What is a bitcoin?

Extremely short answer: a bitcoin is both a cryptographic currency and a tool to conduct financial transactions online.

Bitcoins can be traded easily between users and its value is determined solely by its supply and demand (not unlike traditional currencies), as reflected on bitcoin exchanges like Mt Gox where you can trade bitcoins against euro's, dollars etc.

Bitcoins have a limited and predictable supply; there will never be more than 21 million bitcoins. Bitcoins only exist in a peer to peer network; they dont have physical equivalent and there is no company or organization behind it. The algorithms and software are opensource and can be reviewed by anyone.

It was launched as a small scale experiment some 2,5 years ago, but has so far proven to work so well thats its gained much wider spread adoption than initially intended.

How many bitcoins are there and who makes them?

You! And me. And everyone “mining” bitcoins. There is no central authority governing bitcoins, nor is there an entity to create them. Its a peer to peer network and the coins only exist in this network. Coins are created through a very compute intensive process called mining at a predictable and decreasing rate of currently 1 block of 50 coins per 10 minutes.. The difficulty of mining coins is adjusted automatically by the network to maintain this predefined rate, no matter if there is just 1 miner with a slow PC or 1 billion miners with supercomputers. The total amount of bitcoins in circulation will level off just below 21 million coins in the year 2020.

The entire bitcoin money supply is currently worth less than $50M. In the grand scheme of things, that is stil peanuts. The combined value of bitcoin transactions is more impressive and rivals what paypal achieved in 2008, but for now, most of that value is probably short term speculation and not commerce in the narrower sense of the word, as the number of real world goods and services you can buy with bitcoins is still very limited.

Are bitcoins really worth anything?

Bitcoins have no intrinsic value, just like paper money, it derives its value from its use as a transaction tool and from speculation. To conduct btc transactions, you need bitcoins, and this creates a demand that is fulfilled by mining (see below) or through trade . You can see the current value of bitcoins measured against dollars/euro’s/pounds for instance here: http://bitcoincharts.com/markets/

Those are not hypothetical values, those are exchanges so those are prices people are actually

bidding for them. IOW, its what they are worth today. “What the fool is willing to pay”.

What does this mining app do; what is bitcoin mining and whats a pool?

By running a miner application like the (BFs) BitMinter application, your GPU is used for a mathematical/cryptographic function called hashing which forms the basis of bitcoin security. This process, called “mining”, secures bitcoin transactions and actually produces the bitcoins; although at a very slow rate.

Bitcoins are found in blocks of 50 coins (worth ~$150 now), but the probability of finding a block is -obviously- very low and decreasing with time. Currently an individual could mine for months or even years before finding a single block of 50 coins. Therefore most miners gather their resources in a mining pool; they split the work and distribute the profits according to the number of hashes performed by each member. This results in a more steady and predictable flow of bitcoins for individual miners. The bigger the pool; the more predictable the revenue.

Bitminter is a relatively new and small pool, at the moment on average it will find a block every ~1 day or so; but it can take as little as a few hours or as much a week. So dont panic if you mined all night and didnt receive any payment yet.

Great; but why would I join, and exactly how do I or how does Battle-fields.com benefit from all this?

First of all, understand that mining actually provides bitcoins (or bit cents). So long as bitcoins are used and in demand, people (even if you think they are fools) will pay for them in Euro’s or dollars or whatever. So running a bitcoin miner really provides actual money. Assuming you have the hardware in place, this requires no investment, involves no risk. This isnt some “work at home” or “get rich surfing” scam. it works (Im doing it), its all math and economics. No matter what you think about bitcoins or its future, the profits arent spectacular (see below) but at least for now, they are real, even taking electricity cost in to account.

So if you want to help BFs, one way of doing it is by putting your videocard at work by using the upcoming BFs BitMinter application. A percentage of the proceeds paid by the pool, is sent to Boneheads bitcoin wallet. Details are being worked on; but you will likely be free to select a donation ratio as you like between your own wallet and BFs'.

Until (but also after) the release of that miner app, you can use the regular BitMinter app or any other BTC miner application, and join a pool of your choosing (I would suggest BitMinter at this point, for their bounties and easy to use custom miner app) and voluntarily donate however much you want to Bonehead's wallet manually.

Other popular miner apps are GUIminer and Diablo, the largest mining pools are ABCPool, Slush and Deepbit.

How much does this mining earn me or BFs in real money?

Its variable; if we exclude electricity cost for now, then it depends on 3 parameters. First; how many hashes/second your videocard can process. ATI videocards are much better suited at this than nVidia cards. CPU's are essentially useless (roughly 50x to 200x slower than an ATI card)..

A second parameter is the difficulty level of the blocks. This difficulty level is in itself variable, its automatically adjusted by the network to maintain a predefined growth rate. The more people mine, the harder it will become to find something and the less you will earn. And vice versa.

The third parameter is the value of bitcoins, which is very volatile. It has been as high as $30 in june and as low as $0.1 last year. A bitcoin trades for around $3 at the time of writing but who knows what it is when you read this.

As for the mining revenue, to give you an idea; with an ATI 5850 you can process roughly 300 million hashes per second. Running 24/7 this will net you on average ~5.2 BTC per month with the current difficulty.

Mind you, electricity costs are not taken into account here, but they are real so be sure to do that math as well before you get too excited. In winter you could subtract some of the electricity cost because you also get the heating, in summer you might have to add airconditioning cost.

To get an idea of the hashrate your videocard(s) can achieve, look here:
https://en.bitcoin.it/wiki/Mining_hardware_comparison

Then you can do your own math here:
http://www.alloscomp.com/bitcoin/calculator.php

And find out how much you could donate to BFs by just running an app. Really.

Isnt this a bubble? Who says it a bitcoin will be worth anything next year?

No one knows that for sure. It doesnt seem likely that bitcoins will become worth nothing, but for sure their value could either explode or implode due to short term speculation or depending on its growing (or lacking) popularity as a transaction tool.

Bitcoin value has already had significant ups and downs, and as a new currency and new technology its extremely likely it will continue to suffer from bubbles and bursts for quite some time; particularly since most of the transactions today are still short term speculation and most people struggle to assess its long term value. The price will hopefully stabilize (or grow steadily) if bitcoins are used more as a transaction tool and less as a short term investment tool and

when bitcoin future markets develop to hedge against large price swings.

Its important to note however, that **the value of bitcoins is not important** for its usefulness as a transaction tool. Even if bitcoins at some point are worth just $0.00001, that doesnt make it any less useful to make payments. Their exchange rate with regular currencies is arbitrary, its not harder to send 0.00001 BTC as it is to send 1.000.000 BTC. Only the volatility is a bit of a problem, particularly for a merchant accepting or pricing in bitcoins.

Will mining always be profitable?

No. The value of a bitcoin has a big impact on the profitability of mining. Obviously if bitcoins are worth more or less, the immediate result is that mining appears to become proportionally more or less profitable. But its not quite that simple, the difficulty level will catch up with the bitcoin value. If bitcoin price would collapse, fewer people will find it worthwhile to mine, and as a result the difficulty will become lower, so whoever is still mining will make more bitcoins which compensates for the lower price. And vice versa, if BTC price spikes, there will likely be a rush to make easy money through mining and the difficulty will go up. This is precisely what happened in may/june.

The net result is that the profitability of mining simply follows market rules, there will be times when its lucrative there will be times its make no financial sense to mine if you factor in electricity cost. This is not directly related to how much a bitcoin is worth; its possible mining is profitable even if a bitcoin is worth just $0.01 but its equally possible at some time, $50 or $500 per BTC is still not worth it (*). Note that this is in general terms, but individually you might have a “competitive edge” over other miners, for instance because you have cheaper electricity, or you dont have to take into account the cost of hardware because you already own it anyway for gaming or your machine is already running 24/7 for other purposes so you dont have to take the entire rig’s powerconsumption in to account, only the extra load.

(*) That said, If bitcoin’s value would ever explode like that (or bubble however you want to look at it), there is likely a big window of opportunity to make money because its unlikely mining capacity would be able to keep pace. Its easy to shut down a mining machine thats losing money, but it takes time for people to bring them online and there are only so many ATI videocard owners.

What can Bonehead, or you or me do with those bitcoins? Isnt it like monopoly money and essentially worthless?

Unlike monopoly money; you can trade bitcoins for euro's, dollars or pounds. You can also use it as a cheap and convenient way to conduct small transactions between individuals or for donations (like charities), bets, online poker. You can purchase real goods and services, but the number of commercial merchants accepting them is still (very) limited for now. Many freelancers do accept them though, particularly for IT jobs. My personal favorite way to spend them is

online poker, but see here for a list of alternatives ranging from food to VPS server hosting:

Since I assume Bonehead needs to pay his bills in pounds, the logical thing for him to do is convert his BTCs to pounds, but thats up to him obviously.

Whats the advantage, besides mining for profit or speculating, why would I actually want to use Bitcoins to pay for stuff? I already got Paypal and a letterbox full of credit cards.

Bitcoin serves two purposes; its both a currency and a transaction tool. Lets differentiate between them. There are a few advantages to using bitcoins as a transaction tool; the first is that its cheap. Much cheaper than paypal or credit card transactions. The cost of transactions varies with time and you can chose how much you want to pay for a transaction in fees: paying more guarantees faster processing. Typical cost atm is 0.002BTC, which is less than $0.01 per transaction regardless of the amount. This fee will typically result in your transaction being confirmed in a few hours.

A second advantage is that its simple to use. There is no sign up procedure, no need for a credit card or even bank account. Sending or receiving BTCs is literally just a mouseclick. Its really that easy. Particularly for mobile phones I think this has potential to become very popular; you can scan a QR code and send money with the touch of your finger, even ridiculously small amounts.

A third advantage is that its extremely safe as transaction tool, although one has to realize its far less safe as a way to store wealth; see below for more details on safety of either aspect.

Finally, using bitcoins offers fairly good protection of privacy. You may not want all your online transactions to be known by your credit card company or show up on your monthly VISA statements. Or you may not like Paypal or Mastercard deciding for you what you may spend your money on (eg wikileaks donations). You may not like them canceling your cards or freezing your accounts for whatever reason. You might want to sell something online without risking the buyer initiating a chargeback 6 months after the deal, and you losing your money. You may want to donate some money without revealing your identity. For all those cases, Bitcoin offers an alternative as transaction tool.

As a currency, Bitcoin has some interesting properties that one may consider advantages or fatal flaws depending on one's political and economic beliefs; there is no central authority that can issue coins or inflate or deflate its value or manipulate interest rates. There is no central bank or federal reserve; there arent even trustworthy banks at this point. The supply is inherently limited, much like gold, though unlike gold, bitcoin has no industrial or other uses, so demand for it is solely generated by demand for it as a currency or for speculation. Whether those are all good or bad properties, will depend entirely on your economic views. If you are a Keynesian, you will think its a stupid idea that a government can not influence the money supply to adapt to changing economic realities. If you are a “goldbug”, a libertarian or believer in

Austrian school of economics, you may find most of these aspects brilliant.

Either way, whatever your thoughts, bitcoins are so insignificant today that their impact on the world economy is nil. Discussing monetary theories might be interesting but whether its good or bad; in reality I suspect the money hoarding effects of BTC as a deflationary currency on our world economy are less than the impact of speculation on Marklin trains or Smurf comics - at least for now, its irrelevant, and very likely to remain so. If not, if BTC would become so widely used that it would impact worldwide monetary policies, then our mining will make us all dollar millionaires and Bonehead probably able to buy Amazon.com with our BTC donations. Who is going to care about Krugmans opinion on monetary policy then :).

FWIW, and in case you couldnt tell; personally Im on the fence about BTCs quality as a currency, but I dont care a lot since it doesnt matter, but Im completely convinced of its value as a trade tool.

How are bitcoins different from E-gold or other (failed) electronic money schemes?

There are many differences, but perhaps the most fundamental difference is that bitcoins do not rely on a central authority. There is no company or organization behind bitcoins that can go bankrupt or be forced closed and take the currency with it, as happened with E-gold and many others; In fact, there are no claims that bitcoins are backed by oil, gold or silver, or even money so the system can not become insolvent and there can be no surprises or price collapses when it turns out those claimed reserves in money or gold arent there (anymore or never were).

The lack of a central authority also protects you from value risks compared to otherwise somewhat similar alternative electronic “currencies” backed by nothing, like Microsoft points for xbox or WoW gold. No one can decide to print more, freeze your account, change policies or abolish them.

Is it not a Ponzi scheme?

No. Bitcoins dont promise you a return on investment. There is no interest payment. Unlike pyramid or ponzi schemes, there is no need for exponential growth to keep the system solvent and pay non existent profits to new entries - note that our traditional fiat money supply does require global exponential (economic) growth to maintain its solvency, and as such its arguably more of a pyramid scheme than bitcoin.

It is true though that early adopters made lots of money (assuming they cashed in, I have no idea if they did), but that doesnt make it a Ponzi scheme. Early adopters of Apple shares also made a lot of money by risking some money early on. (Thats not to say I predict bitcoins will skyrocket like Apple shares, thats anyone's guess.)

Okay so maybe its not a Ponzi scheme, but how do you know its not a scam or a bubble?

A bubble, just like any traded commodity, it could be. In fact the current price probably is, as its far more a result of speculation based on expectations of future value than current demand for bitcoins for trade. Whether those expectations are warranted is anyone's guess but its safe to say those expectations will go up and down in the future.

But for it to be a scam, someone must be misleading you. Bitcoin is if anything, extremely transparent, with each node having ALL the information of the entire bitcoin monetary system; compare that to your local currency. You probably cant even find out how much of it there really is in circulation. The protocol and the code itself is all opensource, its kinda hard to mislead you with that.

Now if someone tells you a bitcoin investment will guarantee doubling or ten folding your investment in a year; then that person is a scammer. But bitcoin is not.

Is this legal?

AFAIK its untested in court; but from what I understand, almost certainly yes, just about everywhere. However bitcoins are not legal tender anywhere. Using and accepting bitcoins is voluntarily you can not legally enforce settlement of debt with it. So you can not pay your utility bill with bitcoins and demand your utility company to accept that as payment. You cant do that with gold either, or even foreign currencies. Only with legal tender.

Isnt this just used for money laundering or buying illegal drugs?

It can be, and frankly it is used for both. Also for porn and gambling (perhaps even to finance terrorism as some criticizers claim; although I kind of doubt that personally, I cant rule it out). But the same arguments can be made against gold or cash thats used for those purposes as well; Ive yet to hear a drug dealer accepting credit cards and I dont think Al Quada has a paypal address. Just like cash (or gold), its true Bitcoin has some properties that at least make it appear (perhaps wrongly) interesting for such illegal activities, but those very same properties make it attractive for perfectly legal transactions as well. Criminals tend to be early adopters of new technology, but its not because drug dealers use cellphones or Al Quada uses Skype or cash money transfers that those technologies are evil and should be avoided.

I read bitcoins are used for botnets and malware

You read the exact opposite; botnets are used to mine bitcoins and malware is increasingly targetting bitcoin wallets. The latter is no different than malware targetting your paypal or bank account and since there is money to be made from mining (particularly if you dont have to pay the electricity bill) it was predictable cybercriminals would put their botnets at work for mining bticoins. Its probably more lucrative for them than sending spam or DDoS attacks. All that this

proves is that criminals are quick to embrace new technology and see the opportunities they offer.

Isnt this easy to hack or counterfeit? Surely some clever hacker can exploit this?

No, in fact, its virtually impossible today, and if bitcoins become more popular, the risk of fraud will further decrease as the difficulty increases proportionally. Every transaction, including the creation of a coin, involves sending a timestamped broadcast message to the entire bitcoin network, so every user knows that the transaction happened and every node can verify the transaction is legit and the coin has not been spent twice by the same owner. You get such confirmations from miners, who get a tiny (user selectable) share of the transaction as their reward (typically today its 0.002 BC which is ~$0.01 per transaction).

This also means that every node has a complete history of all transactions ever committed, as a chain of events where each event is linked through cryptography to the previous. This makes tampering virtually impossible. Since the cryptographic linking of these events is deliberately made compute intensive, the only way to break this chain of trust, is by having more compute power than the entire bitcoin network.

Wait, so every bitcoin user has a complete history of every bitcoin transaction? Dude, hows that for privacy?

Yes, every node currently has a complete database of all transactions since the creation of the very first bitcoin. This will likely change in the future as the database will grow too big (its already sizable at ~600MB), and some hierarchical or segmented system will be developed, but its true for now, and even if the clients change this, the entire database will always be public in some way or form.

As for privacy, while the transactions are (extremely) public, the ownership of the bitcoin wallets is anything but. Its very difficult to identify the owner of a bitcoin wallet and its trivial to create as many wallets as you want. There is no sign up process involved: you just create one and it comes in to existence when you conduct a transaction with it. You could even create a new wallet for every individual transaction.

The topic of anonymity is heavily debated among the community, and from what I gather, its possible to trace transactions to an IP address, so eg for law enforcement purposes, bitcoin anonymity may not be total, but its pretty private nonetheless.

In simple terms, its more private than traditional banking, but potentially less private than cash transactions.

Is using this bitminter client application safe?

I think so. But unlike most miner apps, BitMinter not opensource, so I can not know for sure. Please note BitMinter is just one of many bitcoin mining apps. I have many reasons to believe the app is completely safe, but you dont have to believe that. If you have any doubts, you can use a different, opensource miner app like cgminer, GUIminer or diablo. These apps are generally slightly harder to configure but can achieve the exact same thing if configured right, provide similar performance and since the source code is available, you can be completely sure its not doing something behind your back.

Is bitcoin safe?

Yes its extremely secure, and no, not at all. It depends why you ask.
Its important to again distinguish two functions of bitcoin: as a way to conduct transactions, and as a storage of wealth.

As a way to conduct transactions, arguably, bitcoin is today the safest way known to man. Depending if you look at it as a seller or buyer, its safer than banking, paypal, credit card or cash transactions. The encryption used in bitcoin exceeds that of all banks and paypal. The difficulty in creating fraudulent transactions is simply monumental; because of the way it works, successfully forging a fake bitcoin transaction or creating counterfeit money or double spending requires more processing power than the entire bitcoin network combined. That makes hacking banks, printing fake $100 bills or counterfeit credit cards look ridiculously easy by comparison. Transactions are also irreversible, making them safer to use for merchants (no 6 months charge back like paypal), though arguably less safe for consumers. In that sense, its once again, just like cash transactions, just with virtually no chance of ever getting counterfeit money.

Bitcoins as a way for storing wealth is infinitely less secure, for several reasons. First, a great concern for bitcoin as a storage of wealth is the volatility of its value. Traditional currencies fluctuate a bit, but tend to be fairly stable and there is a small predictable loss of value with time. At this stage, there is no way to predict what a bitcoins will be worth in 5 months, let alone, 5 years. Anything from almost zero to 1000x more than today is plausible. That makes it useless as storage of wealth; currently owning large amounts of bitcoins is speculative by definition.

As mentioned elsewhere; its important to note however, that the value of bitcoins is not important for its usefulness as a transaction tool. Even if bitcoins at some point are worth just $0.00001, that doesnt make it any less useful to make payments. All the benefits of bitcoin as a transaction tool remain. The price level itself is arbitrary and utterly unimportant for conducting transactions. Even more so as there is no atomic unit, ie, unlike traditional currencies, there is no limit on how divisible it is. You can not trade less than 1 dollar cent, but bitcoin has no such limit (current clients are “limited” to 0.000000001, but even that can be modified if ever the need arises).

A second reason why bitcoins arent great for storing wealth, is the risk of losing them. Lets again think of it as cash. If you store your wealth in cash that you keep in the house, you will

lose that wealth if your house burns down or a thief steals it. Its all too easy to lose cash and depending how prepared you are, its potentially just as easy, if not easier, to lose bitcoins; if you lose your wallet file because you lose your PC, disk crash or your house burns down; your bitcoins will be gone too. If a hacker takes control of your PC; all he needs is a file, the so called bitcoin wallet file, and if he obtains that file, he owns your money and there is no recourse. Its not like your bank account that gets hacked and you can prove it to your bank and get most of your money back, its like a shoebox full of cash that a thief stole from your house. Its gone. For good.

Now if you have a non trivial amount of bitcoins, you can mitigate this risk in several ways. Some say you should use an online bitcoin bank, but at this point, I would **strongly** advice against that. None of them are proven to be trustworthy, none of them are regulated or audited. Any 12 year old script kiddy can start a “bitcoin bank” and run off with your money one day. Dont do it. Perhaps one day trustworthy organizations will offer bitcoin banking services, but today its like entrusting all your cash to a random stranger knocking on your door and offering to store your money for you.

There is a better, albeit somewhat cumbersome solution by storing the bulk of your bitcoins (assuming you have non trivial amounts of bitcoins) in a separate bitcoin wallet, that you encrypt with rigorous encryption, like TrueCrypt with a strong password. To prevent loss of the file (which also means loss of your money, again, just like cash) due to theft of your pc, hdd crash, fire or whatever, send copies of the encrypted file to friends, online storage, gmail, make copies on various PCs, CDs, USB sticks etc.

At some point in the future, perhaps trusted bitcoin service providers will emerge to do this for you, but as of now, I suggest you do some research before committing any significant amount of money.

You say its safe, yet wasnt it hacked a few months ago?

A few months ago, the largest bitcoin exchange (Mt Gox) was indeed hacked. This was not an attack on the currency or network itself, but purely on the exchange, where hackers attempted to profit by manipulating the exchange rates; and succeeded only in a very limited way. To be clear, today Mt Gox is by far the largest BTC exchange, so this was a big event for bitcoin, but you could compare it to someone hacking NYSE or Nasdaq: it would cause shockwaves in the financial industry but it wouldnt undermine the fundamental value of shares you would own in companies listed on Nasdaq..

Isnt this mining business a huge waste of electrical power?

It is indeed (IMO unfortunately) power consuming, but its not wasted; the amount of compute power required to create coins and validate transactions is precisely what makes it so safe and virtually impossible to hack even with brute force. The difficulty level that determines how much

compute power is required scales automatically, both up and down, with the number of users (actually, miners) in the network. The number of miners will adjust due to supply and demand from the network as the reward for miners scales up or down as a result of both the difficulty level and the value of bitcoins.

Okay so I probably lost you there, as I kind of lost myself in that sentence; but the bottom line is that market principles ensure that in the long run, bitcoin miners will always be borderline cost effective, also energy wise. In the short term this may not be the case if there is eg a shortage of miners to keep up with growing demand for the currency as arguably is still the case now (and definitely was the case a few months ago when miners made money hand over fist, power consumption costs be damned)..

In the long run these market dynamics will also drive mining towards more expensive, but far more power efficient solutions like FPGA's, just like mining has shifted away from CPUs towards GPU's today.

You seem to be pushing for this bitcoin thing relentlessly, whats your stake in this?

Full disclosure. At the time or writing I own 1.21 BTC I earned through mining and playing online poker. Thats not even $5. I wouldnt mind that doubling, but I think there are easier ways to make $5 than writing all this :) If Im pushing this its because I love the concept, I believe in its potential and I think its a great way for Bfs to establish a small revenue stream.

Okay; honestly I read all this but I still dont believe it. Im not gonna help with this; I think BTC is little more than a scam and it will come crashing down soon.

Thats quite okay and perhaps you will be proven right. However, until that happens, so as long as bitcoins trade for reasonable prices, there is no denying mining still produces bitcoins and those bitcoins can be sold for “real” money. You dont have to invest any money in it and so thats not a good reason not to mine and help out BFs.

Next month may be different, but at the time of writing mining bitcoins is marginally profitable with appropriate hardware and if you dont suffer from insanely high electricity prices. If or when that changes for any reason, one can (and probably should) stop mining until it makes sense again :)

Keep that in mind, you can always just stop mining, and unless you speculate money on it, the long term success or failure of bitcoin is of no consequence to you or BFs. You dont have to believe.

Okay, Im not sure I believe you, but I got nothing to lose, I may as well run this app overnight and perhaps make BFs a little money. How do I get started?

Stay tuned. Ill post a howto shortly.