BITCOIN OFFLINE VAULT
SERVERLESS WALLET – BA.NET

**How To Safeguard Your Bitcoins
With Your Own Offline Vault**

May 2015

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 CATASTROFIC

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 Serverless Wallet and Vault BA.net App. Search for "banet" at the Apple AppStore for iOS or the MacStore for OSX
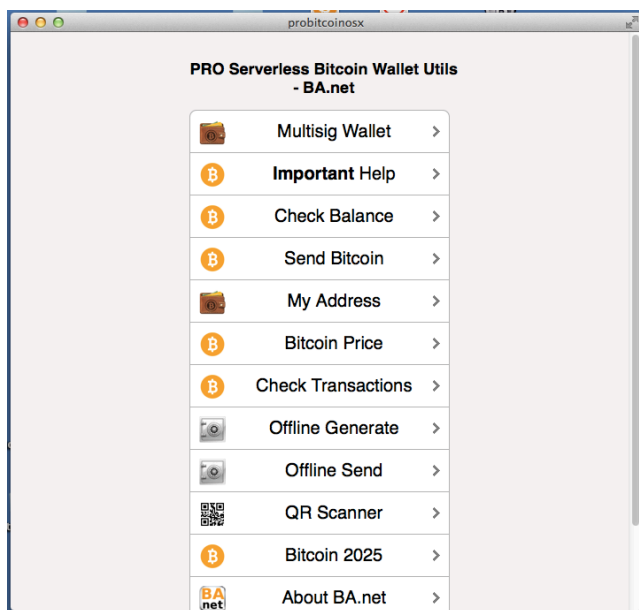
· 2. Retrieve the unspent outputs for your bitcoin address. Use the button Send Bitcoin (the regular online send bitcoin) paste your source address and **click view history**

You need to cut and paste this info into a text file and transfer it to the USB key.
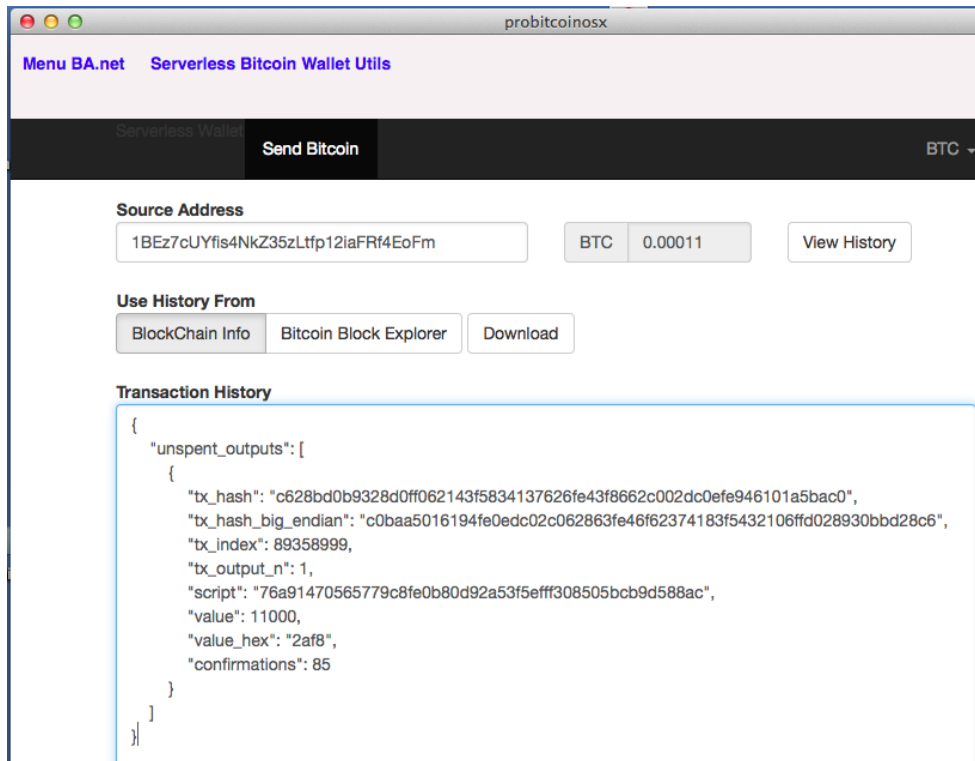
4.3 CREATE YOUR TRANSACTION ON YOUR OFFLINE MACHINE

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.

4.4 SUBMIT THE TRANSACTION TO THE BITCOIN NETWORK

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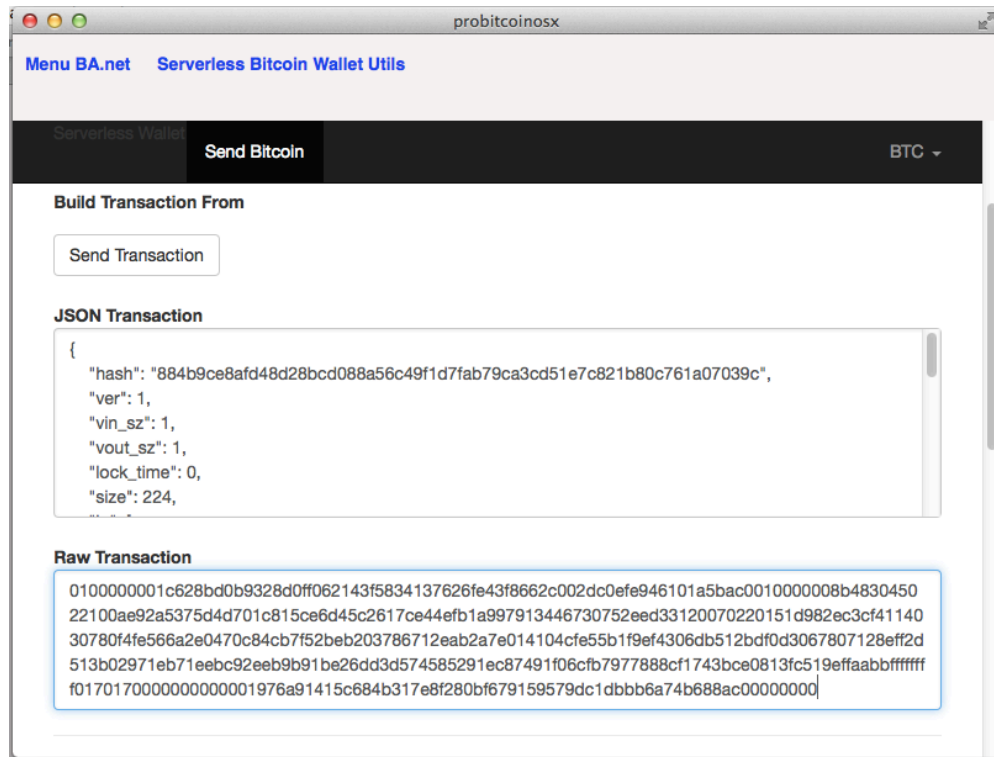
At no point in this process is the private key data exposed through the transaction data. Your private key never touches the internet, for maximum security.

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.

4.5 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!

4.6 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 BITCOIN COLD STORAGE

Cold storage – the storage of valuables, specifically bitcoins, in such a way that they are significantly harder to steal than normal, though at the admitted cost of delay in access times. There are a number of popular methods for performing such bitcoin storage, but to use most of them you still have to wade knee-deep into cryptography jargon and it seems like you need an advanced degree just to keep your coins safe. On this chapter you will find a simple introduction.

One of the bigger benefits Bitcoin has is its cash-like nature. People are used to cash, they understand cash much better than most digital payment systems, so let's make an analogy with cash. You take a million dollars cash to a bank and deposit it.

Would you be surprised at all if you returned to the bank a few months later and were told you'd have to wait a few days to withdraw your million dollars? Probably not. It's well-understood that your branch probably doesn't have enough cash on hand to cash out your million and still do business – they don't feel comfortable holding that kind of money in the same place they hold the smaller amount of cash they transact their daily business with – they have most of their money somewhere much more secure. Even the convenience store on the corner keeps a small amount of cash in the register and the majority of their money in a safe. Cold storage is the Bitcoin version of a safe.

The one tiny bit of terminology you need to understand to fully comprehend the basic concept of cold storage is what techies mean when they refer to systems, databases and other things as "hot" or "cold." A "hot" system is one that's live, running, connected. A "cold" system is powered-down, stopped, offline. To this end what we really mean when we say "cold storage" is that we're storing Bitcoins somewhere that's not connected to the Bitcoin network or, in most cases, even connected to the Internet or even on a computer at all.

There are a multitude of ways to do this, and we'll explore a few in detail, but it all boils down to the very basic principle that if your data isn't on a computer that's connected to internet then someone has to physically gain access to it to compromise it, and it's way easier to secure things physically than digitally.

So how do you ensure the safety of your coins? Most of the options people list fall (often incorrectly) into one of three categories:

5.1 PAPER WALLETS

Paper wallets are one of the most popular methods for storing bitcoins offline. A program of some kind generates the public and private halves of a Bitcoin address (or several). There are usually handy little barcodes that you can scan with your phone, so you don't have to type those monstrously long things in by hand when the time comes to use your coins. You print off what you've generated and send coins to that address.

You have just printed your very own paper money and it can be stored securely in exactly the same ways that cash can.
Update: It is worth noting that there are problems surrounding proper paper wallet use which, since the original publication of this article has led me to no longer categorize them as cold storage.

They are safer than most alternatives and so they remain in this article, but technically, they're not actually cold storage. Also, there's been an improvement called "BIP38″ that means you can now make paper wallets with encrypted private keys. Should you choose any storage system involving paper wallets, you should absolutely choose to encrypt your private key.

5.2 BRAIN WALLETS

Brain wallets are a little more complicated. Where the addresses in paper wallets are generated at random, the addresses in brain wallets follow rules. You memorize something long and random, like a random sequence of words: "steady harbor business last barn test instant begun know silver driver naturally closer sum automobile some" would make a decent passphrase, for example. Again some piece of software comes into play and turns your passphrase into one or more Bitcoin addresses in a completely reproducible way.

There is something of a standard method for turning passphrases into addresses, but that would bring us knee-deep in jargon again. Via the standard method, our above passphrase would yield a Bitcoin address of "1Jkibvu28YqSiSqdyB9jgcAAJCRWqg2QQL" so we could send some coins to that address and as long as we can remember the passphrase. It's also incredibly important to have a long and secure passphrase for this method – longer than most can remember, which makes this method somewhat less popular. If someone can guess your password, they can steal your money.

This address, for example, was generated from the example passphrase from this comic. Someone used a pop culture reference to create their Bitcoin address and if there were actually funds there, we could all steal them now.

While proper brain wallets are now fading out of vogue, a similar technique is often used to back up newer deterministic wallets. A "seed" passphrase is used to generate many addresses so you only have to back one thing up to recover all of them, no matter how many you use. Again, though, this is technically offline key storage, not cold storage.

5.3 COLD STORAGE / HARDWARE WALLETS

While the above are often called "cold storage" they're technically just offline key storage, which means they're only safe when used properly – and since they're basically never used properly, this is problematic. Since this article was first written, however, a new option has become available: True cold storage via hardware wallets. You can now simply buy a device that stores its own keys and does its own message signing all without every touching a potentially-compromised computer system. This is now the preferred method and should be used whenever it is an option since it doesn't require you to know or follow any kind of "best practices" for securing funds. Just use the device and you're good.

It's important to note that, under most circumstances, you generate these addresses, use them for storage once and then never use them again. In order to use the funds in a paper wallet, you have to use the account on an online (hot) computer, which lowers the security of whatever account you just used. Under most circumstances, such addresses should be considered to be single-use addresses only. Which way you should go is up to you, but I'll give you a few tools you can use either way.

First, bitaddress.org is an excellent and accessible tool. Despite looking like a normal web page with multiple tabs, the whole thing is written in such a way that once it's loaded it never needs internet access again. You can go to the page, completely disconnect your computer from the net and it will still work. You can even save a copy of the page to your hard disk and it'll still work locally – As a matter of fact, that's the way the most paranoid among us suggest you do this. Bitaddress.org is also fairly unique in that they offer a huge amount of functionality: they can generate paper wallets one address at a time or in bulk, they do brain wallets too and they even have a special "bulk wallet" function for people who want to accept payments on their web site without actually storing their coins on some scarily-insecure web server.

Users of the popular blockchain.info wallet service can also create a paper wallet through blockchain.info's "offline" functionality and as an added bonus, you can keep monitoring the funds in those accounts through the same site (and apps) you monitor your regular balances with. They even have a method for performing transactions with paper wallet addresses that doesn't "burn" the address – at least not as badly as any other method of spending from such wallets (they prompt you to enter they key and then use it once, never actually storing it).

5.4 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. This can be be carried by an USB key or other means to a machine that is online and the transaction can be broadcast.

Your private key never touches the Internet. Maximum Security.

5.5 HOW DO I CREATE AN OFFLINE TRANSACTION ?

Use the [PRO Serverless Bitcoin Wallet BA.net App](#). Search for "banet" at the Apple AppStore for iOS or the MacStore for OSX

6 BITCOIN CHANGE ADDRESSES COMPLEXITY

Few topics in Bitcoin cause more confusion, anxiety, and loss of money than change addresses. They seem counterintuitive and unnecessary. They're a major contributor to wallet software complexity. When used improperly, they can de-anonymize not just the payer but other parties as well.

Given the many problems with change addresses, why do they exist in the first place? This article explains what change addresses are, why they're essential to Bitcoin, and how to protect your money and privacy.

TEST TIME

If change addresses seem confusing, you may be working under some false assumptions about how Bitcoin works. Try this simple test to see for yourself.

Alice buys Bob's computer for 1.05 BTC. Her wallet contains 2.23 BTC stored in a single address. Assuming no fee is involved, how much of Alice's money will be involved in the transaction?

- A: 1.05 BTC
- B: 2.23 BTC
- C: Not enough information

If you answered A, then you may view Bitcoin as a kind of bank account in which a transaction debits an arbitrary amount of money from one account and credits it to another. This is a very common view that is unfortunately incorrect.

If you answered B, you probably know about change addresses, but don't understand why they exist. What you know isn't enough to prevent you from losing money in certain situations.

The correct answer is C: not enough information. After reading this article, you'll understand why this is the case and what information would be needed to find the exact amount of Alice's payment.

BITCOIN IS A CASH SYSTEM

Humans have been using cash for thousands of years, and cash is still important in most parts of the world. Every cash system assigns a face value to a token that can be used as payment. Paper bank notes and metal coins are examples of tokens we've all used since childhood.

Bitcoin is a cash system that replaces physical tokens with digital tokens called COINS (or more technically, unspent transaction outputs - UTXOs). When you receive a payment, you accept one or more of these digital coins. When you make a payment, you reassign ownership of one or more of your coins. A single address can hold multiple coins at the same time. Likewise, a transaction may gather coins from the same address, or multiple addresses.

Many cash transactions generate change. For example, if you pay for $64.89 worth of groceries with four $20 bills, the checker owes you $15.11 in change. To make a cash payment, we try to find enough bank notes to meet or exceed the payment amount. Any amount in excess of the required payment is returned as change.

The same holds true for Bitcoin transactions. Change is received by directing it to a designated change address. Change not recovered by a change address is claimed by miners as a transaction fee.

Bitcoin needs change addresses because Bitcoin is a cash system.

WALLETS REINFORCE MISCONCEPTIONS

Software wallets attempt to hide Bitcoin's deep connection to cash by presenting an interface similar to the one used by online banking services. Payment amounts appear to be deducted from your wallet balance and added to the wallet balance of your payee.

As we've already seen, this is not how Bitcoin transactions work. Instead, your wallet digitally signs and broadcasts a transaction to the network. The transaction reassigns ownership of one or more of your coins to your payee, returning any change to an address controlled by the wallet.

Although wallets handle change for you automatically, they can vary greatly in exactly how this is done. Failure to understand the differences can lead to confusion and loss of money.

WALLETS AND CHANGE ADDRESSES

Three main strategies for handling change have been adopted by wallet developers. Each one has different implications for privacy and security.

- **Single Address Wallets** use one address for receiving both payments and change. Addresses can be added by importing a private key or manually adding a new receiving address. Examples of Single Address Wallets include BA.net, Blockchain.info and MultiBit.
- **Random Address Pool Wallets** use a pool of randomly-generated addresses to receive payments and change. If a transaction generates change, it is sent to the next available unused address, causing a new address to be added to the pool. The best-known example of an Address Pool Wallet is Bitcoin Core.
- **Deterministic Address Pool Wallets** use a pool of deterministically-generated addresses to receive payments and change. Given a particular unique SEED, these wallets always generate the same sequence of addresses. Examples include Electrum and Armory.

Wallets can adopt new change-handling behavior depending on user settings and other state. For example, importing a paper wallet into MultiBit results in a two-key system in which change may alternately be sent to the original address and the paper wallet address, a situation with critical implications for security. Likewise, Electrum permits users to send all change to the same address, effectively creating a Single Address Wallet.

WHY NOT USE THE SAME ADDRESS?

It may seem odd that wallets would generate a new address to accept change. Why not return change to the same address? Why the apparently useless complexity of address pools?

The main reason is PRIVACY. By necessity, every Bitcoin transaction becomes part of a permanently viewable global ledger called the BLOCK CHAIN. Maintaining privacy in this system depends on a strict separation between addresses and personal identities, a model referred to as PSEUDONYMITY.

Imagine that a transaction moves a coin from Address A to Address B. If change is returned to the sending address, the block chain makes it trivial to deduce that the person controlling Address A paid the person controlling Address B. If two payments are made, both payees can easily be identified. And so on.
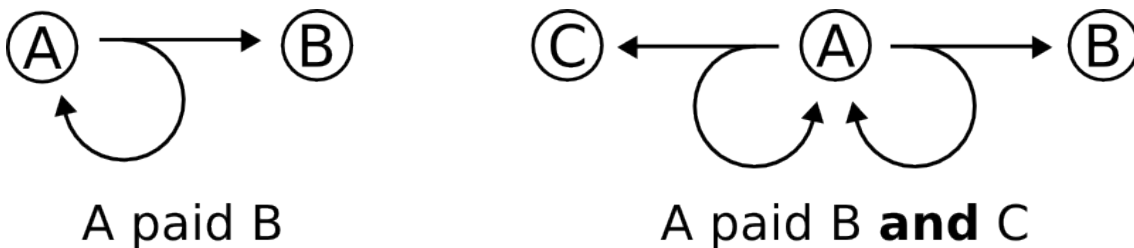
The intended payee address can be trivially determined when change is returned to the sending address (left). Multiple transactions make it possible to determine multiple payees unambiguously (right).

An observer able to link a real-world identity to Addresses A, B, or C may be able to deduce the identities of the other parties as well.

Now imagine that a transaction moves a coin from address A to Address B, but directs change to Address C. Without additional information, the only thing an outside observer can conclude is that a payment to the person controlling Address B and/or C was made. Given another transaction from Address C, the picture becomes even less clear.
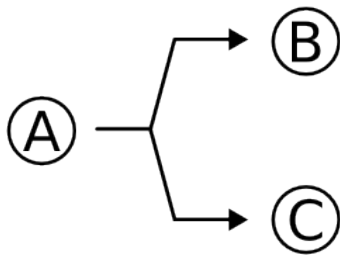
A paid (B **and/or** C)
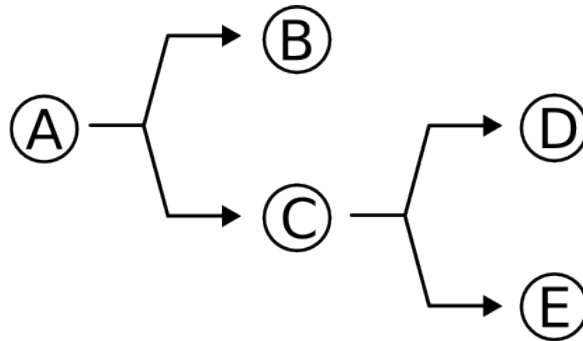
A paid B **and/or** C;
C paid D **and/or** E

Change is returned to a one-use address (left). Each additional payment makes the intended payee more ambiguous (right).

An observer trying to link real-world identities to Bitcoin addresses must gather more secondary information and work harder when all parties direct change to one-use addresses.

This isn't the end of the story. As transactions generate change, eventually this change will be recombined to make purchases. Bringing coins from various change addresses together into a single transaction suggests (but does not by itself prove) a link to a common user. Countering this problem requires that additional privacy-enhancing steps be taken. CoinJoin offers one solution, but this is still an area of active research.

STAYING SAFE

Change addresses open the door to loss of funds through several avenues. The most serious problem is that many Bitcoin users are

unaware of the existence of change addresses in the first place. However, change addresses can cause problems even for users who understand them.

Discussion forums like the Bitcoin subreddit are filled with stories of users who either lost money or thought they lost money through change addresses. For some specific scenarios based on these stories, and ways to avoid them, see *Five Ways to Lose Money with Bitcoin Change Addresses*.

BACK TO ALICE AND BOB

Given a basic understanding of Bitcoin as a cash system, we can return the the problem of deciding how much of Alice's money will be involved in a payment to Bob.

We have no way to know whether a Alice's wallet contains a coin with a face value of the payment amount (1.05 BTC). As a result, we can't say for sure if this will be the amount of Alice's payment.

Although Alice's address could just happen to contain only one coin, we have no reason to think this is the case, either. For example, her address may contain dozens of coins with face values totaling 2.23 BTC.

To answer the question, we'd need to know the values of each coin at Alice's address. Not only that, but we'd need to know exactly how Alice's wallet selects coins when making payments.

CONCLUSIONS

Like any cash payment, Bitcoin transactions often generate change. This change must be claimed by a change address or lost. The methods that change addresses are created and used lead to important implications for privacy and security. As a Bitcoin user, you owe it to yourself to understand change and how your wallet handles it.

7 BITCOIN SECURITY

Securing bitcoin is challenging because bitcoin is not an abstract reference to value, like a balance in a bank account. Bitcoin is very much like digital cash or gold. You've probably heard the expression, "Possession is nine-tenths of the law." Well, in bitcoin, possession is ten-tenths of the law. Possession of the keys to unlock the bitcoin is equivalent to possession of cash or a chunk of precious metal. You can lose it, misplace it, have it stolen, or accidentally give the wrong amount to someone. In every one of these cases, users have no recourse, just as if they dropped cash on a public sidewalk.

However, bitcoin has capabilities that cash, gold, and bank accounts do not. A bitcoin wallet, containing your keys, can be backed up like any file. It can be stored in multiple copies, even printed on paper for hard-copy backup. You can't "back up" cash, gold, or bank accounts. Bitcoin is different enough from anything that has come before that we need to think about bitcoin security in a novel way too.

SECURITY PRINCIPLES

The core principle in bitcoin is decentralization and it has important implications for security. A centralized model, such as a traditional bank or payment network, depends on access control and vetting to keep bad actors out of the system. By comparison, a decentralized system like bitcoin pushes the responsibility and control to the users. Because security of the network is based on proof of work, not access control, the network can be open and no encryption is required for bitcoin traffic.

On a traditional payment network, such as a credit card system, the payment is open-ended because it contains the user's private identifier (the credit card number). After the initial charge, anyone with access to the identifier can "pull" funds and charge the owner again and again. Thus, the payment network has to be secured end-to-end with encryption and must ensure that no eavesdroppers or

intermediaries can compromise the payment traffic, in transit or when it is stored (at rest). If a bad actor gains access to the system, he can compromise current transactions AND payment tokens that can be used to create new transactions. Worse, when customer data is compromised, the customers are exposed to identity theft and must take action to prevent fraudulent use of the compromised accounts.

Bitcoin is dramatically different. A bitcoin transaction authorizes only a specific value to a specific recipient and cannot be forged or modified. It does not reveal any private information, such as the identities of the parties, and cannot be used to authorize additional payments. Therefore, a bitcoin payment network does not need to be encrypted or protected from eavesdropping. In fact, you can broadcast bitcoin transactions over an open public channel, such as unsecured WiFi or Bluetooth, with no loss of security.

Bitcoin's decentralized security model puts a lot of power in the hands of the users. With that power comes responsibility for maintaining the secrecy of the keys. For most users that is not easy to do, especially on general-purpose computing devices such as Internet-connected smartphones or laptops. Although bitcoin's decentralized model prevents the type of mass compromise seen with credit cards, many users are not able to adequately secure their keys and get hacked, one by one.

7.1.1 DEVELOPING BITCOIN SYSTEMS SECURELY

The most important principle for bitcoin developers is decentralization. Most developers will be familiar with centralized security models and might be tempted to apply these models to their bitcoin applications, with disastrous results.

Bitcoin's security relies on decentralized control over keys and on independent transaction validation by miners. If you want to leverage Bitcoin's security, you need to ensure that you remain within the Bitcoin security model. In simple terms: don't take control of keys away from users and don't take transactions off the blockchain.

For example, many early bitcoin exchanges concentrated all user funds in a single "hot" wallet with keys stored on a single server. Such a design removes control from users and centralizes control over keys in a single system. Many such systems have been hacked, with disastrous consequences for their customers.

Another common mistake is to take transactions "off blockchain" in a misguided effort to reduce transaction fees or accelerate transaction processing. An "off blockchain" system will record transactions on an internal, centralized ledger and only occasionally synchronize them to the bitcoin blockchain. This practice, again, substitutes decentralized bitcoin security with a proprietary and centralized approach. When transactions are off blockchain, improperly secured centralized ledgers can be falsified, diverting funds and depleting reserves, unnoticed.

Unless you are prepared to invest heavily in operational security, multiple layers of access control, and audits (as the traditional banks do) you should think very carefully before taking funds outside of Bitcoin's decentralized security context. Even if you have the funds and discipline to implement a robust security model, such a design merely replicates the fragile model of traditional financial networks, plagued by identity theft, corruption, and embezzlement. To take advantage of Bitcoin's unique decentralized security model, you have to avoid the temptation of centralized architectures that might feel familiar but ultimately subvert Bitcoin's security.

7.1.2 THE ROOT OF TRUST

Traditional security architecture is based upon a concept called the ROOT OF TRUST, which is a trusted core used as the foundation for the security of the overall system or application. Security architecture is developed around the root of trust as a series of concentric circles, like layers in an onion, extending trust outward from the center. Each layer builds upon the more-trusted inner layer using access controls, digital signatures, encryption, and other security primitives. As software systems become more complex, they are more likely to contain bugs, which make them vulnerable to security compromise.

As a result, the more complex a software system becomes, the harder it is to secure. The root of trust concept ensures that most of the trust is placed within the least complex part of the system, and therefore least vulnerable, parts of the system, while more complex software is layered around it. This security architecture is repeated at different scales, first establishing a root of trust within the hardware of a single system, then extending that root of trust through the operating system to higher-level system services, and finally across many servers layered in concentric circles of diminishing trust.

Bitcoin security architecture is different. In Bitcoin, the consensus system creates a trusted public ledger that is completely decentralized. A correctly validated blockchain uses the genesis block as the root of trust, building a chain of trust up to the current block. Bitcoin systems can and should use the blockchain as their root of trust. When designing a complex bitcoin application that consists of services on many different systems, you should carefully examine the security architecture in order to ascertain where trust is being placed. Ultimately, the only thing that should be explicitly trusted is a fully validated blockchain. If your application explicitly or implicitly vests trust in anything but the blockchain, that should be a source of concern because it introduces vulnerability. A good method to evaluate the security architecture of your application is to consider each individual component and evaluate a hypothetical scenario where that component is completely compromised and under the control of a malicious actor. Take each component of your application, in turn, and assess the impacts on the overall security if that component is compromised. If your application is no longer secure when components are compromised, that shows you have misplaced trust in those components. A bitcoin application without vulnerabilities should be vulnerable only to a compromise of the bitcoin consensus mechanism, meaning that its root of trust is based on the strongest part of the bitcoin security architecture.

The numerous examples of hacked bitcoin exchanges serve to underscore this point because their security architecture and design fails even under the most casual scrutiny. These centralized implementations had invested trust explicitly in numerous components

outside the bitcoin blockchain, such as hot wallets, centralized ledger databases, vulnerable encryption keys, and similar schemes.

USER SECURITY BEST PRACTICES

Humans have used physical security controls for thousands of years. By comparison, our experience with digital security is less than 50 years old. Modern general-purpose operating systems are not very secure and not particularly suited to storing digital money. Our computers are constantly exposed to external threats via always-on Internet connections. They run thousands of software components from hundreds of authors, often with unconstrained access to the user's files. A single piece of rogue software, among the many thousands installed on your computer, can compromise your keyboard and files, stealing any bitcoin stored in wallet applications. The level of computer maintenance required to keep a computer virus-free and trojan-free is beyond the skill level of all but a tiny minority of computer users.

Despite decades of research and advancements in information security, digital assets are still woefully vulnerable to a determined adversary. Even the most highly protected and restricted systems, in financial services companies, intelligence agencies, and defense contractors, are frequently breached. Bitcoin creates digital assets that have intrinsic value and can be stolen and diverted to new owners instantly and irrevocably. This creates a massive incentive for hackers. Until now, hackers had to convert identity information or account tokens—such as credit cards, and bank accounts—into value after compromising them. Despite the difficulty of fencing and laundering financial information, we have seen ever-escalating thefts. Bitcoin escalates this problem because it doesn't need to be fenced or laundered; it is intrinsic value within a digital asset.

Fortunately, bitcoin also creates the incentives to improve computer security. Whereas previously the risk of computer compromise was vague and indirect, bitcoin makes these risks clear and obvious. Holding bitcoin on a computer serves to focus the user's mind on the need for improved computer security. As a direct result of the

proliferation and increased adoption of bitcoin and other digital currencies, we have seen an escalation in both hacking techniques and security solutions. In simple terms, hackers now have a very juicy target and users have a clear incentive to defend themselves.

Over the past three years, as a direct result of bitcoin adoption, we have seen tremendous innovation in the realm of information security in the form of hardware encryption, key storage and hardware wallets, multi-signature technology, and digital escrow. In the following sections we will examine various best practices for practical user security.

7.1.3 PHYSICAL BITCOIN STORAGE

Because most users are far more comfortable with physical security than information security, a very effective method for protecting bitcoins is to convert them into physical form. Bitcoin keys are nothing more than long numbers. This means that they can be stored in a physical form, such as printed on paper or etched on a metal coin. Securing the keys then becomes as simple as physically securing the printed copy of the bitcoin keys. A set of bitcoin keys that is printed on paper is called a "paper wallet," and there are many free tools that can be used to create them. I personally keep the vast majority of my bitcoins (99% or more) stored on paper wallets, encrypted with BIP0038, with multiple copies locked in safes. Keeping bitcoin offline is called COLD STORAGE and it is one of the most effective security techniques. A cold storage system is one where the keys are generated on an offline system (one never connected to the Internet) and stored offline either on paper or on digital media, such as a USB memory stick.

7.1.4 HARDWARE WALLETS

In the long term, bitcoin security increasingly will take the form of hardware tamper-proof wallets. Unlike a smartphone or desktop computer, a bitcoin hardware wallet has just one purpose: to hold bitcoins securely. Without general-purpose software to compromise and with limited interfaces, hardware wallets can deliver an almost foolproof level of security to nonexpert users. I expect to see hardware

wallets become the predominant method of bitcoin storage. For an example of such a hardware wallet, see the Trezor.

7.1.5 BALANCING RISK

Although most users are rightly concerned about bitcoin theft, there is an even bigger risk. Data files get lost all the time. If they contain bitcoin, the loss is much more painful. In the effort to secure their bitcoin wallets, users must be very careful not to go too far and end up losing the bitcoin. In July of 2011, a well-known bitcoin awareness and education project lost almost 7,000 bitcoins. In their effort to prevent theft, the owners had implemented a complex series of encrypted backups. In the end they accidentally lost the encryption keys, making the backups worthless and losing a fortune. Like hiding money by burying it in the desert, if you secure your bitcoin too well you might not be able to find it again.

7.1.6 DIVERSIFYING RISK

Would you carry your entire net worth in cash in your wallet? Most people would consider that reckless, yet bitcoin users often keep all their bitcoin in a single wallet. Instead, users should spread the risk among multiple and diverse bitcoin wallets. Prudent users will keep only a small fraction, perhaps less than 5%, of their bitcoins in an online or mobile wallet as "pocket change." The rest should be split between a few different storage mechanisms, such as a desktop wallet and offline (cold storage).

7.1.7 MULTI-SIG AND GOVERNANCE

Whenever a company or individual stores large amounts of bitcoin, they should consider using a multi-signature bitcoin address. Multi-signature addresses secure funds by requiring more than one signature to make a payment. The signing keys should be stored in a number of different locations and under the control of different people. In a corporate environment, for example, the keys should be generated independently and held by several company executives, to ensure no single person can compromise the funds. Multi-signature

addresses can also offer redundancy, where a single person holds several keys that are stored in different locations.

7.1.8 SURVIVABILITY

One important security consideration that is often overlooked is availability, especially in the context of incapacity or death of the key holder. Bitcoin users are told to use complex passwords and keep their keys secure and private, not sharing them with anyone. Unfortunately, that practice makes it almost impossible for the user's family to recover any funds if the user is not available to unlock them. In most cases, in fact, the families of bitcoin users might be completely unaware of the existence of the bitcoin funds.

If you have a lot of bitcoin, you should consider sharing access details with a trusted relative or lawyer. A more complex survivability scheme can be set up with multi-signature access and estate planning through a lawyer specialized as a "digital asset executor."

7.1.9 CONCLUSION

Bitcoin is a completely new, unprecedented, and complex technology. Over time we will develop better security tools and practices that are easier to use by nonexperts. For now, bitcoin users can use many of the tips discussed here to enjoy a secure and trouble-free bitcoin experience.

---

8   FREQUENTLY ASKED QUESTIONS

8.1.1 WHAT IS BITCOIN?

Bitcoin is a consensus network that enables a new payment system and a completely digital money. It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. From a user perspective, Bitcoin is pretty much like cash for the Internet. Bitcoin can also be seen as the most prominent triple entry bookkeeping system in existence.

8.1.2 WHO CREATED BITCOIN?

Bitcoin is the first implementation of a concept called "cryptocurrency", which was first described in 1998 by Wei Dai on the cypherpunks mailing list, suggesting the idea of a new form of money that uses cryptography to control its creation and transactions, rather than a central authority. The first Bitcoin specification, and proof of concept was published in 2009 in a cryptography mailing list by Satoshi Nakamoto. Satoshi left the project in late 2010 without revealing much about himself. The community has since grown exponentially with many developers working on Bitcoin.

Satoshi's anonymity often raised unjustified concerns, many of which are linked to misunderstanding of the open-source nature of Bitcoin. The Bitcoin protocol and software are published openly and any developer around the world can review the code or make their own modified version of the Bitcoin software. Just like current developers, Satoshi's influence was limited to the changes he made being adopted by others and therefore he did not control Bitcoin. As such, the identity of Bitcoin's inventor is probably as relevant today as the identity of the person who invented paper.

8.1.3 WHO CONTROLS THE BITCOIN NETWORK?

Nobody owns the Bitcoin network much like no one owns the technology behind email. Bitcoin is controlled by all Bitcoin users around the world. While developers are improving the software, they can't force a change in the Bitcoin protocol because all users are free to choose what software and version they use. In order to stay compatible with each other, all users need to use software complying with the same rules. Bitcoin can only work correctly with a complete consensus among all users. Therefore, all users and developers have a strong incentive to protect this consensus.

8.1.4 HOW DOES BITCOIN WORK?

From a user perspective, Bitcoin is nothing more than a mobile app or computer program that provides a personal Bitcoin wallet and allows a user to send and receive bitcoins with them. This is how Bitcoin works for most users.

Behind the scenes, the Bitcoin network is sharing a public ledger called the "block chain". This ledger contains every transaction ever processed, allowing a user's computer to verify the validity of each transaction. The authenticity of each transaction is protected by digital signatures corresponding to the sending addresses, allowing all users to have full control over sending bitcoins from their own Bitcoin addresses. In addition, anyone can process transactions using the computing power of specialized hardware and earn a reward in bitcoins for this service. This is often called "mining". To learn more about Bitcoin, you can consult the dedicated page and the original paper.

8.1.5 IS BITCOIN REALLY USED BY PEOPLE?

Yes. There is a growing number of businesses and individuals using Bitcoin. This includes brick and mortar businesses like restaurants, apartments, law firms, and popular online services such as Namecheap, WordPress, and Reddit. While Bitcoin remains a relatively new phenomenon, it is growing fast. At the end of August

2015, the value of all bitcoins in circulation exceeded US$ 3.1 billion with millions of dollars worth of bitcoins exchanged daily.
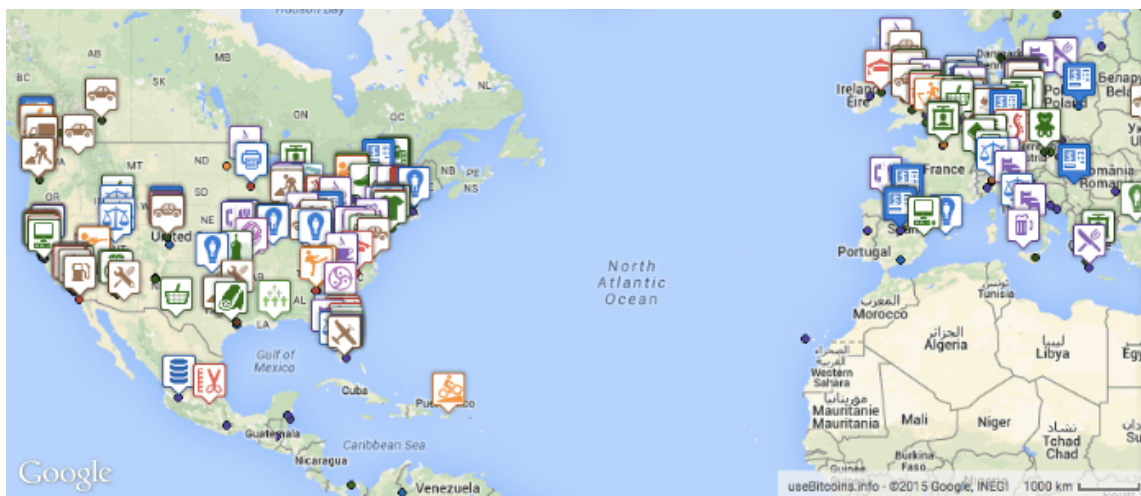
8.1.6 HOW DOES ONE ACQUIRE BITCOINS?

- As payment for goods or services.
- Purchase bitcoins at a Bitcoin exchange.
- Exchange bitcoins with someone near you.
- Earn bitcoins through competitive mining.

While it may be possible to find individuals who wish to sell bitcoins in exchange for a credit card or PayPal payment, most exchanges do not allow funding via these payment methods. This is due to cases where someone buys bitcoins with PayPal, and then reverses their half of the transaction. This is commonly referred to as a chargeback.

8.1.7 HOW DIFFICULT IS IT TO MAKE A BITCOIN PAYMENT?

Bitcoin payments are easier to make than debit or credit card purchases, and can be received without a merchant account. Payments are made from a wallet application, either on your computer or smartphone, by entering the recipient's address, the payment amount, and pressing send. To make it easier to enter a recipient's address, many wallets can obtain the address by scanning a QR code or touching two phones together with NFC technology.
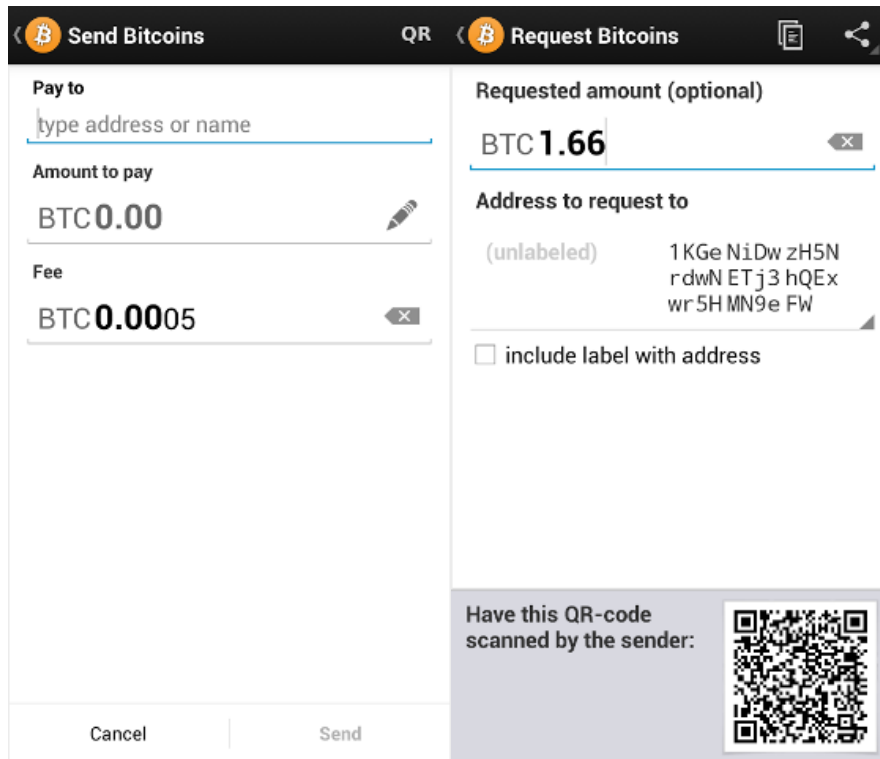
8.1.8 WHAT ARE THE ADVANTAGES OF BITCOIN?

- **PAYMENT FREEDOM** - It is possible to send and receive any amount of money instantly anywhere in the world at any time. No bank holidays. No borders. No imposed limits. Bitcoin allows its users to be in full control of their money.
- **VERY LOW FEES** - Bitcoin payments are currently processed with either no fees or extremely small fees. Users may include fees with transactions to receive priority processing, which results in faster confirmation of transactions by the network. Additionally, merchant processors exist to assist merchants in processing transactions, converting bitcoins to fiat currency and depositing funds directly into merchants' bank accounts daily. As these services are based on Bitcoin, they can be offered for much lower fees than with PayPal or credit card networks.
- **FEWER RISKS FOR MERCHANTS** - Bitcoin transactions are secure, irreversible, and do not contain customers' sensitive or personal information. This protects merchants from losses caused by fraud or fraudulent chargebacks, and there is no need for PCI compliance. Merchants can easily expand to new

markets where either credit cards are not available or fraud rates are unacceptably high. The net results are lower fees, larger markets, and fewer administrative costs.

- **SECURITY AND CONTROL** - Bitcoin users are in full control of their transactions; it is impossible for merchants to force unwanted or unnoticed charges as can happen with other payment methods. Bitcoin payments can be made without personal information tied to the transaction. This offers strong protection against identity theft. Bitcoin users can also protect their money with backup and encryption.

- **TRANSPARENT AND NEUTRAL** - All information concerning the Bitcoin money supply itself is readily available on the block chain for anybody to verify and use in real-time. No individual or organization can control or manipulate the Bitcoin protocol because it is cryptographically secure. This allows the core of Bitcoin to be trusted for being completely neutral, transparent and predictable.

8.1.9 WHAT ARE THE DISADVANTAGES OF BITCOIN?

- **DEGREE OF ACCEPTANCE** - Many people are still unaware of Bitcoin. Every day, more businesses accept bitcoins because they want the advantages of doing so, but the list remains small and still needs to grow in order to benefit from network effects.

- **VOLATILITY** - The total value of bitcoins in circulation and the number of businesses using Bitcoin are still very small compared to what they could be. Therefore, relatively small events, trades, or business activities can significantly affect the price. In theory, this volatility will decrease as Bitcoin markets and the technology matures. Never before has the world seen a start-up currency, so it is truly difficult (and exciting) to imagine how it will play out.

- **ONGOING DEVELOPMENT** - Bitcoin software is still in beta with many incomplete features in active development. New tools, features, and services are being developed to make Bitcoin more secure and accessible to the masses. Some of these are still not ready for everyone. Most Bitcoin businesses

are new and still offer no insurance. In general, Bitcoin is still in the process of maturing.

8.1.10 WHY DO PEOPLE TRUST BITCOIN?

Much of the trust in Bitcoin comes from the fact that it requires no trust at all. Bitcoin is fully open-source and decentralized. This means that anyone has access to the entire source code at any time. Any developer in the world can therefore verify exactly how Bitcoin works. All transactions and bitcoins issued into existence can be transparently consulted in real-time by anyone. All payments can be made without reliance on a third party and the whole system is protected by heavily peer-reviewed cryptographic algorithms, like those used for online banking. No organization or individual can control Bitcoin, and the network remains secure even if not all of its users can be trusted.

8.1.11 CAN I MAKE MONEY WITH BITCOIN?

You should never expect to get rich with Bitcoin or any emerging technology. It is always important to be wary of anything that sounds too good to be true or disobeys basic economic rules.

Bitcoin is a growing space of innovation and there are business opportunities that also include risks. There is no guarantee that Bitcoin will continue to grow even though it has developed at a very fast rate so far. Investing time and resources on anything related to Bitcoin requires entrepreneurship. There are various ways to make money with Bitcoin such as mining, speculation or running new businesses. All of these methods are competitive and there is no guarantee of profit. It is up to each individual to make a proper evaluation of the costs and the risks involved in any such project.

8.1.12 IS BITCOIN FULLY VIRTUAL AND IMMATERIAL?

Bitcoin is as virtual as the credit cards and online banking networks people use everyday. Bitcoin can be used to pay online and in physical stores just like any other form of money. Bitcoins can also be exchanged in physical form such as the Casascius coins, but paying

with a mobile phone usually remains more convenient. Bitcoin balances are stored in a large distributed network, and they cannot be fraudulently altered by anybody. In other words, Bitcoin users have exclusive control over their funds and bitcoins cannot vanish just because they are virtual.

8.1.13   IS BITCOIN ANONYMOUS?

Bitcoin is designed to allow its users to send and receive payments with an acceptable level of privacy as well as any other form of money. However, Bitcoin is not anonymous and cannot offer the same level of privacy as cash. The use of Bitcoin leaves extensive public records. Various mechanisms exist to protect users' privacy, and more are in development. However, there is still work to be done before these features are used correctly by most Bitcoin users.

Some concerns have been raised that private transactions could be used for illegal purposes with Bitcoin. However, it is worth noting that Bitcoin will undoubtedly be subjected to similar regulations that are already in place inside existing financial systems. Bitcoin cannot be more anonymous than cash and it is not likely to prevent criminal investigations from being conducted. Additionally, Bitcoin is also designed to prevent a large range of financial crimes.

8.1.14   WHAT HAPPENS WHEN BITCOINS ARE LOST?

When a user loses his wallet, it has the effect of removing money out of circulation. Lost bitcoins still remain in the block chain just like any other bitcoins. However, lost bitcoins remain dormant forever because there is no way for anybody to find the private key(s) that would allow them to be spent again. Because of the law of supply and demand, when fewer bitcoins are available, the ones that are left will be in higher demand and increase in value to compensate.

8.1.15   CAN BITCOIN SCALE TO BECOME A MAJOR PAYMENT
         NETWORK?

The Bitcoin network can already process a much higher number of transactions per second than it does today. It is, however, not entirely

ready to scale to the level of major credit card networks. Work is underway to lift current limitations, and future requirements are well known. Since inception, every aspect of the Bitcoin network has been in a continuous process of maturation, optimization, and specialization, and it should be expected to remain that way for some years to come. As traffic grows, more Bitcoin users may use lightweight clients, and full network nodes may become a more specialized service. For more details, see the Scalability page on the Wiki.

LEGAL

8.1.16   IS BITCOIN LEGAL?

To the best of our knowledge, Bitcoin has not been made illegal by legislation in most jurisdictions. However, some jurisdictions (such as Argentina and Russia) severely restrict or ban foreign currencies. Other jurisdictions (such as Thailand) may limit the licensing of certain entities such as Bitcoin exchanges.

Regulators from various jurisdictions are taking steps to provide individuals and businesses with rules on how to integrate this new technology with the formal, regulated financial system. For example, the Financial Crimes Enforcement Network (FinCEN), a bureau in the United States Treasury Department, issued non-binding guidance on how it characterizes certain activities involving virtual currencies.

8.1.17   IS BITCOIN USEFUL FOR ILLEGAL ACTIVITIES?

Bitcoin is money, and money has always been used both for legal and illegal purposes. Cash, credit cards and current banking systems widely surpass Bitcoin in terms of their use to finance crime. Bitcoin can bring significant innovation in payment systems and the benefits of such innovation are often considered to be far beyond their potential drawbacks.

Bitcoin is designed to be a huge step forward in making money more secure and could also act as a significant protection against many forms of financial crime. For instance, bitcoins are completely

impossible to counterfeit. Users are in full control of their payments and cannot receive unapproved charges such as with credit card fraud. Bitcoin transactions are irreversible and immune to fraudulent chargebacks. Bitcoin allows money to be secured against theft and loss using very strong and useful mechanisms such as backups, encryption, and multiple signatures.

Some concerns have been raised that Bitcoin could be more attractive to criminals because it can be used to make private and irreversible payments. However, these features already exist with cash and wire transfer, which are widely used and well-established. The use of Bitcoin will undoubtedly be subjected to similar regulations that are already in place inside existing financial systems, and Bitcoin is not likely to prevent criminal investigations from being conducted. In general, it is common for important breakthroughs to be perceived as being controversial before their benefits are well understood. The Internet is a good example among many others to illustrate this.

8.1.18   CAN BITCOIN BE REGULATED?

The Bitcoin protocol itself cannot be modified without the cooperation of nearly all its users, who choose what software they use. Attempting to assign special rights to a local authority in the rules of the global Bitcoin network is not a practical possibility. Any rich organization could choose to invest in mining hardware to control half of the computing power of the network and become able to block or reverse recent transactions. However, there is no guarantee that they could retain this power since this requires to invest as much than all other miners in the world.

It is however possible to regulate the use of Bitcoin in a similar way to any other instrument. Just like the dollar, Bitcoin can be used for a wide variety of purposes, some of which can be considered legitimate or not as per each jurisdiction's laws. In this regard, Bitcoin is no different than any other tool or resource and can be subjected to different regulations in each country. Bitcoin use could also be made difficult by restrictive regulations, in which case it is hard to determine what percentage of users would keep using the technology. A

government that chooses to ban Bitcoin would prevent domestic businesses and markets from developing, shifting innovation to other countries. The challenge for regulators, as always, is to develop efficient solutions while not impairing the growth of new emerging markets and businesses.

8.1.19   WHAT ABOUT BITCOIN AND TAXES?

Bitcoin is not a fiat currency with legal tender status in any jurisdiction, but often tax liability accrues regardless of the medium used. There is a wide variety of legislation in many different jurisdictions which could cause income, sales, payroll, capital gains, or some other form of tax liability to arise with Bitcoin.

8.1.20   WHAT ABOUT BITCOIN AND CONSUMER PROTECTION?

Bitcoin is freeing people to transact on their own terms. Each user can send and receive payments in a similar way to cash but they can also take part in more complex contracts. Multiple signatures allow a transaction to be accepted by the network only if a certain number of a defined group of persons agree to sign the transaction. This allows innovative dispute mediation services to be developed in the future. Such services could allow a third party to approve or reject a transaction in case of disagreement between the other parties without having control on their money. As opposed to cash and other payment methods, Bitcoin always leaves a public proof that a transaction did take place, which can potentially be used in a recourse against businesses with fraudulent practices.

It is also worth noting that while merchants usually depend on their public reputation to remain in business and pay their employees, they don't have access to the same level of information when dealing with new consumers. The way Bitcoin works allows both individuals and businesses to be protected against fraudulent chargebacks while giving the choice to the consumer to ask for more protection when they are not willing to trust a particular merchant.

ECONOMY

8.1.21   HOW ARE BITCOINS CREATED?

New bitcoins are generated by a competitive and decentralized process called "mining". This process involves that individuals are rewarded by the network for their services. Bitcoin miners are processing transactions and securing the network using specialized hardware and are collecting new bitcoins in exchange.

The Bitcoin protocol is designed in such a way that new bitcoins are created at a fixed rate. This makes Bitcoin mining a very competitive business. When more miners join the network, it becomes increasingly difficult to make a profit and miners must seek efficiency to cut their operating costs. No central authority or developer has any power to control or manipulate the system to increase their profits. Every Bitcoin node in the world will reject anything that does not comply with the rules it expects the system to follow.

Bitcoins are created at a decreasing and predictable rate. The number of new bitcoins created each year is automatically halved over time until bitcoin issuance halts completely with a total of 21 million bitcoins in existence. At this point, Bitcoin miners will probably be supported exclusively by numerous small transaction fees.

8.1.22   WHY DO BITCOINS HAVE VALUE?

Bitcoins have value because they are useful as a form of money. Bitcoin has the characteristics of money (durability, portability, fungibility, scarcity, divisibility, and recognizability) based on the properties of mathematics rather than relying on physical properties (like gold and silver) or trust in central authorities (like fiat currencies). In short, Bitcoin is backed by mathematics. With these attributes, all that is required for a form of money to hold value is trust and adoption. In the case of Bitcoin, this can be measured by its growing base of users, merchants, and startups. As with all currency, bitcoin's value comes only and directly from people willing to accept them as payment.

8.1.23   WHAT DETERMINES BITCOIN'S PRICE?

The price of a bitcoin is determined by supply and demand. When demand for bitcoins increases, the price increases, and when demand falls, the price falls. There is only a limited number of bitcoins in circulation and new bitcoins are created at a predictable and decreasing rate, which means that demand must follow this level of inflation to keep the price stable. Because Bitcoin is still a relatively small market compared to what it could be, it doesn't take significant amounts of money to move the market price up or down, and thus the price of a bitcoin is still very volatile.

Bitcoin price over time:

8.1.24   CAN BITCOINS BECOME WORTHLESS?

Yes. History is littered with currencies that failed and are no longer used, such as the German Mark during the Weimar Republic and, more recently, the Zimbabwean dollar. Although previous currency failures were typically due to hyperinflation of a kind that Bitcoin makes impossible, there is always potential for technical failures, competing currencies, political issues and so on. As a basic rule of thumb, no currency should be considered absolutely safe from failures or hard times. Bitcoin has proven reliable for years since its inception and there is a lot of potential for Bitcoin to continue to grow. However, no one is in a position to predict what the future will be for Bitcoin.

8.1.25   IS BITCOIN A BUBBLE?

A fast rise in price does not constitute a bubble. An artificial over-valuation that will lead to a sudden downward correction constitutes a bubble. Choices based on individual human action by hundreds of thousands of market participants is the cause for bitcoin's price to fluctuate as the market seeks price discovery. Reasons for changes in sentiment may include a loss of confidence in Bitcoin, a large difference between value and price not based on the fundamentals of the Bitcoin economy, increased press coverage stimulating speculative demand, fear of uncertainty, and old-fashioned irrational exuberance and greed.

8.1.26   IS BITCOIN A PONZI SCHEME?

A Ponzi scheme is a fraudulent investment operation that pays returns to its investors from their own money, or the money paid by subsequent investors, instead of from profit earned by the individuals running the business. Ponzi schemes are designed to collapse at the expense of the last investors when there is not enough new participants.

Bitcoin is a free software project with no central authority. Consequently, no one is in a position to make fraudulent representations about investment returns. Like other major currencies such as gold, United States dollar, euro, yen, etc. there is no guaranteed purchasing power and the exchange rate floats freely. This leads to volatility where owners of bitcoins can unpredictably make or lose money. Beyond speculation, Bitcoin is also a payment system with useful and competitive attributes that are being used by thousands of users and businesses.

8.1.27   DOESN'T BITCOIN UNFAIRLY BENEFIT EARLY ADOPTERS?

Some early adopters have large numbers of bitcoins because they took risks and invested time and resources in an unproven technology that was hardly used by anyone and that was much harder to secure properly. Many early adopters spent large numbers of bitcoins quite a

few times before they became valuable or bought only small amounts and didn't make huge gains. There is no guarantee that the price of a bitcoin will increase or drop. This is very similar to investing in an early startup that can either gain value through its usefulness and popularity, or just never break through. Bitcoin is still in its infancy, and it has been designed with a very long-term view; it is hard to imagine how it could be less biased towards early adopters, and today's users may or may not be the early adopters of tomorrow.

8.1.28 WON'T THE FINITE AMOUNT OF BITCOINS BE A LIMITATION?

Bitcoin is unique in that only 21 million bitcoins will ever be created. However, this will never be a limitation because transactions can be denominated in smaller sub-units of a bitcoin, such as bits - there are 1,000,000 bits in 1 bitcoin. Bitcoins can be divided up to 8 decimal places (0.000 000 01) and potentially even smaller units if that is ever required in the future as the average transaction size decreases.

8.1.29 WON'T BITCOIN FALL IN A DEFLATIONARY SPIRAL?

The deflationary spiral theory says that if prices are expected to fall, people will move purchases into the future in order to benefit from the lower prices. That fall in demand will in turn cause merchants to lower their prices to try and stimulate demand, making the problem worse and leading to an economic depression.

Although this theory is a popular way to justify inflation amongst central bankers, it does not appear to always hold true and is considered controversial amongst economists. Consumer electronics is one example of a market where prices constantly fall but which is not in depression. Similarly, the value of bitcoins has risen over time and yet the size of the Bitcoin economy has also grown dramatically along with it. Because both the value of the currency and the size of its economy started at zero in 2009, Bitcoin is a counterexample to the theory showing that it must sometimes be wrong.

Notwithstanding this, Bitcoin is not designed to be a deflationary currency. It is more accurate to say Bitcoin is intended to inflate in its

early years, and become stable in its later years. The only time the quantity of bitcoins in circulation will drop is if people carelessly lose their wallets by failing to make backups. With a stable monetary base and a stable economy, the value of the currency should remain the same.

8.1.30 ISN'T SPECULATION AND VOLATILITY A PROBLEM FOR BITCOIN?

This is a chicken and egg situation. For bitcoin's price to stabilize, a large scale economy needs to develop with more businesses and users. For a large scale economy to develop, businesses and users will seek for price stability.

Fortunately, volatility does not affect the main benefits of Bitcoin as a payment system to transfer money from point A to point B. It is possible for businesses to convert bitcoin payments to their local currency instantly, allowing them to profit from the advantages of Bitcoin without being subjected to price fluctuations. Since Bitcoin offers many useful and unique features and properties, many users choose to use Bitcoin. With such solutions and incentives, it is possible that Bitcoin will mature and develop to a degree where price volatility will become limited.

8.1.31 WHAT IF SOMEONE BOUGHT UP ALL THE EXISTING BITCOINS?

Only a fraction of bitcoins issued to date are found on the exchange markets for sale. Bitcoin markets are competitive, meaning the price of a bitcoin will rise or fall depending on supply and demand. Additionally, new bitcoins will continue to be issued for decades to come. Therefore even the most determined buyer could not buy all the bitcoins in existence. This situation isn't to suggest, however, that the markets aren't vulnerable to price manipulation; it still doesn't take significant amounts of money to move the market price up or down, and thus Bitcoin remains a volatile asset thus far.

8.1.32   WHAT IF SOMEONE CREATES A BETTER DIGITAL
          CURRENCY?

That can happen. For now, Bitcoin remains by far the most popular
decentralized virtual currency, but there can be no guarantee that it
will retain that position. There is already a set of alternative currencies
inspired by Bitcoin. It is however probably correct to assume that
significant improvements would be required for a new currency to
overtake Bitcoin in terms of established market, even though this
remains unpredictable. Bitcoin could also conceivably adopt
improvements of a competing currency so long as it doesn't change
fundamental parts of the protocol.

TRANSACTIONS

8.1.33   WHY DO I HAVE TO WAIT 10 MINUTES?

Receiving a payment is almost instant with Bitcoin. However, there is
a 10 minutes delay on average before the network begins to confirm
your transaction by including it in a block and before you can spend
the bitcoins you receive. A confirmation means that there is a
consensus on the network that the bitcoins you received haven't been
sent to anyone else and are considered your property. Once your
transaction has been included in one block, it will continue to be
buried under every block after it, which will exponentially consolidate
this consensus and decrease the risk of a reversed transaction. Every
user is free to determine at what point they consider a transaction
confirmed, but 6 confirmations is often considered to be as safe as
waiting 6 months on a credit card transaction.

8.1.34   HOW MUCH WILL THE TRANSACTION FEE BE?

Most transactions can be processed without fees, but users are
encouraged to pay a small voluntary fee for faster confirmation of their
transactions and to remunerate miners. When fees are required, they
generally don't exceed a few pennies in value. Your Bitcoin client will
usually try to estimate an appropriate fee when required.

Transaction fees are used as a protection against users sending transactions to overload the network. The precise manner in which fees work is still being developed and will change over time. Because the fee is not related to the amount of bitcoins being sent, it may seem extremely low (0.0005 BTC for a 1,000 BTC transfer) or unfairly high (0.004 BTC for a 0.02 BTC payment). The fee is defined by attributes such as data in transaction and transaction recurrence. For example, if you are receiving a large number of tiny amounts, then fees for sending will be higher. Such payments are comparable to paying a restaurant bill using only pennies. Spending small fractions of your bitcoins rapidly may also require a fee. If your activity follows the pattern of conventional transactions, the fees should remain very low.

8.1.35   WHAT IF I RECEIVE A BITCOIN WHEN MY COMPUTER IS POWERED OFF?

This works fine. The bitcoins will appear next time you start your wallet application. Bitcoins are not actually received by the software on your computer, they are appended to a public ledger that is shared between all the devices on the network. If you are sent bitcoins when your wallet client program is not running and you later launch it, it will download blocks and catch up with any transactions it did not already know about, and the bitcoins will eventually appear as if they were just received in real time. Your wallet is only needed when you wish to spend bitcoins.

8.1.36   WHAT DOES "SYNCHRONIZING" MEAN AND WHY DOES IT TAKE SO LONG?

Long synchronization time is only required with full node clients like Bitcoin Core. Technically speaking, synchronizing is the process of downloading and verifying all previous Bitcoin transactions on the network. For some Bitcoin clients to calculate the spendable balance of your Bitcoin wallet and make new transactions, it needs to be aware of all previous transactions. This step can be resource intensive and requires sufficient bandwidth and storage to accommodate the full size of the block chain. For Bitcoin to remain secure, enough

people should keep using full node clients because they perform the task of validating and relaying transactions.

MINING

8.1.37   WHAT IS BITCOIN MINING?

Mining is the process of spending computing power to process transactions, secure the network, and keep everyone in the system synchronized together. It can be perceived like the Bitcoin data center except that it has been designed to be fully decentralized with miners operating in all countries and no individual having control over the network. This process is referred to as "mining" as an analogy to gold mining because it is also a temporary mechanism used to issue new bitcoins. Unlike gold mining, however, Bitcoin mining provides a reward in exchange for useful services required to operate a secure payment network. Mining will still be required after the last bitcoin is issued.

8.1.38   HOW DOES BITCOIN MINING WORK?

Anybody can become a Bitcoin miner by running software with specialized hardware. Mining software listens for transactions broadcast through the peer-to-peer network and performs appropriate tasks to process and confirm these transactions. Bitcoin miners perform this work because they can earn transaction fees paid by users for faster transaction processing, and newly created bitcoins issued into existence according to a fixed formula.

For new transactions to be confirmed, they need to be included in a block along with a mathematical proof of work. Such proofs are very hard to generate because there is no way to create them other than by trying billions of calculations per second. This requires miners to perform these calculations before their blocks are accepted by the network and before they are rewarded. As more people start to mine, the difficulty of finding valid blocks is automatically increased by the network. This is to ensure that the average time to find a block remains equal to 10 minutes. As a result, mining is a very competitive

business where no individual miner can control what is included in the block chain.

The proof of work is also designed to depend on the previous block to force a chronological order in the block chain. This makes it exponentially difficult to reverse previous transactions because this requires the recalculation of the proofs of work of all the subsequent blocks. When two blocks are found at the same time, miners work on the first block they receive and switch to the longest chain of blocks as soon as the next block is found. This allows mining to secure and maintain a global consensus based on processing power.

Bitcoin miners are neither able to cheat by increasing their own reward nor process fraudulent transactions that could corrupt the Bitcoin network because all Bitcoin nodes would reject any block that contains invalid data as per the rules of the Bitcoin protocol. Consequently, the network remains secure even if not all Bitcoin miners can be trusted.

8.1.39   ISN'T BITCOIN MINING A WASTE OF ENERGY?

Spending energy to secure and operate a payment system is hardly a waste. Like any other payment service, the use of Bitcoin entails processing costs. Services necessary for the operation of currently widespread monetary systems, such as banks, credit cards, and armored vehicles, also use a lot of energy. Although unlike Bitcoin, their total energy consumption is not transparent and cannot be as easily measured.

Bitcoin mining has been designed to become more optimized over time with specialized hardware consuming less energy, and the operating costs of mining should continue to be proportional to demand. When Bitcoin mining becomes too competitive and less profitable, some miners choose to stop their activities. Furthermore, all energy expended mining is eventually transformed into heat, and the most profitable miners will be those who have put this heat to good use. An optimally efficient mining network is one that isn't actually consuming any extra energy. While this is an ideal, the economics of mining are such that miners individually strive toward it.

8.1.40   HOW DOES MINING HELP SECURE BITCOIN?

Mining creates the equivalent of a competitive lottery that makes it very difficult for anyone to consecutively add new blocks of transactions into the block chain. This protects the neutrality of the network by preventing any individual from gaining the power to block certain transactions. This also prevents any individual from replacing parts of the block chain to roll back their own spends, which could be used to defraud other users. Mining makes it exponentially more difficult to reverse a past transaction by requiring the rewriting of all blocks following this transaction.

8.1.41   WHAT DO I NEED TO START MINING?

In the early days of Bitcoin, anyone could find a new block using their computer's CPU. As more and more people started mining, the difficulty of finding new blocks increased greatly to the point where the only cost-effective method of mining today is using specialized hardware. You can visit BitcoinMining.com for more information.

SECURITY

8.1.42   IS BITCOIN SECURE?

The Bitcoin technology - the protocol and the cryptography - has a strong security track record, and the Bitcoin network is probably the biggest distributed computing project in the world. Bitcoin's most common vulnerability is in user error. Bitcoin wallet files that store the necessary private keys can be accidentally deleted, lost or stolen. This is pretty similar to physical cash stored in a digital form. Fortunately, users can employ sound security practices to protect their money or use service providers that offer good levels of security and insurance against theft or loss.

8.1.43   HASN'T BITCOIN BEEN HACKED IN THE PAST?

The rules of the protocol and the cryptography used for Bitcoin are still working years after its inception, which is a good indication that the concept is well designed. However, security flaws have been

found and fixed over time in various software implementations. Like any other form of software, the security of Bitcoin software depends on the speed with which problems are found and fixed. The more such issues are discovered, the more Bitcoin is gaining maturity.

There are often misconceptions about thefts and security breaches that happened on diverse exchanges and businesses. Although these events are unfortunate, none of them involve Bitcoin itself being hacked, nor imply inherent flaws in Bitcoin; just like a bank robbery doesn't mean that the dollar is compromised. However, it is accurate to say that a complete set of good practices and intuitive security solutions is needed to give users better protection of their money, and to reduce the general risk of theft and loss. Over the course of the last few years, such security features have quickly developed, such as wallet encryption, offline wallets, hardware wallets, and multi-signature transactions.

8.1.44   COULD USERS COLLUDE AGAINST BITCOIN?

It is not possible to change the Bitcoin protocol that easily. Any Bitcoin client that doesn't comply with the same rules cannot enforce their own rules on other users. As per the current specification, double spending is not possible on the same block chain, and neither is spending bitcoins without a valid signature. Therefore, It is not possible to generate uncontrolled amounts of bitcoins out of thin air, spend other users' funds, corrupt the network, or anything similar.

However, powerful miners could arbitrarily choose to block or reverse recent transactions. A majority of users can also put pressure for some changes to be adopted. Because Bitcoin only works correctly with a complete consensus between all users, changing the protocol can be very difficult and requires an overwhelming majority of users to adopt the changes in such a way that remaining users have nearly no choice but to follow. As a general rule, it is hard to imagine why any Bitcoin user would choose to adopt any change that could compromise their own money.

8.1.45 IS BITCOIN VULNERABLE TO QUANTUM COMPUTING?

Yes, most systems relying on cryptography in general are, including traditional banking systems. However, quantum computers don't yet exist and probably won't for a while. In the event that quantum computing could be an imminent threat to Bitcoin, the protocol could be upgraded to use post-quantum algorithms. Given the importance that this update would have, it can be safely expected that it would be highly reviewed by developers and adopted by all Bitcoin users.

Bitcoins are created as a reward for payment processing work in which users offer their computing power to verify and record payments into the public ledger. This activity is called mining and is rewarded by transaction fees and newly created bitcoins.

Bitcoin as a form of payment for products and services has grown, have warned that bitcoin users are not protected by refund rights or chargebacks.

The use of bitcoin by criminals has attracted the attention of financial regulators,

9.1.1 BLOCK CHAIN

The *block chain* is a public ledger that records bitcoin transactions. A novel solution accomplishes this without any trusted central authority: maintenance of the block chain is performed by a network of communicating nodes running bitcoin software.

9.1.2 UNITS

The unit of account of the bitcoin system is bitcoin. As of 2014 One *microbitcoin* equals to 0.000001 bitcoin, which is one millionth of bitcoin. A microbitcoin is sometimes referred to as a *bit*.

On 7 October 2014, the Bitcoin Foundation revealed a plan to apply for an ISO 4217 currency code for bitcoin,

9.1.3 OWNERSHIP
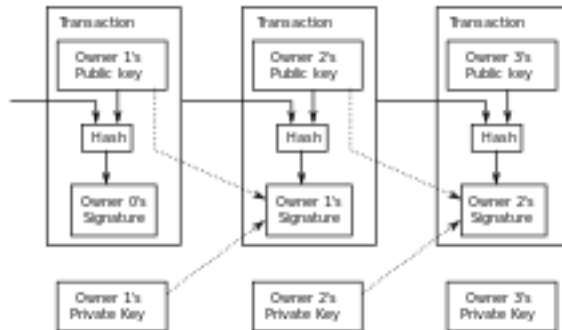
Simplified chain of ownership. In reality, a transaction can have more than one input and more than one output.

Ownership of bitcoins implies that a user can spend bitcoins associated with a specific address. To do so, a payer must digitally sign the transaction using the corresponding private key. Without knowledge of the private key the transaction cannot be signed and bitcoins cannot be spent. The network verifies the signature using the public key.

9.1.4 TRANSACTIONS

See also: Bitcoin network

A transaction must have one or more inputs. For the transaction to be valid, every input must be an unspent output of a previous transaction. Every input must be digitally signed. The use of multiple inputs corresponds to the use of multiple coins in a cash transaction. A transaction can also have multiple outputs, allowing one to make multiple payments in one go. A transaction output can be specified as an arbitrary multiple of satoshi. Similarly as in a cash transaction, the sum of inputs (coins used to pay) can exceed the intended sum of payments. In such case, an additional output is used, returning the change back to the payer. Any input satoshis not accounted for in the transaction outputs become the transaction fee.

To send money to a bitcoin address, users can click links on webpages; this is accomplished with a provisional bitcoin URI scheme

using a template registered with IANA. Bitcoin clients like Electrum and Armory support bitcoin URIs. Mobile clients recognize bitcoin URIs in QR codes, so that the user does not have to type the bitcoin address and amount in manually. The QR code is generated from the user input based on the payment amount. The QR code is displayed on the mobile device screen and can be scanned by a second mobile device.

9.1.5 MINING
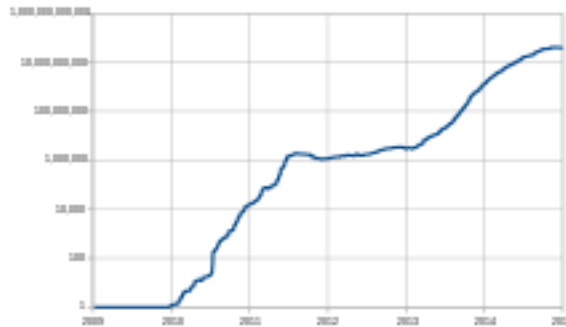
Relative mining difficulty from 2009-01-09 to 2014-12-31 (the difficulty scale is logarithmic). Relative mining difficulty is defined as the ratio between the difficulty target on 9 January 2009 and the current difficulty target.

ASICMiner Block Erupter, a type of mining hardware used in 2013.

Mining is a record-keeping service.

In order to be accepted by the rest of the network, a new block must contain a so-called *proof-of-work*. The proof-of-work requires miners to find a number called a *nonce*, such that when the block content is hashed along with the nonce, the result is numerically smaller than the network's *difficulty target*.) before meeting the difficulty target.

Every 2016 blocks (approximately 14 days), the difficulty target is adjusted based on the network's recent performance, with the aim of keeping the average time between new blocks at ten minutes. In this way the system automatically adapts to the total amount of mining power on the network.

The proof-of-work system, alongside the chaining of blocks, makes modifications of the block chain extremely hard as an attacker must modify all subsequent blocks in order for the modifications of one block to be accepted. As new blocks are mined all the time, the difficulty of modifying a block increases as time passes and the number of subsequent blocks (also called *confirmations* of the given block) increases.

9.1.5.1   Practicalities

It has become common for miners to join organized mining pools,

The rewards of mining have led to ever-more-specialized technology being utilized. The most efficient mining hardware makes use of custom designed application-specific integrated circuits, which outperform general purpose CPUs while using less power.

As of 2015, even if all miners used energy efficient processes, the combined electricity consumption would be 1.46 terawatt-hours per year—equal to the consumption of about 135,000 American homes.

9.1.6 SUPPLY
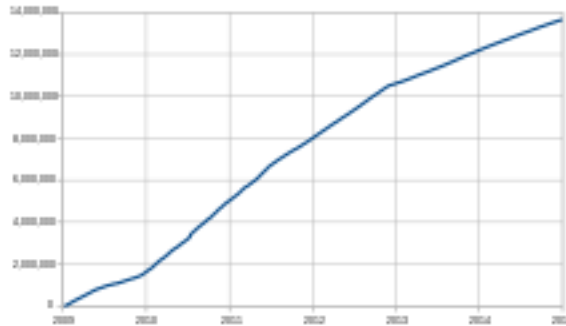
Total bitcoins in circulation. Horizontal axis: date ranging from 2009-01-09 to 2014-12-31.

The successful miner finding the new block is rewarded with newly created bitcoins and transaction fees.

9.1.7 TRANSACTION FEES

Paying a transaction fee is optional, but may speed up confirmation of the transaction.

9.1.8 WALLETS

See also: Digital wallet and Armory (software)
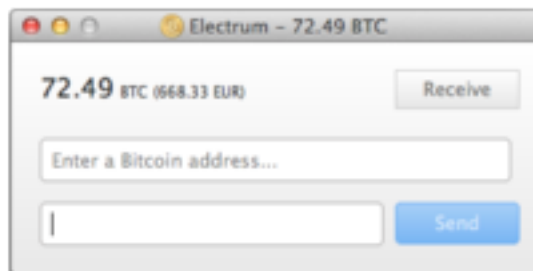
BA.net bitcoin wallet

Bitcoin paper wallet generated at ba.net

Trezor hardware wallet

A *wallet* stores the information necessary to transact bitcoins. While wallets are often described as a place to hold At its most basic, a wallet is a collection of these keys.

There are several types of wallet. *Software wallets* connect to the network and allow spending bitcoins in addition to holding the credentials that prove ownership.

9.1.8.1   Reference implementation

The first wallet program was released in 2009 by Satoshi Nakamoto as open-source code and was originally called bitcoind.

9.1.9 PRIVACY

Privacy is achieved by not identifying owners of bitcoin addresses while making other transaction data public. Bitcoin users are not

identified by name, but transactions can be linked to individuals and companies.

9.1.10   FUNGIBILITY

Wallets and similar software technically handle bitcoins as equivalent, establishing the basic level of fungibility. Researchers have pointed out that the history of every single bitcoin is registered and publicly available in the block chain ledger, and that some users may refuse to accept bitcoins coming from controversial transactions, which would harm bitcoin's fungibility.

HISTORY

Main article: History of bitcoin
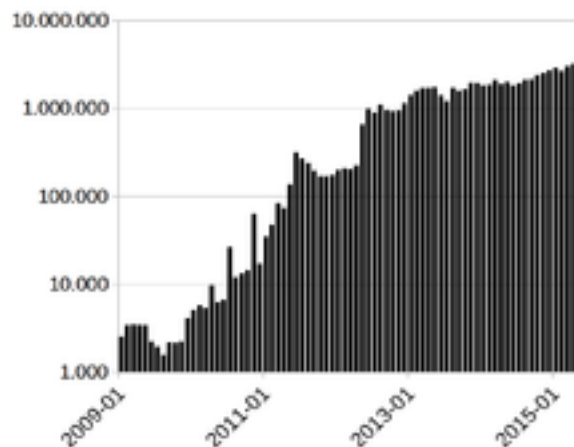
Number of bitcoin transactions per month (logarithmic scale)

Bitcoin was invented by Satoshi Nakamoto,

One of the first supporters, adopters, contributor to bitcoin and receiver of the first bitcoin transaction was programmer Hal Finney. Finney downloaded the bitcoin software the day it was released, and received 10 bitcoins from Nakamoto in the world's first bitcoin transaction.

Other early supporters were Wei Dai, creator of bitcoin predecessor *b-money*, and Nick Szabo, creator of bitcoin predecessor *bit gold*.

In 2010, an exploit in an early bitcoin client was found that allowed large numbers of bitcoins to be created.

Based on bitcoin's open source code, other cryptocurrencies started to emerge in 2011.

In March 2013, a technical glitch caused a fork in the block chain, with one half of the network adding blocks to one version of the chain and the other half adding to another. For six hours two bitcoin networks operated at the same time, each with its own version of the transaction history. The core developers called for a temporary halt to transactions, sparking a sharp sell-off.

In 2013 some mainstream websites began accepting bitcoins. WordPress had started in November 2012,)

In May 2013, the Department of Homeland Security seized assets belonging to the Mt. Gox exchange.

In October 2013, Chinese internet giant Baidu had allowed clients of website security services to pay with bitcoins.

The first bitcoin ATM was installed in October 2013 in Vancouver, British Columbia, Canada.

With about 12 million existing bitcoins in November 2013,

In the US two men were arrested in January 2014 on charges of money-laundering using bitcoins; one was Charlie Shrem, the head of now defunct bitcoin exchange BitInstant and a vice chairman of the Bitcoin Foundation. Shrem allegedly allowed the other arrested party to purchase large quantities of bitcoins for use on black-market websites.

In early February 2014, one of the largest bitcoin exchanges, Mt. Gox,

On June 18, 2014, it was announced that bitcoin payment service provider BitPay would become the new sponsor of St. Petersburg Bowl under a two-year deal, renamed the Bitcoin St. Petersburg Bowl.

Bitcoin was to be accepted for ticket and concession sales at the game as part of the sponsorship, and the sponsorship itself was also paid for using bitcoin.

Less than one year after the collapse of Mt. Gox, Bitstamp announced that the exchange would be taken offline while they investigate a hack which resulted in about 19,000 bitcoins (equivalent to roughly US$5 million at that time) being stolen from their hot wallet.

The bitcoin exchange service Coinbase launched the first regulated bitcoin exchange in 25 US states on January 26, 2015. At the time of the announcement, CEO Brian Armstrong stated that Coinbase intends to expand to thirty countries by the end of 2015.

ECONOMICS

9.1.11   CLASSIFICATION

According to the director of the Institute for Money, Technology and Financial Inclusion at the University of California-Irvine there is "an unsettled debate about whether bitcoin is a currency".

Economists define money as a store of value, a medium of exchange, and a unit of account and agree that bitcoin has some way to go to meet all these criteria.

Journalists and academics also dispute what to call bitcoin. Some media outlets do make a distinction between "real" money and bitcoins,

The People's Bank of China has stated that bitcoin "is fundamentally not a currency but an investment target".

9.1.12   BUYING AND SELLING

Bitcoins can be bought and sold both on- and offline. Participants in online exchanges offer bitcoin buy and sell bids. Using an online exchange to obtain bitcoins entails some risk, and, according to a study published in April 2013, 45% of exchanges fail and take client bitcoins with them.

9.1.13   PRICE AND VOLATILITY

Price Left vertical axis: price, the scale is logarithmic. Right vertical axis: volatility. Horizontal axis: date ranging from 2010-08-17 to 2014-12-31.

To improve access to price information and increase transparency, on 30 April 2014 Bloomberg LP announced plans to list prices from bitcoin companies Kraken and Coinbase on its 320,000 subscription financial data terminals.

According to Mark T. Williams, as of 2014

Attempting to explain the high volatility, a group of Japanese scholars stated that there is no stabilization mechanism.

There are uses where volatility does not matter, such as online gambling, tipping, and international remittances.

The price of bitcoins has gone through various cycles of appreciation and depreciation referred to by some as bubbles and busts.

9.1.14   SPECULATIVE BUBBLE DISPUTE

Bitcoin has been labelled a *speculative bubble* by many including former Fed Chairman Alan Greenspan

9.1.15   PONZI SCHEME DISPUTE

Various journalists,

U.S. economist Nouriel Roubini, former senior adviser to the U.S. Treasury and the International Monetary Fund, has stated that bitcoin is "a Ponzi game".

Others have expressed the opinion that bitcoin is not a Ponzi scheme. The Huffington Post asked, "is bitcoin a Ponzi scheme, yes or no?" answering the question with a definitive "no!".

9.1.16   VALUE FORECASTS

Financial journalists and analysts, economists, and investors have attempted to predict the possible future value of bitcoin. In April 2013, economist John Quiggin stated, "bitcoins will attain their true value of zero sooner or later, but it is impossible to say when".

9.1.17   BITCOIN OBITUARIES

The "death" of bitcoin has been proclaimed numerous times.

9.1.18   RECEPTION

Some economists have responded positively to bitcoin, but many have not. François R. Velde, Senior Economist at the Chicago Fed described it as "an elegant solution to the problem of creating a digital currency".

David Andolfatto, Vice President at the Federal Reserve Bank of St. Louis, stated that bitcoin is a threat to the establishment, which he argues is a good thing for the Federal Reserve System and other central banks because it prompts these institutions to operate sound policies.

Free software movement activist Richard Stallman has criticized the lack of anonymity and called for reformed development.

Similarly, Peter Schiff, a bitcoin sceptic understands "the value of the technology as a payment platform" and his Euro Pacific Precious Metals fund partnered with BitPay in May 2014, because "a wire transfer of fiat funds can be slow and expensive for the customer".

Kevin Dowd, Professor of Finance and economics at Durham University has a bearish outlook on bitcoin. His presentation at the Cato Institute 2014 Annual Conference, Alternatives to Central Banking: Toward Free-Market Money, touched on bitcoin.

9.1.19 ACCEPTANCE BY MERCHANTS

Bitcoins are accepted in this café in the Netherlands as of 2013

In 2015, the number of merchants accepting bitcoin exceeded 100,000.

As of September 2014 PayPal allows North American merchants using its system the ability to receive payment in bitcoins.

Organizations accepting donations in bitcoin include: Greenpeace,

9.1.19.1 Mainstream use of bitcoin

As of February 2015

9.1.20 FINANCIAL INSTITUTIONS

Bitcoin companies have had difficulty opening traditional bank accounts because lenders have been leery of bitcoin's links to illicit activity.

One financial institution has been bullish on bitcoin. In a 2013 report, Bank of America Merrill Lynch stated that "we believe bitcoin can

become a major means of payment for e-commerce and may emerge as a serious competitor to traditional money-transfer providers."

9.1.21 AS INVESTMENT

Some Argentinians have bought bitcoins to protect their savings against high inflation or the possibility that governments could confiscate savings accounts.

In 2013 and 2014, the European Banking Authority

In May 2015, Intercontinental Exchange Inc., parent company of the New York Stock Exchange, announced a bitcoin index initially based on data from Coinbase transactions.

9.1.22 VENTURE CAPITAL

Venture capitalists, such as Peter Thiel's Founders Fund, which invested US$3 million in BitPay, do not purchase bitcoins themselves, instead funding bitcoin infrastructure like companies that provide payment systems to merchants, exchanges, wallet services, etc.

9.1.23 POLITICAL ECONOMY

Bitcoin appeals to tech-savvy libertarians, because it so far exists outside the institutional banking system and the control of governments.

Bitcoin's appeal reaches from left wing critics, "who perceive the state and banking sector as representing the same elite interests, [...] recognising in it the potential for collective direct democratic governance of currency"

LEGAL STATUS AND REGULATION

In April 2013, Steven Strauss, a Harvard public policy professor, suggested that governments could outlaw bitcoin,

9.1.24   AUSTRALIA

Australia classifies bitcoin as property and an asset for capital gains purposes, however capital gains or losses arising from personal use of bitcoins is disregarded providing the cost of the bitcoins was less than $10,000.

9.1.25   CHINA

While private parties can hold and trade bitcoins in China, regulation prohibits financial firms like banks from doing the same.

9.1.26   EUROPEAN UNION

The European Central Bank classifies bitcoin as a convertible decentralized virtual currency.

9.1.27   ICELAND

As of 2014, foreign exchange activities with bitcoin are illegal in Iceland.

9.1.28   RUSSIA

CNBC reported that bitcoin was illegal in Russia in December, 2014,

9.1.29   TAIWAN

While bitcoin itself is not illegal here, bitcoin ATMs are prohibited.

9.1.30   THAILAND

In 2013, the Thai monetary authority, the Bank of Thailand, "issued a preliminary ruling that using bitcoins as described was illegal."

9.1.31   UNITED STATES

The U.S. Treasury classified bitcoin as a convertible decentralized virtual currency in 2013.

The U.S. Government Accountability Office (GAO) recommended in May 2013, that the Internal Revenue Service (IRS) formulate a tax guidance for bitcoin businesses.

In November 2013, the United States Senate held a committee hearing titled "Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies" to discuss virtual currencies.

The Federal Election Commission (FEC) deadlocked in November 2013 on whether to allow bitcoin in political campaigns with three Democrat members voting nay, three Republicans voting yea.

In May 2014, Brett Stapper, co-founder of Falcon Global Capital, registered to lobby members of Congress and federal agencies on issues related to bitcoin.

In January 2014, the U.S. Securities and Exchange Commission (SEC) focused on whether bitcoin-denominated stock exchanges were illegal, and inquired into unregistered securities offerings of the gambling site SatoshiDice and FeedZeBirds.

The U.S. Commodity Futures Trading Commission (CFTC) stated in March 2014 it considered regulation of digital currencies

In June 2014 California Assemblyman Roger Dickinson (D–Sacramento) submitted draft legislation (Assembly Bill 129) to legalize bitcoin and other forms of alternative and digital currency.

As of May 2015

9.1.32   VIETNAM

Vietnamese authorities have deemed bitcoin trading illegal.

CRIMINAL ACTIVITY

The use of bitcoin by criminals has attracted the attention of financial regulators, legislative bodies, law enforcement, and the media.

Several news outlets have asserted that the popularity of bitcoins hinges on the ability to use them to purchase illegal goods.

9.1.33   THEFT

There have been many cases of bitcoin theft.

Theft also occurs at sites bitcoins are used to purchase illicit goods. In late November 2013, an estimated $100 million in bitcoins were stolen from the online illicit goods marketplace Sheep Marketplace, which immediately closed.

Sites where users exchange bitcoins for cash are another target for theft. In late February 2014 Mt. Gox, one of the largest virtual currency exchanges, filed for bankruptcy in Tokyo amid reports that 744,000 bitcoins had been stolen.

9.1.34   BLACK MARKETS

A CMU researcher estimated that in 2012, 4.5% to 9% of all transactions on all exchanges in the world were for drug trades on a single deep web drugs market, Silk Road. are also available on black market sites that sell in bitcoin.

Several deep web black markets have been shut by authorities. In October 2013 Silk Road was shut down by U.S. law enforcement

Some black market sites may seek to steal bitcoins from customers. The bitcoin community branded one site, Sheep Marketplace, as a scam when it prevented withdrawals and shut down after an alleged bitcoins theft.

According to the Internet Watch Foundation, a U.K. based charity, bitcoin is used to purchase child pornography, and almost 200 such websites accept it as payment. Bitcoin isn't the sole way to purchase child pornography online, as Troels Oertling, head of the cybercrime unit at Europol, states, "Ukash and Paysafecard... have [also] been used to pay for such material." However, the Internet Watch Foundation lists around 30 sites that exclusively accept bitcoins.

9.1.35   MONEY LAUNDERING

Bitcoins may not be ideal for money laundering because all transactions are public.

9.1.36   PONZI SCHEME

In a Ponzi scheme that utilized bitcoins, The Bitcoin Savings and Trust promised investors up to 7 percent weekly interest, and raised at least 700,000 bitcoins from 2011 to 2012.

9.1.37   MALWARE

Bitcoin-related malware includes software that steals bitcoins from users using a variety of techniques, software that uses infected computers to mine bitcoins, and different types of ransomware, which disable computers or prevent files from being accessed until some payment is made. Security company Dell SecureWorks said in February 2014 that it had identified almost 150 types of bitcoin malware.

9.1.37.1   Unauthorized mining

In June 2011, Symantec warned about the possibility that botnets could mine covertly for bitcoins.

In mid-August 2011, bitcoin mining botnets were detected,

In April 2013, electronic sports organization E-Sports Entertainment was accused of hijacking 14,000 computers to mine bitcoins; the company later settled the case with the State of New Jersey.

German police arrested two people in December 2013 who customized existing botnet software to perform bitcoin mining, which police said had been used to mine at least $950,000 worth of bitcoins.

For four days in December 2013 and January 2014, Yahoo! Europe hosted an ad containing bitcoin mining malware that infected an estimated two million computers.

Several reports of employees or students using university or research computers to mine bitcoins have been published.

9.1.37.2 Malware stealing

Some malware can steal private keys for bitcoin wallets allowing the bitcoins themselves to be stolen. The most common type searches computers for cryptocurrency wallets to upload to a remote server where they can be cracked and their coins stolen. This method is effective because bitcoin transactions are irreversible.

One virus, spread through the Pony botnet, was reported in February 2014 to have stolen up to $220,000 in cryptocurrencies including bitcoins from 85 wallets.

A type of Mac malware active in August 2013, Bitvanity posed as a vanity wallet address generator and stole addresses and private keys from other bitcoin client software.

9.1.37.3 Ransomware

Another type of bitcoin-related malware is ransomware. One program called CryptoLocker, typically spread through legitimate-looking email attachments, encrypts the hard drive of an infected computer, then displays a countdown timer and demands a ransom, usually two bitcoins, to decrypt it.

SECURITY

Various potential attacks on the bitcoin network and its use as a payment system, real or theoretical, have been considered. The bitcoin protocol includes several features that protect it against some of those attacks, such as unauthorized spending, double spending, forging bitcoins, and tampering with the block chain. Other attacks, such as theft of private keys, require due care by users.

9.1.38   UNAUTHORIZED SPENDING

Unauthorized spending is mitigated by bitcoin's implementation of public-private key cryptography. When Alice sends a bitcoin to Bob, Bob becomes the new owner of the bitcoin. Eve observing the transaction might want to spend the bitcoin Bob just received, but she cannot sign the transaction without the knowledge of Bob's private key.

9.1.39   DOUBLE SPENDING

A specific problem that an internet payment system must solve is double-spending, whereby a user pays the same coin to two or more different recipients. An example of such a problem would be if Eve sent a bitcoin to Alice and later sent the same bitcoin to Bob. The bitcoin network guards against double-spending by recording all bitcoin transfers in a ledger (the block chain) that is visible to all users, and ensuring for all transferred bitcoins that they haven't been previously spent.

9.1.40   RACE ATTACK

If Eve offers to pay Alice a bitcoin in exchange for goods and signs a corresponding transaction, it is still possible that she also creates a different transaction at the same time sending the same bitcoin to Bob. By the rules, the network accepts only one of the transactions. This is called race attack, since there is a race which transaction will be accepted first. Alice can reduce the risk of race attack stipulating that she will not deliver the goods until Eve's payment to Alice appears in the block chain.

A variant race attack (which has been called a Finney attack by reference to Hal Finney) requires the participation of a miner. Instead of sending both payment requests (to pay Bob and Alice with the same coins) to the network, Eve issues only Alice's payment request to the network, while the accomplice tries to mine a block that includes the payment to Bob instead of Alice. There is a positive probability that the rogue miner will succeed before the network, in which case the payment to Alice will be rejected. As with the plain

double-spending attack, Alice can reduce the risk of a Finney attack by waiting for the payment to be included in the block chain.

9.1.41   HISTORY MODIFICATION

The other principal way to steal bitcoins would be to modify block chain ledger entries.

For example, Eve could buy something from Alice, like a sofa, by adding a signed entry to the block chain ledger equivalent to *Eve pays Alice 100 bitcoins*. Later, after receiving the sofa, Eve could modify that block chain ledger entry to read instead: *Eve pays Alice 1 bitcoin*, or replace Alice's address by another of Eve's addresses. Digital signatures cannot prevent this attack: Eve can simply sign her entry again after modifying it.

To prevent modification attacks, each block of transactions that is added to the block chain includes a cryptographic hash code that is computed from the hash of the previous block as well as all the information in the block itself. When the bitcoin software notices two competing block chains, it will automatically assume that the chain with the greatest amount of work to produce it is the valid one. Therefore, in order to modify an already recorded transaction (as in the above example), the attacker would have to recalculate not just the modified block, but all the blocks after the modified one, until the modified chain contains more work than the legitimate chain that the rest of the network has been building in the meantime. Consequently, for this attack to succeed, the attacker must outperform the honest part of the network.

Each block that is added to the block chain, starting with the block containing a given transaction, is called a confirmation of that transaction. Ideally, merchants and services that receive payment in bitcoin should wait for at least one confirmation to be distributed over the network, before assuming that the payment was done. The more confirmations that the merchant waits for, the more difficult it is for an attacker to successfully reverse the transaction in a block chain—unless the attacker controls more than half the total network power, in which case it is called a 51% attack.

9.1.42   SELFISH MINING

This attack was first introduced by Ittay Eyal and Emin Gun Sirer at the beginning of November 2013. In this attack, the attacker finds blocks but does not broadcast them. Instead, the attacker mines their own private chain and eventually (when another miner or network of miners finds their own block) publishes several private blocks in a row. This forces the "honest" network to abandon their previous work and switch to the attacker's branch. As a result, honest miners lose a significant part of their revenue, while the attacker increases their profits due to changes in relative hashpowers.

According to the authors, a rational miner observing a selfish mining attacker would have an incentive to join the attacker's pool, thereby increasing the attacker's hashpower. This makes the attack and incentives even stronger, thus potentially leading to a 51% attack and the collapse of the currency.

Gavin Andresen and Ed Felten disagreed with this conclusion,

9.1.43   DEANONYMISATION OF CLIENTS

Along with transaction graph analysis, which may reveal connections between bitcoin addresses (pseudonyms),

NON-BITCOIN APPLICATIONS OF THE BLOCK CHAIN

In January 2015 IBM's Institute for Business Value announced ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) where network-connected devices can interact autonomously on the Internet of things using freely available technology including bittorrent, Telehash, and bitcoin.

In May 2015 NASDAQ announced its intention to use bitcoins of negligible value, called "colored coins", to represent and transfer pre-IPO trading shares on Nasdaq Private Markets.

BLOCK CHAIN SPAM

While it is possible to store any digital file in the block chain, the larger the transaction size the larger any associated fees become.

IN THE MEDIA

Several lighthearted songs celebrating bitcoin have been released.

In Season 3 CBS show *The Good Wife* featured an episode alluding to the creator of bitcoin as well as the FBI investigating the case. The episode titled 'Bitcoin for Dummies' was shown in early 2012.

A bitcoin documentary film called *The Rise and Rise of Bitcoin* was released in late 2014 and features interviews with people who use bitcoin such as a computer programmer and a drug dealer.

In the fall of 2014, undergraduate students at the Massachusetts Institute of Technology (MIT) each received bitcoins worth $100 "to better understand this emerging technology".

In early 2015, the CNN series *Inside Man* featured an episode about bitcoin. Filmed in July, 2014, it featured Morgan Spurlock living off of bitcoins for a week to figure out whether the world is ready for a new kind of money.

In science fiction novel *Neptune's Brood* by Charles Stross a modification of bitcoin is used as the universal interstellar payment system. The functioning of the system is a major plot element of the book.

10 HISTORY OF BITCOIN

From Wikipedia, the free encyclopedia
Jump to: navigation, search
Further information: Bitcoin
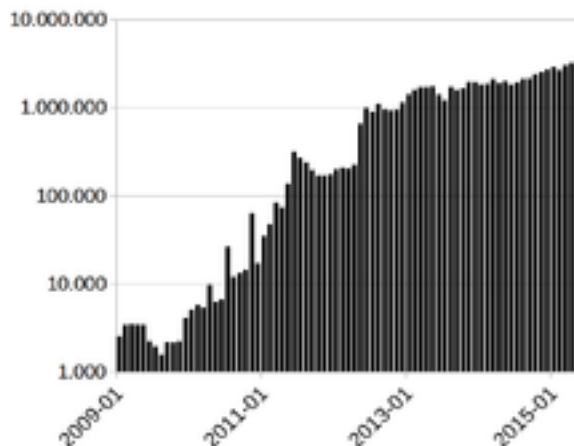
Number of Bitcoin transactions per month (logarithmic scale)

Bitcoin is a cryptocurrency, a form of money that uses cryptography to control its creation and management, rather than relying on central authorities. However, not all of the technologies and concepts that make up Bitcoin are new; the presumed pseudonymous Satoshi Nakamoto (the creator of Bitcoin, see below) integrated many existing ideas from the cypherpunk community when creating bitcoin.

CONTENTS

- 1 Pre-history
- 2 Creation
- 3 Growth
- 4 Prices and value history
- 5 Satoshi Nakamoto
- 6 The fork of March 2013
- 7 Regulatory issues
- 8 Theft and exchange shutdowns

PRE-HISTORY

Prior to the release of Bitcoin there were a number of precursor ecash technologies starting with the issuer based ecash protocols of David Chaum and Stefan Brands, and moving on to distributed digital scarcity based ecash protocols starting from Adam Back's hashcash, Wei Dai's b-money, Nick Szabo's bit-gold and Hal Finney's RPOW which build on hashcash.

Independently and at around the same time Wei Dai proposed b-money Subsequently Hal Finney implemented and deployed RPOW a reusable form of hashcash based on IBM secure TPM hardware and remote attestation (centralized but with no issuer inflation risk).

Since the initial bit-gold proposal which proposed a collectible market based mechanism for inflation control Nick Szabo also investigated some additional enabling aspects for decentralized asset registers including Byzantine network issues.

There has been much speculation as to the identity of Satoshi Nakamoto with suspects including Wei Dai, Hal Finney and accompanying denials.

CREATION

In November 2008, a paper was posted on the internet under the name Satoshi Nakamoto titled *Bitcoin: A Peer-to-Peer Electronic Cash System*. This paper detailed methods of using a peer-to-peer network to generate what was described as "a system for electronic transactions without relying on trust".

On 6 August 2010, a major vulnerability in the bitcoin protocol was spotted. Transactions weren't properly verified before they were included in the transaction log or "block chain" which let users bypass

bitcoin's economic restrictions and create an indefinite number of bitcoins.

GROWTH

Wikileaks

In January 2012, Bitcoin was featured as the main subject within a fictionalized trial on the CBS legal drama *The Good Wife* in the third season episode "Bitcoin for Dummies". The host of CNBC's *Mad Money*, Jim Cramer, played himself in a courtroom scene where he testifies that he doesn't consider bitcoin a true currency, saying "There's no central bank to regulate it; it's digital and functions completely peer to peer".

In October 2012, BitPay reported having over 1,000 merchants accepting bitcoin under its payment processing service.

In February 2013 the Bitcoin-based payment processor Coinbase reported selling US$1 million worth of bitcoins in a single month at over $22 per bitcoin.

In March the Bitcoin transaction log or "block chain" temporarily forked into two independent logs with differing rules on how transactions could be accepted. The Mt. Gox exchange briefly halted bitcoin deposits and the exchange rate briefly dipped by 23% to $37 as the event occurred

In April, payment processors *BitInstant* and *Mt. Gox* experienced processing delays due to insufficient capacity

Bitcoin gained greater recognition when services such as OkCupid and Foodler began accepting it for payment.

On 15 May 2013, the US authorities seized accounts associated with Mt. Gox after discovering that it had not registered as a money transmitter with FinCEN in the US.

On 23 June 2013, it was reported that the US Drug Enforcement Administration listed 11.02 bitcoins as a seized asset in a United States Department of Justice seizure notice pursuant to 21 U.S.C. § 881.

In July 2013 a project began in Kenya linking bitcoin with M-Pesa, a popular mobile payments system, in an experiment designed to spur innovative payments in Africa.

On 6 August 2013, Federal Judge Amos Mazzant of the Eastern District of Texas of the Fifth Circuit ruled that bitcoins are "a currency or a form of money" (specifically securities as defined by Federal Securities Laws), and as such were subject to the court's jurisdiction,

In October 2013, the FBI seized roughly 26,000 BTC from website Silk Road during the arrest of alleged owner Ross William Ulbricht.

Two companies, Robocoin and Bitcoiniacs launched the world's first bitcoin ATM on 29 October 2013 in Vancouver, BC, Canada, allowing clients to sell or purchase bitcoin currency at a downtown coffee shop.

In November 2013, the University of Nicosia announced that it would be accepting bitcoin as payment for tuition fees, with the university's chief financial officer calling it the "gold of tomorrow".

In September 2014 TeraExchange, LLC, received approval from the U.S.Commodity Futures Trading Commission "CFTC" to begin listing an over-the-counter swap product based on the price of a bitcoin. The CFTC swap product approval marks the first time a U.S. regulatory agency approved a bitcoin financial product.

PRICES AND VALUE HISTORY

The price of a bitcoin reached an all-time high of US$1124.76 on 29 November 2013, up from just US$13.36 on 5 January at the start of the year; the price subsequently dropped into the $200-$300 range.

Among the factors which may have contributed to this rise were the European sovereign-debt crisis—particularly the 2012–2013 Cypriot financial crisis—statements by FinCEN improving the currency's legal standing and rising media and Internet interest.

As the market valuation of the total stock of bitcoins approached US$1 billion, some commentators called bitcoin prices a bubble. bitcoin passed a US$1000 all-time high on 28 November 2013 at MtGox.

Prices fell to around $400 in April 2014, before rallying in the middle of the year. They then declined to not much more than $200 in early 2015.

Until 2013 almost all market with bitcoins were in US $.

Bitcoin value history (comparison to US$)

Date	Price for 1 BTC	Notes
Jan 2009 – Jan 2010	basically none	No exchanges or market, users were mainly cryptography fans who were sending bitcoins for low or no value.

Feb 2010 – May 2010	less than $0.01	User "laszlo" made the first real-world transaction – he bought 2 pizzas for 10,000 BTC.
June 2010	$0.08	In five days, the price grew 1000%, rising from $0.008 to $0.08 for 1 bitcoin.
Feb 2011 – April 2011	$1	Bitcoin takes parity with US dollar.
8 July 2011	$31	top of first "bubble", followed by the first price drop
Dec 2011	$2	minimum after few months
Dec 2012	$13	slowly rising for a year
April 11, 2013	$266	top of a price rally, during which the value was growing by 5-10% daily.
May 2013	$130	basically stable, again slowly rising.
June 2013	$100	in June slowly dropping to $70, but rising in July to $110
Nov 2013	$350 – $1250	from October $150–$200 in November, rising to $400, then $600, eventually reaching $900 on 11/19/2013 and breaking $1000 threshold on 27 November 2013.
Dec 2013	$600 – $1000	Price crashed to $600, rebounded to $1,000, crashed again to the $500 range. Stabilized to the ~$650–$800 range.
Jan 2014	$750 – $1000	Price spiked to $1000 briefly, then settled in the $800–$900 range for the rest of the month.
Feb 2014	$550 – $750	Price fell following the shutdown of MTGOX before recovering to the $600–$700 range.
Mar 2014	$450 – $700	Price continued to fall due to a false report regarding bitcoin ban in China
Apr 2014	$340 – $530	The lowest price since the 2012–2013 Cypriot financial crisis had been reached at 3:25 AM on April 11
May 2014	$440 – $630	The downtrend first slow down and then reverse, increasing over 30% in the last days of

May.

Mar 2015	$200 – $300	Price fell through to early 2015.

SATOSHI NAKAMOTO

Main article: Satoshi Nakamoto

"Satoshi Nakamoto" is presumed to be a pseudonym for the person or people who designed the original bitcoin protocol in 2008 and launched the network in 2009. Nakamoto was responsible for creating the majority of the official bitcoin software and was active in making modifications and posting technical information on the BitcoinTalk Forum.

Investigations into the real identity of Satoshi Nakamoto were attempted by *The New Yorker* and *Fast Company*. *The New Yorker's* investigation brought up at least two possible candidates: Michael Clear and Vili Lehdonvirta. *Fast Company's* investigation brought up circumstantial evidence linking an encryption patent application filed by Neal King, Vladimir Oksman and Charles Bry on 15 August 2008, and the bitcoin.org domain name which was registered 72 hours later. The patent application (#20100042841) contained networking and encryption technologies similar to bitcoin's, and textual analysis revealed that the phrase "... computationally impractical to reverse" appeared in both the patent application and bitcoin's whitepaper.

Nakamoto's involvement with bitcoin does not appear to extend past mid-2010.

Stefan Thomas, a Swiss coder and active community member, graphed the time stamps for each of Nakamoto's 500-plus bitcoin forum posts; the resulting chart showed a steep decline to almost no posts between the hours of 5 a.m. and 11 a.m. Greenwich Mean Time. Because this pattern held true even on Saturdays and Sundays, it suggested that Nakamoto was asleep at this time, and the hours of 5 a.m. to 11 a.m. GMT are midnight to 6 a.m. Eastern Standard Time (North American Eastern Standard Time). Other clues suggested that Nakamoto was British: A newspaper headline he had encoded in the genesis block came from the UK-published newspaper *The Times*,

and both his forum posts and his comments in the bitcoin source code used British English spellings, such as "optimise" and "colour".

An Internet search by an anonymous blogger of texts similar in writing to the bitcoin whitepaper suggests Nick Szabo's "bit gold" articles as having a similar author.

In a March 2014 article in *Newsweek,* journalist Leah McGrath Goodman doxed Dorian S. Nakamoto of Temple City, California, saying that Satoshi Nakamoto is the man's birth name.

THE FORK OF MARCH 2013

On 12 March 2013, a bitcoin miner running version 0.8.0 of the bitcoin software created a large invalid block. This created a split or "fork" in the block chain since computers with the recent version of the software accepted the invalid block and continued to build on the diverging chain, whereas older versions of the software rejected it and continued extending the block chain without the offending block. This split resulted in two separate transaction logs being formed without clear consensus, which allowed for the same funds to be spent differently on each chain. In response, the Mt. Gox exchange temporarily halted bitcoin deposits.

Miners resolved the split by downgrading to version 0.7, putting them back on track with the canonical blockchain. User funds largely remained unaffected and were available when network consensus was restored.

REGULATORY ISSUES

On 18 March 2013, the Financial Crimes Enforcement Network (or FinCEN), a bureau of the United States Department of the Treasury, issued a report regarding centralized and decentralized "virtual currencies" and their legal status within "money services business" (MSB) and Bank Secrecy Act regulations.

Additionally, FinCEN claimed regulation over American entities that manage bitcoins in a payment processor setting or as an exchanger:

"In addition, a person is an exchanger and a money transmitter if the person accepts such de-centralized convertible virtual currency from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency."

In summary, FinCEN's decision would require bitcoin exchanges where bitcoins are traded for traditional currencies to disclose large transactions and suspicious activity, comply with money laundering regulations, and collect information about their customers as traditional financial institutions are required to do.

Patrick Murck of the Bitcoin Foundation criticized FinCEN's report as an "overreach" and claimed that FinCEN "cannot rely on this guidance in any enforcement action".

Jennifer Shasky Calvery, the director of FinCEN said, "Virtual currencies are subject to the same rules as other currencies. ... Basic money-services business rules apply here."

In its October 2012 study, *Virtual currency schemes*, the European Central Bank concluded that the growth of virtual currencies will continue, and, given the currencies' inherent price instability, lack of close regulation, and risk of illegal uses by anonymous users, the Bank warned that periodic examination of developments would be necessary to reassess risks.

In 2013, the U.S. Treasury extended its anti-money laundering regulations to processors of bitcoin transactions.

In June 2013, Bitcoin Foundation board member Jon Matonis wrote in *Forbes* that he received a warning letter from the California Department of Financial Institutions accusing the foundation of unlicensed money transmission. Matonis denied that the foundation is engaged in money transmission and said he viewed the case as "an opportunity to educate state regulators."

In late July 2013, the industry group Committee for the Establishment of the Digital Asset Transfer Authority began to form to set best

practices and standards, to work with regulators and policymakers to adapt existing currency requirements to digital currency technology and business models and develop risk management standards.

In 2014, the U.S. Securities and Exchange Commission filed an administrative action against Erik T. Voorhees, for violating Securities Act Section 5 for publicly offering unregistered interests in two bitcoin websites in exchange for bitcoins.

THEFT AND EXCHANGE SHUTDOWNS

Theft of bitcoin has been documented on numerous occasions. At other times, bitcoin exchanges have shut down, taking their clients' bitcoins with them. A *Wired* study published April 2013 showed that 45 percent of bitcoin exchanges end up closing.

On 19 June 2011, a security breach of the Mt. Gox bitcoin exchange caused the nominal price of a bitcoin to fraudulently drop to one cent on the Mt. Gox exchange, after a hacker used credentials from a Mt. Gox auditor's compromised computer illegally to transfer a large number of bitcoins to himself. They used the exchange's software to sell them all nominally, creating a massive "ask" order at any price. Within minutes, the price reverted to its correct user-traded value.

In July 2011, the operator of Bitomat, the third-largest bitcoin exchange, announced that he lost access to his wallet.dat file with about 17,000 bitcoins (roughly equivalent to US$220,000 at that time). He announced that he would sell the service for the missing amount, aiming to use funds from the sale to refund his customers.

In August 2011, MyBitcoin, a now defunct bitcoin transaction processor, declared that it was hacked, which caused it to be shut down, paying 49% on customer deposits, leaving more than 78,000 bitcoins (equivalent to roughly US$800,000 at that time) unaccounted for.

In early August 2012, a lawsuit was filed in San Francisco court against Bitcoinica — a bitcoin trading venue — claiming about US$460,000 from the company. Bitcoinica was hacked twice in 2012,

which led to allegations that the venue neglected the safety of customers' money and cheated them out of withdrawal requests.

In late August 2012, an operation titled Bitcoin Savings and Trust was shut down by the owner, leaving around US$5.6 million in bitcoin-based debts; this led to allegations that the operation was a Ponzi scheme.

In September 2012, Bitfloor, a bitcoin exchange, also reported being hacked, with 24,000 bitcoins (worth about US$250,000) stolen. As a result, Bitfloor suspended operations.

On 3 April 2013, Instawallet, a web-based wallet provider, was hacked,

On 11 August 2013, the Bitcoin Foundation announced that a bug in a pseudorandom number generator within the Android operating system had been exploited to steal from wallets generated by Android apps; fixes were provided 13 August 2013.

In October 2013, Inputs.io, an Australian-based bitcoin wallet provider was hacked with a loss of 4100 bitcoins, worth over A$1 million at time of theft. The service was run by the operator TradeFortress. Coinchat, the associated bitcoin chat room, has been taken over by a new admin.

On 26 October 23, a Hong-Kong based bitcoin trading platform owned by Global Bond Limited (GBL) vanished with 30 million yuan (US$5 million) from 500 investors.

On 3 March 2014, Flexcoin announced it was closing its doors because of a hack attack that took place the day before. Users can no longer log in to the site.

TAXATION AND REGULATION

In 2012, the Cryptocurrency Legal Advocacy Group (CLAG) stressed the importance for taxpayers to determine whether taxes are due on a bitcoin-related transaction based on whether one has experienced a

"realization event": when a taxpayer has provided a service in exchange for bitcoins, a realization event has probably occurred and any gain or loss would likely be calculated using fair market values for the service provided."

In August 2013, the German Finance Ministry characterized bitcoin as a unit of account,

On 5 December 2013, the People's Bank of China announced in a press release regarding bitcoin regulation that whilst individuals in China are permitted to freely trade and exchange bitcoins as a commodity, it is prohibited for Chinese financial banks to operate using bitcoins or for bitcoins to be used as legal tender currency, and that entities dealing with bitcoins must track and report suspicious activity to prevent money laundering.

SPORTS SPONSORSHIP

On June 18, 2014, it was announced that Bitcoin payment service provider BitPay would become the new sponsor of St. Petersburg Bowl under a two-year deal, renamed the *Bitcoin St. Petersburg Bowl*. Bitcoin will be accepted for ticket and concession sales at the game as part of the sponsorship, and the sponsorship itself was also paid for using Bitcoin.

11 PGP QUICK START

PGP is a public key encryption program created by Philip R. Zimmermann. It allows users to perform several useful functions:

- **Sign a plaintext message** so that someone will be sure it came from you.
- **Encrypt a message** so that only one user (or a list of users) can decrypt it.
- **Sign and encrypt a message** so that it can only have come from you and can only be decrypted one user (or a list of users).

And once you're set up, other users will be able to do the same to you. It is remarkably easy to use once you get over the initial learning curve. The purpose of this page is just to be a cookbook to get you over that hump.

The BA.net PGP WebApp is the simplest way to get started and experimen with PGP.

GETTING STARTED

11.1.1   KEY PAIR GENERATION

The first thing you must do is generate your pgp key pair. You will be asked for user ID which should usually be your full name and email address, and a "pass phrase" which proves to PGP you are allowed to use your secret key to sign or decrypt messages.

11.1.2   KEY EXTRACTION

The next thing you need to do is to extract you public key so that you can distribute it to others with whom you communicate.

iPad 📶   14:55   99% 🔋

ba.net/util/pgp/new/generate1.html   Google

Hacker News   ✕ BA.net Bitcoin Address - Best Client Side Serverl...   +

Store Keys . Web PGP/GPG 🔒
Generate Keys . Decrypt . Encrypt
Bitcoin . PGP Help

Web Based PGP / GPG

Use our simple and secure online system to create new PGP key
pairs, and to encrypt and decrypt messages.

Generate PGP Keys

Your name:

Your e-mail address:

Choose a password:

Key Size:

2048 bits - recommended ▾

Your browser may not respond during key generation.

Generate PGP Keys

Public Key

Private Key

SIMPLE USAGE

11.1.3   SIGNING A PLAINTEXT MESSAGE

You can certify that you alone sent a plain text message. This is useful for news postings or email where secrecy isn't wanted.

11.1.4   SENDING AN ENCRYPTED MESSAGE

You can encrypt a message such that it can only be decrypted by a single user (or a list of users).

BITCOIN OFFLINE VAULT WALLET – BA.NET

Web PGP/GPG Utilities

You need to secure a message, but dont have PGP on the machine you are using ? No problem! **This webapp encrypts a message using your browser.**

Insert the ASCII armored PGP Public Key Block with the RSA or Elgamal
public key of the receiver here (contents of exported *.asc file).

Get Public Key Information

Version:

User ID:

Key ID (8 bytes in hex):

Public Key type and values:

The message is PGP encrypted using AES and RSA/Elgamal algorithms:

your text for PGP encryption goes here.

Encrypt Message   bytes. This took   seconds.

Depending on processor speed, message size, public key size and public key type
encryption can take a few seconds.

New Address   Multisig   Wallet

iPad 14:55 99%

ba.net/util/pgp/new/decrypt1.html | Google

Hacker News | × BA.net Bitcoin Address - Best Client Side Serverl... | +

BA.net Bitcoin Address Net

AppStore **Search BANET**

Store Keys Web PGP/GPG
Generate Keys Decrypt Encrypt
Bitcoin PGP Help

Web Based PGP / GPG

Use our simple and secure online system to decrypt PGP messages.

Decrypt a Message

Your password:

Your encrypted message:

Decrypt a Message

Your private key:

12 BEGINNERS' GUIDE TO PGP

If you are new to Bitcoin it's likely you've heard some terms thrown around by Bitcoiners that you have no idea what they mean—PGP, Tor, VPN, OTR, etc. In most cases these are referring to various technologies that people use to protect their data and communications.

This is the first installment of what will likely be a series of articles aimed at introducing new Bitcoiners to these and other technologies that you can use to enhance your privacy and keep sensitive information away from the prying eyes of governments and data thieves.

We're going to start off this series by introducing you to PGP, which is by far the most widely used encryption software available and a critical component to online privacy. Whether you're purchasing drugs from Silk Road or just sending emails to friends and family, it's something with which even casual internet users should familiarize themselves.

What is PGP?

PGP stands for Pretty Good Privacy. At it's core, it is an internet standard (called OpenPGP) used for data encryption and digital signatures. Software that employs this standard is available in both a free, open source version produced by the Free Software Foundation called the GNU Privacy Guard (or GPG for short) as well as a low-cost commercial version.

Let's take a moment to understand some of the basics of how it works. In conventional encryption, a secret key is used to transform PLAINTEXT (the unencrypted data) into unreadable CIPHERTEXT. The SAME key is also used to decrypt the ciphertext and reveal the plaintext. While this process works well for encrypting data stored on your hard drive, it has its drawbacks for use in communication. For one, you need to somehow communicate the secret key to the other party. But how to do this securely? After all, the reason you are using encryption is because you don't believe your communication channel is secure. You could meet in person and exchange the secret key offline, but that isn't very convenient. Protocols have been developed to allow for secure exchange of keys across insecure communication channels, but they tend to work better for real-time chat than, say, sending encrypted emails.

PGP makes use of PUBLIC-KEY ENCRYPTION. One key (a public key) is used to encrypt the data and a separate key (the private key) is used to decrypt it.
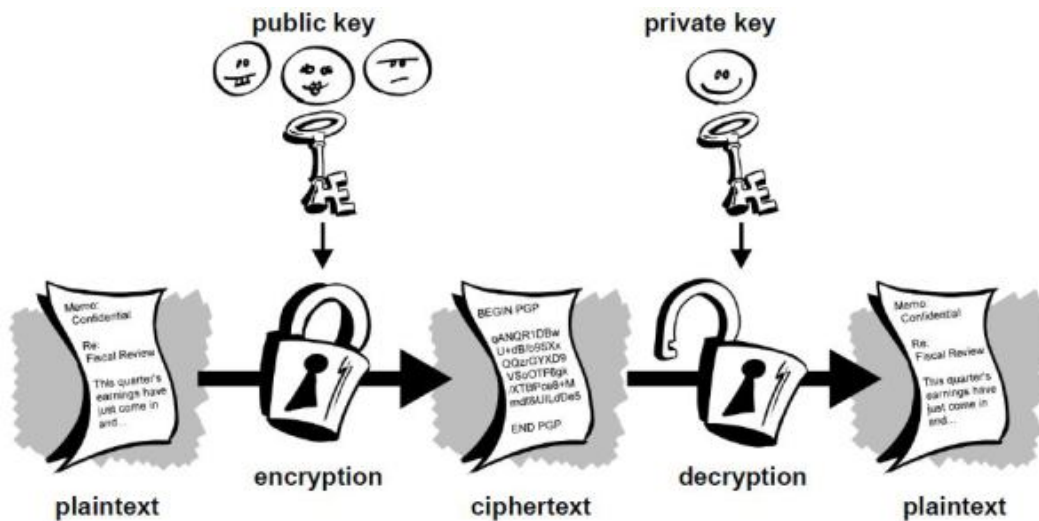
As a new user, you will generate a new public-private key pair. Just like the names suggest, you'll share your public key with others so that they can send you encrypted messages or files, while keeping your private key secret so that you can decrypt the data. The process by which the key pair is generated makes it impossible (given current technology and knowledge of mathematics) for an attacker to derive your private key from the public key.

Use Cases

The most obvious use case for this type of encryption is email. Anyone who has your public key can send you encrypted emails which only you can view. Likewise, you can send encrypted emails to your contacts by first downloading their public keys. In a future post we'll provide a more thorough tutorial demonstrating how to set up an email client to work with PGP. What you need to keep in mind, however, is only the body of the email will be encrypted. The subject and metadata (to, from, cc, and timestamp) will still be visible to anyone snooping on your emails.

You aren't limited to just encrypting emails either. Buyers at anonymous marketplaces like Silk Road frequently download their merchant's public key and use it to encrypt their shipping address so that only the merchant view it. Edward Snowden persuaded journalist Glenn Greenwald to set up PGP prior to leaking the top secret classified documents that revealed the depths of the NSA's spying operation. You can encrypt whole folders and files with your own public key to protect them from attackers who may gain access to your hard drive. In other words, PGP can be used in just about every conceivable case where strong encryption is needed.

Digital Signatures

Another feature of public-key cryptography is it allows for the creation of something called digital signatures. Much like your real life signature, a digital signature can be used to authenticate data but with the added benefit of being completely unforgeable (again given the current state of cryptography).

A digital signature is created by a mathematical algorithm which combines your private key with data you wish to "sign". The validity of the signature can by verified by anyone simply by checking it with your public key.
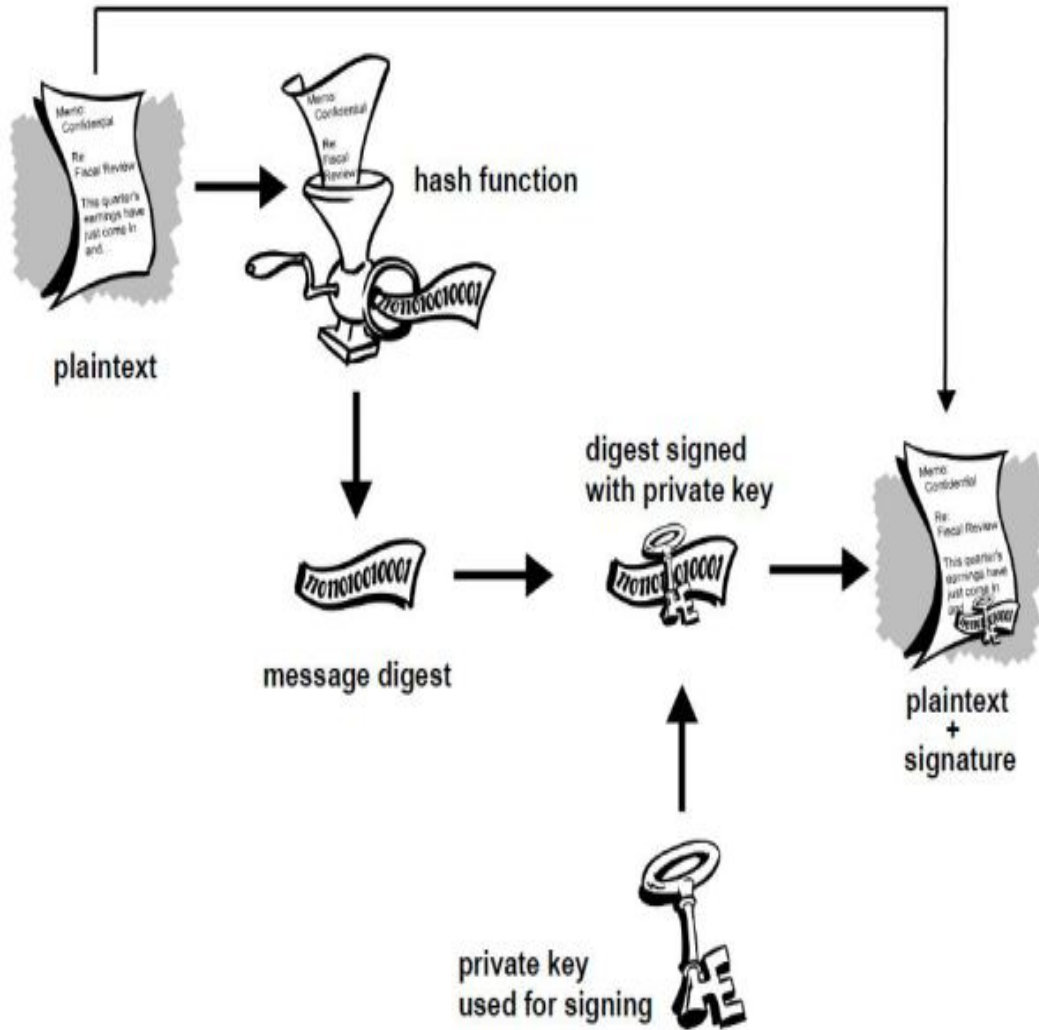
In the above diagram you see that the plaintext is run through a hash function to produce a message digest which is then signed with your private key. What this process ensures is that a signed document cannot be altered without invalidating the signature, allowing people to not only check the document's authenticity but also the integrity of the data. Just to give an example, suppose you sign a 10,000 word document. If someone were change even a single punctuation in that

document, the signature would show as invalid. To see why digital signatures are useful let's consider a few examples:

Returning to Edward Snowden, suppose the NSA had intercepted the classified documents before they reached Glenn Greenwald. The NSA could have removed the sensitive data, replaced it with disinformation, then forwarded it along to Greenwald. The reason this didn't happen is because Snowden signed the data with his private key before sending it along. This allowed Greenwald to use Snowden's public key to verify the files were unaltered. If the NSA tried to switch out some information, the signature would have shown as invalid.

Digital signatures are also extremely useful in verifying the integrity of software. A great example here would be Bitcoin wallets. Given the security implications, you want to be able to trust that the wallet you download is legitimate and wont leak information that would allow someone to steal your bitcoins. While all Bitcoin wallets are open source, unless you check and compile the source code yourself, you will most likely download a pre-compiled version that could contain malicious lines of code. Software developers will typically sign the software and provide a link to download the public key used for signing. With Bitcoin-Qt, lead developer Gavin Andresen signs new versions with his PGP key. Simply by checking the signature with his public key you can guarantee you've downloaded a legitimate copy.

How Secure Is It?

If all of this is new to you, you're likely wondering how secure is the encryption used in PGP. Can we really trust it to protect us from from the NSA and its $52.9 billion black budget? All I can really say is that the cryptographic algorithms used in PGP are all part of the public domain have been heavily vetted by the community of experts. At this point in time there are no feasible attacks known to the general public or academia. It's certainly possible that the NSA has access to highly advanced math that isn't publicly known, but even there the best attacks typically don't reveal the plaintext, rather they just make the keys slightly easier to brute force. The fact that the NSA has pressured Google, Microsoft, Apple etc. into giving them backdoors into their

systems seems to be prima facie evidence that they can't break commercial cryptographic algorithms.

Getting Started

The first thing you need to do to get started is download and install GPG. If you use the Ubuntu operating system you're in luck, you already have it. It can be found in the apps menu as "Passwords and Keys".

Windows users can download Gpg4win here.

And Mac users should download the GPG Suite for OS X from here.
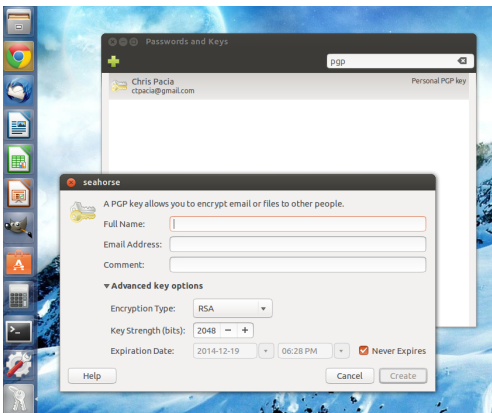
Ubuntu
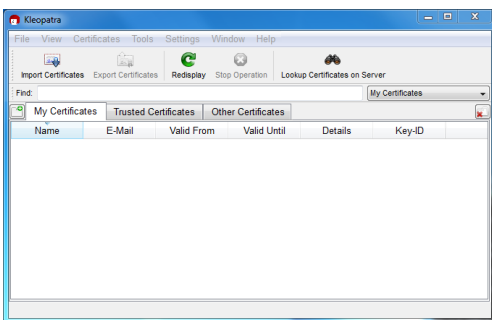
Windows
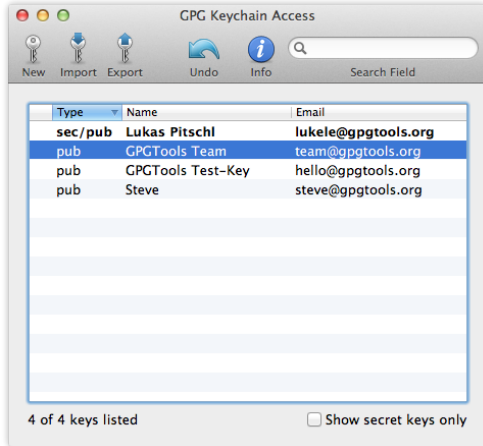
OS X

In each of these operating systems you can access GPG as well as a number of advanced options from the command line, but as a new user, you're better off learning to use the GUI for now.

Generating A New Certificate

In PGP a "certificate" is essentially a public key with extra data attached to help others verify that the key really belongs to you. In practice this is usually your name, email address and one or more digital signatures from others (more on that later).

Depending on your operating system, you'll generate a new certificate by clicking "New", "New Certificate", or "New PGP Key".

At minimum you will have to enter your name, email address, and a strong password that you will use for decrypting and signing data. In the advanced options menu you can select your encryption algorithm (RSA, DSA/ElGamal), key size (in bits), and an expiration date if you want your certificate to expire. The defaults here should suffice for our purposes. The differences are technical and unlikely to affect your overall security (just don't REDUCE to the key size).

Once this process is complete you will have generated a new certificate and private key. You can click on "export" to save your public key to a .asc file for distributing to others, or you can copy the

text of the key block and share it with people that way. A typical public key block will look like this:

-----BEGIN PGP PUBLIC KEY BLOCK----- Version: PGP Universal 2.9.1 (Build 347)
mQMuBFG3x4URCACZ/c7PjmPwOy2qIyKAYRftIT7YurxmZ/wQEwkyLJ4R+A2mFAvw
EfdVjghAKwnXxqeZO9WyAEofqIX5ewXD9J4H6THaWNlDeNwnIUhbVsSEgT6iwGEG
arXvkrMyy+U5KA0x2dcsYRKAPMM1db+4zSQkWTWzufLU7lcKi3gU3pNTxSA0DjCn
wfJQspiyWchSfgZ59+fKaGZJVSElrS2i2ok5mK3ywCXRWvnAC/VxA3N6T4jvkX/+
1gS/oUgdocP31TeV0L20JH9QgmFYC3jMbErAATo2x9Y8g4NofdvSnntbZk9Giycc
cgOWsa8aFtTjvcBp8hkCl3dK5xTZiY0gLSaDAQCXSHI7zw4LiNFfCV+PbO9BEqDA
i4JFV/qX7TgfBNX7nwf/fEFu18V16lVCsRzeuhMsHHzAQ7PZJfdfhyOubq0fnjkk
2RdcleosnP22zP5LoRs1fvIDdL3wnkg1ZUwfICP0HWRzRYcVBaIv9HcqSVBWriJj
uscni5QtX3flU2wqSyP90wquWPkO7jObT0hWihhWPFXiFA6996i/rTZiJH+eFPSW
afxVlRAqH4kaUBen5fSMbBSsfc+GkuuQH7gIYQC2k88soPLuFZGsibDwBqvdUqFG
S39ifNf/2MUx8DrM8bbIPPwiuTelAFVPu7GGzyzAF3yhk/Cdd/YmWlwrwAd4Psev
WpXNSApzSgh/HhY3wVdj9skItQBISXJSVkMD4DLvhwgAh/Ur5JEgtx5dYGpU/nEr
LGEDUgPeBnewReA8wurAnYeOHGVSu84kXceO2tJvnbLn5y1L0dML/u3+S9pDXOfR
1TR9QxWd3QIBUY68Ifa+DiXHSVcfrTPz3q+CHMLj7917hfATWwRTemccp6n8al68
tfGXih9t+lAwuq4KuRk0NkGEKrqeRU3sdGVLdIZ8lteikyYgWcZTYG7oxcj7qpif
ixl0DsI1HXfXQrFVnjOyQuiS8z06+ZuC/8dgi7UBpUkgQLZYosE0fUAdeiAVPGv0
LanXwHRQPDlmBiorge1c1jpbna2K9EyQ1Jbkyn6nkg8OaetO9brLBMk916mn6mQD
ebQfQ2hyaXMgUGFjaWEgPGN0cGFjaWFZ21haWwuY29tPoh6BBMRCAAiBQJRt8eF
AhsDBgsJCAcDAgYVCAIJCgsEFgIDAQIeAQIXgAAKCRC4lW2/7nwQXJ/dAP42O7se
mHDqZnxl4Slrf8AxgCl0DowpBcNxWRM8hNHS2QD/TkbCvy4QNq2QNrP26m183eJM
y6PNCncuwsB5TdoLgYqJASIEEAECAAwFAlKqHEQFAwASdQAACgkQlxC4m8pXrXyE
oAf+JusFcRHVGXDYOlRLwQYUJt9q3czp4cinwdheR24VUZVoE9pibogJcc2Oh4aS
5cpMg3EbmuoyVeLunxp01qpFDfVnfGJ3ZpdPDPlFu6Wy1iM7rVafcSR7CxI+oGRH
DKH0fZLhKKffujevM0Y7lFA80wjItq5Ewqy2UBxl6Vtdzo/ouAJ+EPmJsDOjclwe
Ayx4d/0g1kzf7DIGjUs6loV74zMqruPSPHGC6zFSz6jdA4xkzrlSV5U44TAkTz+1
I65j6I+doTcCmkzv4V8NU9wQ5LblE/flfTVCpnHNH4z4jAN2N8MyGNjAnbd2q752
yG3t651VmyOxa+XPffZ+F06GMbkCDQRRt8eFEAgAg+tZGxFVO3eeEn7R3KBCNCzL
DH3AwxcQs52k6ZbPzfyS59HTbvz1vkNNE/aoSb6HKZ95t3jaSBqbYIs8G3cXqN7h
kc/WJpYGeyKEokELg6Fr5vdaPxQakf63q2Ly+hCFCAorsc2iR50xVFB1befMFPWn
sptPIsel1P47wpRd2HmEwE+vGA90HcYUfdAA7eGCxZeRl8wc0DHbgAb+iKa1bmAY
vMO8FDTBAV9aayLL5qHxCGhR3VHRQi0Pq8P2nYjwwA+eF4M7gTXrB3L8Cf/mTXKi
rEF36kAAKegMmlPBH8/bLsWg7loJcxbPll4qhuJM7ErFF+hpmWbvYUqksFMjrwAE
Cwf7B63AelE+pT1qOFITFQPV30kvbQblMz70yAurUBDRTRQ4L45DnUvZurS0Uojr
nczueK6sHufdsKdl0DKxG2REOz9hZ64+NoZRzB+cYCt0g93M3Wtg3zt6x1q8MwEj
uFcaO0gTKlh1fKSg7cV+VYm0nMo7/kOgupVxtcy65te6EM6KAtRCugqBeY/FxKXN
G4tps+KbzwmDq5G5IAZOLH3kVmSJxOHdTr/jwPlHnq8J+AYIXANEJMmbG3s6Eaf2
/du8FAy4025UUPZdLsJBM3HKoIqR7lsl2T9cCB9Un4fXlF8axb7PojRO6Y68dfSU
to3UsZXERO4NtVI0lT0uhLXh+IhhBBgRCAAJBQJRt8eFAhsMAAoJELiVbb/ufBBc
QjgA/j1J7nN42zDMJxoAKQDvp+H3dErZVY7hJ8qHeGVbExWGAP97G/jWhl6FEg7M
2vOMWRC5GQUM8TU1YkCeAuhsxSj3ew== =dgnf -----END PGP PUBLIC KEY BLOCK-----

Key Servers

You might want to consider uploading your public key to a key server such as the [MIT Key Server](#) or [PGP Global Directory](#). These are searchable directories from which other people can download your

public key without first asking you for it. This functionality comes in especially handy when using email. Some email clients can be configured to search the key servers for the PGP keys of your contacts or anyone who has sent you an encrypted email and import them automatically.

Just keep in mind that once you upload a key to a server, you typically can't remove it. It's probably a good idea to play around with PGP first, get used to it, then once you've created your permanent key, upload it. That way you don't litter the key server with multiple keys bearing your name.

Importing Keys

In order to encrypt files to send to others, you will first need to import their public key into PGP. You can do this by downloading the .asc file containing their public key (either directly from others or from a key server), clicking "Import" or "Import Certificate", and selecting the file. In Linux you can import a key simply by double clicking the .asc file. In Windows you have the option to copy the public key block and import it directly from the clipboard.

The software will typically let you view, edit and sign the public keys on your keyring. More on signing other people's keys later.

Encrypting Data

You have two options for encrypting data in PGP — you can encrypt a plain text message from the clipboard or encrypt whole files. Let's start with encrypting plain text messages. The first thing you need to do is pull up your plain text editor (Notepad in Windows, GNU Emacs works well for this in Linux). You'll have to forgive me for not being familiar with OS X, but I assume you can encrypt from the clipboard in that operating system (though I'm not positive).

Type whatever message you want and copy it to the clipboard. In Windows, you'll need to right click on the Kleopatra tray icon and click Clipboard>>Encrypt. The software will prompt you do select a public key from your keyring with which to encrypt the message. The

encrypted ciphertext will replace the unencrypted plaintext in your clipboard.

In Emacs you'll need to highlight the text, click Options>>Encryption/Decryption>>Encrypt Region. Or you can simply save the file to disk and right click and click encrypt.
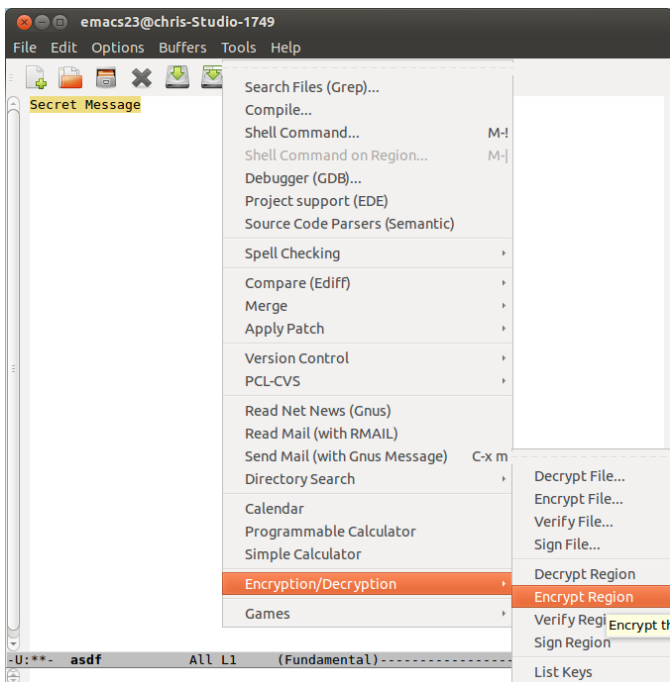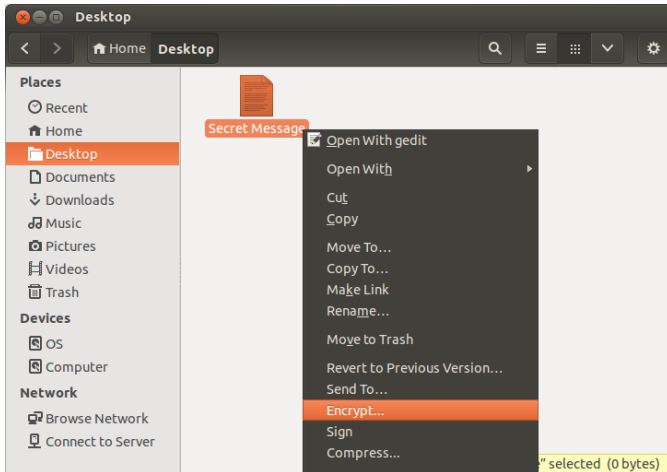
The resulting encrypted message will look like this:

```
  -----BEGIN PGP MESSAGE----- Version: GnuPG v1.4.14 (GNU/Linux)
jA0EAwMCNUyTD6Yu1QtgyemPt3ysidtpK5AXDobS2mB5+ym7/zNqMe4u/fli9pPV
PakBAwNtRCE45qlFUpCj3Pjh3jRoPVmiQOb8n5PuhipuIP4v6ANCboWnCUam7NGd
VHuU2OLX36QWOoPI5Ewl9xto+3iqjlclTaiRlHo0JHU8EOv75BpjahzKhDCV2lMQ
q9QOHBESsU9xhk/t7gnT2EfhxzPHTb2N7fkPRFqltMU949hSvaYtN3AA80qxjkic
jpEbftLl1brvEK2WpyMPDt+YPnIvJ2mHfsmB41VNlr14BS5zpfWTEDjkTJALRWVj
MRARwU8/iE/hh9FMkYb8mB2cmJh6TgqpYF45qtacdKOKVqQBToPwS0dFf5Pw25Qx
jaRKTzfoP9mhD1nkHuNP79zhj9+uTMwRp00d117CuopnTeaTMQTYJeHNpsX79Jx3
EF6QQjrw38UNz2IZGplKHFKT39lal7NywviI7LmfJYHMoIFhdz97Woad1MCMPq/G
qqlA/QRrheMz90NG9OQRtc6q2hNCsQUI7kRV7kTrgPCrzKepLwZ3EBcSea8vyQcH
f43blJP1VucaTf9jvGPX1qgisOFHBYcZKv1+1I4sRlFcSWpKr3VeCr76bq+vMk1D
7+rT8SaYs0efFkfF/Y6+yOoporP0HsxVxAIUZ7zPXIH2UxtGfcfcu/pWxNQ1WrM5 dwWFasQaXg==
=tfo5 -----END PGP MESSAGE-----
```

Some things to keep in mind, once you encrypt something with SOMEONE ELSE'S public key, you can't decrypt it. You can, however, encrypt a message using multiple public keys and the message can be decrypted with any of the corresponding private keys. So you could encrypt a message with someone else's public key AND your public key, then you can both decrypt it at a later date. Also, if you encrypt data using only YOUR public key, it basically works like symmetric key encryption in that only you will be able to decrypt it.

To encrypt an entire file select "Sign/Encrypt File" from the menu and select the file you want to encrypt. Just like before, you'll need to select a public key(s) from your keyring with which to encrypt the file.

Decrypting Data

To decrypt either a message or a file, you need to do all of the above in reverse. Just this time use the decrypt option from the menu. Here you will be prompted to enter your password for your private key that you created along with your key pair. This is what prevents an attacker from stealing your private key and decrypting messages intended for you.

Keep in mind, if you are decrypting data on your normal computer, you could be running the risk that malware could copy and upload the data AFTER you've decrypted it. This might be an acceptable risk for everyday communications, but if you're dealing with extremely sensitive data you should probably transfer the encrypted data to a secure viewing station prior to decryption.

Any air gapped computer (one permanently disconnected from the internet) would work for this purpose. Or you could boot into a Linux live system (such as Tails) from a USB stick to isolate your work environment from preexisting malware.

Signing Data

Just like with encryption you can either sign a message from your clipboard or sign whole files. The process is just as straightforward as before except this time you will select "sign" rather than "encrypt". Here you will again be prompted for your password. The resulting output will look like this:

-----BEGIN PGP SIGNED MESSAGE----- Hash: SHA256 This is an example of a PGP signed message. -----BEGIN PGP SIGNATURE----- Version: GnuPG v1.4.14 (GNU/Linux) iF4EAREIAAYFAlK5pacACgkQuJVtv+58EFxiXgD/QGwQVCZMAlE7fL6V1Kbv4Ogq Sa9VTEw+s9mWwiBInp4A/3guc2PvZb8iIdrCyWGwIMJIOQS8OuhWfjtN3CBhOSA1 =S+B+ ----- END PGP SIGNATURE-----

Notice that the message is at the top under the header, while the signature is at the bottom. If you chose to sign an entire file, the software will generate a separate .sig signature file that you will need to send along with the original file.

Also keep in mind that encrypting and signing are not mutually exclusive. You can opt to both encrypt and sign data to protect the message from eavesdroppers AND allow the recipient to verify the message came from you.

Verifying Signatures

To verify a signature on a signed message or file you will obviously have to first download and import the corresponding public key. Just like with decryption, you can either verify the signed message from your clipboard or by selecting the file. If you're verifying a signed file, you'll likely be prompted to select both the file AND the detached signature (.sig) file.

If you've done it right you will see a response that looks something like this:

Good signature from B8956DBFEE7C105C Chris Pacia (trust ultimate) created at 2013-11-16T12:05:37-0500 using DSA

When verifying the signature on software, the developer will typically provide a link to a .sig file for you to download. However, when releasing software on multiple platforms, it's not uncommon for a developer to provide a single signed message containing the hashes of the files rather than a separate signature for each version. Consider the following release notes for Bitcoin-QT:

-----BEGIN PGP SIGNED MESSAGE----- Hash: SHA256
73495de53d1a30676884961e39ff46c3851ff770eeaa767331d065ff0ce8dd0c bitcoin-0.8.6-
linux.tar.gz ec85816e6cd034230ec5dc83c105334aa91bfa38fd959ba3d1d3bd5d4df3208b bitcoin-
0.8.6-macosx.dmg baac30350a721472bd34e811f16bd68c4e4672cfb47df73aee12376b2adcae8d
bitcoin-0.8.6-win32-setup.exe
582fcb973a29e1a6e44ddc6602400e77fc85b53f6f54a1105d22d84d992e3c83 bitcoin-0.8.6-
win32.zip -----BEGIN PGP SIGNATURE----- Version: GnuPG/MacGPG2 v2.0.20 (Darwin)
iQIcBAEBCAAGBQJSpjKpAAoJEBt7+0V79uISEvgP/2T2Pt1wO2WMaK3DL4D/uFq6
xcuhCjrV1FHt1UoYTdohl112dO3q6qsakguBxvaGMe80KCJS85JT7B2Sbs/goyYT
2WxkEv+ttQFVnB32MlFeGYrPt9I7xmNQqYoQMGsV+VeCfqSDElxVpPCLDYFbBLUk
lkHa4LTkXsGI351iIEjUB4jXSKeJvWQQ6HdxKOIUaxA6AZX8qGKuGbSYUMNy/pBi
lqZNOTWtFjRkPR+qhhjjpx9J9A9l4dFYvH6lJDS9mj2jOUCTtg3hKwYg3KvSOtjl
6Mkm6qkJtf0SxJpx3tQjH4rav7G1WY0Y546X2+uF9BuFKvhDVY74fe8pAh+ASF18
lq4pbpg6pElk94CESPEDxIIB1wgozKBidLSzCtKfqgTDPQtFDny1nA3Km+FGQX5Y
HATPB0EeuB5juJs7rHpO/OhweI1cORPPfhaTiA6Cf6Tioyl+FX/ZmVXclUUYEF1M
fXS8JsAlZxIdDgjeo6xTwI2llN5Gs3JmypGM0dggNslMUEeCX/O5uciyoZ6y+TUZ
TZLRVY4WsS0FpsA07UuYuasi1B1WzGm8BW4Akt3XO7awVwyHSUfePS02qGdUwfDS

117

sDzf5SoBphnBUcRiVoHL1lhn8bfW0henksL6YUJIfY4w5q5S9vM/5uk+vxghWGRk
K6o6VP8xT/1yRhWbR0Yp =DYos -----END PGP SIGNATURE-----

So what is going on here is that the installation files for Linux, OS X, and Windows (.exe and .zip) were run through the SHA-256 hash function and the outputs were then signed. To verify the integrity of the Bitcoin-QT for Windows (say), you would first verify the signature on this message then hash the bitcoin-0.8.6-win32-setup.exe file with SHA-256. The output should look like this:

baac30350a721472bd34e811f16bd68c4e4672cfb47df73aee12376b2adcae8d

Then just compare this output with the hash in the signed release notes. If the two match, you know you have a good file.

You may be asking, how in the world do I calculate a hash function? Some operating systems will let you do this from the terminal. For example in Linux you can just type:

user@users-desktop:~$ sha256sum [FILE]
user@users-desktop:~$ sha1sum [FILE]
user@users-desktop:~$ md5sum [FILE]

Otherwise, you could easily use an [online hash calculator](#).

Key Management

Finally, we should probably talk a little about key management. One of the downsides to PGP is susceptibility to something called a man-in-the-middle attack. This attack works like this: Let's say you want to securely communicate with someone using PGP. The first thing you would do is download their public key. However, it may be possible for an attacker to intercept your internet communications before they reach the server containing the public key. The attacker could send you one of his own public keys and make you think it's the public key of your communication partner. Not knowing any better, you would encrypt your messages with the attacker's public key allowing him view all your communications. Even worse, the attacker could re-encrypt the message with the correct public key and forward it along it

the destination. Neither you nor your communication partner would know the message was intercepted.
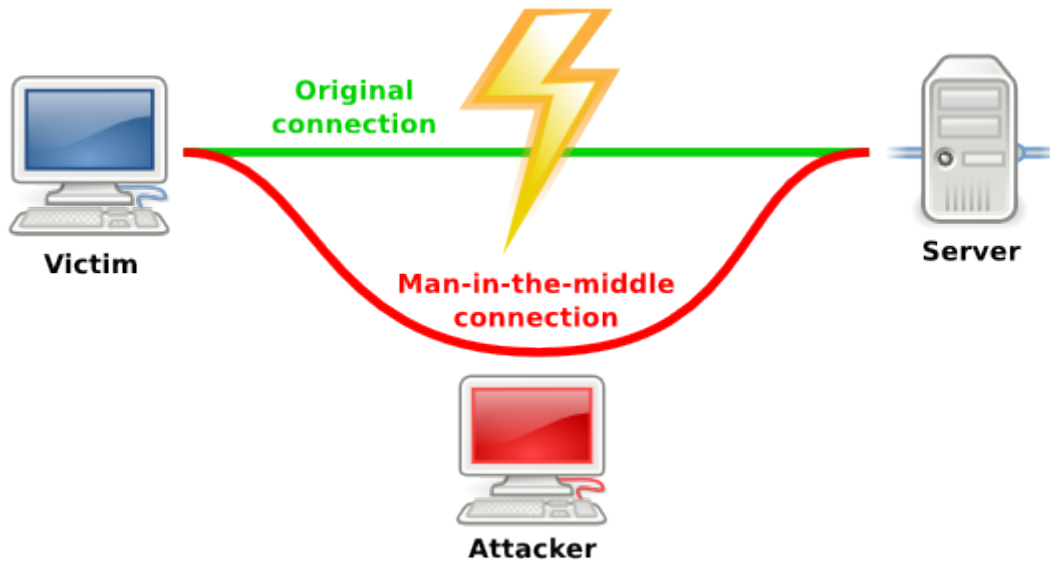
Obviously, a critical part of security in PGP is the ability to trust that the public key belongs to its purported owner. While complete trust is difficult to achieve, there are a few methods you can use to increase your level of trust.

1. **MEET IN PERSON.** If someone physically hands you their public key, then obviously this eliminates the problem of trust. Of course, this is very inefficient.
2. *Verify the fingerprint*. Each PGP certificate has a unique fingerprint which is calculated as the hash of the certificate represented in hexadecimal. It looks like this:

   0150 2502 DD3A 928D CE52 8CB9 B895 6DBF EE7C 105C

   If you can get the key's owner to verify the fingerprint, possibly by reading it over the phone, then you can be fairly confident in the validity of the certificate. Obviously, finding an appropriate communication channel to verify the fingerprint can be tricky.

3. ***Download the key from multiple IP addresses/devices/servers*** A MITM attack is difficult to pull off as it is. It becomes much harder if the attacker has to watch the communications of multiple IP addresses and servers. To this end you can increase the trust in the public key by downloading it from multiple locations (home, work, the library, Starbucks, over Tor, etc), from multiple devices, and from multiple servers. Gather up all the keys and check to make sure they are all they same. If so, you can be reasonably confident the key is valid. It would be extremely difficult to pull off a MITM attack after all that.

4. ***Web of trust***. In PGP you have the ability to use your private key to sign the someone else's public key. This creates the opportunity to introduce a sort of SIX DEGREES OF SEPARATION trust model. Let's say you've downloaded Charlie's public key but don't know if you can trust it. Charlie's key is signed by Bob, who you also don't trust, and Bob's key is signed by Alice, who you do trust. Because you trust Alice, this gives you chain of trust that goes all the way to Charlie, allowing you to trust Charlie's key. The only downside to web of trust is that it can be difficult to get started and make enough connections to link you to all the keys you wish to download.

So that's it for now. While we could go much more in depth, what we covered should be enough to get you started using PGP. Just remember, given the revelations about U.S. government spying and depths to which it is sinking to destroy your online privacy, there is really no excuse for not familiarizing yourself with PGP and using it on a regular basis. In a future installment of the series we'll talk about how to set up an email client to automatically encrypt and decrypt your emails.

13 PROOF OF WORK SYSTEM

A **proof-of-work** (**POW**) **system** (or **protocol**, or **function**) is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer. The concept may have been first presented by Dwork and Naor in a 1993 journal.

A key feature of these schemes is their asymmetry: the work must be moderately hard (but feasible) on the requester side but easy to check for the service provider. This idea is also known as a CPU cost function, client puzzle, computational puzzle or CPU pricing function. It is distinct from a CAPTCHA, which is intended for a human to solve quickly, rather than a computer.

BACKGROUND

One popular system—used in Bitcoin mining and Hashcash— uses partial hash inversions to prove that work was done, as a good-will token to send an e-mail. For instance the following header represents about 2 hash computations to send a message to calvin@comics.net on January 19, 2038:

X-Hashcash: 1:52:380119:calvin@comics.net:::9B760005E92F0DAE

It is verified with a single computation by checking that the SHA-1 hash of the stamp (omit the "X-Hashcash: " portion) begins with 52 binary zeros, that is 13 hexadecimal zeros:**^**

0000000000000756af69e2ffbdb930261873cd71

Whether POW systems can actually solve a particular denial-of-service issue such as the spam problem is subject to debate; the system must make sending spam emails obtrusively unproductive for the spammer, but should also not prevent legitimate users from sending their messages. Proof-of-work systems are being used as a

primitive by other more complex cryptographic systems such as Bitcoin which uses a system similar to Hashcash.

VARIANTS

There are two classes of proof-of-work protocols.

- **Challenge-response** protocols assume a direct interactive link between the requester (client) and the provider (server). The provider chooses a challenge, say an item in a set with a property, the requester finds the relevant response in the set, which is sent back and checked by the provider. As the challenge is chosen on the spot by the provider, its difficulty can be adapted to its current load. The work on the requester side may be bounded if the challenge-response protocol has a known solution (chosen by the provider), or known to exist within a bounded search space.
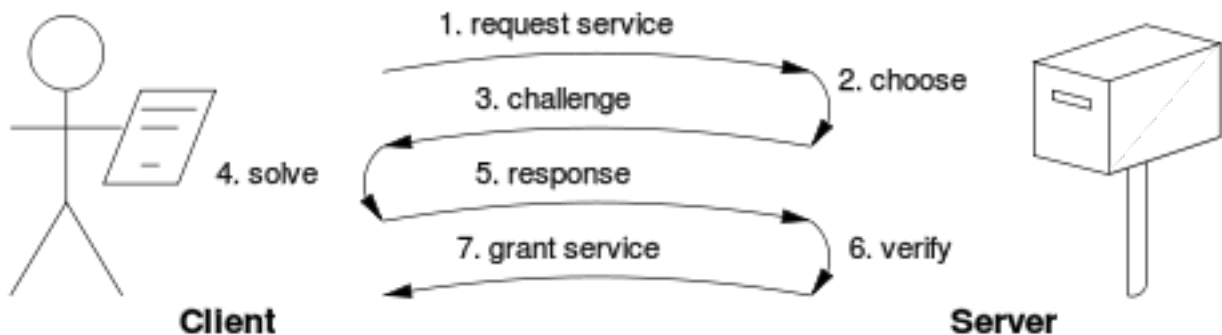
- **Solution-verification** protocols do not assume such a link: as a result the problem must be self-imposed before a solution is sought by the requester, and the provider must check both the problem choice and the found solution. Most such schemes are unbounded probabilistic iterative procedures such as Hashcash.
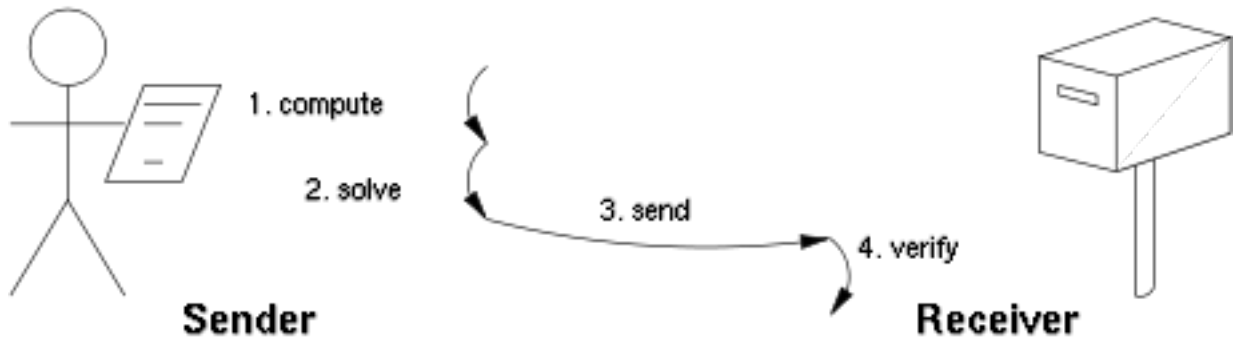
Known-solution protocols tend to have slightly lower variance than unbounded probabilistic protocols, because the variance of a rectangular distribution is lower than the variance of a Poisson distribution (with the same mean). A generic technique for reducing variance is to use multiple independent sub-challenges, as the average of multiple samples will have lower variance.

There are also fixed-cost functions such as the time-lock puzzle.

Moreover, the underlying functions used by these schemes may be:

* **CPU-bound** where the computation runs at the speed of the processor, which greatly varies in time, as well as from high-end server to low-end portable devices.
* **Memory-bound** where the computation speed is bound by main memory accesses (either latency or bandwidth), the performance of which is expected to be less sensitive to hardware evolution.
* **Network-bound** if the client must perform few computations, but must collect some tokens from remote servers before querying the final service provider. In this sense the work is not actually performed by the requester, but it incurs delays anyway because of the latency to get the required tokens.

Finally, some POW systems offer **shortcut** computations that allow participants who know a secret, typically a private key, to generate cheap POWs. The rationale is that mailing-list holders may generate stamps for every recipient without incurring a high cost. Whether such a feature is desirable depends on the usage scenario.

LIST OF PROOF-OF-WORK FUNCTIONS

Here is a list of known proof-of-work functions:

- Integer square root modulo a large prime
- Weaken Fiat–Shamir signatures
- Ong–Schnorr–Shamir signature broken by Pollard
- Partial hash inversion as Hashcash
- Hash sequences
- Puzzles
- Diffie–Hellman-based puzzle
- Moderate
- Mbound
- Hokkaido
- Cuckoo Cycle
- Merkle tree based
- Guided tour puzzle protocol

REUSABLE PROOF-OF-WORK AS E-MONEY

Computer scientist Hal Finney built on the proof-of-work idea, yielding a system that exploited reusable proof of work ("RPOW"). Finney's purpose for RPOW was as token money. Just as a gold coin's value is thought to be underpinned by the value of the raw gold needed to make it, the value of an RPOW token is guaranteed by the value of the real-world resources required to 'mint' a POW token. In Finney's version of RPOW, the POW token is a piece of Hashcash.

A website can demand a POW token in exchange for service. Requiring a POW token from users would inhibit frivolous or excessive use of the service, sparing the service's underlying resources, such as bandwidth to the Internet, computation, disk space, electricity and administrative overhead.

Finney's RPOW system differed from a POW system in permitting random exchange of tokens without repeating the work required to generate them. After someone had "spent" a POW token at a website, the website's operator could exchange that "spent" POW token for a new, unspent RPOW token, which could then be spent at some third

party web site similarly equipped to accept RPOW tokens. This would save the resources otherwise needed to 'mint' a POW token. The anti-counterfeit property of the RPOW token was guaranteed by remote attestation. The RPOW server that exchanges a used POW or RPOW token for a new one of equal value uses remote attestation to allow any interested party to verify what software is running on the RPOW server. Since the source code for Finney's RPOW software was published (under a BSD-like license), any sufficiently knowledgeable programmer could, by inspecting the code, verify that the software (and, by extension, the RPOW server) never issued a new token except in exchange for a spent token of equal value.

Until 2009, Finney's system was the only RPOW system to have been implemented; it never saw economically significant use. In 2009, the Bitcoin network went online. Bitcoin is a proof-of-work cryptocurrency that, like Finney's RPOW, is also based on the Hashcash POW. But in Bitcoin double-spend protection is provided by a decentralized P2P protocol for tracking transfers of coins, rather than the hardware trusted computing function used by RPOW. Bitcoin has better trustworthiness because it is protected by computation; RPOW is protected by the private keys stored in the TPM hardware and manufacturers holding TPM private keys. Hackers who steal a TPM manufacturer key, or anyone capable of obtaining the key by examining the TPM chip itself, could subvert that assurance. Bitcoins are "mined" using the Hashcash proof-of-work function by individual nodes and verified by the decentralized P2P Bitcoin network.

Other cryptocurrencies have used different hashing algorithms, as well as prime chains as proof of work.

NOTES

    1.^ On most Unix systems this can be verified with a command: echo -n 1:52:380119:calvin@comics.net:::9B760005E92F0DAE | openssl sha1

14 PRETTY GOOD PRIVACY (PGP)

Pretty Good Privacy (**PGP**) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. It was created by Phil Zimmermann in 1991.

PGP and similar software follow the OpenPGP standard ([RFC 4880](#)) for encrypting and decrypting data.

DESIGN

Encrypt

Data

Generate Random Key

TlakvAQkCu2u
Random Key

Encrypt data using random key

Encrypt key using receiver public key

RSA

Data

q4fzNeBCRSY(
Encrypted Key

Encrypted Message

Decrypt

Encrypted Message

q4fzNeBCRSY(
Encrypted Key

Decrypt using receiver's private key

RSA

Data

TlakvAQkCu2u

Decrypt data using key
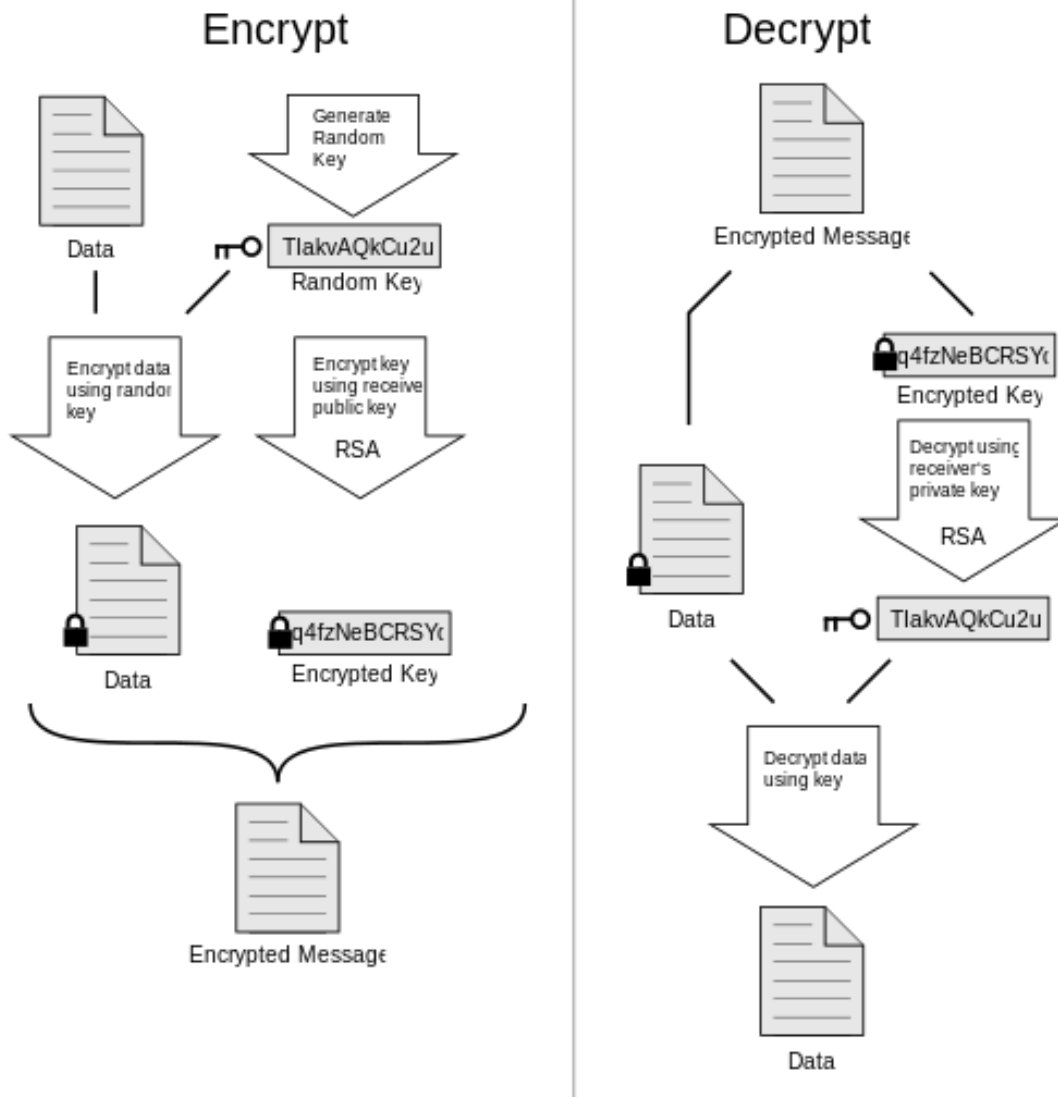
Data

How PGP encryption works

PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a user name and/or an e-mail address. The first version of this system was generally known as a web of trust to contrast with the X.509 system, which uses a hierarchical approach based on certificate authority and which was added to PGP implementations later. Current versions of PGP encryption include both options through an automated key management server.

14.1.1   COMPATIBILITY

As PGP evolves, versions that support newer features and algorithms are able to create encrypted messages that older PGP systems cannot decrypt, even with a valid private key. Therefore it is essential that partners in PGP communication understand each other's capabilities or at least agree on PGP settings.

14.1.2   CONFIDENTIALITY

PGP can be used to send messages confidentially. For this, PGP combines symmetric-key encryption and public-key encryption. The message is encrypted using a symmetric encryption algorithm, which requires a symmetric key. Each symmetric key is used only once and is also called a session key. The message and its session key are sent to the receiver. The session key must be sent to the receiver so they know how to decrypt the message, but to protect it during transmission, it is encrypted with the receiver's public key. Only the private key belonging to the receiver can decrypt the session key.

14.1.3   DIGITAL SIGNATURES

PGP supports message authentication and integrity checking. The latter is used to detect whether a message has been altered since it was completed (the *message integrity* property) and the former to determine whether it was actually sent by the person or entity claimed to be the sender (a *digital signature*). Because the content is encrypted, any changes in the message will result in failure of the decryption with the appropriate key. The sender uses PGP to create a digital signature for the message with either the RSA or DSA algorithms. To do so, PGP computes a hash (also called a message digest) from the plaintext and then creates the digital signature from that hash using the sender's private key.

14.1.4   WEB OF TRUST

Main article: Web of trust

Both when encrypting messages and when verifying signatures, it is critical that the public key used to send messages to someone or some entity actually does 'belong' to the intended recipient. Simply downloading a public key from somewhere is not an overwhelming assurance of that association; deliberate (or accidental) impersonation is possible. From its first version, PGP has always included provisions for distributing user's public keys in an 'identity certificate', which is also constructed cryptographically so that any tampering (or accidental garble) is readily detectable. However, merely making a certificate which is impossible to modify without being detected is insufficient; this can prevent corruption only after the certificate has been created, not before. Users must also ensure by some means that the public key in a certificate actually does belong to the person or entity claiming it. From its first release, PGP products have included an internal certificate 'vetting scheme' to assist with this, a trust model which has been called a web of trust. A given public key (or more specifically, information binding a user name to a key) may be digitally signed by a third party user to attest to the association between someone (actually a user name) and the key. There are several levels of confidence which can be included in such signatures. Although many programs read and write this information, few (if any) include this level of certification when calculating whether to trust a key.

The web of trust protocol was first described by Zimmermann in 1992 in the manual for PGP version 2.0:

As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys.

The web of trust mechanism has advantages over a centrally managed public key infrastructure scheme such as that used by S/MIME but has not been universally used. Users have been willing to

accept certificates and check their validity manually or to simply accept them. No satisfactory solution has been found for the underlying problem.

14.1.5 CERTIFICATES

In the (more recent) OpenPGP specification, *trust signatures* can be used to support creation of certificate authorities. A trust signature indicates both that the key belongs to its claimed owner and that the owner of the key is trustworthy to sign other keys at one level below their own. A level 0 signature is comparable to a web of trust signature since only the validity of the key is certified. A level 1 signature is similar to the trust one has in a certificate authority because a key signed to level 1 is able to issue an unlimited number of level 0 signatures. A level 2 signature is highly analogous to the trust assumption users must rely on whenever they use the default certificate authority list (like those included in web browsers); it allows the owner of the key to make other keys certificate authorities.

PGP versions have always included a way to cancel ('revoke') identity certificates. A lost or compromised private key will require this if communication security is to be retained by that user. This is, more or less, equivalent to the certificate revocation lists of centralised PKI schemes. Recent PGP versions have also supported certificate expiration dates.

The problem of correctly identifying a public key as belonging to a particular user is not unique to PGP. All public key / private key cryptosystems have the same problem, even if in slightly different guises and no fully satisfactory solution is known. PGP's original scheme at least leaves the decision as to whether or not to use its endorsement/vetting system to the user, while most other PKI schemes do not, requiring instead that every certificate attested to by a central certificate authority be accepted as correct.

14.1.6 SECURITY QUALITY

To the best of publicly available information, there is no known method which will allow a person or group to break PGP encryption

by cryptographic or computational means. Indeed, in 1996, cryptographer Bruce Schneier characterized an early version as being "the closest you're likely to get to military-grade encryption.". In addition to protecting data in transit over a network, PGP encryption can also be used to protect data in long-term data storage such as disk files. These long-term storage options are also known as data at rest, i.e. data stored, not in transit.

The cryptographic security of PGP encryption depends on the assumption that the algorithms used are unbreakable by direct cryptanalysis with current equipment and techniques.

In the original version, the RSA algorithm was used to encrypt session keys. RSA's security depends upon the one-way function nature of mathematical integer factoring. Similarly, the symmetric key algorithm used in PGP version 2 was IDEA, which might at some point in the future be found to have previously undetected cryptanalytic flaws. Specific instances of current PGP or IDEA insecurities (if they exist) are not publicly known. As current versions of PGP have added additional encryption algorithms, the degree of their cryptographic vulnerability varies with the algorithm used. In practice, each of the algorithms in current use are not publicly known to have cryptanalytic weaknesses.

New versions of PGP are released periodically and vulnerabilities are fixed by developers as they come to light. Any agency wanting to read PGP messages would probably use easier means than standard cryptanalysis, e.g. rubber-hose cryptanalysis or black-bag cryptanalysis i.e. installing some form of trojan horse or keystroke logging software/hardware on the target computer to capture encrypted keyrings and their passwords. The FBI has already used this attack against PGP in its investigations. However, any such vulnerabilities apply not just to PGP but to any conventional encryption software.

In 2003 an incident involving seized Psion PDAs belonging to members of the Red Brigade indicated that neither the Italian police nor the FBI were able to decrypt PGP-encrypted files stored on them.

A more recent incident in December 2006 (see *In re Boucher*), involving US customs agents who seized a laptop PC that allegedly contained child pornography, indicates that US government agencies find it "nearly impossible" to access PGP-encrypted files. Additionally, a magistrate judge ruling on the case in November 2007 has stated that forcing the suspect to reveal his PGP passphrase would violate his Fifth Amendment rights i.e. a suspect's constitutional right not to incriminate himself.

Evidence suggests that as of 2007, British police investigators are unable to break PGP,

HISTORY

14.1.7   EARLY HISTORY

Phil Zimmermann created the first version of PGP encryption in 1991. The name, "Pretty Good Privacy" was inspired by the name of a grocery store, "Ralph's Pretty Good Grocery", featured in radio host Garrison Keillor's fictional town, Lake Wobegon. This first version included a symmetric-key algorithm that Zimmermann had designed himself, named BassOmatic after a *Saturday Night Live* sketch. Zimmermann had been a long-time anti-nuclear activist, and created PGP encryption so that similarly inclined people might securely use BBSs and securely store messages and files. No license was required for its non-commercial use. There was not even a nominal charge, and the complete source code was included with all copies.

In a posting of June 5, 2001, entitled "PGP Marks 10th Anniversary", Zimmermann describes the circumstances surrounding his release of PGP:

"It was on this day in 1991 that I sent the first release of PGP to a couple of my friends for uploading to the Internet. First, I sent it to Allan Hoeltje, who posted it to Peacenet, an ISP that specialized in grassroots political organizations, mainly in the peace movement. Peacenet was accessible to political activists all over the world. Then, I uploaded it to Kelly Goen, who proceeded to upload it to a Usenet newsgroup that specialized in distributing source code. At my request,

he marked the Usenet posting as "US only". Kelly also uploaded it to many BBS systems around the country. I don't recall if the postings to the Internet began on June 5th or 6th.

It may be surprising to some that back in 1991, I did not yet know enough about Usenet newsgroups to realize that a "US only" tag was merely an advisory tag that had little real effect on how Usenet propagated newsgroup postings. I thought it actually controlled how Usenet routed the posting. But back then, I had no clue how to post anything on a newsgroup, and didn't even have a clear idea what a newsgroup was."

PGP found its way onto the Internet, and it very rapidly acquired a considerable following around the world. Users and supporters included dissidents in totalitarian countries (some affecting letters to Zimmermann have been published, some of which have been included in testimony before the US Congress), civil libertarians in other parts of the world (see Zimmermann's published testimony in various hearings), and the 'free communications' activists who called themselves cypherpunks (who provided both publicity and distribution) and decades later, CryptoParty, who did much the same via Twitter.

14.1.8   CRIMINAL INVESTIGATION

Shortly after its release, PGP encryption found its way outside the United States, and in February 1993 Zimmermann became the formal target of a criminal investigation by the US Government for "munitions export without a license". Cryptosystems using keys larger than 40 bits were then considered munitions within the definition of the US export regulations; PGP has never used keys smaller than 128 bits, so it qualified at that time. Penalties for violation, if found guilty, were substantial. After several years, the investigation of Zimmermann was closed without filing criminal charges against him or anyone else.

Zimmermann challenged these regulations in an imaginative way. He published the entire source code of PGP in a hardback book, via MIT Press, which was distributed and sold widely. Anybody wishing to build their own copy of PGP could buy the $60 book, cut off the

covers, separate the pages, and scan them using an OCR program (or conceivably enter it as a type-in program if OCR software was not available), creating a set of source code text files. One could then build the application using the freely available GNU Compiler Collection. PGP would thus be available anywhere in the world. The claimed principle was simple: export of *munitions*—guns, bombs, planes, and software—was (and remains) restricted; but the export of *books* is protected by the First Amendment. The question was never tested in court with respect to PGP. In cases addressing other encryption software, however, two federal appeals courts have established the rule that cryptographic software source code is speech protected by the First Amendment (the Ninth Circuit Court of Appeals in the Bernstein case and the Sixth Circuit Court of Appeals in the Junger case).

US export regulations regarding cryptography remain in force, but were liberalized substantially throughout the late 1990s. Since 2000, compliance with the regulations is also much easier. PGP encryption no longer meets the definition of a non-exportable weapon, and can be exported internationally except to seven specific countries and a list of named groups and individuals (with whom substantially all US trade is prohibited under various US export controls).

14.1.9   PGP 3 AND FOUNDING OF PGP INC.

During this turmoil, Zimmermann's team worked on a new version of PGP encryption called PGP 3. This new version was to have considerable security improvements, including a new certificate structure which fixed small security flaws in the PGP 2.x certificates as well as permitting a certificate to include separate keys for signing and encryption. Furthermore, the experience with patent and export problems led them to eschew patents entirely. PGP 3 introduced use of the CAST-128 (a.k.a. CAST5) symmetric key algorithm, and the DSA and ElGamal asymmetric key algorithms, all of which were unencumbered by patents.

After the Federal criminal investigation ended in 1996, Zimmermann and his team started a company to produce new versions of PGP

encryption. They merged with Viacrypt (to whom Zimmermann had sold commercial rights and who had licensed RSA directly from RSADSI), which then changed its name to PGP Incorporated. The newly combined Viacrypt/PGP team started work on new versions of PGP encryption based on the PGP 3 system. Unlike PGP 2, which was an exclusively command line program, PGP 3 was designed from the start as a software library allowing users to work from a command line or inside a GUI environment. The original agreement between Viacrypt and the Zimmermann team had been that Viacrypt would have even-numbered versions and Zimmermann odd-numbered versions. Viacrypt, thus, created a new version (based on PGP 2) that they called PGP 4. To remove confusion about how it could be that PGP 3 was the successor to PGP 4, PGP 3 was renamed and released as PGP 5 in May 1997.

14.1.10   NETWORK ASSOCIATES ACQUISITION

In December 1997, PGP Inc. was acquired by Network Associates, Inc. ("NAI"). Zimmermann and the PGP team became NAI employees. NAI was the first company to have a legal export strategy by publishing source code. Under NAI, the PGP team added disk encryption, desktop firewalls, intrusion detection, and IPsec VPNs to the PGP family. After the export regulation liberalizations of 2000 which no longer required publishing of source, NAI stopped releasing source code.

In early 2001, Zimmermann left NAI. He served as Chief Cryptographer for Hush Communications, who provide an OpenPGP-based e-mail service, Hushmail. He has also worked with Veridis and other companies. In October, 2001, NAI announced that its PGP assets were for sale and that it was suspending further development of PGP encryption. The only remaining asset kept was the PGP E-Business Server (the original PGP Commandline version). In February 2002, NAI canceled all support for PGP products, with the exception of the renamed commandline product. NAI (now McAfee) continues to sell and support the product under the name McAfee E-Business Server.

14.1.11   CURRENT SITUATION

In August 2002, several ex-PGP team members formed a new company, PGP Corporation, and bought the PGP assets (except for the command line version) from NAI. The new company was funded by Rob Theis of Doll Capital Management (DCM) and Terry Garnett of Venrock Associates. PGP Corporation supports existing PGP users and honors NAI's support contracts. Zimmermann now serves as a special advisor and consultant to PGP Corporation, as well as continuing to run his own consulting company. In 2003, PGP Corporation created a new server-based product called PGP Universal. In mid-2004, PGP Corporation shipped its own command line version called PGP Command Line, which integrates with the other PGP Encryption Platform applications. In 2005, PGP Corporation made its first acquisition—the German software company Glück & Kanja Technology AG,

Since the 2002 purchase of NAI's PGP assets, PGP Corporation has offered worldwide PGP technical support from its offices in Draper, Utah; Offenbach, Germany; and Tokyo, Japan.

On April 29, 2010 Symantec Corp. announced that it would acquire PGP for $300 million with the intent of integrating it into its Enterprise Security Group.

PGP CORPORATION ENCRYPTION APPLICATIONS

This section describes commercial programs available from PGP Corporation. For information on other programs compatible with the OpenPGP specification, see External links below.

While originally used primarily for encrypting the contents of e-mail messages and attachments from a desktop client, PGP products have been diversified since 2002 into a set of encryption applications which can be managed by an optional central policy server. PGP encryption applications include e-mail and attachments, digital signatures, laptop full disk encryption, file and folder security, protection for IM sessions, batch file transfer encryption, and protection for files and folders stored on network servers and, more recently, encrypted and/or

signed HTTP request/responses by means of a client side (Enigform) and a server side (mod openpgp) module. There is also a Wordpress plugin available, called wp-enigform-authentication, that takes advantage of the session management features of Enigform with mod_openpgp.

The PGP Desktop 9.x family includes PGP Desktop Email, PGP Whole Disk Encryption, and PGP NetShare. Additionally, a number of Desktop bundles are also available. Depending on application, the products feature desktop e-mail, digital signatures, IM security, whole disk encryption, file and folder security, encrypted self-extracting archives, and secure shredding of deleted files. Capabilities are licensed in different ways depending on features required.

The PGP Universal Server 2.x management console handles centralized deployment, security policy, policy enforcement, key management, and reporting. It is used for automated e-mail encryption in the gateway and manages PGP Desktop 9.x clients. In addition to its local keyserver, PGP Universal Server works with the PGP public keyserver—called the PGP Global Directory—to find recipient keys. It has the capability of delivering e-mail securely when no recipient key is found via a secure HTTPS browser session.

With PGP Desktop 9.x managed by PGP Universal Server 2.x, first released in 2005, all PGP encryption applications are based on a new proxy-based architecture. These newer versions of PGP software eliminate the use of e-mail plug-ins and insulate the user from changes to other desktop applications. All desktop and server operations are now based on security policies and operate in an automated fashion. The PGP Universal server automates the creation, management, and expiration of keys, sharing these keys among all PGP encryption applications.

The Symantec PGP platform has now undergone a rename. PGP Desktop is now known as Symantec Encryption Desktop, and the PGP Universal Server is now known as Symantec Encryption Management Server. The current shipping versions are Symantec

Encryption Desktop 10.3.0 (Windows and Mac OS platforms) and Symantec Encryption Server 3.3.2.

Also available are PGP Command Line, which enables command line-based encryption and signing of information for storage, transfer, and backup, as well as the PGP Support Package for BlackBerry which enables RIM BlackBerry devices to enjoy sender-to-recipient messaging encryption.

New versions of PGP applications use both OpenPGP and the S/MIME, allowing communications with any user of a NIST specified standard.

OPENPGP

Inside PGP Inc., there was still concern about patent issues. RSADSI was challenging the continuation of the Viacrypt RSA license to the newly merged firm. The company adopted an informal internal standard called "Unencumbered PGP": "use no algorithm with licensing difficulties". Because of PGP encryption's importance worldwide (it is thought to be the most widely chosen quality cryptographic system), many wanted to write their own software that would interoperate with PGP 5. Zimmermann became convinced that an open standard for PGP encryption was critical for them and for the cryptographic community as a whole. In July 1997, PGP Inc. proposed to the IETF that there be a standard called OpenPGP. They gave the IETF permission to use the name OpenPGP to describe this new standard as well as any program that supported the standard. The IETF accepted the proposal and started the OpenPGP Working Group.

OpenPGP is on the Internet Standards Track and is under active development. The current specification is RFC 4880 (November 2007), the successor to RFC 2440. Many e-mail clients provide OpenPGP-compliant email security as described in RFC 3156. The standard was extended to support Camellia cipher by RFC 5581 in 2009, and encryption based on elliptic curve cryptography (ECDSA, ECDH) by RFC 6637 in 2012. Support of EdDSA will be added by draft-koch-eddsa-for-openpgp-00 proposed in 2014.

The Free Software Foundation has developed its own OpenPGP-compliant program called GNU Privacy Guard (abbreviated GnuPG or GPG). GnuPG is freely available together with all source code under the GNU General Public License (GPL) and is maintained separately from several Graphical User Interfaces (GUIs) that interact with the GnuPG library for encryption, decryption and signing functions (see KGPG, Seahorse, MacGPG). Several other vendors have also developed OpenPGP-compliant software.

There are several iOS and Android OpenPGP-compliant applications such as iPGMail for Android which enable key generation and encryption/decryption of email and files on Apple's iOS and Android.

- PGP
    - [RFC 1991](#) PGP Message Exchange Formats (obsolete)
- OpenPGP
    - [RFC 2440](#) OpenPGP Message Format (obsolete)
    - [RFC 4880](#) OpenPGP Message Format
    - [RFC 5581](#) The Camellia Cipher in OpenPGP
    - [RFC 6637](#) Elliptic Curve Cryptography (ECC) in OpenPGP
    - draft-koch-eddsa-for-openpgp-01 EdDSA for OpenPGP
- PGP/MIME
    - [RFC 2015](#) MIME Security with Pretty Good Privacy (PGP)
    - [RFC 3156](#) MIME Security with OpenPGP

OpenPGP's encryption can ensure secure delivery of files and messages, as well as provide verification of who created or sent the message using a process called digital signing. Using OpenPGP for communication requires participation by both the sender and recipient. OpenPGP can also be used to secure sensitive files when they're stored in vulnerable places like mobile devices or in the cloud.

15 BITCOIN:
A PEER-TO-PEER ELECTRONIC CASH SYSTEM
SATOSHI NAKAMOTO

15.1.1.1 October 31, 2008

ABSTRACT

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. INTRODUCTION

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of

ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. TRANSACTIONS

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the

company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced[1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. TIMESTAMP SERVER

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post[2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

4. PROOF-OF-WORK

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash[6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the

block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.

The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. NETWORK

The steps to run the network are as follows:

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.

5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. INCENTIVE

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. RECLAIMING DISK SPACE

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. SIMPLIFIED PAYMENT VERIFICATION

It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.

As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. COMBINING AND SPLITTING VALUE

Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.

It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. PRIVACY

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. CALCULATIONS

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows[8]:

pqqz=== probability an honest node finds the next block probability the attacker finds the next block probability the attacker will ever catch up from *z* blocks behind
qz={1(*q/p*)*zifp*≤*qifp*>*q*}

Given our assumption that $p>q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and *z* blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$\lambda = zqp$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \left\{ \begin{array}{ll} (q/p)^{(z-k)} & \text{if } k \leq z \\ 1 & \text{if } k > z \end{array} \right\}$

Rearranging to avoid summing the infinite tail of the distribution...

$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} (1 - (q/p)^{(z-k)})$

Converting to C code...

```
#include  double AttackerSuccessProbability(double q, int z) {
        double p = 1.0 - q;    double lambda = z * (q / p);   double sum
= 1.0;  int i, k; for (k = 0; k <= z; k++)          {                       double
poisson = exp(-lambda);              for (i = 1; i <= k; i++)                         poisson *:
```

Running some results, we can see the probability drop off exponentially with *z*.

```
q=0.1 z=0   P=1.0000000 z=1   P=0.2045873 z=2   P=0.0509779 z=3
P=0.0131722 z=4   P=0.0034552  z=5   P=0.0009137 z=6
P=0.0002428 z=7   P=0.0000647 z=8   P=0.0000173 z=9
P=0.0000046 z=10  P=0.0000012  q=0.3 z=0   P=1.0000000 z=5
P=0.1773523 z=10  P=0.0416605 z=15  P=0.0101008 z=20
P=0.0024804 z=25  P=0.0006132 z=30  P=0.0001522 z=35
P=0.0000379 z=40  P=0.0000095 z=45  P=0.0000024 z=50
P=0.0000006
```

Solving for P less than 0.1%...

P < 0.001 q=0.10   z=5 q=0.15   z=8 q=0.20   z=11 q=0.25   z=15 q=0.30   z=24 q=0.35   z=41 q=0.40   z=89 q=0.45   z=340

12. CONCLUSION

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

REFERENCES

1. W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998. ↵
2. H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20TH SYMPOSIUM ON INFORMATION THEORY IN THE BENELUX, May 1999. ↵ ↵
3. S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In JOURNAL OF CRYPTOLOGY, vol 3, no 2, pages 99-111, 1991. ↵
4. D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In SEQUENCES II: METHODS IN COMMUNICATION, SECURITY AND COMPUTER SCIENCE, pages 329-334, 1993. ↵
5. S. Haber, W.S. Stornetta, "Secure names for bit-strings," In PROCEEDINGS OF THE 4TH ACM CONFERENCE ON

COMPUTER AND COMMUNICATIONS SECURITY, pages 28-35, April 1997. ↵ ↵

6. A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002. ↵

7. R.C. Merkle, "Protocols for public key cryptosystems," In PROC. 1980 SYMPOSIUM ON SECURITY AND PRIVACY, IEEE Computer Society, pages 122-133, April 1980. ↵

8. W. Feller, "An introduction to probability theory and its applications," 1957. ↵