BITCOIN OFFLINE VAULT
SERVERLESS WALLET – BA.NET

How To Safeguard Your Bitcoins
With Your Own Offline Vault

May 2015

Bitcoin Offline Vault and Serverless Wallet - BA.net (c) ba.net
iphone@ba.net android@ba.net

Chapter 7 and portions of other chapters part of Bitcoin.org and Wikipedia.org with GNU Documentation License.

The optional software ba.net/bitcoin is licensed MIT open source and (c) ba.net

1 Why buy bitcoins? 9

1.1 Online shopping 9

1.2 Privacy 9

1. 3 Personal freedom 10

1.4 Financial independence 10

1.5 Limited quantity 10

2 Bitcoin Wallet BA.net 13

2.2 BA.net Bitcoin Web Wallet 13

2. 3 To Safeguard This Web Wallet 13

2. 4 Add Funds 13

2. 5 Check Your Balance 14

2. 6 Spend Your Bitcoins 14

2. 7 Advanced Multisig Wallet 14

2.8 Offline (or Air-Gapped) Bitcoin Transaction 15

3 Design Objectives 16

3.1 Private key loss is catastrophic 16

3.2 Mitigate risk by having more keys for shorter durations 16

3.4 Do not trust servers with your keys 17

3.5 Serverless Wallet Simplicity Advantage 17

3.6 Downloaded Wallets Limitations 18

4 Offline Bitcoin Transactions 19

4.1 Why Offline Bitcoin ? 19

4.1 What is an Offline Bitcoin Transaction ? 19

4.2 How do I create an offline transaction ? 20

4.4 Create your transaction on your offline machine 21

4.5 Submit the transaction to the Bitcoin network 22

4.6 Take Time to get Familiar with the Process 23

5 Unique Bitcoin Addresses 25

5.1 Bitcoin Addresses 25

6 Bitcoin Cold Storage 30

6.1 Paper Wallets 31

6.2 Brain Wallets **31**

6.3 Cold Storage / Hardware Wallets **32**

6.4 Offline Bitcoin Transaction *34*

6.5 How do I create an offline transaction ? *34*

7 Bitcoin Change Addresses Complexity **35**

Test Time *35*

Bitcoin is a Cash System *36*

Wallets Reinforce Misconceptions *37*

Wallets and Change Addresses *37*

Why Not Use the Same Address? *38*

Staying Safe *39*

Back to Alice and Bob *40*

Conclusions *40*

8 Bitcoin Security **41**

Security Principles *41*

8.1.1 Developing Bitcoin Systems Securely 42
8.1.2 The Root of Trust 43

User Security Best Practices *45*

8.1.3 Physical Bitcoin Storage 46
8.1.4 Hardware Wallets 46
8.1.5 Balancing Risk 47
8.1.6 Diversifying Risk 47
8.1.7 Multi-sig and Governance 47
8.1.8 Survivability 48
8.1.9 Conclusion 48

9 Frequently Asked Questions **49**

9.1.1 What is Bitcoin? 49
9.1.2 Who created Bitcoin? 49
9.1.3 Who controls the Bitcoin network? 50
9.1.4 How does Bitcoin work? 50
9.1.5 Is Bitcoin really used by people? 50
9.1.6 How does one acquire bitcoins? 51
9.1.7 How difficult is it to make a Bitcoin payment? 51
9.1.8 What are the advantages of Bitcoin? 52
9.1.9 What are the disadvantages of Bitcoin? 53
9.1.10 Why do people trust Bitcoin? 54
9.1.11 Can I make money with Bitcoin? 54
9.1.12 Is Bitcoin fully virtual and immaterial? 54
9.1.13 Is Bitcoin anonymous? 55
9.1.14 What happens when bitcoins are lost? 55
9.1.15 Can Bitcoin scale to become a major payment network? 55

Legal *56*

9.1.16 Is Bitcoin legal? 56
9.1.17 Is Bitcoin useful for illegal activities? 56

9.1.18 Can Bitcoin be regulated? 57
9.1.19 What about Bitcoin and taxes? 58
9.1.20 What about Bitcoin and consumer protection? 58

Economy *59*
9.1.21 How are bitcoins created? 59
9.1.22 Why do bitcoins have value? 59
9.1.23 What determines bitcoin's price? 60
9.1.24 Can bitcoins become worthless? 60
9.1.25 Is Bitcoin a bubble? 61
9.1.26 Is Bitcoin a Ponzi scheme? 61
9.1.27 Doesn't Bitcoin unfairly benefit early adopters? 61
9.1.28 Won't the finite amount of bitcoins be a limitation? 62
9.1.29 Won't Bitcoin fall in a deflationary spiral? 62
9.1.30 Isn't speculation and volatility a problem for Bitcoin? 63
9.1.31 What if someone bought up all the existing bitcoins? 63
9.1.32 What if someone creates a better digital currency? 64

Transactions *64*
9.1.33 Why do I have to wait 10 minutes? 64
9.1.34 How much will the transaction fee be? 64
9.1.35 What if I receive a bitcoin when my computer is powered off? 65
9.1.36 What does "synchronizing" mean and why does it take so long? 65

Mining *66*
9.1.37 What is Bitcoin mining? 66
9.1.38 How does Bitcoin mining work? 66
9.1.39 Isn't Bitcoin mining a waste of energy? 67
9.1.40 How does mining help secure Bitcoin? 68
9.1.41 What do I need to start mining? 68

Security *68*
9.1.42 Is Bitcoin secure? 68
9.1.43 Hasn't Bitcoin been hacked in the past? 68
9.1.44 Could users collude against Bitcoin? 69
9.1.45 Is Bitcoin vulnerable to quantum computing? 70

10 Bitcoin Wikipedia 71

10.1.1 Block chain 71
10.1.2 Units 71
10.1.3 Ownership 72
10.1.4 Transactions 72
10.1.5 Mining 73
10.1.5.1 Practicalities 74
10.1.6 Supply 75
10.1.7 Transaction fees 75
10.1.8 Wallets 75
10.1.8.1 Reference implementation 76
10.1.9 Privacy 76
10.1.10 Fungibility 77

History *77*

Economics *79*
10.1.11 Classification 79
10.1.12 Buying and selling 79

10.1.13 Price and volatility 80
10.1.14 Speculative bubble dispute 80
10.1.15 Ponzi scheme dispute 80
10.1.16 Value forecasts 81
10.1.17 Bitcoin obituaries 81
10.1.18 Reception 81
10.1.19 Acceptance by merchants 82
10.1.19.1 Mainstream use of bitcoin 82
10.1.20 Financial institutions 82
10.1.21 As investment 83
10.1.22 Venture capital 83
10.1.23 Political economy 83

Legal status and regulation *83*
10.1.24 Australia 84
10.1.25 China 84
10.1.26 European Union 84
10.1.27 Iceland 84
10.1.28 Russia 84
10.1.29 Taiwan 84
10.1.30 Thailand 84
10.1.31 United States 84
10.1.32 Vietnam 85

Criminal activity *85*
10.1.33 Theft 86
10.1.34 Black markets 86
10.1.35 Money laundering 87
10.1.36 Ponzi scheme 87
10.1.37 Malware 87
10.1.37.1 Unauthorized mining 87
10.1.37.2 Malware stealing 88
10.1.37.3 Ransomware 88

Security *88*
10.1.38 Unauthorized spending 89
10.1.39 Double spending 89
10.1.40 Race attack 89
10.1.41 History modification 90
10.1.42 Selfish mining 91
10.1.43 Deanonymisation of clients 91

Non-bitcoin applications of the block chain *91*

Block chain spam *92*

In the media *92*

11 History of Bitcoin 93

Contents *93*

Pre-history *94*

Creation *94*

Growth *95*

Prices and value history *97*

Satoshi Nakamoto *99*
The fork of March 2013 ..... *100*
Regulatory issues *100*
Theft and exchange shutdowns *102*
Taxation and regulation *103*
Sports sponsorship *104*

12 PGP quick start **105**
Getting started *105*
12.1.1 Key pair generation 105
12.1.2 Key extraction 105
Simple usage *107*
12.1.3 Signing a plaintext message 107
12.1.4 Sending an encrypted message 107

13 Beginners' Guide To PGP **110**

14 Proof Of Work System **126**
Background *126*
Variants *127*
List of proof-of-work functions *129*
Reusable proof-of-work as e-money *129*
Notes *130*

15 Pretty Good Privacy (PGP) **131**
Design *132*
15.1.1 Compatibility 133
15.1.2 Confidentiality 133
15.1.3 Digital signatures 133
15.1.4 Web of trust 133
15.1.5 Certificates 135
15.1.6 Security quality 135
History *137*
15.1.7 Early history 137
15.1.8 Criminal investigation 138
15.1.9 PGP 3 and founding of PGP Inc. 139
15.1.10 Network Associates acquisition 140
15.1.11 Current situation 141
PGP Corporation encryption applications *141*
OpenPGP *143*

16 Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto **145**
16.1.1.1 October 31, 2008 145
Abstract *145*

1. Introduction *145*
2. Transactions *146*
3. Timestamp Server *147*
4. Proof-of-Work *147*
5. Network *148*
6. Incentive *149*
7. Reclaiming Disk Space *150*
8. Simplified Payment Verification *150*
9. Combining and Splitting Value *151*
10. Privacy *152*
11. Calculations *152*
12. Conclusion *155*
References *155*

1 WHY BUY BITCOINS?

Many people have heard of Bitcoin, but far fewer understand why someone would want to buy bitcoins. "What is it used for?", "Why not use a credit card?" and other questions are common. So, here are the main reasons people just like you buy bitcoins.

1.1 ONLINE SHOPPING

Buying products and services online is often cheaper, faster, and results in higher overall customer satisfaction than other options. Unfortunately, credit cards and paypal can put limitations on what you can buy, from where. Growing costs paid to combat fraud and identity theft are passed onto you when you use them but are largely eliminated with Bitcoin.

1.2 PRIVACY

Identity theft is among the greatest costs to society. To combat identity theft, people subscribe to identity protection services and online shops require lots of personal info. Bitcoin payments can be trusted by the shop with no additional personal information. That means, unless you're getting something shipped to you, you may not even need to provide your name or address when shopping. Bitcoin is not anonymous but if additional steps are taken, nobody but you and the merchant are likely to know what you buy online.

1. 3 PERSONAL FREEDOM

Nobody can limit who you send your bitcoins to. Visa, Mastercard, and PayPal block payments to perfectly legal businesses, some political organizations, and to anyone that may bring them legal or PR problems. Bitcoin payment is a protocol that doesn't care who you're paying or why.

1.4 FINANCIAL INDEPENDENCE

When handled securely, Bitcoin can be even better than gold for savings. The exchange rate of early Bitcoin versus other currencies is volatile. If Bitcoin is successful at growing in usage, most of that volatility will increase its price and make you money. The fact remains that your bitcoins cannot be bailed-in or seized without your cooperation. You can even store bitcoin using a password that only you know. This places more power back in your hands to become financially independent.

1.5 LIMITED QUANTITY

There will only ever be twenty-one million bitcoins as sure as we all agree that 2 + 2 = 4. Contrast this with central banks around the world that create money with the click of a mouse. Bitcoin reduces monetary policy to a straightforward schedule.

1.6 Current and Future Valuation of Bitcoin

We argue that Bitcoin is currently not primarily valued as a medium of exchange or transactional currency, but as a gold-like store of value and speculative investment (an excellent one, if you agree with Peter Thiel that it has a 20% chance of going mainstream - a 20% chance of 100x or 1000x growth), and why this is not a bad thing.

It is important to distinguish between the reason for Bitcoin's present valuation and the reasons it will likely be valued in the future. For example, the fact that Bitcoin will probably save online retailers a lot of of money in the future makes Bitcoin valuable not as a currency now, but as an investment now and a currency in the future. It is easy to misinterpret the fact that its *future* as a currency is largely what is driving its current valuation to mean that it is right now, today, valued largely because it enables transactions. People buying bitcoins now because they believe they will be sought out for transactional purposes *in the future* is not the same as people buying bitcoins now because they are sought out for transactional purposes *now*.

Investors who understand Bitcoin's potential do it an important service. They inform the public, through price information, of that which most of the public is unable or unwilling to figure out on their own: that Bitcoin has tremendous potential to change the world and warrants serious attention, both currently for certain people as a hide-able, unconfiscate-able, transportable, no-third-party-risk store of wealth and in the future for everyone as a transactional currency.

Just because it turned out to be better for the "store of value" function first is no reason to worry overly about the transactional function taking time to blossom - that's what investors are for. The ones that invest based on a sound assessment of Bitcoin's future potential serve as a proxy for actual present commercial adoption by boosting the price in the present to a degree commensurate with how likely commercial adoption will be to take hold in the future.

Prematurely using commercial adoption as a measuring stick for Bitcoin's success doesn't really make much sense. Bitcoin is a many-splendored thing, and is valued by investors for both its current and future uses.

2 BITCOIN WALLET BA.NET

2.1 A Bitcoin Wallet

A Bitcoin wallet is as simple as a single pair of a Bitcoin address with its private key. A wallet has been generated for you in your web browser and is displayed above.

2.2 BA.NET BITCOIN WEB WALLET

The easiest way to send a receive bitcoins without installing any software. No need to register username, email or any info.

Create a Bitcoin address, private key, experiment, test away. All code runs on your own web browser and does not depend on any central server. You are in control.

2. 3 TO SAFEGUARD THIS WEB WALLET

You must print or record the Bitcoin address and private key. You can use the My Address Webapp.

Make a backup copy of the private key and store it in a safe, separate location. This site does not have knowledge of your private key.

If you leave/refresh the site or press the "Generate New Address" button then a new private key will be generated and the previously displayed private key will be lost.

2. 4 ADD FUNDS

Add funds to this wallet by telling people to send bitcoins to your Bitcoin address. Make sure you made a backup copy of the private key.

2. 5 CHECK YOUR BALANCE

You can check your balance using the BA.net Bitcoin Web Wallet or by going to blockexplorer.com and enter your Bitcoin address.

2. 6 SPEND YOUR BITCOINS

Spend your Bitcoins using the Send Bitcoin Option.

Remaining change will be sent back to the sending bitcoin address (source address). Simple.

The amount of bitcoins you can spend will be checked before sending. Use the view history button for details. If the address has transactions pending with 0 confirmations, you will have to wait to send funds. 1 confirmation is enough to send bitcoins.

You can set the miner transaction fee to any value you choose. or 0.

2. 7 ADVANCED MULTISIG WALLET

You can create a private key with 3 components. Send the 3 components to 3 friends. And 2 friends are required to create an usable private key to spend the bitcoins. Also called split wallet.

Click on Multisig for split wallets and more advanced features. Cold Storage, Paper Wallet, Brain Wallet, BIP38 Encrypt, Bulk Wallet, Vanity Wallet and more.

If you don't have the private key, you don't own Bitcoin. Be your own bank Design Objective.

2.8 OFFLINE (OR AIR-GAPPED) BITCOIN TRANSACTION

An offline Bitcoin transaction is created with a computer that is not connected to the Internet (or any network). Assuming the installation process was secure the computer can not be reached by hackers.

3 DESIGN OBJECTIVES

If you don't have the private key, you don't own Bitcoin. If you store the key on someone else's server, even if encrypted, your key is not safe. Be you own bank.

3.1 PRIVATE KEY LOSS IS CATASTROPHIC

The primary problem is that losing a key means that all bitcoins stored with that key are lost forever. The way to deal with this is: Create keys frequently and destroy them as soon as they are no longer needed

3.2 MITIGATE RISK BY HAVING MORE KEYS FOR SHORTER DURATIONS

A more secure mitigation against key loss is to generate new addresses/keys frequently, use them for specific operations, and then destroy them.

For example, when traveling, create a new **Travel Key** and use that until you are back home. That way if anyone compromises your travel laptop or phone they only breach the compartment for the duration of your travel.

The impact of the compromise is contained by the limitation on the utility of the key.

For storing bitcoins create a cold paper wallet. You can create your address/key on a computer with no Internet connection. Air-gap computer running the ba.net serverless wallet.

3.3 Why use Offline Bitcoin ?

Computer security is hard. Physical security is much easier to accomplish.

Using Offline Bitcoin allows you to store your wealth securely in an offline vault. Your own vault that you control physically.

You can transfer needed amounts to online wallets on your phone or computer. Bitcoin is just like cash, you should only carry around spending money.

3.4 DO NOT TRUST SERVERS WITH YOUR KEYS

If you don't have the private key, you don't own Bitcoin. If you store the key on someone else's server, even if encrypted, your key is not safe. Be you own bank.

Backup your keys in different locations. You can keep them encrypted with a password.

3.5 SERVERLESS WALLET SIMPLICITY ADVANTAGE

Spend Your Bitcoins using the Send Bitcoin Option. Remaining change will be sent back to the sending bitcoin address (source address).

This allows you to make the backup of your key at the creation time only. As opposed to, backing up your wallet all the time on a downloaded wallet. Downloaded wallets create a new change address for each transaction. This is the reason for confusion and the need of constant backups.

The BA.net serverless Wallet needs only one backup when you create it!

3.6 DOWNLOADED WALLETS LIMITATIONS

You can download a bitcoin client and import your private key. Note that on downloaded bitcoin clients, usually remaining change goes to a new address. That is why Satoshi recommended never to delete a wallet!

3.7 Bitcoin Address and Private Key Reuse

When you reuse your Bitcoin Address you reveal your balance and transaction history of that address to your counterparty. Losing financial privacy.

Another un-desirable problem is that for each use there is a hash signature on the blockchain generated with the private key. There is a theoretical attack exploting information from this signatures. This attack has not been seen yet, but it could be possible.

So both for privacy and security, bitcoin addresses should not be reused. Especially for large amounts of coins.

4 OFFLINE BITCOIN TRANSACTIONS

4.1 WHY OFFLINE BITCOIN ?

Computer security is hard. Physical security is much easier to accomplish.

Using Offline Bitcoin allows you to store your wealth securely in an offline vault. Your own vault that you control physically.

You can transfer needed amounts to online wallets on your phone or computer. Bitcoin is just like cash, you should only carry around spending money.

4.1 WHAT IS AN OFFLINE BITCOIN TRANSACTION ?

An offline Bitcoin transaction is created with a computer that is not connected to the internet (or any network). Assuming the installation process was secure the computer can not be reached by hackers.

To create a Bitcoin payment the offline machine can create a Bitcoin transaction which can then be carried by an USB key. This information can then be copied to a machine that is online, and the transaction can be broadcast.

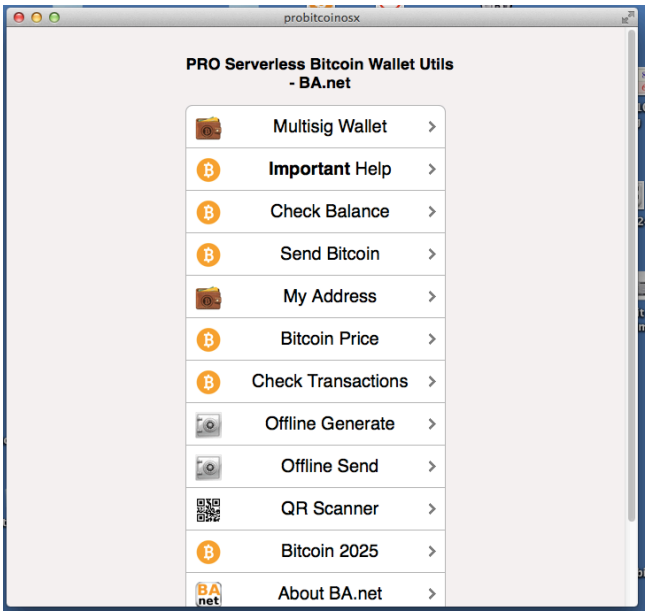
Your private key never touches the Internet. Maximum Security.

4.2 HOW DO I CREATE AN OFFLINE TRANSACTION ?

Use the PRO Bitcoin Wallet and Vault BA.net App. Search for “banet” at the Apple AppStore for OSX.

Also available on iPhone, iPad, or Flashboot Software Appliance

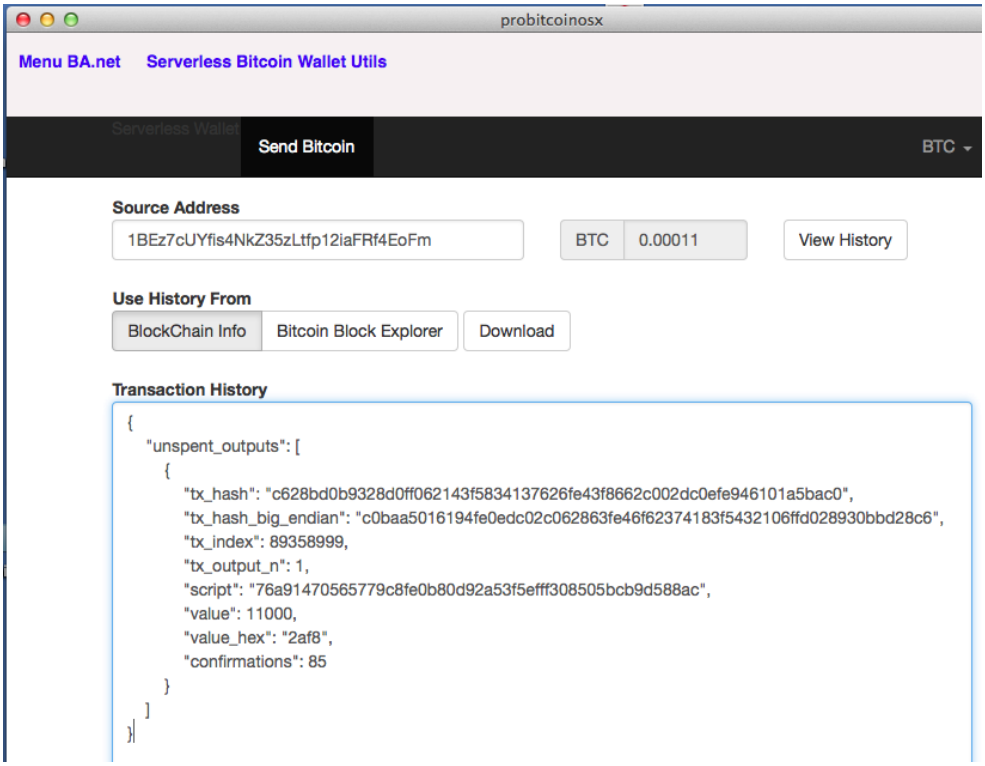
Featured by Apple on top 10 Finance Apps



4.3 Retrieve Unspent Outputs

Retrieve the unspent outputs for your bitcoin address. Use the button Send Bitcoin (the regular online send bitcoin) paste your source address and **click view history**

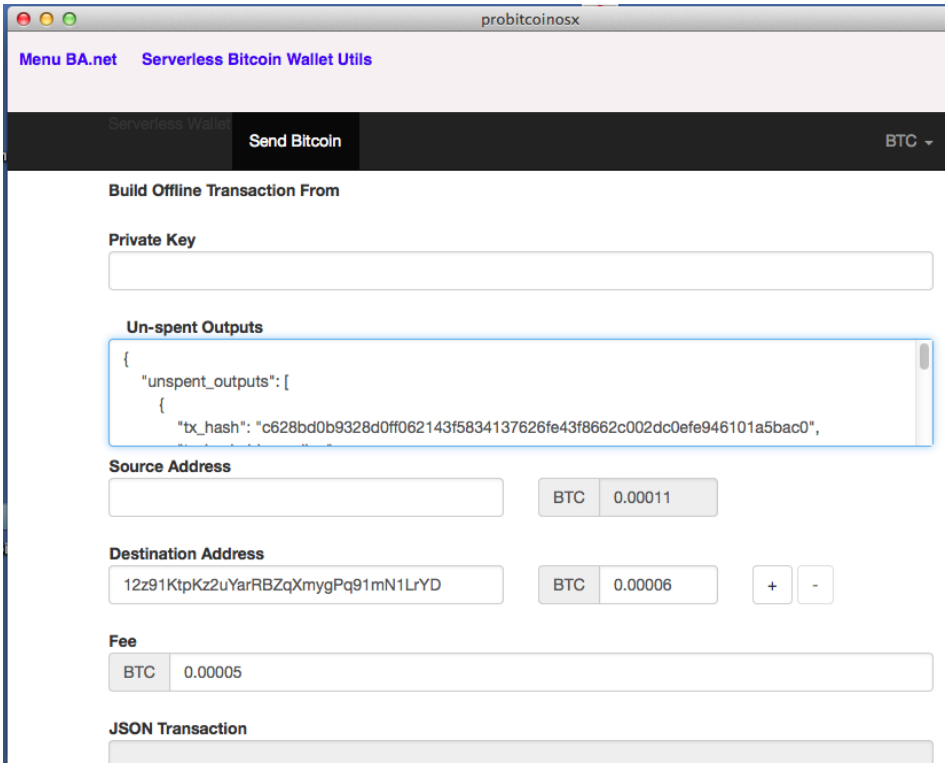
You need to cut and paste this info into a text file and transfer it to the USB key.



4.4 CREATE YOUR TRANSACTION ON YOUR OFFLINE MACHINE

Use the button **Offline Generate**.

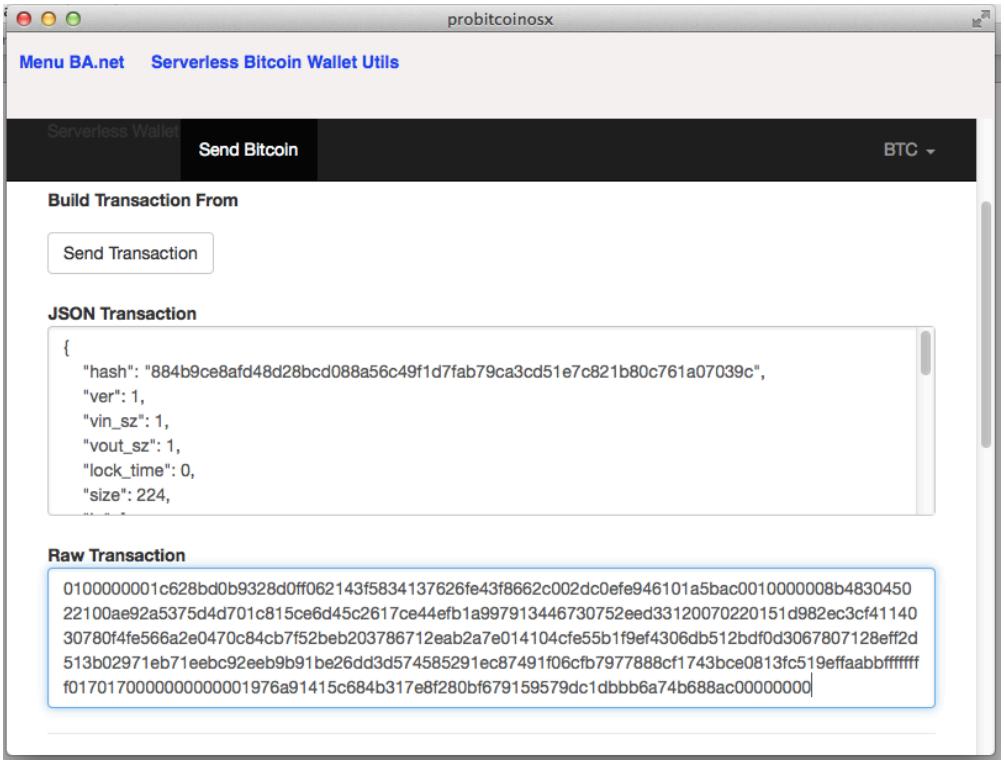
To do this you will need the private key of the address you want to send from, destination address and the amount you want to send.



Cut and Paste the values into the form and generate a transaction. Cut and the paste the generated transaction RAW HEX from the form field into a text file and place it on your USB key.

4.5 SUBMIT THE TRANSACTION TO THE BITCOIN NETWORK

Use the button **Offline Send**.



At no point in this process is the private key data exposed through the transaction data. Your private key never touches the internet, for maximum security.

The biggest threat to an offline wallet is an USB-key virus that executes when plugged in. However, such viruses would have to be highly targeted, and can be mostly mitigated by disabling USB-auto-run on the offline computer.

Alternatively, you can transfer this information using the new QR Code Generator Option. No networking of any kind needed.

4.6 TAKE TIME TO GET FAMILIAR WITH THE PROCESS

It is normal to be uneasy using new software to store your savings, especially with advanced features. Make a few offline transactions with new addresses/keys and small amounts of bitcoins.

After a couple of offline transactions you will be doing them in less than a minute. You will be able to say that you are your own bank!

4.7 Bitcoin Address and Private Key Reuse

When you reuse your Bitcoin Address you reveal your balance and transaction history of that address to your counterparty. Losing financial privacy.

Another un-desirable problem is that for each use there is a hash signature on the blockchain generated with the private key. There is a theoretical attack exploting information from this signatures. This attack has not been seen yet, but it could be possible.

So both for privacy and security, bitcoin addresses should not be reused. Especially for large amounts of coins.

For offline cold wallet storage the simplicity of having only one address/key to backup is important. As well as not having any more change addresses to add complexity. Once the coins come out of cold storage it is best practice not to reuse addresses.

5 UNIQUE BITCOIN ADDRESSES

5.1 BITCOIN ADDRESSES

Bitcoins are 'stored' in something called **bitcoin addresses** - they look something like
this: 1j2m5TakK99HvJUTfg2b2b8EGWQenmdTh. There are two parts to a bitcoin address – the public key (commonly just called the address) and the private key – the important part that lets you spend the bitcoins on its corresponding public key. Bitcoin is an example of public key encryption, as you can give out the public key freely but you must keep the private key to yourself.

To send bitcoins to an address, a message is broadcast from the owner of the sending address to the network that X amount of coins from that address now belong to the new address. This operation is authorized by the sender's private key, and if he doesn't have the private key he can't spend the coins, plain and simple.

BItcoin addresses are created by first picking a random number (for the all important key) and creating an ECDSA (Elliptic Curve Digital Signature Algorithm) public / private key pair with them. This operation alone generates the private key – but Bitcoin addresses are not simply public keys, but rather modified versions of them. The generated public key is then put through several SHA-256 and RIPEMD-160 operations, until eventually being converted into a format called Base-58. Base 58 is an encoding that removes the possibility of similar looking characters, such as lowercase L and uppcase I, as well as 0 and O. Finally an identifying number is added to the beginning of the address – for most bitcoin addresses, this is generally 1, indicating it is a public bitcoin network address.

It is infeasible though technically possible that two different people could generate the same bitcoin address. In such a case, both would be able to spend the coins on that particular address. The odds of this