Introduction to Bitcoin

Konstantinos Karasavvas <kkarasavvas@gmail.com>

This document [1] is an easy to understand tutorial that introduces new users to Bitcoin. It is targeted to non-technical users. We discuss what Bitcoin is and its basic characteristics, why it is useful and finally we go through the basic concepts to help us understand basic usage.

1. What is Bitcoin?

Simply put Bitcoin is a *decentralized digital (crypto)currency*. There were many attempts to create digital currencies in the 80s and 90s (e.g. DigiCash[2], e-Gold[3], Liberty Reserve[4], etc.) but all of them failed to achieve their goals. The primary reason was that they were centralized.

Typically countries issue their own currency, through a central bank, and have complete control of its circulation. They can issue more currency to increase liquidity in the markets (which increases inflation). The companies mentioned above were creating an alternative currency that the respective governments did not have control of. This was in direct *competition* to the governments which found ways to target those companies and consequently shut them down.

The primary difference with Bitcoin is that it is decentralized, ie. there is no single entity that controls the Bitcoin network and thus cannot be targeted. This is achieved with the combination of several technologies some existing and some new and very innovative. You will hear a lot of things about what Bitcoin is:

- software project
- a peer-to-peer network/protocol
- an immutable public transaction ledger (aka blockchain)

[2] https://en.wikipedia.org/wiki/DigiCash

[3] https://en.wikipedia.org/wiki/E-gold

[4] https://en.wikipedia.org/wiki/Liberty_Reserve

- a proof-of-work system
- a decentralized trustless platform using elliptic-curve cryptography (PKI)
- a novel consensus mechanism

and while there is some overlap in the above they are all accurate, and if you do find the time to study them you will see that they are not just buzzwords.

The most important thing that I would like you to remember is that it is an innovative technology that allows us to do things in Computer Science that we could not do before. It is a technology, a tool at our disposal, neither good nor bad.

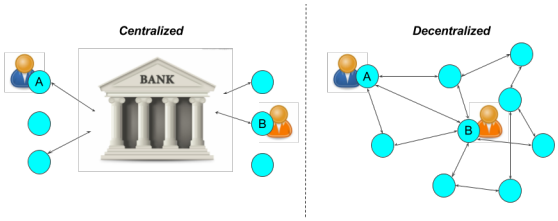

Figure 1. Centralized & Decentralized Models

1.1. Decentralized Digital Cryptocurrency

So let us examine each of the words we used in the definition in respect to traditional financial systems (centralized) and the Bitcoin network (decentralized) to highlight the differences (see figure 1).

Decentralized

In a centralized financial system a central bank creates and controls all aspects of the currency. If user Alice wants to send money digitally to Bob it makes a request to the bank and the latter sends the money to Bob. Having an intermediary also incurs higher fees to cover their costs. In contrast, in a decentralized model like Bitcoin's the currency is created and distributed algorithmically and there is no intermediary between users, ie. Alice sends bitcoins directly to Bob. Disintermediacy has also the benefit of lower fees.

Digital

In tradtional financial systems you can make digital payments anytime you want. However, the transactions are actually settled at specific periods of time. For example if you send money on Friday evening your transaction

is going to be processed on Monday[5]. Furthermore, if you send money to a different bank, especially in a different country, you need to pay (even higher) inter-institution fees. In contrast, in the Bitcoin payment network all transactions are settled when you make them (24/7), it is a global network (no inter-institution fees) and the only pre-requisite to use the network is an internet connection and a cheap smartphone.

Cryptocurrency

The crypto in cryptocurrency stands for cryptography and it is used to emphasize that the currency is based on cryptographic principles. In Bitcoin, security and anti-counterfeiting measures are enforced by cryptography and algorithms. It is an open security infrastructure and anyone can verify its operation. Traditional centralized systems have a closed security infrastructure and can be verified only by 3rd parties behind closed doors. Indirectly, anti-counterfeiting measures are enforced by the central bank and the government, ie. the police.

1.2. Other characteristics

Fixed Supply

Bitcoins supply is fixed; bitcoins are issued algorithmically every (approximately) 10 minutes. When it begun in 2009, 50 bitcoins were issued and that number is halved every 4 years. Coin creation over time can be seen in figure 2.

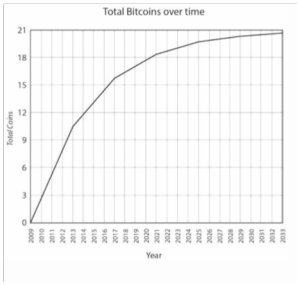

Figure 2. Bitcoin has Fixed Supply

Currently, 12.5 bitcoins are issued every 10 minutes and that is going to stop around 2140. In practice, however, more than 99.5% is going to be issued up until

[5] Different financial institutions have different settlement periods.

around 2036 from which point on the currency will be deflationary (which means that if demand increases its value will increase accordingly).

Fiat currencies are by their nature inflationary. Governments can issue more when they need to increase the liquidity in the market. The latter helps control outside market forces/pressure but has the tradeoff of reducing the currency value (e.g. your savings worth less).

Transparent rules

Another important aspect is that all the rules of how the Bitcoin payment network operates are out in the open. Questions like:

- Which transactions are valid?
- How is ownership determined?
- How are new coins created and distributed?
- etc.

are all transparent. The Bitcoin software is open sourced under the MIT license and anyone can download its source to verify which are the exact rules and how they are applied.

Consensus-based

Furthermore, the valid ruleset is determined by a large majority[6]. This is determined by supporting (running) a specific version of the Bitcoin software that implements the rules that you prefer. This consensus-based decision-making is one of the biggest innovations that Bitcoin introduced[7].

[6] To be more precise, majority of mining processing power.

[7] Although it is not perfect and recently we have seen improvements in the consensus mechanisms in alternative coins.

Transaction immutability

A complete history of all the transactions that ever occurred from Bitcoin's creation in 2009 [8] up to now are stored in a data structure in all the computers that support the network. This structure is called blockchain and it is immutable[9]. That means that noone can delete or modify entries. It is only possible to add new entries.

The more time passes after the creation of a Bitcoin transaction the less the chance of potential modification. After about an hour it is almost impossible to modify/reverse.

Transaction transparency

Interestingly enough, the blockchain, this ledger with all the transactions that ever occurred, is public. Anyone can access it and see exactly how many bitcoins moved and where thus making transactions easy to audit. The combination of transparency and immutability in transactions make for an incorruptible structure.

Pseudonymity

It is important to note that Bitcoin's accounts[10] are represented by a sequence of (seemingly) random characters. Thus, no real user information is attached to it which lead to the popular belief that Bitcoin is anonymous.

However, most people will get their first bitcoins through centralized services, like exchanges. These services will require your real world information (credit card or bank transfer details, etc.) to allow you to buy bitcoins from them. That service provider will know your identity thus your anonymity can be compromised. Similarly, if you buy something with bitcoins the online store would be able to associate the bitcoin account where you paid from with the postal address.

[8] Bitcoin was created by someone or a group of people under the pseudonym of Satoshi Nakamoto [https://en.wikipedia.org/wiki/Satoshi_Nakamoto]. Historical details [https://en.wikipedia.org/wiki/Bitcoin#History] have been omitted deliberately from this tutorial. Since the software is open source and the code verifiable it is of little importance who its original creator was (other than a fun endeavor).

[9] Some people prefer the term *tamper resistant* to be less absolute since there are infinitesimal possibilities of change.

[10] It is not exactly equivalent to an account but it is a pretty good analogy and makes it easier to understand.

That is why we should consider Bitcoin pseudonymous rather than anonymous[11].

1.3. How it works (bird's eye view)

Bitcoin consists of a peer-to-peer network of Bitcoin nodes (computers which run the Bitcoin software) that run and secure the network. The complete transaction history, the blockchain, is available to everyone to see but is immutable.

But why run a Bitcoin node?
Some nodes are run by volunteers, eg. ideologists like liberitatians or anarchists or anyone else who wants complete control over their money. Most, however, run nodes because there is a monetary incentive to do so. Users that secure the network are called miners [12] and they get part of the newly created bitcoins (that are generated every about 10 minutes) as a reward for their services.

2. Why Bitcoin?

Lets discuss some of the use cases that Bitcoin and more generally blockchain technology [13] can offer us. Below you can see a categorization of several possible applications of the technology:

Remittances
: Sending money anywhere in the world.

Payments
: Buying/selling goods online.

Bank Services
: A lot of people globaly have no access to bank services.

Store of Value
: Safe-guard the value of your currency from inflation.

[11] Note, that there are ways for more advanced users to remain completely anonymous.
[12] Mining secures the network via a proof-of-work [https://en.wikipedia.org/wiki/Proof-of-work_system] process and it is also the process that new coins are minted. It is called mining as a parallel to gold and its mining process.
[13] Blockchain is the term used to describe the complete architecture behind Bitcoin. Although this is not necessarily accurate it is widely used and accepted.

Digital tokens

Send ownership of anything anywhere in the world.

Decentralized Applications

Decentralize control and disintermediate most internet applications (crowdfunding, e-commerce, cloud storage, DNS, social media/platforms and more)

Micropayments

Enable micropayments; sending only a couple of cents, e.g. to pay for WiFi connectivity on a per second basis

Proof of Existence

Prove that a document (e.g. patent) was in your possession by time-stamping it and storing it in an immutable ledger (ie. blockchain)

Smart Contracts

Allows to make trustless agreements (contracts) with anyone in the world; the agreement will be enforced by algorithms (no intermediary, like a notary, is required)

Decentralized Autonomous Organisations

Allows to create self-governed entities that will run online organizations (from simple decision-making logic to strong AI) that will act on behalf of itself or its stakeholders

Internet of Things / Machine to Machine

Machines can now pay each other with micropayments. Internet of things is now finally incentivized and re-invigorated

Voting / Identity

Trustless and secure voting will become a reality; several projects work on solving the online identity problem which in combination with blockchain technology will finally enable secure and incorruptible e-voting systems

Private Blockchains

Will enable competitors to cooperate to achieve common goals without the need to disclose private information to each other

Other?

People always find ways to innovative around open technologies. We expect to see things that would be very difficult to imagine today

There is an overlap between some of the categories (e.g. decentralized applications or smart contracts will be typically using some kind of token, DAO's will be using smart contracts, etc.) but we believe they were worth to mention separately since they expose different point of views.

Let us go into a bit more detail in some of the more straightforward use cases leaving the rest for background reading.

2.1. Remittances

The use case is sending money abroad, anywhere in the world, fast. Remittances is a $600 billion global market and major companies on this market are Western Union (15% market share) and MoneyGram. We will use Western Union (WU) in our examples. The fees when transferring with WU can reach up to 15% of the transferred amount depending on how remote the location of the transfer is. And that is for 1-3 working days delivery service. The commission is even higher for same day delivery. You can sent/receive anywhere there is an agent of WU and whenever they are available: normal working hours plus some extended hours for some agents.

During the past years Bitcoin slowly and steadily gained momentum as a remittances alternative. That is because it offers several advantages over companies like WU. For example, the fee for a Bitcoin transaction is only about 6 cents[14]. The transfer can take up to 1 hour but in practice it is much faster. You can send bitcoins anytime (24/7) and anywhere there is a connected device to the Internet (a cheap smartphone suffices).

Although there are no intermediaries to use the Bitcoin network itself, in practice because Bitcoin is not widely adopted yet there is a need for intermediaries to convert the bitcoins to the local currency. Not many merchants accept bitcoin yet and sending bitcoins to e.g. Africa might not be very useful if no supermarket, or fruit-seller accepts it. To this end centralized services appeared to solve this issue.

[14] This was calculated with an exchange rate of 1 bitcoin =~ 630 dollars.

Companies like Rebit[15], BitPesa[16], BitSpark[17] and others allow users to convert bitcoin remittances to local currencies and they usually charge around 1%.

2.2. Online payments

The use case is buying or selling for services or goods online. Currently, the only way to accept money online is with the use of credit/debit cards and services like PayPal. The charges for those services are 2%-6% of the product value plus a small flat rate fee. When accepting Bitcoin payments the merchant pays zero fees[18]. That means that merchants can offer discounts when selling with bitcoins or alternatively just increase their profit margin.

The Bitcoin network is public and any merchant can integrate their online store with it given some technical expertize is hired. Moreover, there are (centralized) payment processors, like Bitpay[19], Coinbase[20] and others that make this process trivial. Payment processors have several advantages, allowing automatic conversion of a percentage (or all) of the amount to your local currency, create appropriate records for tax authorities and other. Again, fees are reasonable, e.g. Bitpay has zero fees[21] for a certain number of transactions and 1% for unlimited transactions.

It is estimated that there are more than 100.000 [22] sites that accept bitcoins. Some of the big sites include: Overstock, Microsoft, Dell, Expedia, Time Inc., DISH Network, Zynga, Steam, AirBaltic, CheapAir, and many others.

2.3. Bank services for the unbanked

There are 2.5 billion adults in the world without access to banking services and many more with only partial services. The use case for these people is that they can now be part of a global market. They can use bitcoins to make and receive

15 https://www.rebit.ph/
16 https://www.bitpesa.co/
17 https://bitspark.io/
18 Only the sender pays approximately 6 cents as previously discussed.
19 https://bitpay.com/
20 https://www.coinbase.com/
21 https://bitpay.com/pricing
22 There are online catalogs like SpendBitcoins [http://spendbitcoins.com/] and CoinMap [https://coinmap.org/] that aim to help buyers find appropriate merchants.

payments or donations or to make remittances and many more. From being isolated to having global reach the opportunities are immense for these people.

Moreover, even for people with full access to financial institutions there is the use case that people would just want more control over their money. There are plenty of examples of such institutions censoring specific people or applying capital controls and some people found alternatives solutions with Bitcoin.

2.4. Store of value

The Bitcoin network is operational for more than 7.5 years now and it has a market capitalization of more than 10 billions dollars. It is the wealthiest *online* system in existence. There is no other open system that can provide such wealth to a hacker than actually cracking the Bitcoin network. And hackers all over the world have tried; they have tried hard and failed. Over the years trust in the network has increased tremendously, so much so, that people in countries with high inflation would just buy bitcoins as store of value.

Traditionally, gold or reserve currencies (dollars, euros) are used for that purpose; although these are still inflationary currencies they are much less inflationary than most other currencies. However, since Bitcoin started to prove it is secure and in combination with its deflationary nature it offers an even bigger incentive for store of value which is why it started to gain popularity for that purpose.

There were periods in countries like Argentina that hyper-inflation was causing the local currency to lose half its value every week. And in some countries, like Zimbabwe, it even happened daily! But even people in countries with only high inflation like China, Russia and others have high incentives to protect the *value* they own through gold, reserve currencies and lately bitcoins, which is also the most secure way in respect to actual ownership.

2.5. Digital tokens

Until now we have discussed about transfering (ownership) of currency between two or more parties anywhere in the world. This use case deals with transfering ownership of anything via the technology Bitcoin introduced. Users can create their own digital tokens that represent real world objects that they sell or services that they provide or anything else you may think of. The tokens can then be sold

and the token issuer promises that the token holders can redeem them to get the goods or services that the tokens represent. The issuers reputation is at stake; if they cannot fullfil their promise the market value of their token will diminish.

Some token examples:

Concert tickets

You buy a token that represents a ticket for a concert in, say, Germany. However, you cannot attend the concert and you decide to transfer (ownership) of the ticket to a friend of yours in Germany. Your friend can then go to the concert just by using his mobile phone in the cashier.

Consultancy hours

Experts can sell consultancy hours in the form of digital tokens, e.g. Kostas-1Hour tokens would be redeemable for a one hour consultancy session per token. The expert could sell those tokens online for anyone to access and token holders can actually trade it if they see fit. For example, if the expert becomes well known his services value will increase and thus the value of the token.

Authentication mechanism

Ownership of specific tokens may give entry to online sites or even in the physical world with smart locks[23] to only members of your organisation or for whatever other purposes.

Stock market shares

Equity shares ownership can be represented as tokens on a blockchain and indeed this is already used for a couple of years now in the pre-IPO trading of private company equity shares in the Nasdaq Composite Index.

New currency

A digital token can even represent a new currency that you may use and promote for your own reasons. An example would be for a company to issue tokens and give them as reward points to their customers, ie. what most supermarkets already do with other technologies. Or it could be a currency for your new club or, again, anything you can imagine.

[23] https://en.wikipedia.org/wiki/Smart_lock

Car key, house or land deed, …

A token could also represent your car key or your house deed and more. While you may think that this is far-fetched there are several projects that try to implement these solutions. For example, the Swedish National Land Survey has a blockchain solution [24] on trial that automates the process of buying and selling land in Sweden. It is a process that currently takes months or weeks and the goal is to reduce it to days or hours using blockchain technology.

Although some of the above examples already exist, the existing technology does not have the same properties as blockchain technology. For example, the land survey needs to be public (transparency) but only very specific people (the owner of the deed) could initiate a transfer of ownership and no one else could tamper with the records (immutability). Although, for some people, it might sound improbable that government officials would change records of land deeds (effectively stealing the land!) but there have been several cases that it occurred around the world.

2.6. Applications and potential

Bitcoin introduced a new innovative technology that can be applied and improve several different industries and more general aspects of society. While the examples we saw where mostly about improving existing applications there are many more potential use cases that would not be possible without blockchain technology.

If you are a developer or have general interest in computer science we strongly recommend that you delve into the technology behind bitcoin. The opportunities that this innovation brings are staggering and the earlier you are involved the better. It is usually compared to the Internet as it was in the 90s where some people were pessimistic about it but the technology paid off ten-fold in later years. Actually, we believe that it is the most important digital innovation that the world has seen after the Internet.

[24] The specific solution does not use Bitcoin's blockchain. Nowadays, there are several other technologies on top of Bitcoin or similar to Bitcoin with their own blockchain called alternative coins or alt-coins.

3. Basic concepts and usage

3.1. Accounts

A Bitcoin account [25] consists of two things (see figure 3): an address and a private key.

Figure 3. Bitcoin address and private key

Both are represented as long sequences of characters or by their equivalent QR codes since typing those long strings is not very practical. The address (1Lu4RFbBxGL58dSuF38x93bhmk5PL4np6G) can be shared to anyone wishing to send you money. Similar to an email address where you share it, so that people can send you digital content. The private key should always remain a secret. Whoever knows the private key (KxsifKB1eTf81ttipQGYfaTMLVKM4zJuKvdZAWjLkjEQKCAZpySp) can spend the bitcoins in that specific address [26].

Important

> This cannot be emphasized enough. One should never lose or share the private key or access to the funds is forfeited.

3.2. Wallets

To manage your bitcoin accounds (addresses and keys) users use Bitcoin wallets; software specialized in making easy to manage accounts and allow you send (or receive) bitcoins.

There are several different categories of wallets. Some are for your desktop some for your mobile phone some online/web wallets and even hardware wallets. There

[25] Although it could be argued that there are some differences it is conceptually much easier to think about it as an account.

[26] There are strong cryptographic ties between these two character sequences based on public key cryptography and specifically based on the elliptic curve digital signature algorithm (ECDSA)

are several wallets for each category but an easy one to use is Copay[27] and is available in all major platforms for your mobile phone or desktop computer. Another option is an online/web wallet like Blockchain.info[28] which is also very easy to use. More advanced users can visit the website bitcoin.org[29] to help you choose another wallet depending on your security requirements.

3.3. Example usage

We will now provide a simple example between two users, say Alice and Bob. For the purposes of this example Alice wants to sent Bob 1 euro worth of bitcoins and they will both use their mobile phones which have the Copay application installed.

In figure 4 we can see the main screen of the application; Alice's balance and transaction history is shown for her account. A user has the option to receive or send bitcoins.

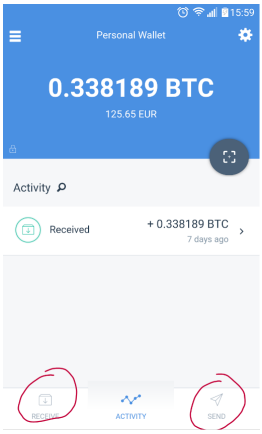

Figure 4. Copay's application activity screen

Bob, who expects to receive some bitcoins selects "Receive" and he sees figure 5.

[27] https://copay.io/
[28] https://blockchain.info/wallet/
[29] https://bitcoin.org/en/choose-your-wallet

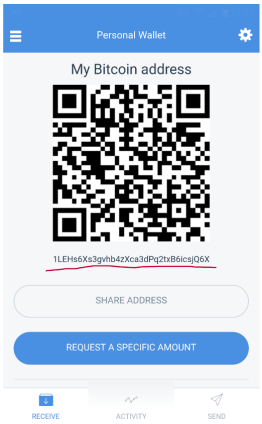

Figure 5. Copay's application receive screen

The application displays Bob's address and QR code so that he can show to users that want to send him bitcoins. And he does exactly that, ie. he shows that QR code to Alice. Alice selects to "Send" some bitcoins and she is presented with figure 6.

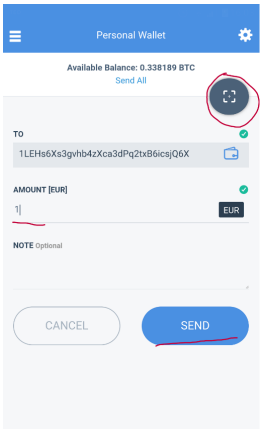

Figure 6. Copay's application send screen

The "TO" field is not filled in yet and she presses the scan QR code button to get Bob's Bitcoin address. She uses the phone to scan the QR code from Bob's phone and Bob's address appears in the "TO" field. Then all Alice has to do is fill in the amount (1 euro) and select "SEND". After some seconds Bob's phone will notify him that he received some bitcoins.

3.4. How to get bitcoins?

There are several ways to get bitcoins. We will list them and briefly explain them.

Mine bitcoins

You can mine bitcoins by spending computational resources to secure the Bitcoin network. Aside from the technicalities, Bitcoin mining is extremely competive nowadays. It is very difficult to start, it needs a considerable investment and requires very cheap electricity. Only professionals can do profitable mining.

Buy bitcoins online

There are several online sites, e.g. exchanges that users can buy bitcoins. You need to create an account to that service and send some fiat currency via bank transfer or credit card. Then you can login to that site and buy bitcoins. You can then send those bitcoins to your private wallet in your mobile or desktop, etc. [30]. Some examples of online exchanges or other services are: Bitstamp[31], Kraken[32], Coinbase[33], Xapo[34] and many others.

Buy bitcoin from an ATM

Yes, there are ATMs that you can buy bitcoins. Consult CoinAtmRadar[35] to find ATMs near your location.

Buy bitcoin from another user

Very simple, like the example usage we saw above. They send you bitcoins and you provide the equivalent in your local currency. There are sites, like LocalBitcoins[36] to facilitate a safer exchange using escrow.

[30] You can also leave the bitcoins in the website as long as you understand that they have control of your money. If they are hacked or run away with your bitcoins there is little you can do.
[31] https://www.bitstamp.net/
[32] https://www.kraken.com/
[33] https://www.coinbase.com/
[34] https://xapo.com/
[35] https://coinatmradar.com/countries/
[36] https://localbitcoins.com/

Sell services or goods for bitcoins

We consider this to be the best way to get bitcoins. Not only do you expand to a new and global market but at the same time you contribute to its wider adoption creating a virtuous cycle.

4. Next steps

For casual users.

You can learn more by searching the web but a good starting point would be Bitcoin.com.

For developers.

There are several resources online but we recommend an excellent book, *Mastering Bitcoin*, which is also available for free[37] and the *Developer Documentation* [38].

For merchants.

Again, there are several resources online; one starting point would be from Bitcoin's wiki page[39].

[37] https://github.com/bitcoinbook/bitcoinbook
[38] https://bitcoin.org/en/developer-documentation
[39] https://en.bitcoin.it/wiki/How_to_accept_Bitcoin,_for_small_businesses