitcoin

by Rijk Ravestein, savapage.org

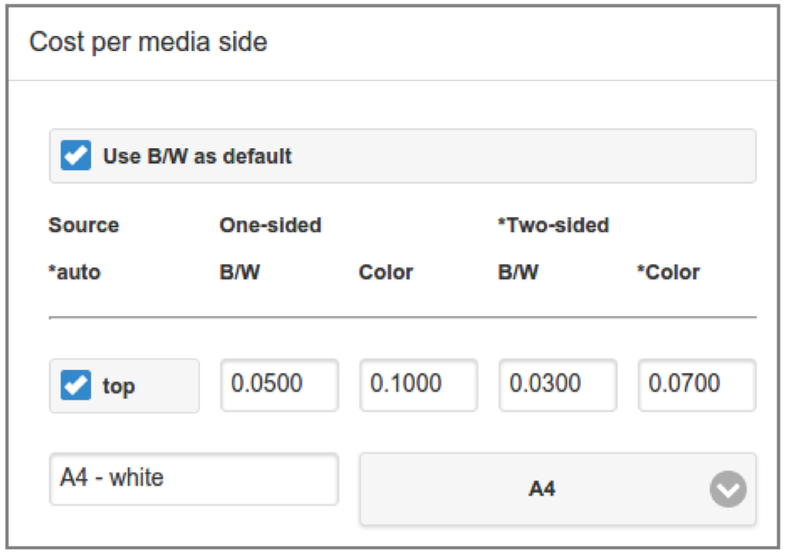
Agenda

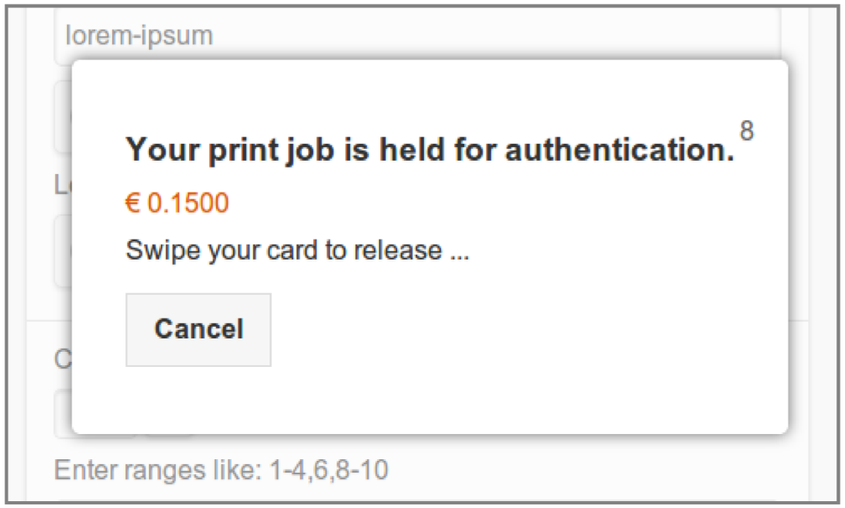
SavaPage is a Libre Print Management Solution that uses Open Standards and Commodity Hardware for Secure Pull-Printing, Pay-Per-Print, Tracking & Tracing and PDF Creation. It is licensed under AGPL version 3.

- Use Case
  - Pay-per-Print
- Payment Transactions
  - Accounts
- Bitcoin Payments
  - Why, how?
- Lessons Learned
- What's Next?



Pay-per-Print





How can the financial transaction be established?

Pay-per-Print: transaction criteria

- Fast
  - Real-time
- Micro-payments
  - Low (no) fees
- Software only
  - Open API
  - No proprietary hardware

Pay-per-Print: transaction models 1/2

- Cash
  - Micro-payments
  - Time consuming
  - Hardware needed

- Centralized Account
  - Bank, Credit Card, PayPal, . . .
  - Time consuming
  - High fees, no micro-payments

Pay-per-Print: transaction models 2/2

- Stored-value Card
  - Monetary value stored on card (public or closed system)
  - Real-time transaction
  - Micro-payments
  - Hardware needed
- Bitcoin wallet
  - ~Micro-payments
  - Real-time transaction?
    - 0 confirmation ~ immediate
      - Because of low value considered an acceptable risk of a reversed transaction
    - 1 confirmation ~ 10 minutes, 6 confirmations . . .

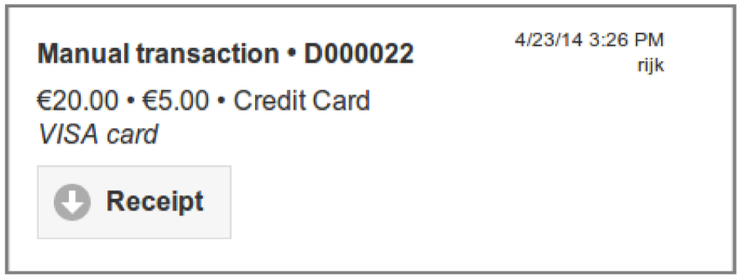
Pay-per-Print: transaction model conclusion

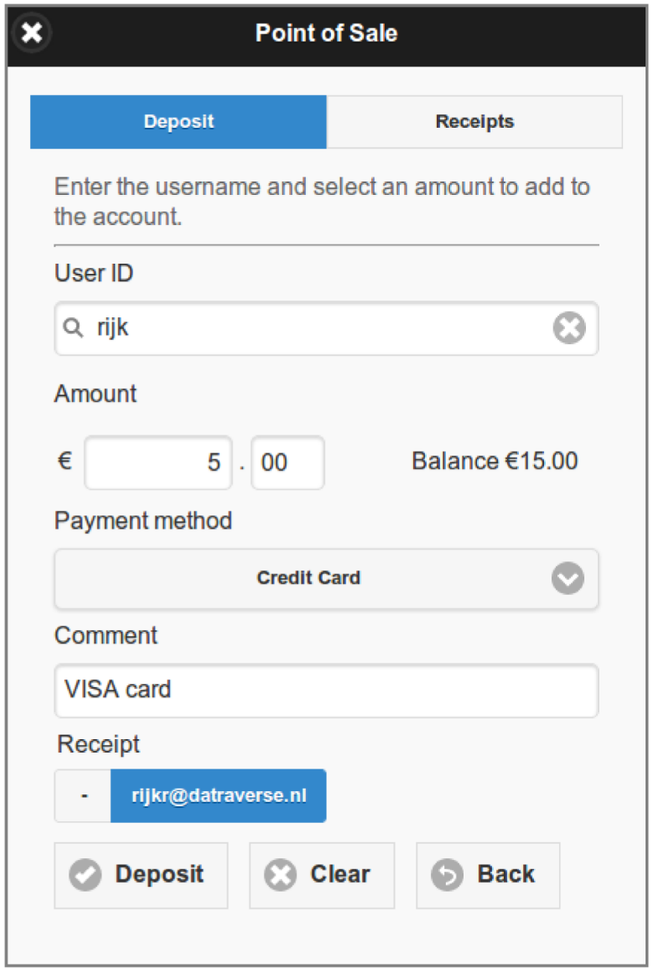
There is no transaction model that meets all criteria, that's why we use a …

- Personal Account in the SavaPage database
  - Real-time
  - Micro-payments
  - (Re)charge account
  - Charge back

Personal Account Recharge Option 1/5

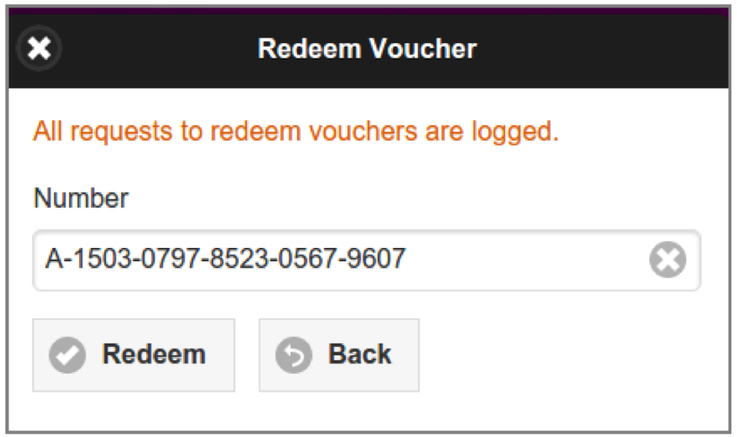
- Point-of-Sale
  - Manual transaction
    - Cash
    - Maestro Card
    - Credit Card
    -

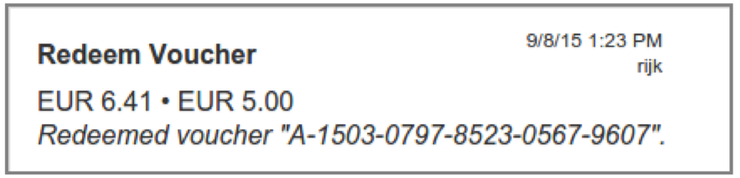




Personal Account Recharge Option 2/5

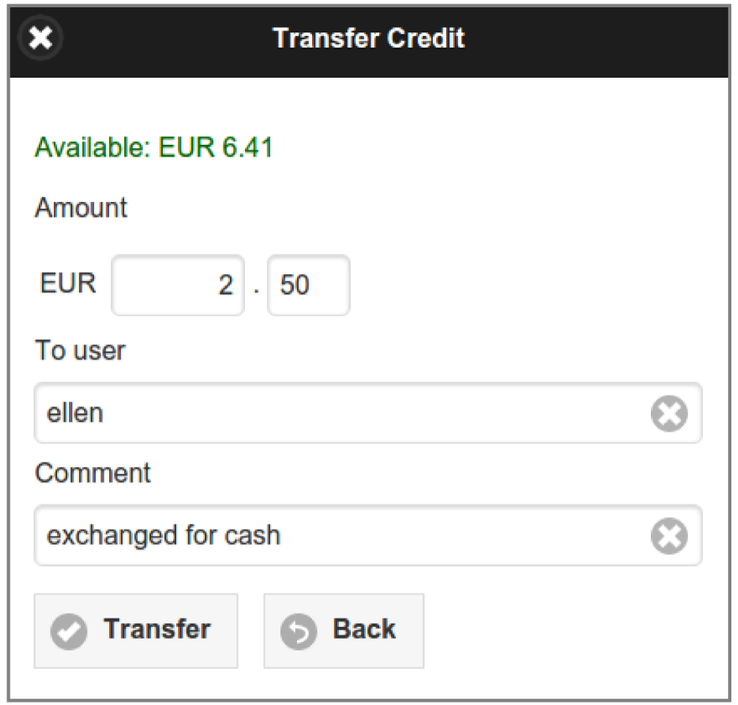
- Vouchers
  - Buy at counter and redeem in Web App

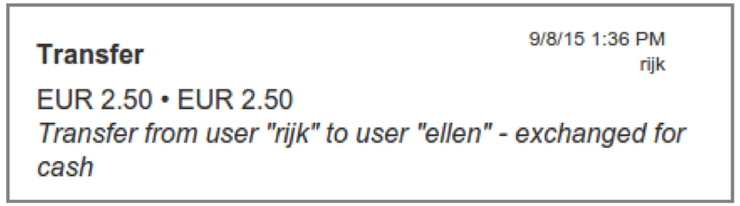




Personal Account Recharge Option 3/5

- Transfer credit to another user





Recharge from External Accounts: Payment Gateways

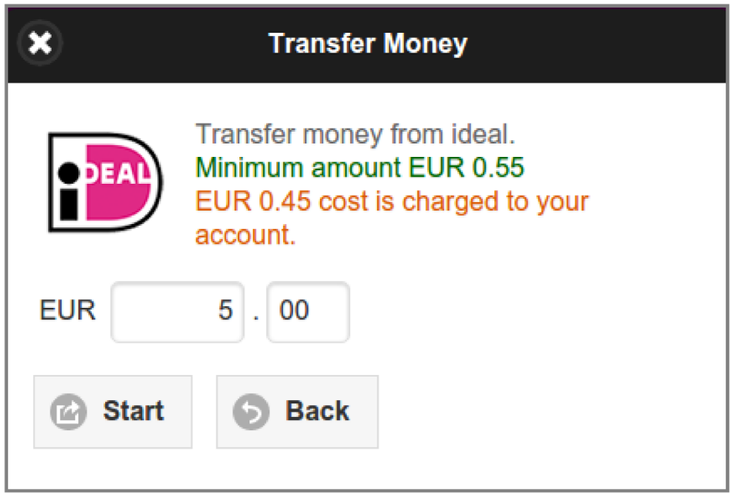
- Native communication with a Payment Provider is expensive
  - financially and technically
- On-line payment integrators offer . . .
  - Plurality of payment methods
  - Simple uniform Web API
  - Pay-per-transaction
- SavaPage is an intranet application
  - Any Callback URL must be port-forwarded in a router or firewall.

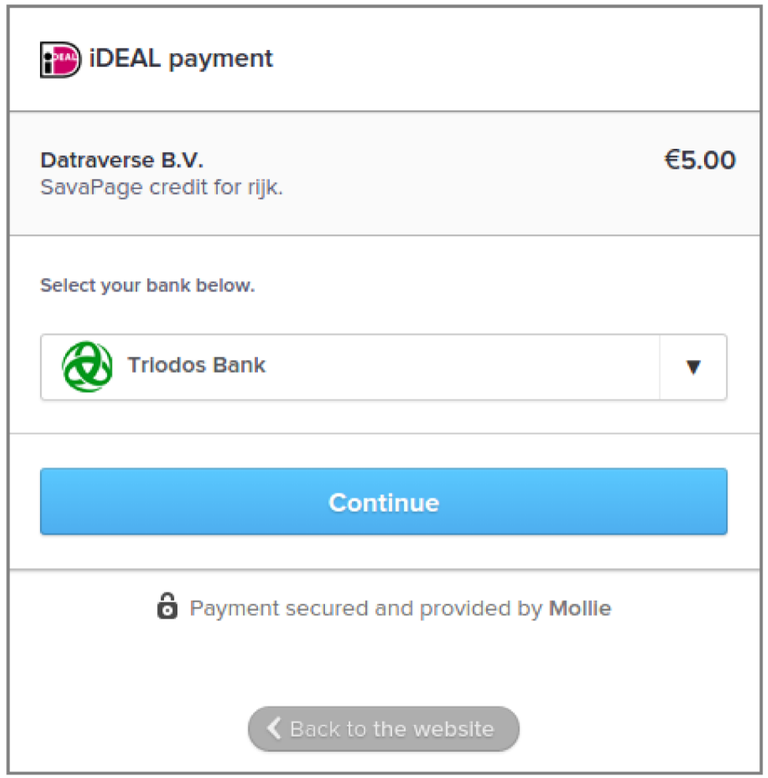
Personal Account Recharge Option 4/5

External Account

- Creditcard
- PayPal
- Paysafecard
- SOFORT, SEPA (Europe)
- Bancontact/Mister Cash, Belfius Direct Net (Belgium)
- IDEAL (Netherlands)
- . . . Bitcoin

https://api.mollie.nl/v1



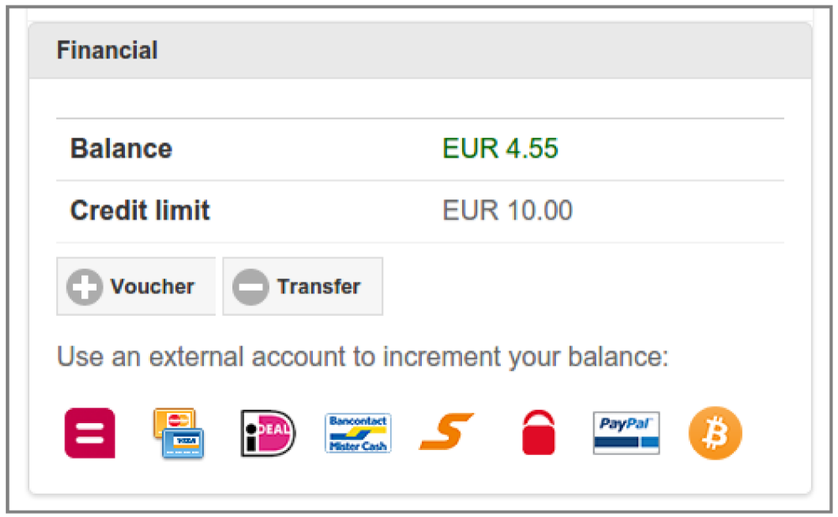


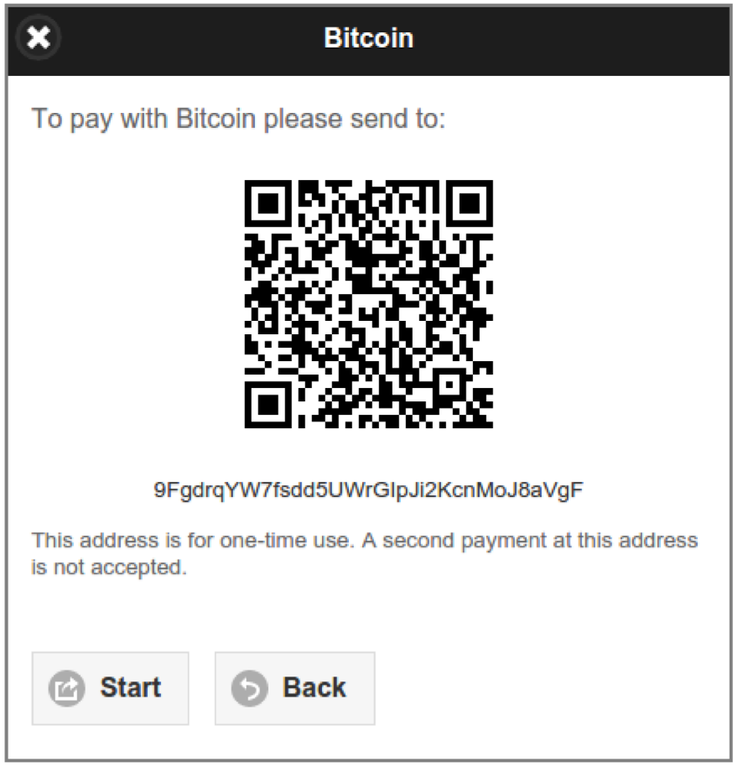
SavaPage is an intranet application. The Web API callback must be port-forwarded in a router or firewall.

Recharge from External Accounts: Bitcoin Payment Gateway

- Fees of other methods are too high for smaller amounts
  - IDEAL €0.45 | Creditcard €0.25 + 2.8% | PayPal €0.10 + Fee | Bitcoin €0.25
    - Fees charged to the merchant are passed to the user by SavaPage.
  - Recharge is real-time
- Bitcoin transaction fees are low
  - 0.0001 BTC ~ € 0.022
  - Recharge is real-time, when acknowledged at 0 confirmation
- Charge back use-case is within reach
- Be prepared for the crypto-currency revolution :-)
  - **Hands-on experience is crucial**
  - A first step towards real-time micro-payments?

Personal Account Recharge Option 5/5





URI scheme as used in QR-code and Start button is according to Bitcoin Improvement Proposal (BIP) 0021

https://en.bitcoin.it/wiki/BIP_0021

". . . a new key pair should be used for each transaction to keep them from being linked to a common owner"

Bitcoin whitepaper: Satoshi Nakamoto

- Local Bitcoin Wallet
  - Bitcoin Core ?
  - 3rd Party Bitcoin Libraries ?
- On-line Bitcoin Wallet
  - Web API ?

Option #1 – Bitcoin Core

*As part of Bitcoin Core, **bitcoind** is a program that implements the Bitcoin protocol for remote procedure call (RPC) use.*

- Promising
  - JSON-RPC interface over HTTP
- However . . .
  - "Bitcoin Core initial synchronization will take time and download a lot of data. You should make sure that you have enough bandwidth and storage for the full block chain size (over 20GB)."
    - https://bitcoin.org/en/download

Option #2 – bitcoinj.github.io

***bitcoinj** is a Java library for working with the Bitcoin protocol. It can maintain a wallet, send/receive transactions without needing a local copy of Bitcoin Core.*

- Promising
  - "fast micro-payments that avoid miner fees."
- But, bugs and other problems . . .
  - "The Wallet code doesn't scale well. All transactions that were ever relevant to the wallet are loaded into memory, all the time, and re-written every time the wallet is saved. This results in a simple on-disk format accessible to many kinds of apps, but has poor performance for heavy users. In time we'll probably switch to a log structured wallet file format to solve this."
    - https://bitcoinj.github.io/limitations

***Blockchain.info** Wallet API to send and receive payments from an on-line Wallet Account: https://blockchain.info/api*

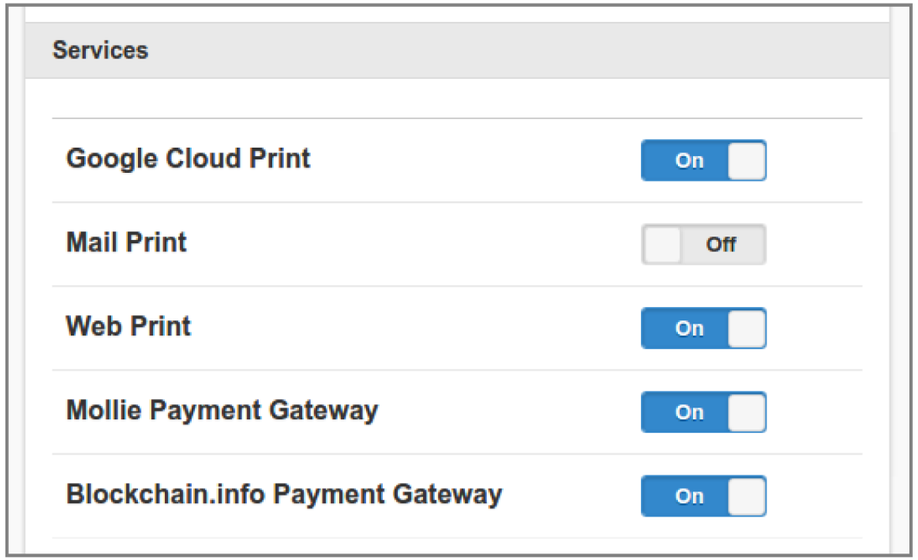
- Simple
- ~Security
  - Keep wallet balance low by regularly transferring bitcoins to more secure places.
    - For example: to IBAN with https://bitonic.nl/
- ~QoS
  - We'll see . . .

savapage-ext-blockchain-info.properties 1/4

```
#------------------------------------------------------------------
# The callback URL is set at your Blockchain.info account and has
# the following <placeholder> format:
#
# https://<yoursite>/callback/payment/live/<savapage.plugin.id>?<callback.secret.parm>=<callback.secret.value>
#
#------------------------------------------------------------------

#------------------------------------------------------------------
# Unique ID of this plug-in
#------------------------------------------------------------------
savapage.plugin.id=blockchain.info

#------------------------------------------------------------------
# Descriptive name
#------------------------------------------------------------------
savapage.plugin.name=Blockchain.info Payment Gateway

#------------------------------------------------------------------
# Plug-in class
#------------------------------------------------------------------
savapage.plugin.class=org.savapage.ext.payment.bitcoin.blockchaininfo.BlockchainInfoPlugin

#------------------------------------------------------------------
# true | false
#------------------------------------------------------------------
savapage.plugin.enable=true
```

savapage-ext-blockchain-info.properties 2/4

```
#-----------------------------------------------------------------
# Is plug-in turned online when loaded? (true | false)
#
# When the plug-in is turned offline, users are not able to make
# a payment, but Web APi callbacks are handled.
#-----------------------------------------------------------------
savapage.plugin.online=true

#-----------------------------------------------------------------
# Documented at: https://blockchain.info/api/blockchain_wallet_api
# Note: enable Api Access in Blockchain.info Account settings
#-----------------------------------------------------------------
wallet.api.url=https://blockchain.info/merchant

#-----------------------------------------------------------------
# Your Blockchain.info Wallet
#-----------------------------------------------------------------
wallet.identifier=************************************
wallet.password.main=************
wallet.password.second=************

#-----------------------------------------------------------------
# The URL to your Wallet identifier or alias used as link in the
# Admin Dashboard (optional).
#-----------------------------------------------------------------
wallet.url=https://blockchain.info/my-alias
```



savapage-ext-blockchain-info.properties 3/4

```
#------------------------------------------------------------------
# The cycle in hours to perform the auto_consolidate action. Consolidation is lazy triggered
# after an acknowledged payment is committed.
#
# “Queries to wallets with over 10 thousand addresses will become sluggish especially in the web interface.
# The auto_consolidate command will remove some inactive archived addresses from the wallet and insert them
# as forwarding addresses (see receive payments API). You will still receive callback notifications for these
# addresses however they will no longer be part of the main wallet and will be stored server side.”
#------------------------------------------------------------------
bitcoin.address.consolidation.cycle.hours=48

#------------------------------------------------------------------
# Number of days after which bitcoin addresses, that have not
# received transactions, will be consolidated.
#------------------------------------------------------------------
bitcoin.address.consolidation.days=60

#------------------------------------------------------------------
# Documented at: https://blockchain.info/api/exchange_rates_api
#------------------------------------------------------------------
ticker.api.url=https://blockchain.info/ticker

#------------------------------------------------------------------
# A comma separated value list of ISO currency codes for which
# exchanges rates are available.
#------------------------------------------------------------------
ticker.currency-codes=USD,JPY,CNY,SGD,HKD,CAD,NZD,AUD,CLP,GBP,DKK,SEK,ISK,CHF,BRL,EUR,RUB,PLN,THB,KRW,TWD
```

savapage-ext-blockchain-info.properties 4/4

```
#------------------------------------------------------------------
# Acknowledge the transaction at zero confirmations. This will
# charge the user's personal account almost immediately after
# the BTC payment is done.
#
# The confirmation callback of a transaction continues until the
# trust limit is reached. This is for auditing purposes only.
#------------------------------------------------------------------
trust.confirmations.acknowledge=0
trust.confirmations.trust=1

#------------------------------------------------------------------
# These values must match the URL parameter of the callback URL
# specified in [Account Settings] of your Blockchain.info Wallet.
# CAUTION: max length of the callback URL is 255.
#------------------------------------------------------------------
callback.secret.parm=sp_secret
callback.secret.value=****************************************
```

Bitcoin Transaction Details

BLOCKCHAIN info

Home Charts Stats Markets API Wallet

Transaction View information about a bitcoin transaction

96212ee6cd2a7b3ccd8349651ca6fc0774c859389e17d88fca432f15f0182710

13rGtbiUiFioTLdFPnHxRbcpcF5eRKNcJ1	1JMG1FMnVu17s3VpYc6rnNxmTdcQ6f4ry4	0.004 BTC
	13rGtbiUiFioTLdFPnHxRbcpcF5eRKNcJ1	0.01299701 BTC
		0.01699701 BTC

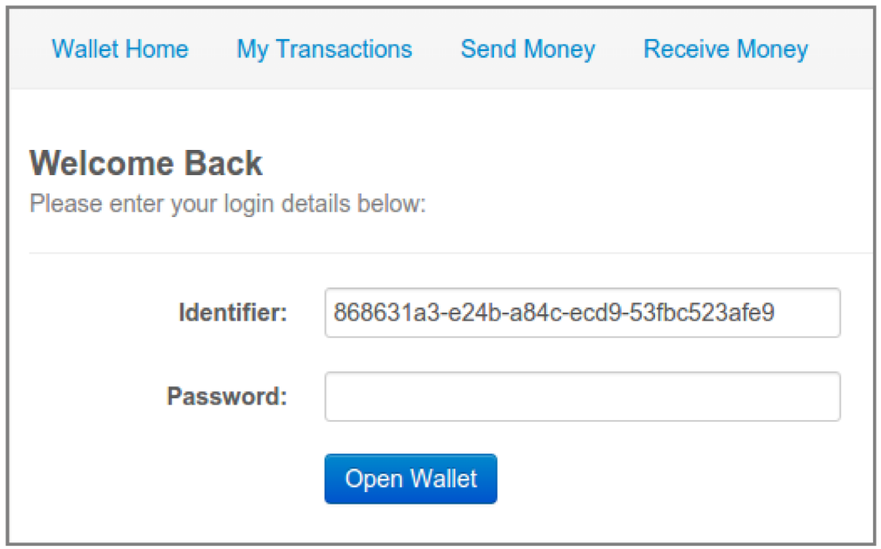
Summary	
Size	225 (bytes)
Received Time	2015-06-15 14:57:01
Included In Blocks	361068 (2015-06-15 15:09:28 + 12 minutes)
Confirmations	12391 Confirmations
Relayed by IP	Blockchain.info
Visualize	View Tree Chart

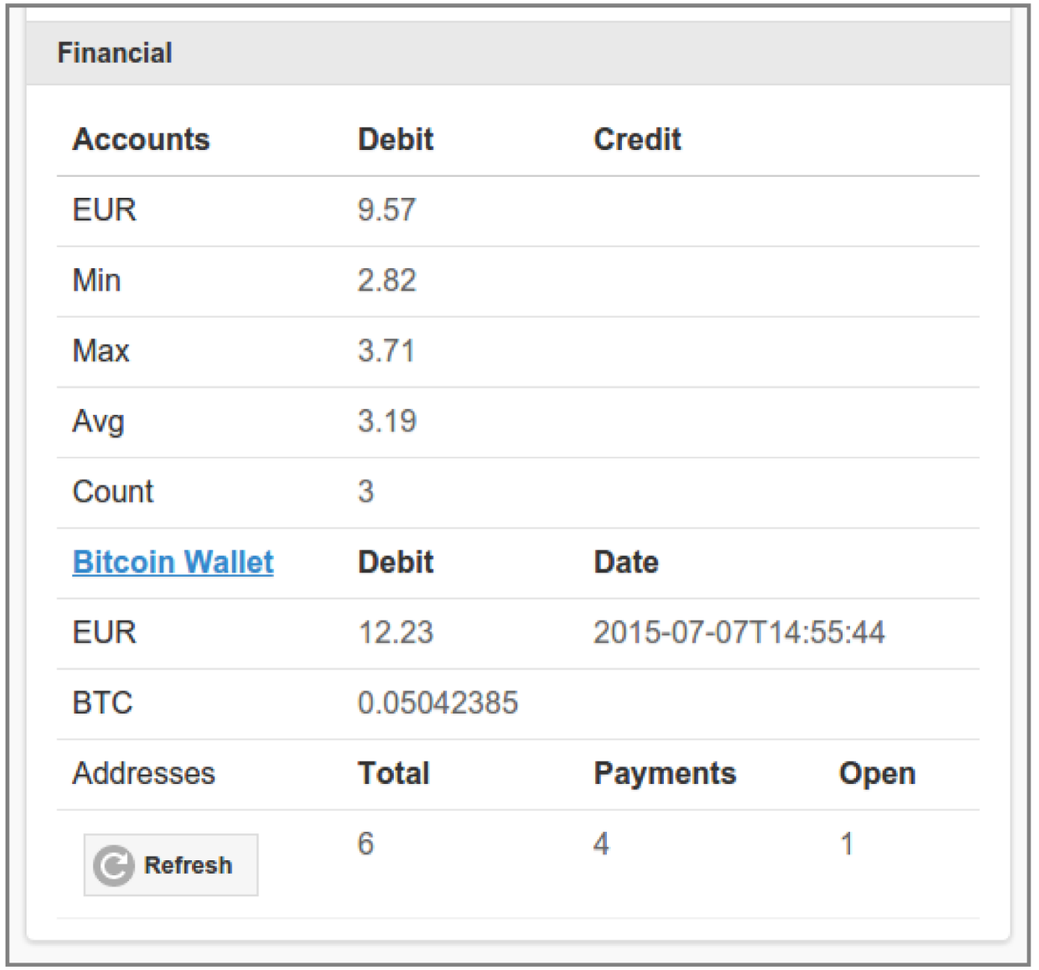
Inputs and Outputs	
Total Input	0.01709701 BTC
Total Output	0.01699701 BTC
Fees	0.0001 BTC
Estimated BTC Transacted	0.004 BTC
Scripts	Show scripts & coinbase

Bitcoin Wallet

The Total number of Bitcoin Addresses in the wallet are split into . . .

- Addresses that received *Payments*
- *Open* addresses waiting for payments.
- Other addresses, not created by our Bitcoin Payment Plug-in
  - in our example there is one such address.





Bitcoin Payment Gateway: Pitfalls 1/2

- Bitcoin payments are anonymous, so . . .
  - A payment confirmation callback message only contains the Bitcoin address and transaction hash as identification.
- Fortunately, we can trace the identity of the user who made the payment
  - by the one-time Bitcoin address, that we generated and reserved for the user at the start of the Send Bitcoins dialog, or . . .
  - by the Bitcoin transaction hash, that we linked to a user payment transaction at the callback of the first confirmed payment.
- When a user can not be traced, the payment confirmation is ignored
  - This can happen when a database export is restored and either the user, the reserved Bitcoin address or transaction hash is missing from the database.
    - This case becomes more unlikely as the number of confirmations after which the payment is acknowledged is set lower, causing a shorter latency between a user's BTC payment and the charge of his personal account.

Bitcoin Payment Gateway: Pitfalls 2/2

- A payment confirmation for a Bitcoin *address,* for which a user payment transaction link is present with a different *transaction hash*, is **ignored**. This can happen when:
  - A user, against advice, *reused* the generated Bitcoin address, as offered in the “Send Bitcoins” dialog, to make an extra payment.
  - A payment *from* the Bitcoin Wallet was executed which lead to a transaction with a positive satoshi remainder.
- Ignored confirmations are a written as warning in the Application Log.
  - Address and hash can be used to query the transaction history of the Bitcoin Wallet. Since the Bitcoin address is tagged in the Wallet with the user id, any transaction with a received amount can be used to trace the user. In case an extra user payment is identified, the user balance can be updated manually, either in the Admin WebApp or with a Server Command.

Blockchain.info Limitations

- Blockchain.info wallet can have max 999 active addresses
  - *Transfer* Bitcoins to other wallet or external (IBAN) account before limit is reached.
  - *Archive* addresses dedicated to user payments of which the balance is zero (0) and for which a payment is received.

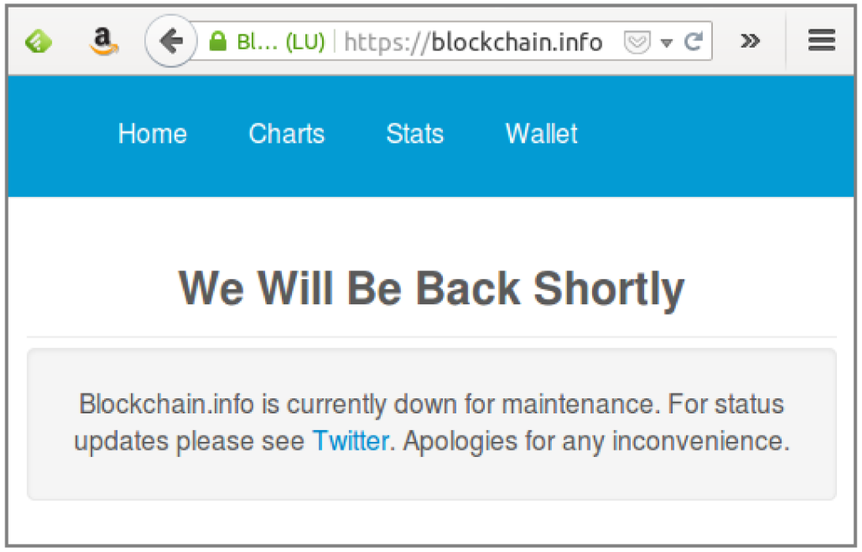
```
2015-06-15 10:06:57,670 |_________________ Request _________________|
/merchant/.../list

2015-06-15 10:06:57,866 |............... Response 200 ............|
{ "addresses" : [ ...
  {
    "address" : "1Adhj12349ajkhq04ghajafdfdhhf7864e",
    "balance" : 1500000,
    "label" : "steven",
    "total_received" : 1500000
  } ... ] }
```

Log, log, log . . .

```
2015-06-15 09:52:29,914 |_________________ Request _________________|
/merchant/.../new_address

2015-06-15 09:52:30,119 |.............. Response 200 ............|
{
  "address" : "1Adhj12349ajkhq04ghajafdfdhhf7864e",
  "label" : "steven"
}
2015-06-15 09:53:17,540 |_________________ Callback _________________|

  destination_address : [1Adhj12349ajkhq04ghajafdfdhhf7864e]
  confirmations : [0]
  address : [1Adhj12349ajkhq04ghajafdfdhhf7864e]
  value : [1500000]
  input_address : [1Adhj12349ajkhq04ghajafdfdhhf7864e]
  input_transaction_hash : [dbe33gad09078ghdghadasd234814767gajgjahegjhbvcn87164nbmbda51313d]
  transaction_hash : [dbe33gad09078ghdghadasd234814767gajgjahegjhbvcn87164nbmbda51313d]
....
2015-06-15 10:06:57,425 |_________________ Callback _________________|

  destination_address : [1Adhj12349ajkhq04ghajafdfdhhf7864e]
  confirmations : [2]
  address : [1Adhj12349ajkhq04ghajafdfdhhf7864e]
  value : [1500000]
  input_address : [1Adhj12349ajkhq04ghajafdfdhhf7864e]
  input_transaction_hash : [dbe33gad09078ghdghadasd234814767gajgjahegjhbvcn87164nbmbda51313d]
  transaction_hash : [dbe33gad09078ghdghadasd234814767gajgjahegjhbvcn87164nbmbda51313d]
```

QoS : Server Down, no JSON response to API call

```
2015-09-04 09:08:44,533 |.......... Response 500 ........|
<!DOCTYPE html>
<html>
...
<p class="well">
Blockchain.info is currently down for maintenance. For
status updates please see
<a href="https://twitter.com/#!/blockchain">Twitter</a>.
Apologies for any inconvenience.
</p>
...
<html>
```



HTTP status code 500 - Internal Server Error

- A generic error message, given when an unexpected condition was encountered and no more specific message is suitable.

QoS : Server Overload or Rate Limiting?

```
2015-09-10 20:15:55,552 |_________________ Request _________________|
/merchant/.../list
2015-09-10 20:15:55,645 |............... Response 429 ............|
Maximum concurrent requests for this endpoint reached. Please try again shortly.
```

- HTTP status code 429: Too Many Requests (RFC 6585)
  - The user has sent too many requests in a given amount of time. Intended for use with rate limiting schemes.
- But, maybe this is meant . . .
  - 503 Service Unavailable
    - The server is currently unavailable (because it is overloaded or down for maintenance). Generally, this is a temporary state.

QoS : Callback lags behind actual confirmation state

```
2015-09-11 21:55:08,432 |_________________ Callback _________________|

destination_address : [e3fjhadgfwuty123adgad163dga13ad23g]
confirmations : [0]
address : [e3fjhadgfwuty123adgad163dga13ad23g]
value : [420000]
input_address : [e3fjhadgfwuty123adgad163dga13ad23g]
input_transaction_hash : [jasghajsgga1687ghadgha109ghjgadg181tgkjadkjqh3khhakh444hdkh144h2]
transaction_hash : [jasghajsgga1687ghadgha109ghjgadg181tgkjadkjqh3khhakh444hdkh144h2]

...

2015-09-11 23:13:59,395 |_________________ Callback _________________|

destination_address : [e3fjhadgfwuty123adgad163dga13ad23g]
confirmations : [8]
address : [e3fjhadgfwuty123adgad163dga13ad23g]
value : [420000]
input_address : [e3fjhadgfwuty123adgad163dga13ad23g]
input_transaction_hash : [jasghajsgga1687ghadgha109ghjgadg181tgkjadkjqh3khhakh444hdkh144h2]
transaction_hash : [jasghajsgga1687ghadgha109ghjgadg181tgkjadkjqh3khhakh444hdkh144h2]
```

Lessons learned, or did we already knew that . . .

- No single payment method is perfect for every situation
  - Offer a broad spectrum of methods to choose from
  - Adopt a tailored mix in your organization
  - Evaluate each method in practice
- Hands-on is crucial before adopting new technology
  - Confront promises with harsh reality
  - Create a working solution, details *do* matter
- A solution delivered with poor QoS is no solution
  - Create fall-backs for Free (as in beer) on-line Services
  - "There ain't no such thing as a free lunch" or is there?

Bitcoin Payments: lessons learned

- Real-time pay-per-print is not feasible
  - No micro payment support
  - QoS insufficient
- Personal Account in SavaPage database is still needed
  - Low value BTC transactions have low risk
    - real-time charge of personal account is possible

What's next?

- **Pilots needed**
  - Please, do try this at your organization!
- Add more features
  - Charge backs
  - Fall-back Bitcoin Gateways
    - https://api.coinbase.com/v2/
- You are invited to visit our community
  - http://savapage.org/w/
  - https://gitlab.com/savapage
    - savapage-ext-blockchain-info