
**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	<i>Online shopping</i>	9
1.2	<i>Privacy</i>	9
1.3	<i>Personal freedom</i>	10
1.4	<i>Financial independence</i>	10
1.5	<i>Limited quantity</i>	10
2	Bitcoin Wallet BA.net	13
2.2	<i>BA.net Bitcoin Web Wallet</i>	13
2.3	<i>To Safeguard This Web Wallet</i>	13
2.4	<i>Add Funds</i>	13
2.5	<i>Check Your Balance</i>	14
2.6	<i>Spend Your Bitcoins</i>	14
2.7	<i>Advanced Multisig Wallet</i>	14
2.8	<i>Offline (or Air-Gapped) Bitcoin Transaction</i>	15
3	Design Objectives	16
3.1	<i>Private key loss is catastrophic</i>	16
3.2	<i>Mitigate risk by having more keys for shorter durations</i>	16
3.4	<i>Do not trust servers with your keys</i>	17
3.5	<i>Serverless Wallet Simplicity Advantage</i>	17
3.6	<i>Downloaded Wallets Limitations</i>	18
4	Offline Bitcoin Transactions	19
4.1	<i>Why Offline Bitcoin ?</i>	19
4.1	<i>What is an Offline Bitcoin Transaction ?</i>	19
4.2	<i>How do I create an offline transaction ?</i>	19
4.3	<i>Create your transaction on your offline machine</i>	21
4.4	<i>Submit the transaction to the Bitcoin network</i>	22
4.5	<i>Take Time to get Familiar with the Process</i>	23
5	Unique Bitcoin Addresses	25
5.1	<i>Bitcoin Addresses</i>	25
6	Bitcoin Cold Storage	28
6.1	<i>Paper Wallets</i>	29
6.2	<i>Brain Wallets</i>	29

6.3	Cold Storage / Hardware Wallets	30
6.4	<i>Offline Bitcoin Transaction</i>	32
6.5	<i>How do I create an offline transaction ?</i>	32
7	Bitcoin Change Addresses Complexity	33
	<i>Test Time</i>	33
	<i>Bitcoin is a Cash System.....</i>	34
	<i>Wallets Reinforce Misconceptions.....</i>	35
	<i>Wallets and Change Addresses.....</i>	35
	<i>Why Not Use the Same Address?.....</i>	36
	<i>Staying Safe</i>	37
	<i>Back to Alice and Bob</i>	38
	<i>Conclusions</i>	38
8	Bitcoin Security	39
	<i>Security Principles.....</i>	39
8.1.1	Developing Bitcoin Systems Securely.....	40
8.1.2	The Root of Trust	41
	<i>User Security Best Practices</i>	43
8.1.3	Physical Bitcoin Storage.....	44
8.1.4	Hardware Wallets.....	44
8.1.5	Balancing Risk.....	45
8.1.6	Diversifying Risk.....	45
8.1.7	Multi-sig and Governance	45
8.1.8	Survivability	46
8.1.9	Conclusion	46
9	Frequently Asked Questions	47
9.1.1	What is Bitcoin?	47
9.1.2	Who created Bitcoin?	47
9.1.3	Who controls the Bitcoin network?.....	48
9.1.4	How does Bitcoin work?.....	48
9.1.5	Is Bitcoin really used by people?	48
9.1.6	How does one acquire bitcoins?.....	49
9.1.7	How difficult is it to make a Bitcoin payment?.....	49
9.1.8	What are the advantages of Bitcoin?	50
9.1.9	What are the disadvantages of Bitcoin?	51
9.1.10	Why do people trust Bitcoin?	52
9.1.11	Can I make money with Bitcoin?	52
9.1.12	Is Bitcoin fully virtual and immaterial?.....	52
9.1.13	Is Bitcoin anonymous?	53
9.1.14	What happens when bitcoins are lost?.....	53
9.1.15	Can Bitcoin scale to become a major payment network?.....	53
	<i>Legal.....</i>	54
9.1.16	Is Bitcoin legal?.....	54
9.1.17	Is Bitcoin useful for illegal activities?.....	54

9.1.18	Can Bitcoin be regulated?.....	55
9.1.19	What about Bitcoin and taxes?	56
9.1.20	What about Bitcoin and consumer protection?.....	56
<i>Economy</i>		57
9.1.21	How are bitcoins created?.....	57
9.1.22	Why do bitcoins have value?.....	57
9.1.23	What determines bitcoin's price?	58
9.1.24	Can bitcoins become worthless?.....	58
9.1.25	Is Bitcoin a bubble?.....	59
9.1.26	Is Bitcoin a Ponzi scheme?.....	59
9.1.27	Doesn't Bitcoin unfairly benefit early adopters?.....	59
9.1.28	Won't the finite amount of bitcoins be a limitation?	60
9.1.29	Won't Bitcoin fall in a deflationary spiral?	60
9.1.30	Isn't speculation and volatility a problem for Bitcoin?.....	61
9.1.31	What if someone bought up all the existing bitcoins?.....	61
9.1.32	What if someone creates a better digital currency?	62
<i>Transactions</i>		62
9.1.33	Why do I have to wait 10 minutes?.....	62
9.1.34	How much will the transaction fee be?.....	62
9.1.35	What if I receive a bitcoin when my computer is powered off?.....	63
9.1.36	What does "synchronizing" mean and why does it take so long?	63
<i>Mining</i>		64
9.1.37	What is Bitcoin mining?	64
9.1.38	How does Bitcoin mining work?	64
9.1.39	Isn't Bitcoin mining a waste of energy?	65
9.1.40	How does mining help secure Bitcoin?	66
9.1.41	What do I need to start mining?.....	66
<i>Security</i>		66
9.1.42	Is Bitcoin secure?	66
9.1.43	Hasn't Bitcoin been hacked in the past?.....	66
9.1.44	Could users collude against Bitcoin?.....	67
9.1.45	Is Bitcoin vulnerable to quantum computing?	68
10	Bitcoin Wikipedia	69
10.1.1	Block chain	69
10.1.2	Units.....	69
10.1.3	Ownership	70
10.1.4	Transactions	70
10.1.5	Mining	71
10.1.5.1	Practicalities	72
10.1.6	Supply.....	73
10.1.7	Transaction fees.....	73
10.1.8	Wallets	73
10.1.8.1	Reference implementation	74
10.1.9	Privacy	74
10.1.10	Fungibility.....	75
<i>History</i>		75
<i>Economics</i>		77
10.1.11	Classification	77
10.1.12	Buying and selling	77

10.1.13	Price and volatility	78
10.1.14	Speculative bubble dispute	78
10.1.15	Ponzi scheme dispute.....	78
10.1.16	Value forecasts.....	79
10.1.17	Bitcoin obituaries.....	79
10.1.18	Reception.....	79
10.1.19	Acceptance by merchants	80
10.1.19.1	Mainstream use of bitcoin	80
10.1.20	Financial institutions.....	80
10.1.21	As investment.....	81
10.1.22	Venture capital	81
10.1.23	Political economy	81
<i>Legal status and regulation</i>		<i>81</i>
10.1.24	Australia.....	82
10.1.25	China.....	82
10.1.26	European Union	82
10.1.27	Iceland.....	82
10.1.28	Russia.....	82
10.1.29	Taiwan	82
10.1.30	Thailand.....	82
10.1.31	United States.....	82
10.1.32	Vietnam.....	83
<i>Criminal activity.....</i>		<i>83</i>
10.1.33	Theft.....	84
10.1.34	Black markets.....	84
10.1.35	Money laundering.....	85
10.1.36	Ponzi scheme.....	85
10.1.37	Malware.....	85
10.1.37.1	Unauthorized mining.....	85
10.1.37.2	Malware stealing.....	86
10.1.37.3	Ransomware	86
<i>Security.....</i>		<i>86</i>
10.1.38	Unauthorized spending	87
10.1.39	Double spending.....	87
10.1.40	Race attack.....	87
10.1.41	History modification	88
10.1.42	Selfish mining.....	89
10.1.43	Deanonymisation of clients.....	89
<i>Non-bitcoin applications of the block chain.....</i>		<i>89</i>
<i>Block chain spam.....</i>		<i>90</i>
<i>In the media</i>		<i>90</i>
11	History of Bitcoin.....	91
<i>Contents.....</i>		<i>91</i>
<i>Pre-history.....</i>		<i>92</i>
<i>Creation.....</i>		<i>92</i>
<i>Growth.....</i>		<i>93</i>
<i>Prices and value history.....</i>		<i>95</i>

<i>Satoshi Nakamoto</i>	97
<i>The fork of March 2013</i>	98
<i>Regulatory issues</i>	98
<i>Theft and exchange shutdowns</i>	100
<i>Taxation and regulation</i>	101
<i>Sports sponsorship</i>	102
12 PGP quick start	103
<i>Getting started</i>	103
12.1.1 Key pair generation.....	103
12.1.2 Key extraction.....	103
<i>Simple usage</i>	105
12.1.3 Signing a plaintext message.....	105
12.1.4 Sending an encrypted message.....	105
13 Beginners' Guide To PGP	108
14 Proof Of Work System	124
<i>Background</i>	124
<i>Variants</i>	125
<i>List of proof-of-work functions</i>	127
<i>Reusable proof-of-work as e-money</i>	127
<i>Notes</i>	128
15 Pretty Good Privacy (PGP)	129
<i>Design</i>	130
15.1.1 Compatibility.....	131
15.1.2 Confidentiality.....	131
15.1.3 Digital signatures.....	131
15.1.4 Web of trust.....	131
15.1.5 Certificates.....	133
15.1.6 Security quality.....	133
<i>History</i>	135
15.1.7 Early history.....	135
15.1.8 Criminal investigation.....	136
15.1.9 PGP 3 and founding of PGP Inc.	137
15.1.10 Network Associates acquisition.....	138
15.1.11 Current situation.....	139
<i>PGP Corporation encryption applications</i>	139
<i>OpenPGP</i>	141
16 Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto	143
16.1.1.1 October 31, 2008.....	143
<i>Abstract</i>	143

<i>1. Introduction</i>	143
<i>2. Transactions</i>	144
<i>3. Timestamp Server</i>	145
<i>4. Proof-of-Work</i>	145
<i>5. Network</i>	146
<i>6. Incentive</i>	147
<i>7. Reclaiming Disk Space</i>	148
<i>8. Simplified Payment Verification</i>	148
<i>9. Combining and Splitting Value</i>	149
<i>10. Privacy</i>	150
<i>11. Calculations</i>	150
<i>12. Conclusion</i>	153
<i>References</i>	153

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 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 hideable, 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 exploiting 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.

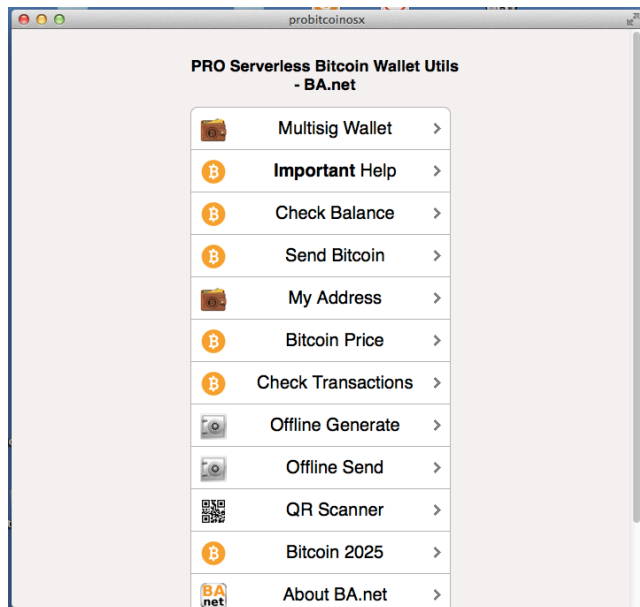
4.2 HOW DO I CREATE AN OFFLINE TRANSACTION ?

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](#)



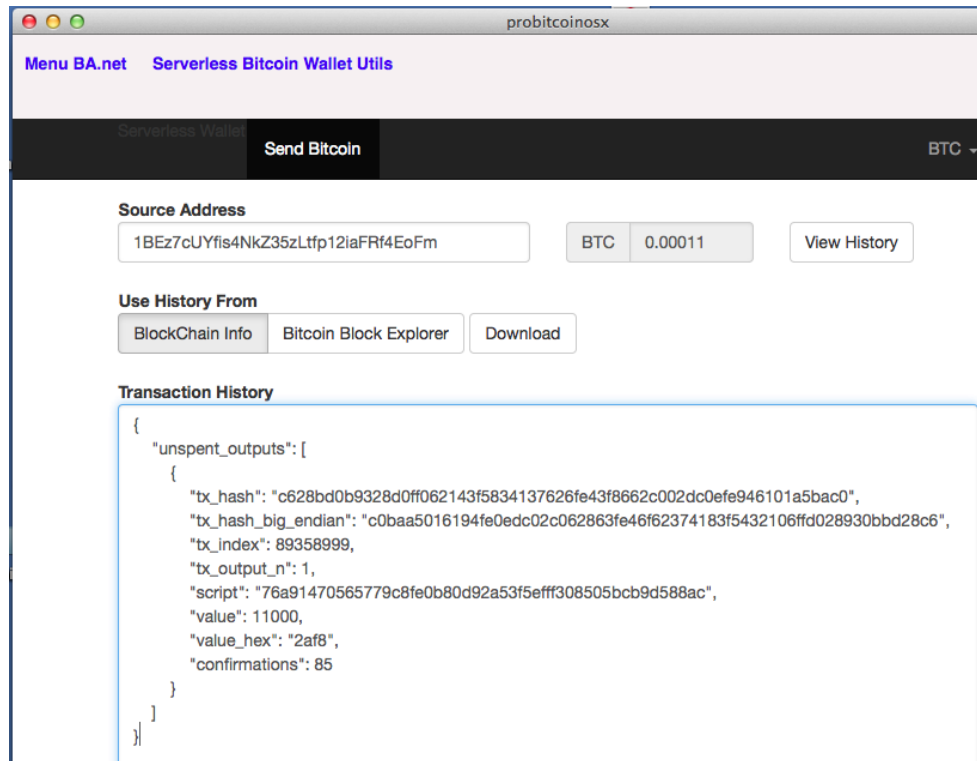
Featured by Apple on top 100 Finance Apps



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.

probitcoinsx

Menu BA.net Serverless Bitcoin Wallet Utiils

Serverless Wallet Send Bitcoin BTC

Build Offline Transaction From

Private Key

Un-spent Outputs

```
{
  "unspent_outputs": [
    {
      "tx_hash": "c628bd0b9328d0ff062143f5834137626fe43f8662c002dc0efe946101a5bac0",

```

Source Address

BTC 0.00011

Destination Address

12z91KtpKz2uYarRBZqXmygPq91mN1LrYD

BTC 0.00006 + -

Fee

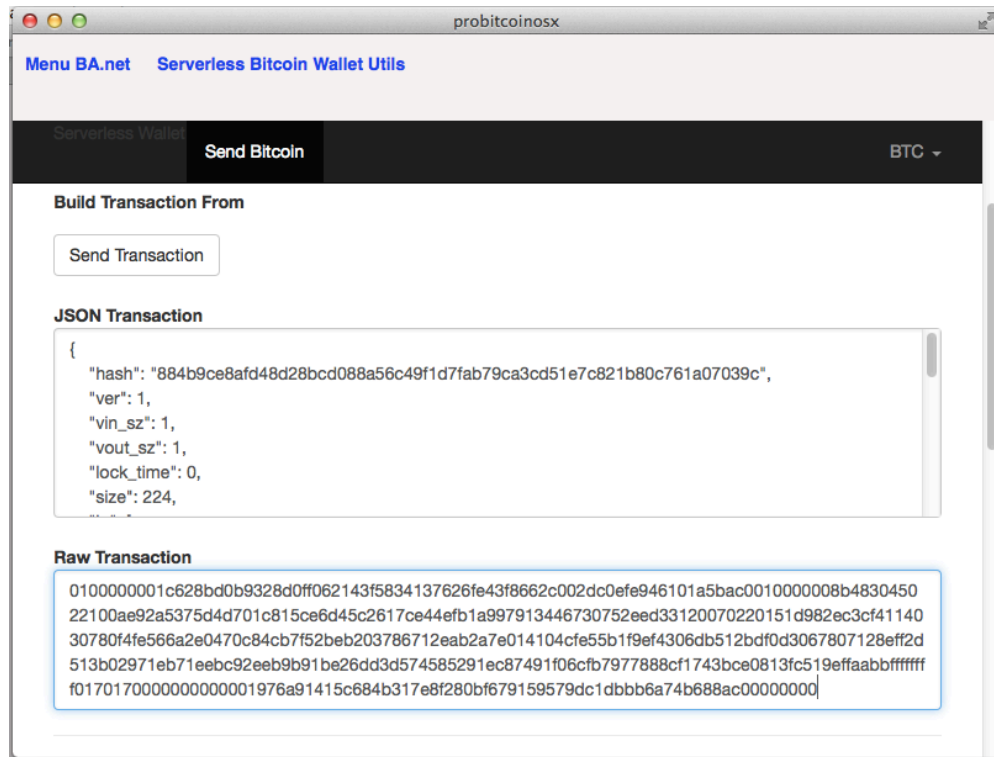
BTC 0.00005

JSON Transaction

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 exploiting 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 uppercase 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

happening are however so small that it is not going to happen in the next couple million years. If you're skeptical, read [Why is \$2^{256}\$ Secure](#) for a stern talking to regarding the security and wonders of exponential growth.

5.2 Why is 2^{256} Secure

There's always a lot of talk about the security of modern cryptographic hash functions, mainly SHA-256. This is a hash function used to verify a lot of important stuff – modern website logins are hashed with it, and Bitcoin relies on it almost entirely. There's always a lot of confusion regarding the safety of the function – as we know in the past things are found to be insecure after being declared 'absolutely secure' a few years prior to them being broken. Why is this particular iteration of hash functions so perfect?

The main problem with this idea is how poorly the human mind can understand the exponential function. Our brains can wrap around the concepts of addition and multiplication fine – but when we get to exponents our minds have trouble wrapping our heads around how quickly numbers get unimaginably big.

So what exactly is 2^{256} ? Well, if we're being technical...

2115792089237316195423570985008687907853269984665
640564039457584007913129639936

So – for all those doubting the security of 2^{256} collision chances, there's the number: There is a 1 in over 115 quattuorvigintillion (that's a 78 digit number) chance of finding a collision. Note: In practice it's actually SLIGHTLY higher than that, due to something called the birthday problem, however the difference is so abysmal that it's hardly worth accounting for.