Easy to Understand Guide to Cryptocurrencies



March 26th, 2015

Tired of your bank charging fees to withdraw and deposit YOUR money?
There are no fees for holding your cryptocurrencies (some cryptos actually give you a type of interest, called staking), and tiny fees compared to banks for sending them.
Is your country's currency inflating out of control?
Most cryptocurrencies have a limit built right into the code, for example, there will only be 21 million Bitcoins ever created.
Want to tip someone for a nice news article or youtube video?
Easily send money to people by tipping them a little crypto!
Want to send money across the globe easily/cheaply?
Cryptocurrency only requires a tiny fee, to send it instantly to anyone around the world.
Tired of businesses keeping track of what you buy?
Afraid of having your personal information getting into the wrong hands during a transaction?
Your personal information is not attached to your wallet address.
Own Your Own Business?
Tired of worrying about Credit Card/Paypal Disputes?
With cryptocurrencies, there are no charge-backs! If you get paid for goods or services, you don't have to wait, worrying that they will do a charge back in a few days.
Tired of having to deal with high credit card fees just to take them? With cryptocurrencies, there are absolutely no fees to receive money!

If you answered yes to any of those questions, you might be a crypto-fan after reading this guide!

Table of Contents

I. Introduction

	1. What is cryptocurrency?	pg. 2
	2. Why should you want some?	
	3. Risks to think about	
	4. More in-depth information	
	5. Cryptocurrency: How it works	
	6. Whales, & Bulls, & Bears, Oh My!	
	7. Differences in Altcoins	
II.	Getting Cryptocurrencies	
	1. Getting a Wallet	pg. 22
	2. Purchasing Them	pg. 25
	3. Cryptocurrency Faucet Websites	2.0
	4. Mining Cryptocurrencies	2.0
	5. Working for Cryptocurrencies	
	6. Gambling for Cryptocurrencies	- 0
	7. Crypto Tipping	
	8. Receiving Sent Cryptocurrencies	
H	. Recommendations	
	1. Strategies	pg. 37
	2. Ways to Diversify	pg. 39
	3. Protecting yourself / Reducing Risk	
	4. How Escrow Works	
	5. Protecting Your Wallets	
	6. Choose a Community	
	7. Pay it Forward	pg. 50
	8. Addendum	

Introduction

What is cryptocurrency?

It's a fairly new form of digital currency used to purchase goods and services. It can also be traded for other forms of fiat money, such as the dollar, or Euros. Fiat money is money that gets its value from a government or law. Some cryptocurrencies are more well known and accepted in trade than others. Bitcoin was the first cryptocurrency (created in 2009), and as such, it is the most accepted.

It's called cryptocurrency because it uses cryptography to secure the transactions and to control the creation of new units. In the case of Bitcoins, there will be 21 million Bitcoins made, and then they will not be able to be created anymore. As of right now there are about 14 million in circulation.



Mining Coins - Creating Money

When you think of mining, you might think of someone working in a cave, mining for gold. Times have changed. Now you can mine for coins on your computer! As I stated above, there will be only 21 million Bitcoins ever made. But they're not all made yet! People right now are using their computers and running a program you can download off of the internet. The program is free to download; in fact there are multiple versions of mining programs to

choose from. You can mine solo, or join mining pools.

(Note: Bitcoin mining is very difficult these days, and it is usually less expensive to buy Bitcoins instead of buying the miners and paying for the electricity needed to do the mining.)



VICE Tours a Bitcoin Mine in China

What is Mining?

When someone uses Bitcoins to purchase something, that transaction has to be verified. And it's not just one transaction that people are trying to verify; there are a lot. All of these transactions are gathered together in a "block chain" that needs to be unlocked. Miners run programs that try to unlock these block chains, and once someone does, these transactions are verified. Right now, for unlocking the block chain you get 25 Bitcoins that hadn't existed until then. You have created money. Now, many people are trying to do the same thing, so the chances are low for someone to find the key themselves. You may get extraordinarily lucky, but most join mining pools and get a smaller piece of the shared action. Since Bitcoins are not real coins that you can touch, they are easily divided. Consequently, people are not usually buying/selling/trading a whole Bitcoin at a time, but rather fractional pieces of one. Think of it in terms of different denominations of fiat currency, such as \$100, \$50, \$20, \$1 bills, or various coins such as dimes, or pennies, etc.

A Satoshi is the smallest fraction of a Bitcoin that can currently be sent: it is 0.00000001 of a Bitcoin. The name comes from Satoshi Nakamoto, the creator of Bitcoin. It is not known whether the name "Satoshi Nakamoto" is real, or a pseudonym. The name may represents one person, or a group of people.

Not all cryptocurrencies allow mining for their units. Their developers require you to purchase them with more widely accepted fiat money.

Multiple Cryptocurrencies

Bitcoin is currently the most well known cryptocurrency, but there have been many others created since Bitcoin was introduced. These others are known as Altcoins (Bitcoin alternatives). One of the more popular Altcoins is Litecoin. It was created in 2011, and offers faster confirmations (which means that the chances for double spending are reduced). Litecoin uses Scrypt in its' Proof of Work algorithm. The reason it was created was in part to allow miners to mine both Bitcoins and Litecoins at the same time, and to avoid giving undue advantage to those miners who would use more specialized equipment to mine. Some examples of this specialized mining would include using a video card's GPU (Graphic Processing Unit), or an ASIC (Application-Specific Integrated Circuit), which is an integrated circuit that is customized for a specific use. In this case it's customized in its design,

purely for mining coins.

The earlier cryptocurrencies were launched initially because their creators were trying to fix something that they thought was wrong with Bitcoins, although some more recent cryptocurrencies seem to have been launched "just because".



Market Capital Listing of Cryptocurrencies: http://coinmarketcap.com/

If you could create a coin and get the whole world to use it, and if you were allowed to trade your coins (that you stored from the beginning) for millions of dollars, would you do it? Everyone wants a piece of the pie. Satoshi Nakamoto is thought to be in possession of roughly I million Bitcoins, which is, as of today, valued at approximately 253 million dollars (USD). Bitcoin has already exceeded a value of \$1,000 per coin since its inception. Like any commodity, daily value fluctuates. Today, as of this writing, the Bitcoin is in the \$250 range.

Bitcoin currently has the strongest backing amongst the cryptocurrencies, because it's the first one, and it's the one that most people know about. However, the reason we made this guide for all Cryptocurrencies versus a guide to Bitcoins alone, is because a cryptocurrency could come along with more improvements, and blow Bitcoins right out of the water, (and fairly easily, in our opinion). Think about this: how many inventions do we actually maintain as a prototype, as opposed to a version(s) that has been altered and perfected?

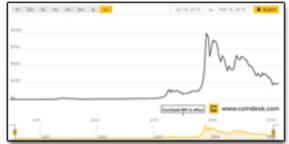
Why Should You Want Some?

Though people may laugh at the notion of cryptocurrency when they hear of it for the first time, there are several compelling reasons why you might want to get your hands on some of these new currencies. People might say, "but you can't hold it". Technically, you can print out a paper wallet and hold it. You can also save it onto a flash drive and hold that.

People might say, "but it doesn't do anything." Neither do paper bills. What makes a 100 dollar bill worth more than a 1 dollar bill? Absolutely nothing, except for the fact that people believe it is worth 100 times the 1 dollar, and because the government will back that up. If the US government broke up, and the country ceased to exist, we might be left with a bunch of pieces of paper that would no longer hold any real value.

Cryptocurrencies are volatile.

I wouldn't suggest spending money you can't afford to lose on cryptocurrencies (or any other investment, for that matter). It's similar to gambling, and it's not unlike the stock market. Don't buy stock in a company if you can't afford to lose all that money if the company fails.



But because cryptocurrencies are volatile, you may be able to make a lot of money if you approach it correctly. As I've said, Bitcoins have hit \$1,000 per coin, and they're around \$250 per coin today. They started out very modestly. Someone tried selling 10,000 Bitcoins for 50 dollars. In other words, each Bitcoin was priced at about half a cent USD. https://bitcointalk.org/index.php?topic=92.0 There were no takers, because people complained it was too expensive. So the auction ended without them even being sold.

Someone also paid 10,000 Bitcoins for 2 pizzas to be delivered to them in 2010: https://bitcointalk.org/index.php?topic=137.0 (If those 10,000 Bitcoins were sold today the person who sold the pizzas would have 2.5 million dollars minus the price of the pizzas of course.)

Can be "Free Money"

Many cryptocurrencies can be mined. The software is free, the work is done by your computer. You're spending your time (to download and set it up) and your electricity costs (to power your computer). You might leave your computer on while you're at work all day anyway, why not let it work for you while you're out?

There are also faucet websites that give away cryptocurrencies for free; all you have to do is answer some captchas to prove that you're a human (and not a bot). Also, people have recently been tipping others online with cryptocurrencies.

Anonymous

It's a lot more anonymous and untraceable than using bank accounts and credit cards. Once you have a wallet you get an address number, which is where the cryptocurrency is sent to, and sent from. Most, if not all cryptocurrencies are transparent. For example, all Bitcoin transactions ever created are logged but all transactions are listed from one address to another with no names attached. Some cryptocurrencies are more anonymous than others, for example Darkcoin (which has recently been rebranded to DASH) has a feature called "Dark Send" to make your transactions even more anonymous than Bitcoin.

Low Inflation

Most cryptocurrencies have a fixed, limited amount of units that are going to be created. Unlike fiat currencies, where money can be printed/created, (causing all other units to be worth less), cryptocurrencies end up with a fixed, predetermined amount in circulation. Actually, over time, it will become a deflationary currency, because (as is the case with Bitcoins), there will be finite units ever made. Also, people have lost some Bitcoins due to hard drive crashes, lost wallets, and other human errors - further safeguarding the value of each unit.

Low Collapse Risk

Cryptocurrencies are global and not tied to a specific government. World-wide, governments are unstable and the money they issue can be devalued unexpectedly.

No chargebacks/Less Fees

One of the benefits of using credit cards to buy things is that you can cancel orders if someone fails to deliver for you. But if you're the seller, and someone just decides to cancel the order for any reason, you're out the money. Once a transaction is made with cryptocurrencies, the money is sent. All transactions are final. Paying with credit cards, bank cards and the like all require the use of a bank, or credit company. These require fees for every transaction. Making transactions online, without the use of a middle man, will cut down on fees. A large Western Union transaction across the globe could cost hundreds of dollars in fees, whereas the cryptocurrency fees for the same transaction might equal only a few cents.

Easy to carry

If an individual had sufficient cryptocurrencies, they could carry millions of dollars worth of cryptos on a flash drive in their pocket. With cryptocurrencies, you can also have an online wallet, or keep a wallet on your phone, tablet, or other mobile device.

Things to do with Cryptocurrencies

- * Purchasing & Selling Goods
- * Sending money without large transaction fees
- * Hiring employees, vendors, or service industry
- * Gambling & Tipping

Noteworthy Businesses Currently Accepting Bitcoin:

Microsoft TigerDirect
Dell 1-800-Flowers

DISH Network BTCTrip
Overstock.com Newegg

Risks to Think About

Volatility

Even though you could make lots of money buying Bitcoins, and other cryptos, you could potentially lose it all. There is never a guarantee that you can sell any cryptocurrency for the same, or higher price, than you paid for it. This is why we would recommend mining for cryptocurrency, working for cryptocurrencies, using faucets, and/or only buying what you can afford to lose.

Governments Trying to Govern Cryptos

Governments are getting more concerned about the increased popularity of cryptocurrencies - which could eventually offer a direct competition to actual fiat currency. Debate exists in many governments as to whether or not income generated from cryptocurrencies should be taxed. Anyone planning on getting involved with cryptocurrencies should try to monitor how this debate is effecting tax laws in their community. Keep in mind that even if governments decide to tax cryptos, such laws will be exceedingly difficult to enforce. If you buy cryptocurrency, and send it to another wallet, the government will have no way to track if you were paying someone, transfering your own money back to yourself, gifting a friend, or donating to an organization. In other words, it will be difficult for anyone to pierce the anonymity of the crypto transactions. But remember if you purchase them with your bank account, you may have to account for them if the government asks about the purchases.

Easy to Lose

If your credit card gets stolen, you can report it to the company, and typically you will not be responsible for purchases made after it was stolen. If someone steals your hard drive, or zip drive, any cryptocurrencies on it are gone forever. A man once threw away a hard drive with 7,500 Bitcoins on it. He didn't remember the Bitcoins were on it, until after the fact, and now they're sitting in a dump somewhere in the UK.

http://www.nbcnews.com/newsother/it-worker-throws-out-hard-drive-loses-7-5-million-f2D11669738

You can lose cash the same way as you can lose cryptocurrencies. So treat it the same way you would treat your cash. You can learn how to backup your wallet. Keep it in a safe place. You can still use banks, and if you have a large portion of cryptocurrency, you can save it on a flash drive, and perhaps put it into the bank's safety deposit box.

Putting all your bits in one basket

You could just buy some Bitcoins and make money if the price goes up. But other alt coins may be capable of making you more money in the long run, because they're cheaper to buy. It's a race for cryptocurrencies, and although Bitcoin is winning right now, another cryptocurrency could easily surpass it one day. In that scenario, the price for Bitcoins could go down.

Each different cryptocurrency requires a seperate wallet; it is not possible to carry more than one crypto type in a particular wallet. So basically, each time you decide to acquire a particular crypto, it will necessitate aquiring a new wallet. We will discuss the pros and cons of the various wallets a little bit later.

Limited Ability to Purchase Goods & Services

At the moment, Bitcoins are not widely accepted online for the purchase of goods and services. Daily transactions, such as paying your rent, buying groceries, etc are also very difficult to do. But as cryptocurrencies gain in popularity, and more people realize the benefits of using these alternate currencies, that is sure to change.



This is a transition period, much as e-mail was at first seldom used, while today it has virtually replaced snail mail as a means of communication. We may currently be witnessing a similar transition to cryptocurrencies from traditional fiat monies.

More In-depth Information

There isn't really any need to know precisely how cryptocurrencies work in order to to use them; much in the same way that you can get in your car, turn the key and drive without understanding how the combustion engine works. The following is here for you only if you're interested in learning how cryptos work, why they work, and to learn some terms that you may run into. If you want to read up further, or participate in the various forums, and/or keep current with news articles, this section may help.

To compare, think of how fiat money works. Account information is shown online, and funds can be transfered online too. But the actual money is in a bank, in a vault, and banks have ledgers that keep track of your account balances. Banks know when you spend money, and they know when you receive money. Problems can occur when banks allow customers to make charges that result in a negative balance.

FIAT MONEY

LEDGER OF BALANCES IS IN BANKER'S HANDS

LARGE FEES

CAN BE REFUNDED BACK

ACTUAL MONEY STORED IN VAULTS

REQUIRES YOU TO USE BANKS OR SERVICES TO PAY SOMEONE ONLINE

CAN HAVE MORE PRINTED WHICH CAUSES INFLATION AND ALL MONEY IS WORTH LESS THAN IT USED TO BE

TRANSACTIONS CAN BE TRACED BACK TO YOU

CRYPTOCURRENCY

LEDGER OF BALANCES IS IN THE WALLET OF EVERYONE ON THE NETWORK AND SHOWN ONLINE

SMALL FEES

CAN'T BE REFUNDED BACK

ACTUAL MONEY STORED IN COMPUTERS, FLASHDRIVES, CDS, PAPER WALLETS, BRAIN WALLETS, COLD WALLETS IN SAFES, ETC.

LETS YOU PAY SOMEONE ONLINE IMMEDITATELY WITH YOUR WALLET BROADCASTING THE CHANGES TO EVERYONE

HAS LIMITS TO HOW MANY WILL BE CREATED. SOME WILL BE LOST WHICH CAUSES DEFLATION OVER TIME, MEANING MONEY WILL BE WORTH MORE OVER TIME

TRANSACTIONS CAN BE ANONYMOUS

If you don't have overdraft protection, banks will charge you exorbitant fees for every transaction that occurs while you are in a negative balance. The bank knows your balance, but no one else does. With cryptocurrency, everyone on the network knows how much balance each wallet address has by checking it on the blockchain. The wallet checks the blockchain to make sure you have enough funds whenever you send some. This allows for more accurate real time accounting, and eliminates any overdraft fees and related expenses.

Cryptocurrency: How it works

Your Wallet - Public & Private Keys

Your wallet creates a Private Key and a Public Key (also known as a public address). You can decrypt a private key to get your public key, but you can't use a public key to find a private key. So you can feel confident in showing your public key, but if someone sees your private key, that's all they need to take the money from that address. Be certain to safeguard your private key.

The Blockchain (Ledger of Transactions)

The blockchain consists of every transaction ever made. You trust your bank to have an accurate ledger of how much you've spent and how much you've deposited. Only the bank can see your ledger. The blockchain is a public ledger that everyone can view at any time. You can search for a public address and see the current balance, how many deposits or withdrawls were made, and how many coins were moved in each transaction. You can even see who they paid, or were paid by. But unless you know the owner of that specific address, you don't really know where the money went. Also you can have, and are encouraged to have, a new address for every transaction. This is explained later, and is simple to do.

Sending Money

When you want to send money from an address, you send a message to the network relaying that task. The message is received by others with their wallet receiving the update immediately. Your digital signature is required and created using your private key. Your wallet software does this for you.

Digital Signature = Private Key + Message

The message is built upon the blockchain (so your signature is different with every transaction). The signature also prevents the transaction from being altered by anybody once it has been issued. Also the other ledgers around the world are able to verify that you have the private key without actually seeing the private key. This blockchain technology, combined with cryptography, make cryptocurrency transactions heavily secured.

Cryptocurrency Transactions

People simplify when they talk about transactions, saying they are "sending" coins across the world, but all you're actually doing is updating the ledgers to reflect that you agree you'll have less and who you "sent to" will have more. Also the ledger doesn't keep track of your balance the way people traditionally think it does. Ownership of funds is verified through links to previous transactions.

To send 5 BTC, you must prove that your address received 5 or more BTC in previous transactions. Since your wallet creates multiple key pairs (public and private), your wallet keeps track of your balance of all of those

1962287189911299112

54.84.54.139

As seen to the right, there

are visualization

1FETSHZY/000088KJU/m82V/NCNQ&JYD66W/
78.47.84.114

programs that allow you

to trace, and follow payments easily.

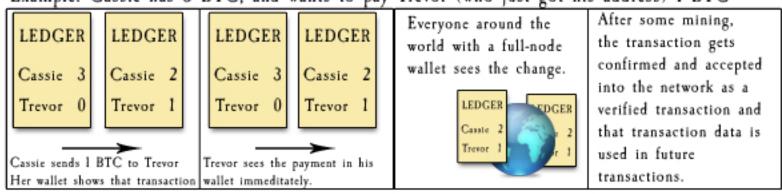
4170 BTC 18TnHKS1gCfLndCS5TBboeLGtgQCxhs 91.188.190.130

● 1000 BTC 1AFbZuU5PufVRhNCChw8br6beo6K78r2H

When you transfer bitcoins, you and the recipient will see the transaction immediately. However, the network needs to check that you have the correct Digital Signature, (proving that it hasn't been tampered with, and you had

the private key), and also that you have, in the past, received more than you want to spend. When people talk about mining bitcoins, they're actually checking that all these transactions are legitimate and then they add them to the blockchain as confirmed transactions.

Example: Cassie has 3 BTC, and wants to pay Trevor (who just got his address) 1 BTC



How Wallets Work

First, you get a wallet (that you can either download or sign up for online). That wallet creates a public address and private key for that address for you. The public address will look something like this: INeN5dNdbeYagJqxRqJa64HBtKx4JKMVbH. That's a Bitcoin address.

To compare to altcoins, they tend to start with the letter of the coin.

Here are some examples:

A Dogecoin address: DDbHgSdCjHmHFsFtLhZptjrtRBAd4cCoxW A Litecoin address: LQz2lrEg6KTa5iHDKRmG56X9679vxBkRiK A Woodcoin address: WRCcgEQV8fkMYJm95yuuPNdPJFlqfszqFT

A Candycoin address: YQC9ru8RWms9fFAtfYWVmXmKndPiQBMo6H (the Y is for YUM)

Though it's not always the case, it helps to quickly tell which address you're most likely looking at. For example: Darkcoin which has now rebranded to DASH, starts with a D like Dogecoin, but their addresses start with an X. Also, Bitcoin addresses often start with a l, but you may see an address with a 3. Addresses beginning with a 3 are pay-to-script-hash addresses (P2SH). Most of the time they are used to do multisig but they are not limited to that. Multi-sig means you need multiple private keys to send money from it. This is done to ensure if you lose one address, you can still get access to your money, or if you're dealing with strangers, that you need multiple people to agree to move the money, and not just one person.

Public addresses are able to be shown to anyone. The general public can't withdraw funds from those addresses since they don't have the private key, however they can send funds to them or view their balances on the blockchain.

How Wallets Work (continued)

Once you have a wallet you can make multiple addresses. All of those addresses would lead to your wallet, but if you hand one address out to your friend, and one address out to your job (for your salary) you can keep track of where your income is coming from.

Label	1	Address
777Bitcoin	1	QGMZedQZF51d46imKauVA5Yq6TqjnFUQq
_1800Flowers	1	2J5H7wn6rF6r4vaG1CLeJ6t9aUUK7jEMk
_Microsoft	1	DKQaCnVYYYkxFmqkKy4pEY9j2Up3ryZ68
_Sarah	1	MxtTKafzmmN9R9cc2GCFMcXvT4ADvKSE
Work	1	5YHLmgXveFXEgSHd27kEeLevWGrwoGWsI

So, now if you were worried that sending out your address to someone would allow them to view your balances, you see you can just have a seperate address dedicated to them, and create a new one anytime. You can also send funds from one address to another of your own addresses (that no one knows belongs to you, but you).

Scan the QR code and watch the video makingmoneyhoney.com/BTCmath.htm





Want more information? "How do you slow down hackers and provide equal access to everyone on earth? Not easy. But Bitcoin's solution is devilishly simple, employing outrageously big numbers. Bitcoin's private keys are made of numbers (called quindecillions) that are so large, they literally choke the best computers..."

How Transactions Work

When you want to make a transaction you need to sign your transaction with your private key, a digital signature of sorts. It proves that you are the owner of your wallet's funds. The wallet does this for you, you aren't asked for anything when you make a transaction from your particular wallet (unless you have added a secondary password, like you should, which it will ask for). Unlike a password, your digital signature is different for each transaction.

Once you have sent a transaction out to someone, it is added to the Blockchain. The Blockchain is a public ledger of all the transactions ever made. All wallets have access to the blockchain, and use it to check balances for funds and to make future payments. The integrity of the blockchain is enforced with cryptography. When you make a transaction, the transaction can't be partially spent, so you're actually sending out all of it, split into what you're sending to someone else, and the rest (minus what's spent on the transaction fee), the change, is sent back to yourself.

Now that the transaction is on the blockchain, miners go to work. Mining is a distributed consensus system that looks at the transactions and attempts to verify that the transactions are valid, have not been manipulated and are in chronological order. It's a consensus system because all the wallets in the world are in consensus that a transaction was valid, and completed, or else it isn't added to the past transactions and is not used in future transactions.

Every transaction is built upon the most recent validated transactions. That is why it is not possible to refund money once it's been sent and confirmed by the network. Once it's confirmed, new transactions are using those older transactions as the backbone of the network. The more confirmations by the network, the less chance it can be refunded or ignored by others in the network. Most people will require 6 confirmations to feel safe that their money has definitely been added to their wallet. This means that people can't force transactions into the blockchain to trick it into giving them extra money. This is what is so great about the currency being built upon cryptography.

Want a visual explanation on how Bitcoin transactions work?

Check out this video from CuriousInventor on youtube.com

Scan the QR code and watch the video

or go here: http://makingmoneyhoney.com/UnderHood.htm

Double Spending & 51% Attack

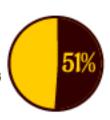
Double spending is when some money is successfully used twice. Bitcoin helps to protect against this when the transactions are added to the block chain because they get checked to see if it has already been spent or not.

Bitcoin is the most vulnerable to double spending when a payment goes out with 0 confirmations, after each confirmation the chances for double spending get less and less because more and more ledgers around the world agree that the money was spent already and therefore cannot be spent again. That is why most people will not pay out until they see their received payment has been confirmed 6 times.

The whole world is covered with people all over who have Bitcoin wallets, each of which hold the ledgers of all transactions on the Bitcoin network. But there is a way someone could, technically prevent transactions of their choosing from gaining any confirmations, so they could spend money, and stop those transactions from ever getting confirmed, thereby keeping the money.

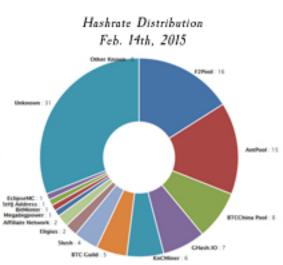
How is that possible?

They'd have to be able to mine 51% of the transactions to keep others from mining the transactions that have the purchase that they want to go unnoticed by the network. As long as the network is split in such a way that no one has that much mining hashrate than no one can stop the network from coming to the right conclusion that the payment has already been spent.



Can that happen?

It has happened for a little bit, in June 2014. Because people have been joining mining pools to mine, they've pooled their mining power together and for a few hours a mining pool, "Ghash.io, did have more than 51% of the hashing power. But members of the pool pulled their computing power out of the pool. There was no evidence that anything malicious was attempted, and mining pools are wary of ever getting to that point.



Types of Forks

Fork



A fork is the name for splitting apart from something to go in a different direction. The majority of altcoins are forks of Bitcoin, meaning they took Bitcoin's source code, and modified it in some way.

A lot of altcoins are extremely similar to Bitcoin, however there are a few altcoins that tried to make Bitcoin's source code better, and so they made more changes to it.

Soft Forks

Examples: New transaction types added, and changing mining fee policies.

Soft Forks are backward-compatible and only require the majority of the miners upgrading to enforce the new rules. Only the sender and receiver and miners have to understand the new fork's changes, because anything changed can be seen by older clients as regular transactions.

Hard Forks

Examples: Changing the block structure, block hash, or difficulty rules.

Hardforks in the network require upgrading because older versions of the program will not accept the new blocks of information.

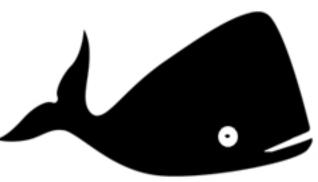
March 26th, 2015: there was a discussion going on about a proposal to hard-fork Bitcoin, to increase the block size from IMB to 20MB. Results of the poll on the official Bitcoin Forum as of this day: 59.4% pro, 19.3% anti, and 21.2% don't care (agnostic or DGAF).

Major Pros: Faster confirmations, less fees, other businesses can use the extra space for new projects, etc

Major Cons: Larger Full Node downloads, and more centralization, (because less people will use full node wallets and internet services will restrict connecting to more peers at one time)

For more information, search "Gavin Andresen 20 MB Fork" online.

Whales, & Bulls & Bears, Oh My!



Whales

The term Whale usually refers to crypto-holders who have a large financial backing. They can be found either buying or selling. The name whale refers to how big they are in the marketplace and the waves they can make with the prices due to their buy or sell orders.



The term Bull refers to someone who is confident in the cryptocurrency in question, and believes it will be successful. They're very optimistic the price will rise, and can be seen buying often, especially when the price dips.

Bears

The term Bear refers to someone who believes that the cryptocurrency is bound to drop in price. They have no confidence in that crypto-market, and will sell if they're even holding any. They're also seen short-selling.

In October of 2014, when the price was usually \$320-340, someone tried selling 30,000 Bitcoins for \$300/ea. They were named the "Whalebear," with stories popping up about the crypto community slaying the whalebear and getting prices back up to their normal price range within hours.

Differences in Altcoins

Proof of Work, Proof of Stake, & Proof of Burn

Proof of work (POW) is what it sounds like. You are proving that you have done work when your computer solves the puzzle of the blockchain. When you solve the puzzle, you get paid. Your computer is using time and processing power to get a result. If you have more processing power, you have a higher chance at getting paid. When you (or your mining pool) succeed you get new coins created and the transaction fees. (This process is called mining)

Proof of stake (POS) is also what it sounds like. You own some of the coins, so you have a stake in the coin, and how much of that coin you own factors into how likely and how much you will get paid. This chance is increased by how long you've had your stake in the coin also. If you are the one to succeed, you get the transaction fees. (This process is called forging)

Proof of Burn (POB) is built upon another cryptocurrency. The idea is to show that you have "burned" some coins instead using the processing power of your computer (POW). Burning coins refers to sending some of one cryptocurrency to an address that is verifiably unable to use those coins. Once coins are sent to an address that can't use them, they are gone forever (they can't be traded back into the economy again).

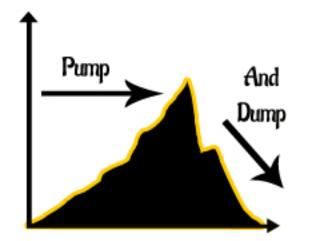
Proof of burn lets slower computers catch up to faster computers, because you aren't trying to prove a hard puzzle, you're just proving that you burned some coins. Since it's less work for computers, this is a more energy efficient form of mining. But it is based on burning Proof-of-Work cryptocurrencies, and as such still requires POW mining to be done.

Pre-mining, Pump & Dumps, & Dead Coins

Pre-mining: Since most coins are mined with increased difficulty over time, you can imagine the best mining is the first mining. Some creators of altcoins, make it so they can mine the coin before publicly releasing it, thereby getting a large chunk for themselves.

There are people who erroneously accuse some creators of pre-mining when they haven't; the actual creators are mining alongside the public at it's release.

Pre-mining by developers can give them excess coins to either be used in positive ways such as giving away coins in promotions (to get the word out) or in negative ways to use coins for bribes to try to get it listed on cryptocurrency exchanges (so they can exchange their new coin for fiat money to cash out).



Pump & Dumps: A pump and dump is when a developer of an altcoin pumps up the coin to investors, and then when it gets to be highly priced, dumps their large stock of coins from their pre-mine and makes off with the money, leaving the altcoin to die.

Dead Coins: There are a ton of coins that have been created since Bitcoin. CryptocoinCharts has 2,900+ coins listed right now. But that doesn't mean the developers have been taking care of all of those coins. Some developers pump and dumped their coins, some just were too greedy for their own good. The baconbits creator refused to pay miners that wanted to breathe new life into the coin even after he promised he would, so they left it to die.

Altcoins: Blockchain Reimagined

Folding Coin: Folding Coin is a token that you earn by helping scientists cure diseases!



"Folding@home is a long running project that began in Oct of 2000 from the folks Stanford University that lets your spare CPU or GPU simulate complex protein folding. The results of all this distributed computation is tabulated and analyzed to help new find new medicines and cures to be derived to some of the worst diseases faced by man." - foldingcoin.net

There was a problem, because in the past there wasn't a way to reward people who put their CPU to use. So they created FoldingCoin.



CureCoin: The Cure for the Common CryptoCurrency

"CureCoin is a CryptoCurrency based on coupling SHA-256 Mining and Folding@Home Protein Folding" - curecoin.net

Marijuana

Cannabis Coin, Mary Jane, & Potcoin: Marijuana companies are finding it extremely difficult to get a bank account. Banks are avoiding dealing with drug businesses, especially in light of the fact that Marijuana is still illegal in some states. This leads to medical Marijuana companies having extensive amounts of cash on them, which leads to very lucrative robberies. What could save them from needing a bank? Having a cryptocurrency

private key locked safely away, and taking payments with their public key.



GetGems: A social messaging app meant to bring cryptocurrency to the masses. Their idea is that current IM apps, like Skype or WhatsApp use information about you and your habits for their benefit. The GetGems app would give GEMZ to users to view

ads, allow advertisers to pay GEMZ to post ads, and would air-drop GEMZ for free to users from time to time. Of coure users can send GEMZ to friends or family with it too.

Getting Cryptocurrencies

Getting a Wallet

In order to get cryptocurrencies you must have a wallet to store them in. You can get a wallet for free, either online, or you can download one onto your computer. The availability for an online wallet varies depending on which cryptocurrency you're dealing with.

Though online wallets are easier to set up, they are more risky. Cryptocurrency is digital. Unlike online banking accounts that send information back and forth about how much you should have, the money is actually in the bank, in a safe. With cryptocurrency you are literally keeping your money in the website's hands and hoping they won't run off with it, or hoping they don't get hacked and have everything stolen. Your money in a bank

If you are looking for a Bitcoin wallet, you can go to the official website here: https://bitcoin.org/en/choose-your-wallet. If you are looking for a wallet for another cryptocurrency you will have to look at their website or search online.

may be FDIC insured, but your cryptocurrency is not.

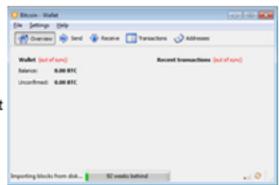
The bitcoin.org website has descriptions about various wallets, including online wallets and downloadable wallets for your computer as seen to right:

Due to the fact that your cryptocurrency is at risk in an online wallet, I suggest downloading a wallet onto your computer, phone or tablet at some point and keeping large amounts on a safely made paper wallet. But there are online wallets for those of you who want a wallet quickly to hold small amounts. You can set it up in minutes and use it for a while, and download a wallet onto your computer, phone or tablet and transfer the Bitcoins from the online wallet to the new wallet.

For safer storage, there are hardware wallets, paper wallets, and brain wallets. These will be described more in the Protecting Yourself / Reducing Risk section.

Getting a Wallet (continued)

If you download the Core Wallet software, it will synchronize with all the other wallets (for that particular currency) in the world. For example, Bitcoins: All the transactions ever made are recorded in a ledger listing wallet numbers for all sent and received transactions. Every transaction ever made is on this ledger.



When you start up a full node wallet on your computer for the first time, it synchronizes with the network of wallets. Your wallet will download all the information about every transaction ever made until it's caught up to the most recent transactions. If you leave it open it will continue to download as new transactions are made. But it can make for a long download to get caught up the first time. When we downloaded it, it took 5 days on and off, we had to turn it off at times because it made the internet slow. If you have faster internet service, or leave it on non-stop, you may be able to download it faster. If you download the wallet in a year from now, it might take longer because there's been another year's worth of transactions that have occurred.

"If you know how to download a torrent file, you can speed up this process by putting bootstrap.dat (a previous copy of the block chain) in the Bitcoin Core data directory before starting the software." (From the Bitcoin Core Download Page)

Phone/Tablet Wallets

You can also put a wallet on your phone/tablet. These aren't full wallets. As was mentioned the download of a full wallet is many gigabytes large and growing every day. So the wallet on a phone or tablet will be smaller in size. These wallets download a small bit of information and rely on other nodes in the network to verify that they have the right information. They can then scan QR

codes for receiving addresses in order to pay in cryptocurrency while you're away from your computer. Always research a wallet before downloading and using it. Also, be sure to backup your wallet and test sending small amounts before loading it up with a large amount of money. If your phone or tablet gets stolen, so are your funds unless you add extra security.

Altcoin Wallets

If you download a Core wallet for an Altcoin, you may find they look a lot like the Bitcoin Core Wallet. There are Phone/Tablet wallets for some altcoins also.



Brain Wallets

An interesting concept, brain wallets take a long phrase of words (that aren't written anywhere, and no one in the world but you

would ever come up with) and turning that phrase into a wallet private key. There are sites online that take a long phrase and turn it into a public key for you. You can send funds to the address listed and then use your passphrase to come up with the private key to unlock it later.

The idea is that your wallet's private key is never written down anywhere, and the numbers are so large, it's never going to get stolen, but you need to use a passphrase that will not be guessed by someone. Even if something happened to you, no one will ever know you created the wallet or how to get the funds unless you tell them. You need to save the information somewhere in the event of your death or becoming otherwise incapacitated otherwise the funds

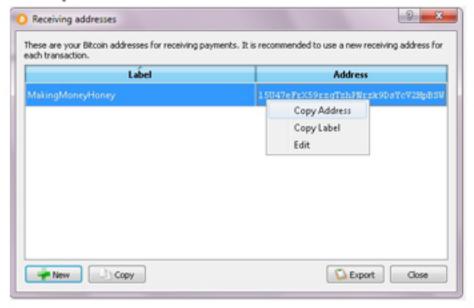
would be lost forever. if you want to make sure the website won't get the information you enter, you can download the zip file on the bottom of the page, and run it on a computer that does not connect to the internet.

There are many things to consider regarding securing your wallets, check out the Protecting Yourself / Reducing Risk section for more information regarding those.

Purchasing Them

Finding Your Address

Once you have a wallet, either online or on your computer, you will be able to find your address. In Bitcoin Core, you click on File>Receiving Addresses, and something like this will show up:



You can right click and copy the address and then paste it, without ever having to type it all out.

On your Phone or Tablet, you will see your address and a QR code. If you meet up with someone in person and they want to pay you, they can open their wallet and scan the code and never have to type in the address.

Now that you have your address, you can purchase some cryptocurrencies.



Purchasing Them (continued)

Remember that since cryptocurrencies can't be refunded once the transactions have gone through, when you go to purchase them, companies will most likely require to set up a bank account or use a money order for the transaction instead of using payments like credit cards that can be reversed.

When purchasing them, the company may give you an address, instead of asking where you want the crypto sent to. If they do, you can trade it from that address to your original address later.

There are ATMs in select cities that take cash and deposit Bitcoins for you.





In the main menu of your phone/tablet wallet, there is an option: "sweep paper wallet." Once you received the receipt, you would sweep the wallet, by scanning the QR code for the private key, which is hidden in the above picture. You can also sweep it, using the alphanumeric code underneath it, into an online wallet, or computer wallet.



Purchasing Bitcoins

Coinbase is a website for buying Bitcoins, in the US only, through your bank account.

Buying Bitcoins (The newbie version) is an easy to read guide on purchasing Bitcoins and it's from the official Bitcoin wiki and is maintained by the Bitcoin community. There are multiple links and explanations. Some of the forms of purchasing include: Wire Transfer, Bank Accounts, Personal Checks, and Cash (from meeting up with someone in person). Paypal is listed, but it's complicated because they haven't quite accepted Bitcoins fully. There are also issues with Paypal's refund policies in disputes, since Bitcoins aren't refundable. It is not advisable to use Paypal to purchase cryptocurrencies as it's easy to get scammed.

How to Buy Bitcoins in the UK is a pretty good guide for UKers.

Purchasing Altcoins

Cryptsy.com is a cryptocurrency exchange dealing with 200 altcoins.

C-Cex.com is another cryptocurrency exchange dealing with over 50 altcoins.

All of the above have Bitcoins listed, so if you're going to purchase other cryptos you can purchase the Bitcoins first and trade them. Please research any exchanges before sending them money. Some of the altcoin exchanges out there exist only to take your money and not let you withdraw. Any sites you see could have been good and working, and decided to break bad. You never want to leave money on an exchange, because they may be hacked and have their funds stolen.







Cryptocurrency Faucet Websites

There are websites online that will give out "free" cryptocurrencies called faucet websites. They are free, but the payouts are small, it takes your time and it takes your effort to get them. The websites are filled with ads, and they tend to not work if you have ad blockers working at the time of your visit, because they make money off of the ads on the website getting views, and clicks.

You paste in your wallet's address, and will probably have to type a captcha in to prove you're not a bot. Because the currency you're getting is very small, you usually have to get a set amount built up before they will send the funds out due to the fees. Though Bitcoin transfers have small fees compared to most currencies, there are fees for transactions because fees incentivize the miners to mine those blockchains and keep people from clogging up the blockchain with dust transactions.

There is a minimum to how much currency you can send, and there are sometimes higher fees for withdrawing early from these websites. Some faucet sites, may have high minimums before you can withdraw, some may be scams. Go to www.makingmoneyhoney.com for a large list of tested faucets.

As more cryptocurrencies gain momentum, you'll see more websites pop up. Do your research first. Always search a website address and/or name and the word "scam" or "scheme" and see if any results pop up. Since these websites are filled with ads, you must pay attention to what you're clicking, and make sure that you are on the website you started on, especially if you're

about to pay someone. Though faucets shouldn't be asking you to pay anything, if you stumble across any site asking for money, always research it first. Now there are Ponzi websites posing as faucets.

Ads are being designed specifically to look like they're part of the website these days to get more clicks, because that's how ads make money. These faucet websites wouldn't exist if they weren't making more money in profit than they're giving out.



Mining Cryptocurrencies

Is it Profitable? Mining Bitcoins is getting less and less profitable if you have to buy or rent the mining hardware and pay for the electricity and cooling. If you can get some hardware for free (through a contest or giveaway), using your own hardware (your GPU for scyrpt cryptocurrencies), or have a deal on electricity, those things will matter less. Mining Bitcoins is now taking a long time to become profitable, partly due to increasing difficulty, but also due to the price coming down, if you're thinking about the very long term, you may want to go ahead and buy a miner, but it is probably better to buy Bitcoins versus mining them right now. Your profitability depends on your individual costs and price flucuations, so there isn't a perfect calculator to figure out if it's worth it or not.

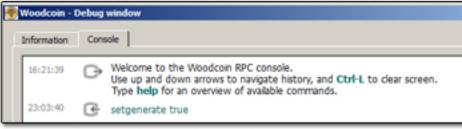
So mining Bitcoins may not be as profitable as it used to be, but you could mine other cryptocurrencies and then use those cryptocurrencies to buy Bitcoins. You may make more money doing that, because newer cryptocurrencies are easier to mine than those that have been around for years.

Downloading the software and setting it up

You can download mining software online and install it. Mining programs have let people use their Central Processing Unit (CPU) to do the mining, but that's already becoming obsolete for most coins. Some will use your Graphics Processing Unit (GPU) which is usually on your video card. Those extremely serious about mining are now using Application-specific integrated circuits (ASIC). When you download the mining software it may detect what you have installed/plugged in. You may need to tell it what you want to use.

As I said, CPU mining is pretty obsolete, however Woodcoin lets you use the wallet to mine with your CPU, it's still working just using a normal computer. You only need the wallet. You would then go to Help->Debug and type setgenerate true. Once you've done that, you can leave it running and you'll notice it uses the spare CPU if you check out Task

Manager.



Easy to Understand Guide to Cryptocurrencies

Malware Detection

Back when Bitcoin came out, hackers were able to mine on computers that weren't theirs. There were stores that had computers for sale, that while set up in the store on display, were mining (unbeknownst to the store) and sending those bitcoins back to the hackers. So, miner software got flagged as a hacking tool. Obviously mining isn't always hacking, so you will see false positives a lot of the time when dealing with mining programs, and wallets (that allow mining through them).

This actually makes people more vulnerable, because they may want to use a new miner program or update a previous version, and just assume it's a false positive if they get a warning. It's easier to infect people who click "ok" automatically. (More information in the section Protecting Yourself / Reducing Risk.)

Mining Pools

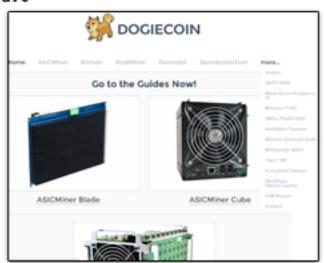
You can mine by yourself, but most people usually join mining pools. There are many to choose from. Each one has different pros and cons, and you will need to compare them based on what you want to get out of it, and how fast your computer can mine. Scan the OR code to visit a nice guide on choosing a mining pool. (https://bitcointalk.org/index.php?topic=51261.0)



Mining Hardware

There is a lot of miner hardware out there. Dogiecoin has a nice guide on setting up miner hardware.







Mining Software

Some wallets let you mine from them, others require you to download miner software. Which miner software you use, depends on what type of coin you are mining. Check out the website and/or forum for the coin you're interested in mining. Every cryptocurrency wants people mining their coin. Feel free to ask around in their forums for advice, that's what they're there for. There are also tutorial videos on Youtube, so if you have problems setting up a particular miner progam, search for it there.

Cloud Mining

A lot of ads are popping up for cloud mining. You give these cloud miners money to mine for you so you don't have to deal with buying the equipment, cooling them with fans, and general upkeep and hassle of Some have been confirmed scams, others are sketchy, please read this

post: Advice for new users regarding CLOUD MINING. Always research a website/service before paying them anything. (https://bitcointalk.org/index.php?topic=739510.0)

Working for Cryptocurrencies

One of the best ways for getting cryptocurrencies, without actually having to lay out money for it, is working for it. Right now many of the jobs people are willing to pay cryptocurrency for are small gigs. However, some of the ones listed online are full-time jobs. Some of the issues to think about when considering taking a job for cryptocurrency are: your government's rules on taxing cryptocurrency, and the fact that what you made one month, could be worth double that the next month, or half of it.

One thing a company hiring someone needs to consider is when they pay a salary with cryptocurrency one month, the same amount may be breaking the minimum wage law by paying too little if the exchange rate falls.

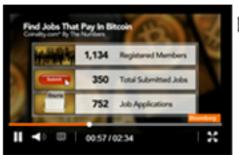
Cryptocurrency Job Boards

Coinality: "Coinality is a job board where employers and job seekers can connect for job opportunities that pay in digital currencies such as Bitcoin, Litecoin, and yes, even Dogecoin. Jobs range from one-time to full-time and negotiations are handled independently between the two parties."

Jobs4Bitcoins - reddit's job board webpage: "We provide you a place to offer your talents and skills in exchange for the fastest growing currency in the world."

Official Bitcoin Forum - Services Section: People post services they are offering, or services they are requesting. Always click their Trust link to check full Trust ratings when doing business with people there.

BitGigs.com - A Bitcoin Job Board



Interview with Dan Roseman founder of Coinality.com:



Gambling for Cryptocurrencies

The laws for gambling differ based on what country you're in and whether you're doing it in person, or online and the laws also change from time to time. Please read up on your laws before actually gambling.

That said, at this time, most countries refer to cryptocurrencies as a commodity and not a currency. Though, it can be argued if you can buy a cryptocurrency like Bitcoins for currency and can change it back, it's still gambling with currency. For now, it seems most, if not all, countries will find gambling with cryptocurrencies to be legal.

As for now, there are a lot of cryptocurrency gambling websites out there. People feel like it's safer to gamble with cryptocurrency, and it is. But gambling is still gambling, and you can win, but remember to never gamble more than you can afford to lose. Always research a website before sending them anything. Especially since it can be easy to make a site have high odds in their favor, or higher withdrawal minimum levels. Pay attention to look for "Provably Fair" games and keep a lookout for sites that require you to deposit a certain amount before being able to withdraw anything.

Some gambling sites have faucets, so you can gamble with free money, to test the site out beforehand. If you're really lucky, you can go from nothing to actually having some cryptocurrency. But as with all other faucet-websites, you need to look at the minimum payout.



Crypto Tipping

Have you ever wanted to reward someone online for a random kindness, some sort of service provided, or for any other reason...and it just wasn't feasible? With cryptocurrencies, "tipping" is quick and easy. In the past, any sort of monetary exchange between parties would have required sending funds through Western Union, PayPal, or some other venue, which would have required at least some sort of personal information exchange. When tipping with cryptocurrency, the anonymity of both parties is preserved, and little gifts of appreciation are easily and readily accomplished. There are little or no real fees involved when tipping, making it a more fiscally prudent transaction, as well.

You can now receive tips from anyone around the world without even having a wallet set up. In an effort to introduce random people to cryptocurrencies, people have been going around tipping them with cryptocurrencies. It's a great plan. If you were on reddit and someone tipped you with a dollar worth of Bitcoins, don't you think you'd look up more information about it? Learn how to either turn it into dollars, or try to get more Bitcoins to go with it?



- [-] AnalyzerX7 [S] 2 points 1 day ago
 Welcome to the changetip revolution bro! /u/changetip 150 Bits permalink save parent report give gold reply
 - ♠ [-] changetip 1 point 1 day ago*
 - The Bitcoin tip for 150 Bits (\$0.06) has been collected by MakingMoneyHoney. ChangeTip info | ChangeTip video | /r/Bitcoin permalink save parent report give gold reply

There are many ways to tip crypto these days. Changetip, as seen above is one. Blockchain.info lets you email Bitcoins to someone, Cryptiv lets you tip Bitcoins and Dogecoins. The Dogetipbot lets you tip or get tipped Dogecoins. And White Puma created apps to be used on Facebook, Instagram and more and lets you use 60+ different cryptocurrencies.

Check out makingmoneyhoney.com for a guide to tipping:

Receiving Sent Cryptocurrencies

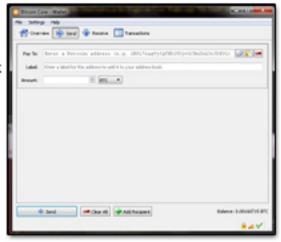
If you know someone with cryptocurrencies, and they just want to donate to you, or trade to you some cryptocurrencies for a product or service. They can pay you in multiple ways.

- Put your address on your website, send it in an email, send it in an IM, or write it down on a piece of paper. They can't take money from your address, they can only deposit onto it. Then they send a payment to that address.
- There are websites that will give you the html code to put buttons on your website for people to pay with Bitcoins. There may be more payment buttons in the future for other cryptocurrencies. You can also use the tipping systems.
- There are Bitcoin wallet apps for Android tablets/phones. The programs will create a QR code that can then be scanned by the other person.
- There are Bitcoin Cards the size and shape of a Credit Card, you can order, with the receiving wallet address printed on them, and a QR code for a smart phone to scan the address in.



Receiving Sent Cryptocurrencies (continued)

If the person sending has a Bitcoin Core Wallet on their computer, they can open it, click the send button, input your wallet number, how much they want to send and click the send button as seen below:



Though the Send button in the Dogecoin Core Wallet says "Plz Send", you can see it's more similar than different.



If the sender has a BlockChain.info Wallet, they can log in and click "Send Money" and they'll see a screen like the one below, where they can input the address to send to, input the

amount, and click "send payment".



Easy to Understand Guide to Cryptocurrencies

Recommendations

Strategies

Working for Bitcoin

If you want Bitcoin, check out the sites offering Bitcoins for jobs. Sometimes people will pay a little for something anyone can do. Most of the jobs are for computer programmers/software developers and website/graphic designers, but there are others if that's not your background. One job listing was for someone with a large online presence to live off of Bitcoin for a month and post about it, they got paid in Bitcoin so they could pay their rent, and food expenses, as long as they posted about it.

Altcoins

If you're new to the world of cryptocurrencies, you may be kicking yourself for not buying Bitcoins when they were 1/10th the price they are now. If you want to get in on the ground floor, keep your eye out for altcoins on the rise. coinmarketcap.com has hundreds of altcoins listed and displays the market capital of them.



Faucets

Start doing faucet offers. If you've got the time, and the energy, you can get free cryptocurrencies, though they may be small amounts, if the price of those currencies rises, you have pure profit. Some people argue that you'd get more if you just worked and bought cryptocurrencies for that money, since faucets are usually giving out payouts that only add up to a few cents after hours of doing them. If you can work for them, it's better, but if you are working and come home, what's it hurt to do a few faucets in your free time?

Faucets (continued)

In the begining there were faucets giving out .5 bitcoin back when they weren't worth much. People didn't think it was worth it to do faucets back then. But it would be great to get that many now a days. To compare:

Then	Now
About .5₿ per faucet collection	About 0.000003₿ per faucet collection

Now, you can get Altcoins for the same amount. The Altcoins may not turn out to be worth much right now, but what if they rise in the price the same way?

Check out MakingMoneyHoney.com for faucets that have been shown to work and some faucet rotators. A faucet rotator is a page that lets you hit the next button to hop from faucet to faucet, saving you time so you can hit a bunch of faucets quickly.

Mining

Mining is not what it used to be, but it might be profitable to mine newer altoins and sell them for Bitcoin. If you go to BitcoinTalk, you can look at the Altcoin announcement section, and look for coins you find interesting, check out the developer and stay on the look out for pump and dump coins, and avoid those. Many IPO and ICO coins seem to be Pump and Dump coins.

38

Ways to Diversify

Types of Coins

Diversify what type of coins you have. Why not keep an eye out to see if you can get some Altcoins for free. Such as the Doge Faucets on our faucet page?

Bitcoins	Others
About 0.000003 \$ per faucet collection	0.5 Woodcoin per hour 1 Frycoin per hour 8 DOGE per hour 50 HTML5 coins per hour 500 Bunnycoins per hour

Methods

Diversify your methods in getting cryptocurrencies. Don't just work for them, or don't just do faucets, why not both? You can also get altcoins and trade them for bitcoins too. The altcoins may be cheap one day and worth more the next, getting you more Bitcoins than your dollar would have.

Do you feel lucky? Try a few gambling games (with faucets) for free fun.

Check the Bitcoin forum section Games & Rounds for other contests and giveaways. And check the Altcoin section for giveaways concerning them. Check out Cryptoinfinity.com for games and giveaways to get free cryptos too!

Follow us on Twitter for links to contests or other giveaways as we learn of them.

Protecting Yourself/Reducing Risk

Multiple Username/Passwords

First off, if you sign up on a forum or wallet online, and pick a password, please don't use the same password on other forums, or to protect your various wallets. Even if the site's owner the most trusted person in the world, the site can be hacked by someone who is not. If you use the same username and password on a forum, and then on an on-line wallet, it's just like handing them the key to the lock on your Bitcoin safe.

Also when dealing with people on the official Bitcoin forum, always check all of their trust using the trust link. The trust system is weird and can show someone as having zero trust, but when you click the link they may have 10 negative trust ratings you just didn't see.

Escrow

Many people doing transactions with cryptocurrencies may offer or require an escrow since once the money is transferred, you can't do a refund like you can with credit cards.

Escrow: a contractual arrangement in which a third party receives and disburses money or documents for the primary transacting parties, with the disbursement dependent on conditions agreed to by the transacting parties.

You can look into respected Escrow services on the official Bitcoin forum or search online, but please do your research first whenever handing out money and always look up reviews for the person or group you're going to be dealing with, and keep an eye on the dates the information is from.

40

Escrow (continued)

How Escrow Works

1. Buyer & Seller Agree to Terms



2. Buyer Pays 1 \$\bar{B}\)
to Escrow Holder



Seller Sends Product or Provides Service



Seller will mail painting for 1 B

4. Buyer Aproves Transfer



5. Escrow Holder Pays Seller





6. If there's a Dispute, Escrow Holder Decides How to Solve the Issue.







If the seller doesn't send the product or perform the service, the escrow holder can refund the money back to the buyer.

Protecting Your Wallets

Wallet Addresses

When you create a wallet address it is unique. However, there was a security breach with CounterParty (another cryptocurrency) in which private keys were leaked for public addresses, giving others a chance to spend Bitcoins from unsuspecting users' wallets. It only happened for those using the CounterParty wallet, in April of 2014. There was a list of affected addresses posted online. Though, this was a limited issue, if you want to feel safe, when you create an address, before sending funds to that address, search for it on the internet. If it comes up with zero results, you should be good.

Online Wallets

You can store some money in an online wallet, but you would be placing your trust in the website you're using. They may be hacked and you could lose everything there. Check out LastPass for a password protection program.



Also, if you are going to have an online wallet, look for one with 2 step verification. When you create the account, you will add your cell phone to it (or some other second form of ID checking), so that when you go to make a payment, it will confirm by sending a code to your cell phone to put into the site. It may feel annoying when you're doing it, but if a hacker were to gain access to your account with your user ID and password, then try to send money from it, you'll be immediately notified on your cell phone, since you'll see the code, and they shouldn't be able to send the money.

There are some sayings about this: "If you don't have access to your own private keys, it's not a wallet. It's a bank," or "if you don't own the private keys to your bitcoins you don't own your bitcoins."

Online Wallet Scam

Since BlockChain.info is a well known on-line wallet, someone decided to go phishing (making a website similar to a well known site and asking targets to sign-in, while taking unsuspecting user ID and passwords to withdraw their funds). The scam was an email from no-reply@blokchains.info (which is misspelled, block is missing a 'c' and chain has an 's') that said you just received "\$2,031.88" (it's for an online Bitcoin wallet, you would be receiving Bitcoins not dollars), and for a transfer of \$2,031.88, the fee was listed as \$34.56, (and we hope by now you know that's a joke, one of the best things about Bitcoin is the low fees). And lastly, the last line of the email said, "If within 48 hours we do not receive your confirmation, your wallet will be erased and all their bitcoins will be reset." (they could never reset your balance, your balance is yours forever, the way people lose access to their money is due to losing the private key to spend their balance, but the balance is still there.)

If you're going to use an online wallet, research it first. It's best if you have your money spread around, and some saved elsewhere. I would suggest having the large portion of your currency in your hands, a safe or safety deposit box using a paper wallet or hardware wallet.

Even if you stay away from scams, mistakes can still happen: Here is a post describing how someone lost 15 BTC due to a mistake from BlockChain.info.

"recently I was using blockchain.info wallet and made two new addresses. I sent a small amount of BTC to one of the new addresses as a test and showed up fine in my wallet balance. So then sent the rest of the 15 BTC to the address. Again, it showed in my balance. So I log out and log back in an hour later and my BTC is gone and so is that address. I emailed customer service and they said the wallet didn't 'sync' properly to their site from my browser or something like that. Basically, they didn't save the private key for that address, so my BTC is still sitting in that address, but the private key for it does not exist...They basically said 'tough luck' and would not reimburse me or do anything to help." - thecosmicl on reddit.com Dec '14



Hard drive Wallet

If you store your wallet on your computer, don't back it up, and your computer crashes, you can lose everything. You aren't technically storing the cryptocurrencies somewhere on the computer, what you're storing is the private key, used to access your bitcoin address and it's transactions, so that you have access to spend the bitcoins your address has acquired. To back up your computer's wallet, save your wallet.dat file somewhere else. You should also encrypt your wallet with a strong password. Better passwords include symbols, capital and lowercase letters, and longer versus shorter ones. The most secure password, if it's not memorable and has to be written down, is still worse than a less secure password,

if someone can walk in and find it written down. Think of something you can use symbols in place of a letter or two. #ell0 could be Hello in your mind, but with the pound symbol and zero replacing letters. Obviously use something longer and less guessable.

If your wallet is saved on your computer, there are

plenty of things that can go wrong. Keep your computer safe from viruses and keyloggers and don't download or run executable files from unknown sources onto a computer you have your wallet on (this includes new Altcoin wallets). Always research new Altcoins, and pay attention to find the official websites for a coin. Some people will quote the developer of a coin, and change the links (like we discussed on the phishing page) to another link. The link looks the same, but if you hover your mouse over it, it shows it goes to a different location. Also, if you know how, you can use a Virtual OS to run a program to check what it does without it affecting your main OS.

Ceron

It is also advisable to use a second computer for faucet offers, downloads, etc. Recently someone posted on the Official Bitcoin Forum, about a new way to make money, with a link, someone downloaded it, ran it and lost their money. It got deleted quickly, but it's that easy to lose everything. If an offer looks too good to be true, it is. Always research first, and never download anything new onto a computer with a wallet (this includes online wallets, as your user name and password may be saved on your computer), unless you know for certain that you can trust it.

If you don't want to deal with worrying about everything you download or do on your computer, look into cold storage such as hardware wallets or paper wallets.

Hardware Wallets

The best thing to do if you have a large amount of bitcoins (that you aren't going to need to access often) is to save them on a "cold" wallet, one that doesn't connect to the internet, that isn't touched, and is stored away in a safe. You can leave a small amount of Bitcoins in a "hot" wallet so that you can send and receive money when you need to, but if your phone or computer is lost, you won't lose your whole fortune (if you've saved some on a cold wallet). It's just like what people do with cash. Put a few small bills in their wallet, and the large amount of cash they have in a bank's safe somewhere.



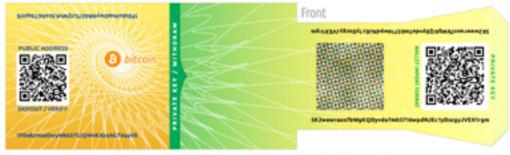


Hardware Wallet

Paper Wallet

Paper Wallets

You can print out paper wallets, which is a piece of paper with a code for receiving currency and another code for spending it. There are a few things are really important when dealing with paper wallets. To send money you need your private key + your public key together they allow you to spend your money. So people fold the paper wallets or have a covering of some sort for the private key. If anyone got a hold of the private key they would have access to your current funds and all of your future funds too.



Easy to Understand Guide to Cryptocurrencies

Paper Wallets (continued)

You can use websites that exist for creating a paper wallet. But there are things to remember. You shouldn't let anyone watch you create the wallet. To be further protected, if there's a chance your computer has been compromised with spyware monitoring your activity, you should use a clean operating system. That way, when you create the wallet, you can be sure what's you're seeing and inputting isn't being seen by someone else.

Also, when you're ready to create the wallet, you should take the computer offline before going ahead and doing it. The printer can have a shadow of the wallet in it's memory after printing the wallet, so make sure it's not connected to a network.

When attempting to create a paper wallet, please find explicit directions, research the websites, and follow each step diligently. Like I said earlier, if anyone gets ahold of your private key they have access to that wallet forever.

Another consideration: paper and ink could degrade over time, and it's incredibly vulnerable to water and fire, and of course, if you lose it, it's gone forever. To take care of your paper wallet, protect it from water, laminate it (if it isn't folded to cover the private code), or place in a sealed plastic bag. Put it in a bank, or a safety deposit box. You can also make a duplicate and place it in multiple safe locations.

At this point, there may be certain altooins that don't have a website to make a paper wallet, but you can research it, and I'm sure as the new currencies take off, more and more programs and/or instructions will come to be in existence. This comes with a warning: There is a chance a theif may come along with a online paper wallet generator and have built-in access to those private keys made with it. This is why you must research a site first.

Always use the feature to decrypt your private key and make sure it matches the public key.

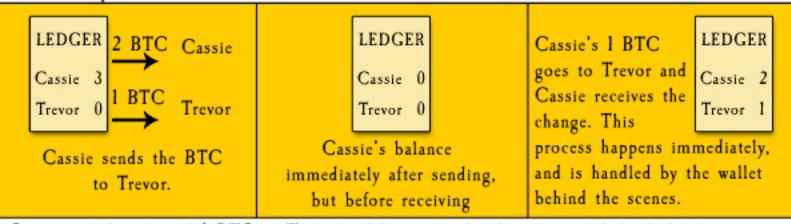


Easy to Understand Guide to Cryptocurrencies

Paper Wallets (continued)

When you go to spend your funds from a paper wallet (or Brain Wallet), remember to account for making a change transaction, since when you send the transaction, you're sending all of it, the first amount that you're sending to someone else, and the change (minus the transaction fee) should be sent back to yourself. A common mistake when importing a private key into a temporary Bitcoin wallet, is making a transaction and then deleting the temporary wallet.

Example: Cassie has 3 BTC, & sends 1 BTC to Trevor, and 2 BTC back to herself



Cassie would just send 1 BTC to Trevor and her wallet handles the rest behind the scenes.

The process of taking the funds off of a paper wallet, is referred to as "Sweeping" it. You can sweep with a cellphone or tablet wallet, an online wallet, or a harddrive wallet. The proceess is a little different for each. Cellphone and tablet wallets usually have an option to scan a QR code on the paper wallet, making it the easiest.

Once you sweep your paper wallet clean of all funds, you can throw it away, and spend your funds from the wallet where you've just swept the funds. Because you're taking the whole balance, you don't want someone else to sweep your wallet as payment, unless you want them to have the whole balance.

Usually paper wallets are kept for larger amounts of BTC, so you would sweep the paper wallet with your new wallet, and then pay someone from your new wallet,. This way your change can come back to the new wallet.

(hoose a Community

Online Communities

There are lots of online communities/forums to join to ask specific questions, read to become more knowledgeable, hang out with people are are interested in the same thing you are, and learn more about new cryptocurrencies.

bitcointalk.org

Bitcointalk - The official Bitcoin forum, with a specific section for discussing altcoins.

Cryptoinfinity - A forum, with a chatbox built-in, about c ryptocurrencies with games, contests, and other giveaways for forum participants.

Reddit also has multiple subforums devoted to Bitcoin, Dogecoin, etc.

Check out www.MakingMoneyHoney.com for more.

Real Life Communities

Meetup.com is a website that lets groups find each other online and to meet in person. When you go to the Bitcoin section of the website, you can type in your zip code and find any meetups of others interested in Bitcoins that are happening near you.





BECOME a Community





Tell your family, tell your friends, tell your co-workers, tell people you meet about cryptocurrencies! Feel free to print this guide out, tweet about the webpage, or click the facebook share button on the site with people you meet, who might be interested but don't know where to start, or don't know what it's all about yet.



Tweet people



Tell people you know on facebook.



Text or call your friends



Write a note to someone



Print out the guide



Share the guide with people

You can also get some cryptocurrencies and start tipping people online to get the word out!

Pay It Forward

If you found this to be easy to understand and helpful, think about donating a bit, any little bit. Donations will help to keep the site going, which I hope will serve to be a warm welcoming to newcomers to the brand new world of digital currencies.

Feel free to donate to:

Bitcoin Address: IM6ELX8clg95ApJzcYCsGGipsAeYf7RvWN

Litecoin Address: LcNQ3pbaAnfjVkdTHoELDZBSFcT7CvymeH

Dogecoin Address: DDbHgSdCjHmHFsFtLhZptjrtRBAd4cCoxW







If you had a wallet you could have donated by now. Imagine how much easier it would be to just scan a code, type in an amount, and pay for things this quickly!

Thank You

Thank you Satoshi Nakamoto, for creating Bitcoin and the blockchain technology.

Thank you to Bitcointalk.org, for having the old posts of when 10,000 Bitcoins were too expensive at \$25, and for the guides on cloudmining, and mining pools, and more.

Thank you Cryptoinfinity, for providing a nice, welcoming forum where people can get their first cryptocurrencies for free or just playing games.

Thanks also to all the businesses out there accepting Bitcoin as payment.

Alpacas are a mascot of sorts for Bitcoin. When Bitcoin was created, one of the first products made available to Bitcoin purchasers were Alpaca Wool Socks from Grass Hill Alpacas run by the Forster family.



Easy to Understand Guide to Cryptocurrencies

Addendum

Creating a Paper Wallet

If you want to create a paper wallet, you can use bitcoinpaperwallet.com or bitaddress.org on an offline (ethernet unplugged and wifi turned off) computer, in a clean Operating System (such as Ubuntu, a free OS, on a flash drive or CD). But what if those sites got hacked or were taken down? If you're absolutely paranoid, you can create your paper wallet yourself.

Creating Private Keys with Dice

A pair of 16-sided hexadecimal dice is a great way to secure random numbers for an address, but there is a way to use normal 6-sided dice too. You can roll the 16-sided dice pair 32 times to get a 64 alpha-numeric number. If you use a normal 6-sided dice you would roll 100 times.

Finding the Public Address from a Private Key

Run Ubuntu live (no need to install it) from a CD or flash drive. Make sure it's not connected to the internet, as long as it isn't installed it won't leave a trace on your computer. Uncheck "Enable Networking" once inside.









16-sided hexadecimal dice

Finding the Public Address from a Private Key (continued)

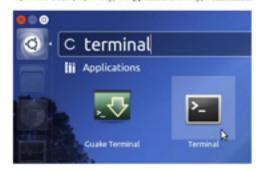
Start the terminal program. Type the following command: source ~/bitcoin.sh

Now, use the script you have just loaded to find the public address for the private key:

newBitcoinKey 0x(your dice digits)

How do I open a terminal:

. Open the Dash (Super Key) or Applications and type terminal



. Use the keyboard shortcut by pressing Con + At + T.

ubuntu@ubuntu:~\$ source ~/bitcoin.sh

ubuntu@ubuntu:~\$ newBitcoinKey 0x8010b1bb119ad37d4b65a1022a314897b1b3614b345974332cb1b9582cf03536

secret exponent: 0x8010B1BB119AD37D4B65A1022A314897B1B3614B345974332CB1B9582CF03536

public key:

X: 09BA8621AEFD3B6BA4CA6D11A4746E8DF8D35D9B51B383338F627BA7FC732731
Y: 8C3A6EC6ACD33C36328B8FB4349B31671BCD3A192316EA4F6236EE1AE4A7D8C9

compressed:

WIF: L1WepftUBemj6H4XQovkiWlARVjxMqaw4oj2kmkYqdG1xTnBcHfC

1HV3WWx56qD6U5yWYZoLc7WbJPV3zAL6Hi

uncompressed:

WIF: 5JngqQmHagNTknnCshzVUysLMWAjT23FWs1TgNU5wyFH5SB3hrP

bitcoin address: 113Pfw4sFqN1T5kXUnKbgZHMJHN9ovjtqD

ubuntu@ubuntu:~\$

bitcoin address:

If you used 6-sided dice, download the dice2key script from https://github.com/swansontec/dice2key onto the Live Ubuntu OS.



Type the following:

source dice2key (100 six-sided dice rolls)

Which will result in a 64-digit hexadecimal number that you can use above to get the public key.

Now you know the private key, and it's never been online or been saved to your computer, and you can give out the public key freely to accept funds.