Redesigning Bitcoin

Improving the user experience
(draft version)

Contents

Preface

By the end of 2017, nearly every media channel was covering bitcoin and other cryptocurrencies. For a brief moment, it was the most-searched-for word on the Internet. Even governments had to look into this phenomenon and create an opinion about it. But it would not take long before that feeling of excitement and attention would soon be over. Market prices crumbled, media attention started to fade away, and many cryptocurrency startups disappeared from the scene.

It was during this period that I wanted to obtain a deeper comprehension of this Bitcoin (r)evolution and understand why it excited so many people. Many hours of videos, books, and conversations followed. But it wasn't until one specific video of Andreas Antonopoulos that changed everything for me. In this video, Andreas presented a talk about Bitcoin with people from a reputable design studio called IDEO. And in that talk, he spoke about some of the "design" flaws of Bitcoin. For a moment, I was dumbstruck. How could this be? One of the most respected proponents and advocates of Bitcoin was talking trash about the technology that he loved so much. What I did not know was that Andreas was setting the stage. At that moment, he intended to challenge the audience of designers to come up with better solutions for Bitcoin so that everyone in the world could use and understand this new technology.

It was at that moment after this video that I had found my mission. With a background in both development and design, I knew that Andreas was right. The next significant challenges would not be faster or more secure blockchains, but to explain Bitcoin as simple as possible, and to as many people as possible.

So with this book, I take you along to view Bitcoin's technology from a (user experience) design perspective. By doing so, I hope that developers, writers, designers, and crypto enthusiasts can create better solutions that are usable for everyone. And although this book mainly focusses on the Bitcoin ecosystem, many of the topics within this book are also applicable to other crypto assets.

Bitcoin vision

As a brand, millions of people have at least heard of bitcoin as a digital currency. But being a digital currency is probably the least exciting aspect of Bitcoin. To truly understand why Bitcoin is so much more than that, let's start at the beginning.

Origin story

The Bitcoin origin story began during the financial crisis of 2007-2008. Property prices evaporated, banks collapsed, companies went bankrupt, and millions of people lost their jobs or their houses. It may have started in the United States, but in this hyper-connected economy, it did not take long before the entire world felt the pain of an economic recession. Trust in banks and financial institutions reached an all-time low.

Meanwhile, somewhere else, a man, a woman, or a group of people imagined a different world; A world where people could exchange money without the need for banks and other intermediaries. An alternative to government-issued fiat currencies. And a world where people are in control over their money, their privacy, and their choices. That someone we now know under the pseudonym, Satoshi Nakamoto.

Probably the first appearance of Satoshi Nakamoto was on October 31st, 2008. On the Cryptography Mailing list at metzdowd.com, Satoshi wrote: "I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party. And with these words, the Bitcoin whitepaper was introduced and shared with the public.

We have only bits and pieces of information about what happened before October 31st. But we know that on January 3rd, 2009, the software started with the intention never to stop running, and mining of the very first Bitcoin block was a fact. And within this genesis block, a piece of text was included, which says: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." This reference to a news article of that exact day, quietly told the world that something new had appeared — an alternative based on cryptographic proof instead of third-party trust.

Not long after, on January 8th, 2009, the first version of the Bitcoin software was announced on The Cryptography Mailing list. People could now see, download and run a Bitcoin node themselves. And with that, Bitcoin started its journey all around the world.

And what happened to Satoshi Nakamoto? After being active on several forums, on December 12th, 2010, Satoshi Nakamoto published the last message under that pseudonym on Bitcointalk. Asides from email exchanges dating back to April 2011, all of the later interactions coming from Satoshi's accounts lie under a shade of doubt cast by the email account allegedly compromised in a hack. Why Satoshi disappeared is still a bit of a mystery. There are some clues, but most of them only lead to more questions than answers.

Vision or Mirage?

Ask a random number of Bitcoin advocates to explain the Bitcoin vision, and you'll get an arbitrary number of explanations for an answer. Why is this? Did Satoshi not clearly share and explain the end-goal?

One explanation which people often refer to is the message left inside the genesis block; "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." This message could both seen as a financial and a political statement. With the birth of Bitcoin on that exact day, it introduced an alternative to the failing of financial institutions.

But did Bitcoin really emerge as a solution at the right time during the financial crisis? Or did the financial crisis coincidentally appear at the right time for Bitcoin? Going through everything Satoshi publicly writing about Bitcoin, we notice a couple of things.

Reading between the lines, early writings of Satoshi, let us believe that technology came first, followed by politics like Libertarianism. More than once, the response includes "I'm better with code than with words though." And speaking in the plural when political concepts need further explanations; "It's very attractive to the libertarian viewpoint if we can explain it properly."

The second clue is the order in which Satoshi created the software and the whitepaper. Although the whitepaper was released before the software went live, Satoshi mentions, "I had to write all the code before I could convince myself that I could solve every problem, then I wrote the paper." This quote meant that the whitepaper was merely a formality of an early proof-of-concept. Most of the code would have already been written and tested on Satoshi's computer(s) before Satoshi made its first appearance.

But in another reply, the following comment reveals even more. "I believe I've worked through all those little details over the last year and a half while coding it,

and there were a lot of them." This sentence could imply that Satoshi has been working on Bitcoin before the start of the financial crisis. In a later post, he confirmed this by saying, "(I've been working on bitcoin's design) since 2007. At some point, I became convinced there was a way to do this without any trust required at all and couldn't resist to keep thinking about it" Assuming this is true, then from a vision point of view, Bitcoin might have been a solution waiting for the right problem at the right moment.

But there is another argument to be made that Bitcoin lacked a clear vision from the start. Without a doubt, Bitcoin was not the first non-government issued digital money. The whitepaper explicitly mentions some predecessors, such as "b-money" and "Hashcash." Either one of those could easily have been an inspiration by their successes and failures. Other technological influences mentioned by Satoshi were Napster, Gnutella, and Tor networks. Therefore like most brilliant solutions, they build upon other ideas as well as combining technologies from different fields. Bitcoin just happened to be a perfect combination.

In quite some conversations, Satoshi talks about the lack of trust in centralized solutions, which leads to central authorities who control and regulate assets. But in typical vision statements, there is a problematic challenge involved. However, Satoshi already proposed the solution to most, if not all, of the problems. Does this mean that the vision died with the solution offered?

There is a counter-argument for this to be made. Within the field of design, there is a principle called "closure." Also, within the field of psychology, this is known as one of the Gestalt principles of perception. In brief, closure is a tendency to complete incomplete or interrupted forms and patterns. And what makes this pattern so interesting, is that the lack of information given by Satoshi leaves gaps and room for interpretation. Because Satoshi is no longer answering all sorts of questions, people will take the snippets of information and connect the dots themselves.

Perhaps this was is the unintended vision Satoshi left behind; to leave room for interpretation about the future of Bitcoin. And in true open, decentralized style, allowing everyone to build upon Bitcoin and create new visions for an always-changing world.

Strategic design principles

In this fast-paced digital world, Bitcoin evolves every day with the help of developers from all over the world. Some things, such as the five pillars of open blockchains by Andreas Antonopoulos, are still holding strong in Bitcoin. Those being: open, borderless, transparent, neutral, and censorship-resistant. Other aspects, such as privacy, speed, and transaction size, are continuously being improved. But something else that is changing for the good is the number of new people with different backgrounds entering the Bitcoin space for the first time. Teachers, marketers, journalists, politicians, designers, artists, lawyers, and many more jobs and skills have a role to play in the upcoming decades of Bitcoin. Companies and organizations would do well to stimulate and invest in the creation of more non-trivial job openings so that the community as a whole becomes more robust. Because with more diversity comes more expertise and new perspectives to help Bitcoin grow bigger and faster than it is growing right now. In the next decade, Bitcoin will need to shake off its reputation as nerd money and geek technology. Instead, it should become a universal, public service available and usable to anyone. What is needed is a broader approach. Not just focussing on Bitcoin as a technology but designing for the complete ecosystem, both digital and physical. A future where products, services, and the community are aligned and share the same beliefs and goals. And with that mindset, five strategic design principles for building Bitcoin will deserve extra attention in the next decades.

Literacy

One of the biggest problems at the moment is Bitcoin's literacy. Most people today do not have enough information and understanding of the things that are related to Bitcoin. This kind of knowledge is essential because basic financial and technological literacy is becoming more mandatory in the digital and global times we live in today. The goal for improving Bitcoin literacy is to leave nobody behind when it comes to comprehending and using financial services through Bitcoin.

When strategic and service designers compose and visualize solutions, they look beyond a single product, service, or system. Also, compared to the design of products, strategic & service designers tend to look at a broader time horizon for change to be implemented. "If you give a man a fish, he eats for a day; If you teach a man to fish, he eats for a lifetime." This saying also applies to Bitcoin when designing sustainable solutions. The benefit of creating short-term solutions is that it takes relatively little effort and has a direct impact. The drawbacks are that these solutions often lack addressing the fundamental issues or target only a specific group of individuals. Designing long-term solutions are

much harder and more challenging to tackle. The impact is often more significant because of the scale and depth of the knowledge shared. The drawback is that long-term solutions tend to take a longer time to implement.

One example of a long-term solution is to formalize Bitcoin fundamentals within the educational system. The long-term goal is to have teachers teach children about money and technology at schools. What teachers can do is help explain the concepts of cash and money creation. Interesting talks are; what gives money value, what is sound money, why we need financial inclusion, what the effects are of inflation, why sovereignty over cash, and personal data is essential. Mid-term goals have designers and developers create and improve products and services within the Bitcoin ecosystem that are easy to understand and use for everyone. They can start by avoiding technical jargon and applying relatable conceptual metaphors. When creating products that interact with Bitcoin, it is good to keep in mind that people are unique, as well as the context they use it. When explaining or onboarding people to Bitcoin, there is no "one-size-fits-all." People learn and approach things in different ways and at different paces.
And when looking at short-term solutions, everyone who is a parent, friend, or social media content creator, can help spread information and knowledge about this technology. The best way is to take people along step-by-step and, if possible, one-to-one. Let people experience and learn to use Bitcoin by doing. Show the risks and responsibilities that come with self-custody.

Usability

Design is about the realization of products and services with a specific purpose or use in mind. Usability is about avoiding and removing obstacles while interacting with these products and services. The goal is to create a seamless, smooth, and comfortable experience. These obstacles can be different things for different people in different situations. For some, it could be installing and using an application with too many steps and technical jargon. For others, simply finding a place to buy or spend bitcoin without repercussions can be challenging by itself. A strong focus on usability aids the adoption and retention of Bitcoin and the products which interact with the Bitcoin system. Ignoring usability will push Bitcoin further in the speculative and technical realms of magical internet money only used by geeks and nerds.

What is needed are more problem-solving people. People who use their minds, skills, and talents to help create better solutions. It can start with a little more empathy and interest in other people. We are all different with specific (dis)abilities and needs. Every little effort to help people understand, use things, save time or effort, will have a compounding impact. As an indication, there are

more outstanding issues on code-repositories, than there are people to solve them. Some of those are as simple as translating them into native languages.

When designing Bitcoin products and services, consider both macro and micro usability challenges. If you are a developer, tester, designer, researcher, architect, or any other digital professional, then try to find out causes that are hindering people using Bitcoin. If you are a policymaker, then create more regulatory clarity. If you are a teacher, include Bitcoin as a topic in your classes. And if you are good at art, then create something related to Bitcoin that makes people happy and think about it.

Autonomy

We seek control over all aspects of our life, the freedom to express ourselves and to do the things we want to do. We challenge ourselves, gain knowledge, and master skills to achieve new things, either alone or with others. Stimulating autonomy will lead to happiness and fulfillment. Take this away, by limiting choice or creating boundaries, and it will negatively affect people's emotions.

The challenges in this area are to make the Bitcoin system safe and easy to use for people so that they become more in control of their data and the tools they use. The strategy is to stimulate sovereignty safely while also allow and support options for personal creativity and expression.

The open, borderless, and public nature of Bitcoin allows much of our behavior and decisions recorded on the blockchain. This level of transparency enhances our trust in the system and reveals any malicious behavior. However, Bitcoin is also neutral and censorship-resistant, and therefore it does not discriminate between good or bad transactions. Once someone or something connects the identity of a person to their blockchain transactions, these can still be used against them by those who do not share the same values. Instead, we should focus more on solutions in which the individual controls the conditions of sharing information with others. But also offer access to the required information and tools for people to become knowledgeable and competent.

Mastery

Over time, training, and gaining experience, people may achieve mastery in their craft. People spend countless amounts of time and effort to get better at things like exercise, playing music, create art, or devote time to other hobbies. The goal is to have fun and to feel good about it while doing it. By showing what is possible, others will try to achieve the same or more.

The mastery design principle focuses on techniques about motivation and stimulation. By positively getting people interested and excited as well as create and maintain desirable habits. Two key components are time and personal attention. Short-term solutions may not be enough to stay motivated. There needs to be a long term incentive to stay motivated. Creating human connections of like-minded people helps bring people together and share experiences.

Getting to the level of mastery is not easy. As with everything, it starts with knowing what to achieve and how to accomplish things. Gaining knowledge and skills can be achieved through sharing, open-sourcing information, and facilitating exploration. Examples of people showing their level of mastery help others inspiring to better envisioning them reaching the same level.

Charity

The design principle of charity is about offering our support to others who will benefit from this act of kindness. Some of the most valuable things we can give are our time and attention. For some, it can be the gift of practical knowledge, skills, or information. For others, it means showing that we care and listen to what somebody else has to say. The chances are that those who receive charity are likely to pass it on to others.

The approach is to emphasize the humanistic approach and stimulate environments where people can find and help each other. The challenge is to support different forms of charity. Open platforms are most suited for sharing knowledge, code, reviews, references, and so on. The more people can help and collaborate, the stronger and happier the community will become. Kind acts of charity are likely to attract more people to join and pitch in.

People have much to give. In social constructs, they are often rewarded either by increasing their social status within the community. Those who give are often more mentioned and referred to as experts. When offering things for free, people are more likely to try new things and engage more often. Giving back recognition to people who positively contribute to helping others should not be forgotten.

Design patterns

Every design solution is only as smart as its use. And the more people use it, the more valuable it becomes. Within the field of economics, this correlation is called the network effect. Design patterns are a way to describe best practices, explain good designs, and capture experience in a way that others can reuse them. This chapter dives deeper into some design patterns that make Bitcoin as a whole more valuable by optimizing the design for use.

Aesthetic-usability effect

The first impression people have when visiting a website or application is crucial because this is a pivotal moment where they decide if they want to interact, or if they will continue to search for alternatives. The one thing people never have enough of is time and makes it a scarce asset to people's lives. First impressions play a crucial role in estimating if something is worth their time or not.

The aesthetically-usability effect dictates that in the eye of the beholder, beautifully designed products are more pleasurable and easy to use than those that are not. There is an unwritten expectation that those who created the look and feel of a product equally thought and cared about the simplicity of using it.

When applying the aesthetic-usability effect, it is essential to meet people's expectations. If the aesthetics are not up to date, people may distrust every other quality aspect of the product. And if the usability aspects are clucky, then people may never consider your product again based on false promises. Both need to be on par with the latest standards. For this reason, third party wallets are becoming increasingly more popular amongst beginning users than native wallets build by the same blockchain team. Developing an attractive looking front-end user interface with a smooth user experience is not the same as developing a stable and secure backend blockchain system.

Anchoring

Because Bitcoin is something very new and different entirely, a lot of people have or had difficulty understanding, explaining, using, or valuing it correctly at first glance. Anchoring is about connecting something people are not familiar with to something which they already know. The consequences of not correctly using anchors can be indecisiveness or making bad decisions.

People use anchors in situations where they try to seek agreements on price, quantity, or quality. For example, when a judge compares a situation to similar verdicts from the past. A good design includes helpful, unbiased, and meaningful

references to help create a frame. When creating correct comparisons, be sure to include the right context and time. Keep in mind that some anchors work better for some people than others because of their situation. Some user research is required to find out what your target audience needs and why.

The one thing people still cannot agree upon is how to value Bitcoin in the past, present, and future. The anchors that people use are going into all directions from comparisons to worthless, digital collectibles to a scarce store of value like gold.

Certainty effect

If offered a choice, people tend to choose for certainty over risk. This behavior is also known as the certainty effect. One of the traps that people fall for is that what people believe to be one-hundred percent true, is in reality, just a perceived certainty. This situation happens when the information people have is incomplete or incorrect.

Use the certainty effect pattern to avoid risk-taking situations such as creating a wallet, safely storing private keys or mnemonic phrases, and sending transactions to a recipient. In these situations, a wallet or service provider should be extra alert on taking safety measures to avoid mistakes. A good practice is to provide clear and understandable insights about the actual risks and benefits of specific actions to prevent people from being misled or uninformed. The more specific, complete, and neutral the information is, the more helpful it will be.

A great example of the certainty effect in practice is the decision for people to keep their assets under the supervision and control of custodians, such as cryptocurrency exchanges or financial institutions. The logic of this being that these custodians have better security measures in place, and offer consumer protection for loss of funds compared individually taking safety measures. The perception is that there is a bigger chance that the majority of people lack the knowledge of safely securing their assets and fear losing it permanently when mistakes occur. As long as people see any perceived risk in using Bitcoin, they will tend to avoid it and choose what they believe is the safest option. That is why the next generation solutions should also consider debasing risk. One approach to do this could mean restricting risky functionality for certain people, or until they are familiar with the risks. Only when they feel confident, can they choose to opt-in for more advanced features. However, the best approach will always be to eliminate and prevent all human errors before they can occur, for example, by including checks and validations as well as easy-to-understand steps tailor-made for different user needs.

Challenges

Research studies confirm that there is a relation between happiness and tackling problems. If things are too easy, and their brains are getting into an automated state of mind, people quickly become bored, and their brain dumbs down. But when things are too hard, people may become overwhelmed and frustrated. In both situations, accidents and human mistakes can happen. Between these two extremes lies a sweet spot to get people engaged and excited. It is this challenge that motivates people and influences behavior. Where to find this sweet spot depends on the challenge, people's skills, and their knowledge of the problem.

The best way of finding out what kinds of challenges are needed is by doing research, observations, and gathering feedback. These activities will give insights into the competence levels from beginner to advanced. Products and services should be flexible enough to support all kinds of challenges to keep people happy during their interactions. Increasing difficulty over time keeps people engaged and motivated. But using this pattern should not be a goal by itself, but a means to an end.
In some cases, a challenge may not be enough to keep people motivated. This lack of motive often happens when people need to do things instead of finding value or fun in doing it. In these situations, there is often the expectation of a reward or follow-up on this achievement after completion.

When taking into account the design principles, using challenges to learn can be a great way to achieve autonomy and mastery. When incentivizing people to learn about Bitcoin, to send and receive bitcoins, or to set up Bitcoin and Lightning nodes, more people would be willing to take the effort and spend their time to gain this knowledge and skills. "Stacking Sats" is a term often used for collecting small amounts of satoshis by performing small tasks such as liking and subscribing to social media. But there are also different kinds of rewards such as access to new features or gaining insights into personal progress to keep people engaged and motivated.

Consistency

Consistency plays a big part in the design of things. When designed correctly, people are more effective and efficient when taking up new tasks that are similar to those who are consistent with previous experiences. Like usability, consistency is not just limited to a single brand but works best when things work the same across multiple products and services. Driving consistency in an open-source ecosystem can be challenging due to the lack of cross-product comparisons and reviews. But eventually, the end-users will have their say on what works well and

whatnot. The benefit of consistency is that it stimulates predictive behavior, and build on long-term trust.

One area which benefits from consistency is standardization. By creating a certain open standard, it allows different protocols to share information and create seamless user experiences. In most cases, this is a win-win situation, especially for the end-user. The way to avoid inconsistency is simply to stick to default or standard, which is already used by others. Deviating from this standard is possible but only for good reasons such as a change of context, like adding more details and options for experts, who are already more familiar with the nuances.

One example of inconsistency is found in naming and terminology, using alternative descriptions for the same thing. Take the concept of a seed phrase, which consists of a list of words to recover a wallet containing private keys, public keys, and addresses. This concept is commonly first introduced when creating a new one for the first time. But depending on the creators of the wallet, this list of words used for recovery is called many things, like seed phrase, recovery phrase, back-up seed phrase, mnemonic phrases, or even more technically a BIP39 wordlist.

Confirmation bias

When people find information that is already in line with their beliefs, they are more likely to assume this as the truth. Although people love to hear about the things that they already believe, it can be refreshing to hear about alternatives that may approach things differently.

Using this pattern can be both helpful or dangerous, depending on how you use it. Within search engines, news, social media, and marketing use this pattern to explicitly find and snow similar results based on people's interests. Often this is referred to as "search optimization." The drawback is that there is often more than one side to a story. When people see with the same kind of information, it may implicitly create a bias towards a particular topic, losing its neutrality.

When people are (emotionally, financially, etc.) invested in a specific blockchain initiative such as Bitcoin, they often seek like-minded people on social media. Many great things can blossom from the interaction between people sharing knowledge and skills. But when this energy is applied negatively, open en free discussions may soon turn toxic. The best way to address this is by people from within the same community.

Control

As people, we desire autonomy and seek out situations where we can exert influence or control over something. Loss of control can make us feel dependent. But giving a choice to others is only desirable if they know that they can wield it properly. Having control over something is not always a guarantee that it will benefit people, and may put them into a worse situation.

When making people autonomous, keep in mind that the level of user control should be related to the proficiency and experience of the user. If they seek to be more independent, help them gain the required knowledge and expertise.

Bitcoin is about giving financial control back to the individual. By doing so, every person will have the autonomy and freedom to exercise their level of control as they see fit. The decentralized network enables direct payments between two or more parties without intermediaries. Decentralization of power is one of the key reasons why people feel free to operate within the network. As long as no individual or group can control the whole network, trust in the system remains intact. But one of the problems is that not everyone utilizes this possibility. They may have the opportunity but fear the responsibility. What could help is creating safe environments where people can try out and experiment, or watch others do it first, will help people become more confident and also take back control.

Curiosity

As humans, we are natural explorers. Our innate curiosity brings us to places we have never seen and do things we have never done. When teased with a small bit of interesting information, people will want to know more.

A big part of curiosity is the incentive or expectation of a reward afterward that encourages particular behavior. It helps motivate people to explore and move them out of their comfort zone. Another approach is to show examples of people like them who have already achieved something through exploration. But sometimes, the mystery of attaining something unknown can become a part of someone's motivation.

One of the biggest challenges for Bitcoin is education. And using curiosity for this can be a great match. Small nuggets of information, could set people to think and motivate them te become eager to know more. Highlight positive facts about Bitcoin and let people discover how these facts came true.

Delayed gratification

Over time, technology helped humans to speed things up by making processes and production faster by automation and digitization. Ever since the clock was widely adopted, people became more aware of time and living by the clock. Now more then ever, every moment is getting more valuable and precious. Nowadays, there is the expectation that things happen instantly or give instant satisfaction. Delayed gratification is about resisting a smaller but more immediate reward now to receive a more substantial or more enduring compensation later. Someone with a high time preference is focused substantially on their needs in the present and the immediate future, while someone with low time preference places more emphasis on their well-being in the distant future.

From a design perspective, delayed gratification is about positively influencing people's behavior over time. There are several strategies to help people increase or decrease their ability to delay gratification. A short-term approach is a distraction to allow them to 'forget' or 'ignore' their impulses to take action. But once they stop being distracted, their minds wander off and turn back to an instant gratification mode. A better approach is to reward people over time with something they may value, such as motivational speeches, recognition for their accomplishments, or unlocking new possibilities. Something else that helps people delay gratification is having a focus on a particular goal in mind. When combined with compounding or increased value of the rewards, the longer they may resist their temptations. But the most drastic and practical approach is to take away people's control over their urges. In this case, the ability to seek satisfaction is removed or forcefully delayed in time. It may seem like an anti-pattern of usability, but adding obstacles may help people resist their bad behaviors.

A person's ability to delay gratification relates to other similar skills such as patience, impulse control, self-control, and willpower, all of which are involved in self-regulation. Within the Bitcoin communities, those who can delay gratification are more commonly known as Hodler's (ability to hold and not sell their bitcoins). Their mindset is more focused on the long-term bitcoin value, rather than short-term bitcoin price. When designing for delayed gratifications, it is good to keep in mind your audience and which approach works the best for them. In general, younger people have a shorter focus span, seek more instant gratification than older adults. But also people with more experience over time are trained to delay their gratification and not to give in easily. Willpower is like a muscle that you can train over time. And those who cannot resist the urge may benefit from Bitcoin's Timelocks in wallets. This way, people are not able to spend their bitcoins until a precise future moment in time.

Delighters

New and unexpected discoveries arouse our brains. We remember and respond favorably to small surprising and playful pleasures. The combination of something unintended and pleasurable makes it very powerful. We like gifts, but when everyone else is receiving the same, it lessens the experience. And those who do not receive anything under the same circumstances will get disappointed. Excluding delighters may not negatively impact the experience because they always happen unexpectedly. But brands that want to distinguish themselves from the rest do use them to bring that extra bit of happiness.

One approach for including delighters is through the use of variable rewards that seem scarce and unpredictable. Especially games uses this in the form of 'drop crates' or 'loot boxes.' The content is often unknown until a player opens it. But a delighter may also come in the form of a compliment or an exclusive invite to some event.

Delighters are perhaps the opposite of Bitcoin. The Bitcoin platform is predictable and works according to rules. Delighters work best when not expected and happen at random. Both are positive and work well together but in different ways. This fact does not imply that those who design products and services on top of Bitcoin should not use this. Quite the opposite. There are infinite opportunities for applying delighters and show that using Bitcoin can be fun and exciting.

Dunning-Kruger effect

When unskilled people overestimate their competence and performance, that is called the Dunning-Kruger effect. The Dunning-Kruger effect showed that this intrinsic versus extrinsic gap could lead to dangerous situations such as causing harm or losing funds.

Security is not just a matter of math and computer science, but also addressing behavioral aspects and education. Instead, it is better to understand people's thoughts and create new or better solutions for their needs. As for safely backing up seed phrases, there is increasing adoption of Shamir's Secret Sharing to address these practical needs.

One of the most common examples is chopping up a seed phrase, thinking that it will enhance security. When it comes to valuable assets, people tend to take protective measures to secure them from theft or damage. Read more about this on the topic of loss aversion for more information. Unfortunately, sometimes the wrong types of measures are being used due to lack of understanding. The result of this could lead to the exact opposite and total loss of the assets people willing

to protect. One such example is how some people try to add extra layers of protection to store their seed phrase. The seed phrase, containing a list of back-up words for recovery, is often stored offline and put away safely. Yet some people are afraid of this list being stolen or damaged when put into one place. A common bad practice is to cut this list of words into multiple parts and store them in different locations. But what these people do not realize is that by cutting them up, they increase the chance of losing or destroying a part of this list. And when one part is missing, the incomplete seed phrase cannot be used for recovery.

Duration effects

Even though time itself can be objectively measured, the perception of time is subjective. Something long may seem quick, and something brief may seem to take forever. The duration effect pattern allows designers to play with perceptions of time so that the recollection of a situation tends to become more positive.

Theme parks have mastered the arts of this in each step of an attraction. By entertaining and keeping customers moving in long waiting lines, they take away their focus on time and waiting. Whereas the opposite is happening for the attraction itself that is short, but very intense, making it appear a bit longer.

When designing for time-consuming experiences, be sure to include indicators in every part of the user-journey process. Allow people to have control over each step, by either opt-out, finish at a later moment, or speed things up by skipping steps. One such example is sending and receiving transactions. Some may take minutes, where others may take hours to verify. Although Bitcoin has it's own inner working, how we present and use this information may differ from one solution to the next. When designing for on-chain bitcoin transactions, be informative on how much time some steps may take. When receiving bitcoin transactions, be clear and transparent when and what options people may have to speed things up. Advanced users may understand the concept of transaction fees and network validations. But people new to the technology are more familiar with existing progress bars and status indicators such as; "processing" and "received." When in doubt, pick the option that works best for most people.

Error-handling

When overlooking or underdeveloping proper error-handling, you leave people hanging with little help to get back on the right path. A good error-handling is a combination of multiple good practices such as error-prevention, constraints, confirmation, formulation, forgiveness, and undo-actions. By including some kind

of forgiveness, helps people avoid errors and protect them from harm when they do occur. Assets put onto the blockchain often hold value, and nobody wants to lose value. Solutions that prevent people from making mistakes will keep their customers. Those who don't will search for alternatives.

When designing for proper error-handling, consider the following chronological order. First, design solutions to prevent mistakes, then include warnings for potential problems, followed by options to reverse mistakes when they occur, and when all else fails, add a safety net.

Especially in the Bitcoin system, actions are often permanent. A good practice is to prevent errors by requiring confirmation or verification before performing impactful operations. Triggers are small nudges placed on our regular paths to remind and motivate us to take action. But be careful not to overdo this technique because else they will be ignored or blindly clicked upon after too many repetitions. Another method that can be helpful is adding constraints to the design of products. Adding constraints might help prevent destructive actions if users have not proven to have mastered the knowledge or skills needed to perform specific actions successfully. Related to this are two other design patterns; control and mastery. These explain that the level of user control should be related to the proficiency and experience of the user. But constraints may also be useful to restrict certain users from doing actions that are not approved by other users — for example, one child claiming the entire inheritance without approval from the other spouse. A multi-signature contract is an example of adding rules and constraints. There is another guideline that often functions as a last resort; the confirmation prompt. This dialog acts as the final step before setting things into motion. Although many people find this additional step annoying, for destructive or irreversible actions such as sending a transaction to an immutable ledger, it may act as a last resort. Be clear about what is going to happen and always set the cancel option as the default operation. But even after all preventative measures, people unintentionally make mistakes. By design, Bitcoin is not very forgiving, and most actions are final, making it difficult to support "rollback" or "undo" effects. But with a bit of exploration and imagination, there are exceptions such as the mempool. The mempool is the place where miners can pick and choose what to include (or not) in the next block. Once added inside the Bitcoin blockchain, after about six commits (or 1 hour), changes become near impossible. But when a transaction is still inside the mempool, there is an option to overwrite it with some alterations. Currently, it is up to software wallet providers to include this as an advanced option or not. But what should be included are clear (error) messages. A good (error) message contains the following elements; a short description of what happened, followed by why it happened, and, if possible, a suggestion on some follow-up action. Avoid

technical jargon and write the message in an easy to understand human language. Only computers understand error-codes, so avoid including these in the prompt.

Education & learning

Although more and more people know about Bitcoin, only a tiny percentage understands it well. Bitcoin is many things depending on who you ask it, for they may need and use it for different reasons. But whatever their interest in Bitcoin, practical education and learning is required when using this technology.

Understanding what Bitcoin is will help people try it out. Using it without understanding it, may result in losing funds. Bitcoin products can adopt positive mimicry & sequencing: learn by modeling other's behaviors. YouTube tutorials. Instructions. Break it down into smaller tasks (setting up a wallet).

At the moment, education and learning are still a bit of an afterthought. The past has shown that most occurring security breach for people losing bitcoins are not 51% attacks, but simple avoidable human errors and mistakes. In most cases, people should have some basic or even advanced understanding. But who teaches them? Ideally, schools will be teaching the basics of Bitcoin. And hopefully, parents also educate their children about money and cryptocurrencies at home. And finally, exchanges and wallet providers should be offering the basics already. Unfortunately, not everybody is interested in macro-level economics, the creation of money, decentralized networks, privacy, or financial sovereignty. Like politics, these things can be too conceptual and too far off people's daily life, or so they believe. But the fact is that people could lose stuff. In Bitcoin, things are irreversible thanks to the immutable blockchain. In Bitcoin, people become their banks, along with all of the responsibilities of a bank. That is why if people want or need to use Bitcoin, they must know what they are doing and the best way of doing it. As for the companies who wish to act as an interface between people and the Bitcoin network, this can be an excellent opportunity to help onboard new people and build long-lasting relations with your products and services.

Factor of safety

This pattern states that the number of safety measures should correspond to the level of uncertainty in the design parameters, and vice versa. If the impact of something going wrong is very small, do not add additional safety and security measures, which only decreases usability.

Small payments in shops should be easy and fast. Large amounts should emphasize safety and security.

Bitcoin is very well known for being the most secure cryptocurrency network with the support of over a hundred million terra hashes every second to process and validate network transactions into the blockchain. Not even the most powerful supercomputers combined can compete against this. But with a market cap worth in the billions of dollars, it is no surprise that security is a top priority for storing, sending, and receiving value.

Feedback loops

Feedback occurs when outputs of a system are routed back as inputs as part of a chain of cause-and-effect that forms a circuit or loop. The system can then be said to feed back into itself. Simple causal reasoning about a feedback system is difficult because the first system influences the second, and the second system affects the first, leading to a circular argument.

Feedback loops work by removing uncertainty and doubt. People who see their actions modify subsequent results are more engaged.

A feedback loop is a cycle in which output feeds back into a system as input, changing subsequent outcomes. Without feedback, people may become insecure and helpless. Feedback loops keep people interacted and engaged in situations in which we see our actions modify future results. Games are perfect examples of continuous actions and reactions. But when tasks feel unimportant or boring, feedback loops may become counterproductive and decreases people's attention and motivation to complete tasks. Positive mimicry is that we learn by modeling our behavior after others. Tutorials often use feedback loop for demonstrating the use of a product or service. This way, people can simply redo the same steps, as seen in the example. When adding feedback loops, make sure they add value or reduce risk. Also, make them feel instant. If it takes more than 10 seconds, then consider adding an intermediate step to show that something is happening. A simple message or indicator indicating that a transaction has been received but not yet processed is often enough.

Let people quickly onboard your products and services. Positive feedback loops stimulate learning and growth. Feedback loops are essential after the user takes action, such as sending, receiving assets.

Flexibility trade-offs

As the flexibility of a design increases, the usability, security, and performance of the design decrease. Related to this is the concept of feature-creep. With software, it is easy to add new features and generalize functionality, but very

hard to remove something which is already in there. The problem with this is that more features require more mental strain for users. But also, developers will have a more difficult time managing complexity and keeping the code clean and error-free. Managing complexity is one of the most challenging things to do.

In an ever-demanding world, people expect everything to be possible. Yet, in practice, there are always trade-offs to make. Solutions that function as a jack-of-all-trades are also a master of none. Pleasing everyone simply means that everyone will need to make compromises, and nobody ends up happy. Specialized solutions that excel at just a few core beliefs will always find their target audience. The less you change on these core beliefs; the more people stay as brand evangelists.

Bitcoin's approach is to be very strict in adding new features to the code. Much easier is it to add a little bit of flexibility in the base layer, which allows much more flexibility in the layers above it. But most of the changes are focused on optimization regarding increased security, privacy, and transactions.

Form follows function

This pattern states that the shape of an object should primarily relate to its intended function or purpose. If not, then often, the interactions and overall experience will suffer from aesthetic compromises. Although this principle is mostly associated with the architectural design of buildings or industrial product design, it is increasingly used in digital design as well. The effect of this pattern is to create awareness that design should not be confused with art, wherein every form and shape is allowed. Design, on the other hand, is the creation of intent. It has to have a purpose other than itself. If a function is well-executed, it can be both useful as well as beautiful.

Mobile-first approach. Mobile devices are a standard technology around the world and are the thing that users use every day. Developers are increasingly building solutions for mobiles. App stores have a better set of rules and protocols to clarify what can be done and protect users from scams, mobile devices, and operating systems have better-designed security environments and built-in 2FA (even helped by Fortnite).

The crypto industry has, until now, been a desktop-first industry. It is inconceivable that this remains so when the most used computing devices are mobile. When designing products and services, consider using both the optimal as well as the most practical context. Consumers will most likely use their mobile devices for small payments on-the-go. But more significant amounts are more

often a combination between a dedicated hardware-wallet and a desktop application to safely set up, store, and manage funds coming from exchanges. Online companies such as stores and exchanges may use a desktop as well, but physical retailers might be better off with dedicated tablet-sized terminals. Each participant in the network has a preferred method of interaction.

Game theory

Game theory is a branch of applied sciences, and economics that looks at situations where multiple parties make decisions in an attempt to maximize their returns. Systems can be designed in such a way to either stimulate competition between single parties (zero-sum game) or to stimulate cooperation where multiple parties will benefit.

Game theory can help motivate certain behaviors within a situation. Systems which do not include a substantial benefit on strategic decision making, often lack fewer incentives for parties to participate or take actions. However, people dislike being overly-controlled and losing their freedom of choice. This feeling might lead to people leaving or abandoning the game-theoretical system altogether.

One of the most known collaborative game theory mechanisms in Bitcoin is mining. The system incentivizes miners to run a mining node and compete against other miners. Those who validate transactions, and solve the nonce problem, need to find ways to maximize their returns strategically. As a result, the incentives given to the miners benefit the Bitcoin ecosystem as a whole for having a very secure network.

Gamification

People are more likely to engage in activities in which meaningful achievements give them recognition for their work. Gamification techniques stimulate people's natural desires for socializing, learning, mastery, competition, progress, status, and self-expression. The goal of gamification is helping people achieve some desirable outcomes. But when using gaming elements for the wrong reasons, with false incentives, they are considered a dark pattern.

Early gamification strategies use rewards for players who accomplish desired tasks or competition to engage players. Types of bonuses include points, achievement badges or levels, the filling of a progress bar, or providing the user with virtual currency. Making the rewards for accomplishing tasks visible to other players or providing leader boards are ways of encouraging players to compete.

Bitcoin is full of gamification elements, often created by the community. One such example is the prestigious 1 million club, for holding at least 21 bitcoins. Another example is the creation of vanity-addresses, where people specifically try to include certain words or numbers within their bitcoin address.

Humor effect

People enjoy and more easily remember humorous or outrages situations. Only a small percentage of companies add a bit of humor or to their products and services. Yet nearly everybody likes to laugh. When done right, it can boost the likeability of your brand. But get it wrong, and it may hurt the brand perception.

Memes can be particularly supportive during harsher times to lighten up the mood. As a brand, it is good to use humor effect only in the most positive way. Particular forms of humor, such as sarcasm or irony, may not be appreciated by everybody. Sometimes the most exciting and smart jokes are the ones that also contain a message related to a particular task or activity. As a tip, be careful not to put humor into every aspect of the design. Use it sparingly or make people make a little effort to get to the joke. Puzzles and cryptography have often been a good match.

Probably the best examples of humor within the Bitcoin ecosystem are the use of memes. These images, videos, or pieces of text, are typically humorous and spread rapidly by Internet users, often with slight variations of the original material. Memes work very well because they are concise in their message; nearly everyone can create and share often strengthens like-minded communities.

IKEA effect

The IKEA effect comes from the name of Swedish retailer IKEA, which is known for selling unassembled boxed furniture. By putting things together, people feel a sense of accomplishment and fulfillment when they succeed. The items they bought are valued higher by those who put additional energy into building it. This subjective added value by doing things can be applied to many more aspects to drive behavior.

One way to use this principle is by allowing people to create or modify things within your product or service so that it becomes more personalized and valued by the effort they put into it. Customizing layouts, background, or allowing personal images or texts take little effort, yet have a significant effect on people appreciating the product or service. Another way is allowing people to build and extend products such as wallets or exchanges so that they become valuable for these persons through the work they have done.

Things that people have helped make, whether software or digital assets, they place a level of ownership over. Collaborative tools and services such as GitHub or Fiverr allow people to work on Bitcoin's products and services. Open marketplaces may help more people work on creating better products as well as promoting their skills and services as professionals.

Inclusion

In the past, accessibility was considered when designing products or services for people with disabilities. The scope for inclusion has broadened a lot in the last couple of decades. Nowadays, it has become common practice to embrace accessibility as part of everyday design. Some differences between individuals may be physical of body or place, but inclusion also concerns about the diversity of beliefs, thoughts, and feelings.

Creators who adopt inclusion into their products and services will be able to make a major difference and impact on people's lives. Designing for inclusion may end up being a key differentiator until this is adopted by every competitor. Not focussing on inclusion may very well negatively affect adoption and retention. But the first step to inclusion is to ignore the way things currently work for us and to try achieving the same things with one handicap at a time. This way, you will find out where the barriers are and how to fix them.

One of the major effects of not considering accessibility is exclusion. And that is the opposite of what Bitcoin stands for. Designing for accessibility is not easy because there are many types of barriers. Some barriers can be physical disabilities, which means a loss or limitation to a physical function that may affect a person's mobility, dexterity, or stamina. Other barriers can be sensory disabilities, which affect one or more senses like sight, hearing, smell, touch, taste, or spatial awareness. Or mental barriers that are related to skills, knowledge, or proficiencies. And not to forget contextual barriers like laws, regulations, social conventions, access to information, and more. Keep in mind that all kinds of people benefit from well-designed implementations, not just those who need additional help.

KISS

The acronym KISS stands for "keep it simple, stupid" or "keep it stupid simple" and was noted as a design principle by the U.S. Navy in 1960. One of the problems today is not the lack of, but the excess of information. When there is too much information to process, it may lead to indecisiveness, more complexity, and an

increase in decision time. The KISS principle states that simple designs work better and are more reliable.

The advice is to hide complexity from the end-user. Be careful when adding new features. Consider if these features are core or non-core features that people will use every day. Use the opt-in methodology for non-core features.

For Bitcoin, different levels of simplicity are related to the level of control and self custody people want to have. With each increasing level, more knowledge and experience are required to become in full control. At the top level, it starts with basic Bitcoin knowledge. Since everything is decentralized and no single company owns or controls bitcoin, getting the right information can be challenging. Most likely, the knowledge they received is the information from the media, which isn't always the closest and most neutral source of information. At the second level are basic interactions such as purchasing, transacting digital assets. Typically exchanges act as a starting point for many new people getting into space. But unlike a physical exchange, everything is digital and online. And sometimes, before people can exchange, they are required to supply the exchange with proof of their identity and residence. It is typically taking some hours or days to complete. Then at the third level starts self-custody, which includes safely and securely creating and managing a wallet with passwords, seeds, keys, and addresses. The fourth level includes mastery, which includes additional steps and measures to enhance privacy and security, such as offline storage and mixing services. The last level is full autonomy and custody by being part of the network and managing transactions on a personal node.

Legibility

As humans, we are very dependent on our sight when it comes to digital processing information. Much of the information is presented on a screen. When designers are not optimizing the content for the right context, it makes it unnecessarily difficult to take in and process. Legibility is the visual clarity of text, generally based on size, typeface, contrast, line length, and spacing. But most of the same elements for text apply shapes and forms as well.

When designing highly secured solutions like hashed transactions and private keys, keep in mind that humans prefer patterns which they are familiar with them and easy to read, process, and remember. Good practices are to convert unique strings into human-readable words, splitting large strings into smaller chunks, highlighting certain aspects, and validating or correcting complex information.

In general, they are still dependent on the options and functionality that the network provides. One example is how bitcoin addresses are represented by default; they typically consist of a large string of letters and numbers starting with a 1, 3, or bc1. The latter starting with bc1 is a good example of a new native segwit address, based on the Bech32 standard. Besides the performance benefits (smaller transactions) or financial benefits (lower transaction costs), this standard also includes some usability improvements. The first being that no mistakes on capital letters can be made. For example, the letter O is removed because this looks like the number 0. But also able to correct mistakes, via validations & checksum. Or a fixed-length check incase someone entered too many or too little. But perhaps even more practical solutions come from human-readable addresses. This approach lets people choose a unique domain that they can link to their public address. This way, they can simply remember and give this name (like satoshi.eth or satoshi.crypto) to someone who uses a wallet that supports this kind of blockchain domain names.

Literacy

Literacy is traditionally defined by dictionaries as the ability to read and write, although broader interpretations insist that any particular instance of reading and writing is always taking place in a specific context, as the proliferation of concepts like "conventional or basic literacy, functional literacy, digital literacy, media literacy, legal literacy, computer literacy, medical literacy, and information literacy" suggest. The general consensus among researchers that literacy always includes social and cultural elements is reflected by UNESCO's inclusion of numbers, images, digital media, cultural consciousness, and other means of understanding, communicating, gaining useful knowledge, problem-solving, and using the dominant symbol systems of a culture in its definition of literacy. The concept of literacy is expanding across OECD countries to include skills to access knowledge through technology and the ability to assess complex contexts.

More education is needed. On schools, at home, amongst friends, government, and social media.

When considering literacy in Bitcoin, we refer to the ability to understand Bitcoin.

Loss aversion

We hate losing or letting go of what we have (even if more could be had). In cognitive psychology and decision theory, loss aversion refers to people's tendency to prefer avoiding losses to acquiring equivalent gains: it is better not to lose $5 than to find $5. The principle is very prominent in the domain of economics. What distinguishes loss aversion from risk aversion is that the utility

of a monetary payoff depends on what was previously experienced or was expected to happen. Some studies have suggested that losses are twice as powerful, psychologically, as gains. Loss aversion was first identified by Amos Tversky and Daniel Kahneman. Humans may be hardwired to be loss averse due to asymmetric evolutionary pressure on losses and gains: for an organism operating close to the edge of survival, the loss of a day's food could cause death, whereas the gain of an extra day's food would not cause an extra day of life (unless the food could be easily and effectively stored).

Do not trade, but dollar-cost-average. For spending, use lightning and small amounts.

Loss aversion happens at trading. But it also prevents people from spending bitcoins, because it is considered more precious than fiat currencies.

Metaphors

The most powerful approach to learning something new is to tie it to something we or are familiar with or already know. This prior knowledge of how something works is also called a mental model. When people interact with a new object or person, they recall previous experiences and mental models that may be relatable to the new situation.

When designing new products and services, use familiarity bias and conceptual metaphors so that people will have the right expectations on how it is used.

To help people understand what Bitcoin, it is best to find similar generic models to which people can relate. Unfortunately, in the last decade, some poor mental models have been chosen to explain how people should interact with Bitcoin's products and services. One example is the metaphor used to manage bitcoins. Nearly everyone knows this as a cryptocurrency wallet. And although this is used to send and receive money, it is a common misconception that wallets hold people's funds. This, however, isn't true, but what they do contain are the private and public keys. Therefore perhaps a better metaphor would have been a keychain to gain access to funds stored in the blockchain. Another metaphor often for bitcoin is being digital gold. It helps people frame the concept better and how to use it. But if the future decides to use it in a different way, the metaphor is no longer correct.

Modularity

Managing system complexity by dividing large systems into smaller, self-contained systems. Modular design, or "modularity in design," is an approach

(design theory and practice) that subdivides a system into smaller parts called modules that can be independently created and then used in different systems. A modular design can be characterized by functional partitioning into discrete scalable, reusable modules; rigorous use of well-defined modular interfaces; and making use of industry standards for interfaces. A modular system with this limited modularity is generally known as a platform system that uses modular components. Examples are Auto platforms or the USB port in CE platforms. In design theory, this is distinct from a modular system which has higher dimensional modularity and degrees of freedom. Modular system design has no distinct lifetime and exhibits flexibility in at least three dimensions. In this respect, modular systems are very rare in markets. Mero architectural systems are the closest example of a modular system in terms of hard products in markets. Weapons platforms, especially in Aerospace, tend to be modular systems, wherein the airframe is designed to be upgraded multiple times during its lifetime, without the purchase of a completely new system. Modularity is best defined by the dimensions affected or the degrees of freedom in form, cost, or operation. Modularity offers benefits such as a reduction in cost (due to less customization), interoperability, shorter learning time, flexibility in design, non-generationally constrained augmentation, or updating (adding new solution by merely plugging in a new module), and exclusion. Modularity in platform systems, offer benefits in returning margins to scale, reduced product development cost, reduced O&M costs, and time to market. Platform systems have enabled the wide use of system design in markets and the ability for product companies to separate the rate of the product cycle from the R&D paths. The biggest drawback of modular systems is the designer or engineer. Most designers are poorly trained in systems analysis, and most engineers are poorly trained in design. The design complexity of a modular system is significantly higher than a platform system and requires experts in design and product strategy during the conception phase of system development. That phase must anticipate the directions and levels of flexibility necessary in the system to deliver the modular benefits. Modular systems could be viewed as more complete or holistic design, whereas platforms systems are more reductionist, limiting modularity to components. Complete or holistic modular design requires a much higher level of design skill and sophistication than the more common platform system.

When creating new open-source products and services on top of Bitcoin, keep in mind that others might want to look or reuse parts of your code as well. Separate your code into functional units that do one thing. This way, it is easier to collaborate or perhaps even replace this functionality with something new.

One of the biggest strengths of Bitcoin is being an open-source project. This allowed everyone to see, download, and adjust the code wherever they wanted.

But large and complex projects such as Bitcoin, it needs a logical separation of functionality when multiple people are working on certain parts simultaneously. Looking at the Bitcoin code, developers can work independently on several modules and components. Some of the more recognizable components are the consensus rules, network nodes, scripts.

Nudge

A nudge is a way of modifying behavior without restricting options or changing incentives. Nudge is a concept in behavioral science, political theory, and behavioral economics that proposes positive reinforcement and indirect suggestions as to ways to influence the behavior and decision making of groups or individuals. Nudging contrasts with other ways to achieve compliance, such as education, legislation, or enforcement. The nudge concept was popularized in the 2008 book Nudge: Improving Decisions About Health, Wealth, and Happiness, by two American scholars at the University of Chicago: economist Richard Thaler and legal scholar Cass Sunstein. It has influenced British and American politicians. Several nudge units exist around the world at the national level (UK, Germany, Japan, and others) as well as at the international level (e.g., World Bank, UN, and the European Commission). It is disputed whether "nudge theory" is a recent novel development in behavioral science or merely a new term for one of many methods for influencing behavior, investigated in the science of behavior analysis.

A nudge, as we will use the term, is an aspect of the choice architecture that alters people's behavior predictably without forbidding any options or significantly changing their economic incentives. The intervention of nudges must be easy and cheap to avoid. Nudges are not mandates. Putting fruit at eye level counts as a nudge. Banning junk food does not. Add nudges to your products and services where you positively want to help people do the right thing for them or prevent them from making mistakes. When a nudge only serves your interest, refrain from using it, for this can work counter-effective.

The use of nudges is applicable mostly for products and services build on top of the Bitcoin system because that is where most of the interaction happens with people. But when looking at Bitcoin from a holistic view, then any form of communication may include nudges. For some, this may start with the Bitcoin website, social media, or cryptocurrency exchanges. These offer some great opportunities to help people understand why Bitcoin is, in some ways, a better alternative for a currency than fiat money. A nudge could be a reference or link to the Bitcoin whitepaper or to books written about economic models, to gain a better understanding of why.

Ownership bias

We more highly value goods or services once we feel like we own them. We also feel more connected to people who share the things we believe in or own. In psychology and behavioral economics, the endowment effect (also known as divestiture aversion and related to the mere ownership effect in social psychology) is the finding that people are more likely to retain an object they own than acquire that same object when they do not own it. This is typically illustrated in two ways. In a valuation paradigm, people's maximum willingness to pay (WTP) to acquire an object is typically lower than the least amount they are willing to accept (WTA) to give up that same object when they own it—even when there is no cause for attachment, or even if the item was only obtained minutes ago. In an exchange paradigm, people given a good are reluctant to trade it for another good of similar value. For example, participants were first given a Swiss chocolate bar were generally unwilling to trade it for a coffee mug, whereas participants were first given the coffee mug were generally unwilling to trade it for the chocolate bar. A more controversial third paradigm used to elicit the endowment effect is the mere ownership paradigm, primarily used in experiments in psychology, marketing, and organizational behavior. In this paradigm, people who are randomly assigned to receive a good ("owners") evaluate it more positively than people who are not randomly assigned to receive the good ("controls"). The distinction between this paradigm and the first two is that it is not incentive-compatible. In other words, participants are not explicitly incentivized to reveal the extent to which they truly like or value the good. The endowment effect can be equated to the behavioral model Willingness to Accept or Pay (WTAP), a formula sometimes used to find out how much a consumer or person is willing to put up with or lose for different outcomes.

Although ownership bias can lead to creating healthy communities and brand-loyalty, there are also darker sides to keep in mind. Taking a negative approach could lead to diversity and toxic tribalism. It is important to invest, especially in the things which we share with others and respect the differences we have.

Bitcoin is all about sovereignty and ownership of digital assets through private keys. Andreas Antonopoulos also has a famous quote about this saying; “Your keys, your bitcoin. Not your keys, not your bitcoin.”. This is a common warning to new people who leave their bitcoins at third-parties like exchanges or custody funds. When these get hacked or someone who does have access, decides to go AWOL, then this often leads to loss of funds without any means of getting their funds back. Creating awareness for ownership bias is good. Proof of Keys is an

example of a yearly event on January 3rd, to everyone to withdraw their funds from exchanges into wallets of which they own their private keys. By doing so, people are also made aware that they are responsible for safekeeping the assets they control and own. This makes people more emotionally invested in the things they own. Endowment effect: We overvalue things that we own, regardless of their objective market value. This is illustrated simply in two examples: people become reluctant to part with goods they own for their cash equivalent and when people are willing to pay less for a good than they are willing to accept when selling it. The endowment effect is an illustration of status quo bias and can be explained with loss aversion and prospect theory. Simply by owning a cryptocurrency, you value it more than you would otherwise. In traditional finance, traders have been known to stick with assets they own even if they become unprofitable simply because of their emotional attachment to them.

Paradox of choice

Having an excessive amount of options in a particular decision can lead to worse outcomes. Choice overload can lead you to question the decisions you make before you even make them, set you up for unrealistically high expectations, and make you blame yourself for any failures. As people, we love to choose from options. And for certain things, this is true. But when it comes to decision-making, studies have shown that we are less likely to make a choice when the number of options increases. We cannot decide and have the urge to postpone. This is also related to another research theory called Hick's law. Hick's law, or the Hick–Hyman law, named after British and American psychologists William Edmund Hick and Ray Hyman, describes the time it takes for a person to decide as a result of the possible choices he or she has: increasing the number of choices will increase the decision time logarithmically.

The general rule is to keep things simple and support shortcuts with a minimum amount of steps or time. Sequencing is an approach that is often used in these cases. We are more likely to take action when complex activities are broken down into smaller tasks. This does not always imply that all steps need to be taken at the same moment. Sometimes a gentle reminder, later on, to finish certain steps is a good option as well.

Giving users too many choices for goods and services to exchange for a utility token may lead them to a bad choice. Technological innovation doesn't stop, and neither does Bitcoin. While moving forward, Bitcoin also holds one foot in the past as it strives always to be backward compatible. This means that whatever was possible in the past, should also be possible in the future. The drawback is that this creates an endless supply of options. Let's take the creation of a wallet, for

example. This is by far the most common exercise when sending and receiving bitcoins. However, in most cases, the beginning user is immediately confronted with the type of wallet they want to create; Legacy, SegWit (P2SH), or HD SegWit (BIP84 Bech32 native). For those who are just starting, this is too many options and too advanced options, and some may choose to exit.

Peak-end rule

We judge our past experiences almost entirely by their peaks (pleasant or unpleasant) and how they ended. The peak-end rule is a psychological heuristic in which people judge an experience largely based on how they felt at its peak (i.e., its most intense point) and its end, rather than based on the total sum or average of every moment of the experience. The effect occurs regardless of whether the experience is pleasant or unpleasant. According to the heuristic, other information aside from that of the peak and end of the experience is not lost, but it is not used. This includes net pleasantness or unpleasantness and how long the experience lasted. A peak-end rule is thereby a specific form of the more general extension neglect and duration neglect.

When creating products and services, ask yourself which moment do you want people to remember. Especially the beginning and the end of interaction between your customer and your product are moments that will be most remembered. Moments such as sending and receiving digital assets are great for bringing a smile to people's faces. Or if this style does not suit your audience, think about what they do want to remember. Perhaps you should focus on reassuring people and keeping them updated along every step of the process after sending a transaction.

Within Bitcoin, there are many opportunities for including peak-end rules, yet they are scarcely implemented. Luckily many brands are successfully using this technique to optimize their customer journey by ending on a high note. Even banking apps are not shy of using this pattern to delight people with funny quotes or animations after they successfully paid payment requests from friends or family.

Privacy

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby express themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals. When something is private to a person, it usually means that something is inherently special or sensitive to them. The domain of privacy partially overlaps with security, which can include the concepts of appropriate

use, as well as protection of information. Although the level of privacy protection law differs from country to country, it is advisable to adopt privacy by design by default.

Within Bitcoin, the community needs to think hard about which path to take in the future. Since Bitcoin not restricted to borders or laws, the community decides which approach is best for those who would like to make use of Bitcoin. Both transparency, as well as privacy, have their benefits. Several projects, such as Monero and Grim, have their privacy protection mechanisms. But they also allow the user to choose if they would publicly share parts of information with others.

Bitcoin from the beginning includes a high-level of privacy by hiding the identity behind anonymous private keys and addresses. However, when someone's identity can be linked to a certain address, a lot of information becomes exposed through the traceability of transactions on the blockchain. Full privacy is not yet implemented, and many initiatives are currently being explored and tested.

Readability

The ease with which text can be understood, based on the complexity of words and sentences. In natural language, the readability of text depends on its content (the complexity of its vocabulary and syntax) and its presentation (such as typographic aspects like font size, line height, and line length). The goal of higher readability is to ease the reading effort and speed for any reader, but it is especially important for those who do not have high reading comprehension. In readers with average or poor reading comprehension, raising the readability level of a text from mediocre to good can make the difference between success and failure of its communication goals.

When designing products and services, be very clear who your target audience is and adjust your vocabulary accordingly. The second part is about keeping the information as simple, short, unique, and relatable as possible. Be mindful of every word you put into your product or service. But allow people to take a sidestep if they would like to know more about a certain topic.

Readability within Bitcoin is still a big issue for newcomers. Almost immediately, they are faced with technical terminology, which is very helpful for developers, but counterproductive to people simply using it. The concept of "balance" within a bitcoin wallet, is a good example which is helpful for people because this relates to something they already know. However, under the hood, what a user sees as the balance is a collection of unspent transaction outputs.

Recognition over recall

It is easier to recognize things we have previously experienced than it is to recall them from memory. Many situations nowadays require us to recall information such as passwords or codes, each different from each other. Yet all of these adds up to the mental and physical effort required to complete a task. There are two types of performance load; cognitive and kinematic. Cognitive is the mental effort, and the kinematic load is physical steps.

Different circumstances require different solutions. However, whenever possible, allow people to recognize solutions based on recognition rather than recall the entire piece of information. Support suggestions such as the format of the information or auto-complete words from fixed lists such as seed phrases. And because people are mostly visually oriented people, sometimes recognizing images work better than recognizing words, yet the level of security remains the same.

Although the Bitcoin system heavily relies on the use of private key cryptography, it is not doable to remember long hashes of information. Instead, they are stored inside wallet applications, which by default, require a passphrase or number to access. There are brain wallets that refer to the concept of memorizing a seed phrase, which can be used to access funds on the blockchain indirectly. However, if a brain wallet is forgotten or the person dies or is permanently incapacitated, access is lost forever. Regardless if people remember their seed or not, the fact that words can be used to restore public and private keys is an improvement from a human perspective.

Reinforcement

The term reinforce means to strengthen and is used in psychology to refer to anything stimulus which strengthens or increases the probability of a specific response. In behavioral psychology, reinforcement is a consequence applied that will strengthen an organism's future behavior whenever that behavior is preceded by a specific antecedent stimulus. This strengthening effect may be measured as a higher frequency of behavior (e.g., pulling a lever more frequently), longer duration (e.g., pulling a lever for longer periods of time), greater magnitude (e.g., pulling a lever with greater force), or shorter latency (e.g., pulling a lever more quickly following the antecedent stimulus).

There are four types of reinforcement: positive, negative, punishment, and extinction. We'll discuss each of these and give examples. Positive Reinforcement - the examples above describe what is referred to as positive reinforcement. Think of it as adding something in order to increase a response. For example, adding a

treat will increase the response of sitting; adding praise will increase the chances of your child cleaning his or her room. The most common types of positive reinforcement or praise and rewards, and most of us have experienced this as both the giver and receiver. Negative Reinforcement - think of negative reinforcement as taking something negative away in order to increase a response. Imagine a teenager who is nagged by his mother to take out the garbage week after week. After complaining to his friends about the nagging, he finally one day performs the task, and to his amazement, the nagging stops. The elimination of this negative stimulus is reinforcing and will likely increase the chances that he will take out the garbage next week. Punishment - punishment refers to adding something aversive in order to decrease a behavior. The most common example of this is disciplining (e.g., spanking) a child for misbehaving. The reason we do this is that the child begins to associate being punished with negative behavior. The punishment is not liked, and therefore to avoid it, he or she will stop behaving in that manner. Extinction - when you remove something in order to decrease a behavior, this is called extinction. You are taking something away so that a response is decreased.

Research has found positive reinforcement is the most powerful of any of these. Adding a positive to increase a response not only works better but allows both parties to focus on the positive aspects of the situation. Punishment, when applied immediately following the negative behavior, can be effective, but results in extinction when it is not applied consistently. Punishment can also invoke other negative responses, such as anger and resentment. A good example of positive reinforcement is rewarding people with cryptocurrencies after learning about them, what problem they solve, and how to use them. Another example is reminding people to store or backup their private key or seed phrases. Some people may find these reminders annoying, but they are rewarded for doing something they will benefit from later on.

Reputation

We care more deeply about personal behaviors when they may affect how peers or the public perceive us. In online social contexts, sharing actions with others helps encourage good conduct. People build a reputation through things like sharing information, connecting people, and keeping a record of their activities. And through our interactions, we assess if they either enhance or diminish our standings relative to others and our personal best.

Building a good reputation takes time and hard work. Yet when you abuse your reputation and lose trust, the negative effects occur in the blink of an eye. But good reputable people may act as examples to new people willing to enter the

space and seeking for information and guidance. With all the distrust and scams that happen on the internet, finding people with a good reputation is difficult. More people are needed to help others by taking the time and teaching them to become self-sovereign in this space, and hopefully becoming trustworthy and reputable people themselves.

When creating a new solution like Bitcoin, focussing on the technology is not enough. Although incentivized, people did not know for sure if this internet money was going to fly. Back then, using Bitcoin was much harder than it is today, and there were nearly no instructions, videos, or exchange support. The only thing people had was each other chatting on forums, via email and IRC channels. You often had to trust someone on the other side, to exchange bitcoins for dollars, which could take days or weeks to process. Eventually, out of those interactions and conversations with other people, trust and reputation were earned. And build on this intangible reputation, others would follow, and the Bitcoin community would grow to the millions today.

Scarcity

We infer value into something that has limited availability or is promoted as being scarce. Things become more desirable when they are in short supply or occur infrequently. Given a choice between action and inaction, a limited time/duration to respond increases the likelihood that people will participate.

Scarcity focusses on limited resources such as time, energy, art, exclusivity. The harder it is to obtain, the desirable something becomes. Scarcity in design can help create focus and awareness on what is considered valuable and what is not. Something which cannot be bought is time. Every person has only a limited amount of it. Therefore in creating solutions, be careful not to waste this valuable asset with poor designs that hinder people from reaching their goals.

There have been many forms of money in history, but in some ways, bitcoin works better as sound money than others because, in the open bitcoin market, there will never be more than 21 million bitcoins ever in existence. Another characteristic of bitcoin is the deflationary production rate of newly minted bitcoins, which will be cut in half, approximately every four years (210,000 blocks). Unlike any other asset, this cannot be changed and makes it easy to predict. Especially bitcoin-miners like this fact because they can build their business around this certainty.

One of the key features of bitcoin is being a scarce asset. Unlike any other fiat currency, no more than 21 million bitcoins can ever be created. Combine this with

a deflationary supply, where the supply of new bitcoins is halved nearly every four years, and you end up with a difficult to get asset over time. For some, obtaining one single bitcoin and thus to belong to the 21 million-club, is perceived as very desirable. We naturally desire things that are perceived as exclusive or belonging to a select few.

Seamlessness

Seamlessness in design is about the ease of switching between one product or service to another. Or when switching from one device to another. Often this occurs when the functionality of one product or service stops, and another continues.

When creating a product or service, look beyond your solution. Consider the whole end-to-end customer journey to map which other products and services people may be used in combination with your own. Then adapt your solution accordingly to either receive (import) information from other apps or send (export) information to other applications. When creating seamless services, do not take the 'zero-sum game' approach, where third party solutions are considered competitors. Instead, imagine that people love your product, but use it in conjunction with other functions that you may not have heard about or be offering. For example, people using your wallet in combination with a third party bookkeeping program for filing tax.

Bitcoin, in a way, acts as a platform for many applications and services which are built on top of it. One example in which devices interact with each other is by sharing QR-codes, which contains information such as private keys or wallet addresses.

Security

Security nowadays needs no introduction. Security by design has been the default for nearly every professional developer when it comes to the protection and processing of data. With our world becoming ever more digital and dependent on digital technologies, things can go seriously wrong when certain data is being misused or manipulated. The impact of security breaches is extremely high for both individuals as for nations as a whole.

From a technical perspective, there are a lot of cool privacy and security related features being created for Bitcoin. Yet it is easily overlooked that the biggest security risks are not quantum computers, but simple human mistakes. The greatest risk for security is complexity. When creating new security measures, it is good to keep in mind that humans with all of their capabilities, but also their

disabilities need to use Bitcoin. Increasing security also implies making it easier and not harder for people to use. Decide which security measures are mandatory and which ones are offered optionally. The level of usability should be according to the proficiency and experience of the user. And the level of security should be proportional to the value. The Bech32 standard is an example wherein several safety checks are included to help a user recover from entering mistakes.

Security has been one of Bitcoin's greatest achievements. With a dozen mining farms competing for 24/7 for a block reward and securing a ledger from malicious transactions. But do not forget the strong cryptographic hash functions which are used for data encryption.

Self-expression

People seek opportunities to express their personalities, feelings, or ideas. How we share and express ourselves to others forms the basis of our personality, as understood by everyone but us, and sets the tone for our entire lives.

When taking a look at all the products and services to build on top of Bitcoin, the possibilities of expressing oneself are endless. On the blockchain, everything of value can be an asset. And ownership of data is controlled by whoever controls the private keys. This means that sharing and removing data based on a self-sovereign identity is much easier than asking a company to remove all personal related data. Or the opposite, centralized entities find it harder to prevent people from expressing themselves on decentralized systems like Bitcoin.

Within Bitcoin, self-expression is tightly related to self-sovereign identity. Behind every address and key, some people use the Bitcoin system as a way to share value. Where they spend it on is up to them. Bitcoin by itself is censorship-resistant and allows people to choose; however, they want to use it. In this sense, bitcoin is a way of expression and communication.

Sensory appeal

We are engaged by and more likely to recall things that appeal to multiple senses.

Where Bitcoin may be disappearing into the background, on the edges, there is much to be gained. After all, people will bring their mental models of how things build on top of Bitcoin's works. Depending on what type of device people are using, more or fewer options are available. A modern smartphone app has multiple input and output possibilities which can be used when using bitcoin as a currency. As a designer, consider integrating additional cues besides visual information on a screen. Perhaps vibrate, flashlight, or play a sound when a

transaction is sent or received — this way, people don't need to keep an eye on their phones all the time.

The Bitcoin network is probably the least expected place to apply sensory appeal. Eventually, Bitcoin should, like the Internet, be omnipresent but invisible and disappeared into the background. The interactions we now see with the network are often the results of poor user-experiences.

Serial position effect

The serial position effect is the tendency of a person to recall the first and last items in a series best, and the middle items worst. The term was coined by Hermann Ebbinghaus through studies he performed on himself and referred to the finding that recalls accuracy varies as a function of an item's position within a study list. When asked to recall a list of items in any order (free recall), people tend to begin recall with the end of the list, recalling those items best (the recency effect). Among earlier list items, the first few items are recalled more frequently than the middle items (the primacy effect).

In the ideal situation, most people should not have to see and use this kind of complex information. Either they are hidden or replaced by human-readable substitutes such as unique domain addresses for all types of bitcoin addresses. In cases where this is not possible, using serial positioning can help reduce cognitive load for people. A technique called chunking helps splitting up large pieces of information, like a hash, into several smaller pieces, often separated with a whitespace character. This way, people often look at the first and last pieces to faster recognize, compare, or validate the information.

Those who are familiar with sending and receiving bitcoin transactions know that the Bitcoin system is heavily based on cryptography. To users, this manifests itself by large, complex, and seemingly random strings (which they are not). These strings are everywhere, such as private keys, bitcoin addresses, and transaction hashes.

Set completion

The closer a collection is to be complete, the more we desire to collect all pieces. People like to see the whole image completed and dislike incomplete sets. Where there is interest, people like to amass units that add to or complete a set.

When creating sets or rewards, be sure that they add value to the user. Meaningless rewards are not motivating enough to keep people interested. Also, consider the condition under which rewards are received. When people mined

bitcoins on their laptops, they held less value then compared the bitcoins, which are mined with dedicated ASIC miners because it is much harder now, then it was in the beginning.

In Bitcoin, the scarcest assets are the 21 million bitcoins. In all reality, this is a set that nobody can fully complete. Yet many people strive to possess at least one single bitcoin. However, bitcoin is just one application on top of the Bitcoin network. When creating colored coins, new sets representing any digital asset can be created. Another standard known as ERC721 seems to be getting more traction for creating unique, non-fungible tokens. These tokens can represent anything of a limited edition, such as digital clothing or virtual land ownership.

Standardization

Create standards so that others can adopt them and work seamlessly together. The more people and products follow a certain standard, the more it benefits the ecosystem. Producers benefit from standardization in a way that may reduce the cost of not reinventing the wheel. Consumers also benefit from standardization because it allows them to recall and apply previous experiences to something new.

A standard is often agreed upon by multiple parties when a certain implementation has proven to work well between the producers. They try to find a balance and agree upon the quality, cost, and flexibility. However, in the end, it is up to the consumer to choose which standard works best for them.

Bitcoin and other cryptocurrencies are continuously experimenting with new and different solutions for different problems. The cryptocurrency Monero, for example, has a different standard to mnemonic seeds, compared to Bitcoin's BIP39 standard, which includes The English-language wordlist of 2048 words. From a consumer perspective, one single standard for all managing different blockchains within one wallet would be much appreciated.

Status quo

The status quo states that people tend not to change their behaviors unless they are incentivized. This implies that adopting complex technologies like Bitcoin can take a long time before being used. Global changes and adoption happen slowly for good reasons. If everything in the world were in constant flux, humanization would collapse. One could argue that this is already happening due to accelerators like the Internet.

When designing something new, it is good to keep in mind the reasons why people should come into action and show the benefits for their effort or mention the drawbacks if they do not. To help people on board more easily, consider using an easy onramp from one system to another. And allow the option to switch back if they have a change of heart.

Bitcoin so far has also challenged the status quo quite a bit. For those in need of something radically different, challenging the current systems is a good thing. But those who do not see any benefits, are inclined to keep things as they are.

Storytelling

Telling and sharing stories is as old as human civilization. Good, vivid, and compelling stories bind people together, informs, or entertains people. Storytelling is a technique often used to add flavor to cut and dry information. It also brings structure, narrative, context, and emotion to the mix, which is often lost in bullet points. When creating a story, people are better at visualizing the information which they are being told. Also, it aids in better recalling information over time.

Short stories can be very helpful when teaching people new things. The bitcoin story is one example, but there are no limits to what a story should be. Typically, every piece of interaction between people and a part of the Bitcoin ecosystem can be eligible for a good story.

The creation of Bitcoin by itself has all the ingredients of a great story. But the media and politics seem to create negative twists around it. Instead, Bitcoin needs more promotional material highlighting the uniqueness and origin stories that deeply hit common people on an emotional level. For this, it is good to look beyond swag, such as t-shirts, but take an example on commercial companies and how they are advertising their brand story. Bitcoin's ecosystem needs more knowledge from marketers to strongly put down an attractive and lovable brand that is unique and of the highest quality.

Value attribution

Value attribution describes our tendency to imbue people or objects with certain qualities based on perceived value, rather than on objective data. We value things when they cost more. Where this undercurrent gets dangerous is in ongoing engagements. Once we attribute a certain value to something, it dramatically alters our perception of subsequent information. Not only that, it affects us even when the value is assigned completely arbitrarily. So once we have attributed

value to something, it is very difficult to view it in any other light. And this has the power to derail objective, professional judgment.

The best strategy to employ here is to be mindful and observe things for what they are, not what they appear to be. Accept that initial impressions could be wrong. Price-models such as stock-to-flow are interesting, but the value of Bitcoin is much more than that, depending on the geopolitical needs of people searching for a solution. When assessing bitcoin's value, consider including the context of why people use it. For some, it may be speculation on scarcity & stock-to-flow. Others may find value in portability, sovereignty, accessibility, privacy, or programmable money. Price follows value.

Once the price reaches new all-time highs, the more coverage it gets from news and media. Also, more people will believe bitcoin is a good investment. Yet the market price and Bitcoin's more objective fundamentals might be two different things. Dr. Julian Hosp, the author of Blockchain 2.0, once said, "every price will eventually come down to its value." With this, he referred that price and value are related, but two different things. An anonymous Dutch financial expert under the pseudonym 'Plan□,' introduced a stock-to-flow model for bitcoin. In this model, he found a high correlation between price and scarcity — nearly every bitcoin-halving causing a decrease in supply and an increase in price valuation.

Dark patterns

The previous chapter about design patterns will help create better and more enjoyable products and services. The effects of not correctly implementing those may lead to annoyed or frustrated customers, but if they need your product without an alternative, then they may still use it. Dark patterns are the opposite of design patterns. The primary focus is to trick people into doing things they would normally not do.

Addiction

How to protect our children from making financial mistakes? Alcohol, drugs, cigarettes are age-restricted for good reasons. What is the best approach to protecting people from creating a harmful addiction?

At a social level, this is something where communities can help people. They should stimulate open conversations about these issues. Sites such as exchanges should include links for help and do KYC checks. Those who have a huge amount of followers should include preventative measures such as warnings.

Speculating on price can be dangerous. 90% lose money. Because of this, they often lost more than they could afford, taking too much of a risk. But even worse, it also affects people's physical and mental health. People have already been going to clinics for this or committed suicide.

Confirmation bias

Confirmation bias is the tendency to search for, interpret, favor, and recall information in a way that affirms one's prior beliefs or hypotheses. It is a type of cognitive bias and a systematic error of inductive reasoning. People display this bias when they gather or remember information selectively or when they interpret it in a biased way. The effect is stronger for desired outcomes, for emotionally charged issues, and deeply-entrenched beliefs.

Instead of focussing on differences, talk about the aspects which are the same or which can be used together to strengthen both. Stimulate the creation of differences. More explorations will lead to more solutions so that everyone may benefit. Share knowledge, people, and code.

The negative happens when people advocate only one coin as the one true solution. This creates toxic communities and maximalism. They act as if it is a zero-sum game with only one winner. Also, sometimes people such as Youtubers

are paid to promote and highlight certain perspectives. This leads to a fear of missing out and limited offers.

Confirmshaming

Were you ever tricked into buying something you regretted afterward? Did they make you feel guilty or pressured at that moment right before you bought it? You may not be the only one who fell for this trick of guilting into opting in. Confirmshaming is when the product or commercial encourages the users to do something "positive" (like subscribing to a newsletter) by shaming them if they won't do it.

Don't tell people they are missing out, or when they were too late. Or worse than you were earlier then they were. Stay humble.

This happens a lot in social media, where people are ridiculed for not taking part. This leads to fomo-ing.

Dunning–Kruger effect

Do you think you know everything there is to know about something? Well, think again. Often the more you learn about something, the more you find out that you about the things that you do not know yet. The Dunning-Kruger effect is a cognitive bias in which people think they are smarter than they are, and because they live in this illusion for long - they never admit the reality that they may be lacking. David Dunning and Justin Kruger described this phenomenon, hence the name.

Promote and include information and education. Show how many pieces there are to show the gaps in people's lack of knowledge.

People overestimate their assumptions and knowledge on Bitcoin, be it price or development speed. Bitcoin is complex and is a non-correlated asset.

Friend Spam

Spam (not the meat) is still one of the most effective ways of bringing certain products or services under attention. Yet, most people are not eager to receive these messages because often they are more harmful than helpful. In some cases, you yourself are responsible for giving personal information away to third parties who may contact you in the future with "exciting new opportunities." But in some cases, your friends or contacts may be responsible for giving away your contact information in exchange for a small benefit. When they do, they befell for the friend spam pattern.

The product asks for your email or social media permissions under the pretense it will be used for a desirable outcome (e.g., finding friends), but then will spam all your contacts in a message that claims to be from you. Focus on natural adoption, rather than peer-pressure.

This often happens when ICO's or other companies want to spread their message in return for free coins, discounts, or other benefits.

Hidden Costs

Who never fell for a "too good to be true" deal, only to find out that at last step of the checkout process, only to discover some unexpected charges have appeared, e.g., delivery charges, tax, etc.

The way costs are hidden due to the lack of full transparency about all costs along the way.

Just list fees clearly and make them adjustable transaction speed versus cost. Some people are surprised when paying $3,60 tx fees for a $20,00 transfer. Clearly show them why they pay more and offer them a choice between fast confirmation and fees.

Limited time

"Buy today, or wait for another year!" The limited-time practice is often used to create a false sense of urgency. When there is a reason to design for time-critical actions, like people dying or need to take their medicine, then this practice is justified. However, what makes the pattern limited time a dark pattern is because the time-critical aspect is created and driven by the creators of a product or service.

Often used by ICO's, used to create FoMo (fear of missing out). It is also related to a perceived scarcity.

Limited time happens when people are not given enough time to onboard. Allow people the time to do research. Allow people the time to create their own opinions.

Misdirection

The design purposefully focuses your attention on one thing to distract your attention from another. Focus on speed, neglect security.

Misdirection is used for promoting products and services. Often they include what they are better at in comparison, but neglect the things which they are sacrificing.

Be transparent open about the limitations of a system by showing all information. Explain why certain decisions or compromises have been made.

Privacy Zuckering

When you are tricked into publicly sharing more information about yourself than you wanted or intended to, then you may succumb to privacy zuckering. This pattern is named after Facebook CEO Mark Zuckerberg, who lies under scrutiny for giving or selling personal information to third parties. Giving away personal information is not without risks. It can be used for good, but also for bad. Identity theft, extortion, and scamming people is happening every day due to the loss and theft of personal data. Keeping personal data safe and secure should be a top priority for everybody.

It is typically used in exchange for free tokens. But an upcoming trend is seen within exchanges that need to comply with AML and KYC regulations. People willing to buy cryptocurrencies are required to send personal documentation to be stored and validated by private companies.

Consider other revenue models where both sides may benefit. When giving away something for free, like a bitcoin faucet, do not collect personal information. Create solutions that enhance people's privacy. If personal data is required, consider opt-in models. And also include opt-out and complete removal of personal information if people indicate their right to be forgotten.

Rent-seeking

Rent-seeking is a concept in public choice theory as well as in economics that involves seeking to increase one's share of existing wealth without creating new wealth. Rent-seeking results in reduced economic efficiency through misallocation of resources, reduced wealth-creation, lost government revenue, heightened income inequality, and potential national decline.

From a business perspective, rent-seeking is very appealing because it allows for a passive income at the cost of nearly nothing. Who does not like to be in this position? Unfortunately for those intermediaries who profit from this, these kinds of activities are at risk of being replaced by cheaper and more efficient technologies.

The challenge in the Bitcoin ecosystem is to find waste and remove things that add no value. Since much of the code is open-source, it will become easier to automate and replace people and services that profit from connecting things.

Reciprocity

Reciprocity is listed both under the strategic design principles as it is under dark patterns. As with so many other things, how the act is used, determines the outcome. The tendency for people to give back to those who have given to them.

In cultural anthropology, reciprocity refers to the non-market exchange of goods or labor ranging from direct barter (immediate exchange) to forms of gift exchange where a return is eventually expected (delayed exchange) as in the exchange of birthday gifts. It is thus distinct from the true gift, where no return is expected. When an exchange is immediate, e.g., in barter, it does not create a social relationship. When the exchange is delayed, it creates both a relationship as well as an obligation for a return (i.e., debt). Hence, some forms of reciprocity can establish a hierarchy if the debt is not repaid. The failure to make a return may end a relationship between equals. Reciprocal exchanges can also have a political effect through the creation of multiple obligations and the establishment of leadership, as in the gift exchanges (Moka) between Big Men in Melanesia. Some forms of reciprocity are thus closely related to redistribution, where goods and services are collected by a central figure for eventual distribution to followers. Negative reciprocity occurs when an action that harms someone is returned with an action that has an approximately equal negative effect. For example, if an individual commits a violent act against a person, it is expected that a person would return with a similar act of violence. If, however, the reaction to the initial negative action is not approximately equal in a negative value, this violates the norm of reciprocity and what is prescribed as allowable. Retaliatory aspects, i.e., the aspects of trying to get back and cause harm, are known as negative reciprocity. This definition of negative reciprocity is distinct from the way negative reciprocity is defined in other domains. In cultural anthropology, negative reciprocity refers to an attempt to get something for nothing. It is often referred to as "bartering" or "haggling."

Scarcity

Scarcity becomes a dark pattern when it negatively manipulates people's behavior for the benefit of others. One example is to trick people into pressure buying at a certain moment (FOMO).

Focus on uniqueness instead of scarcity. Allow for unlimited post-personalization and -customization instead of pre-defined limited editions.

Social proof

We often look up to experts. We often follow what our friends do and say. Social pressure, when not following the herd.

Social media (Youtubers) often shill their bags after they already bought their share first.

Focus on what people do, rather than what people say. Objectify as much as possible. Do not include social pressure — partner with people who have a good reputation and not one of selling things to others.

Destroying Bitcoin

The German philosopher Friedrich Nietzsche once said, "That which does not kill us makes us stronger." This mindset is very applicable to Bitcoin. Ever since it's conception, Bitcoin had to resist all sorts of attacks by all kinds of people declaring Bitcoin being useless and worth nothing. However, Bitcoin has shown them wrong and is stronger than ever, giving its honey badger status for being smart and tough as nails. It even has its obituary to prove it.

It is good to put Bitcoin under a loop and test it until it breaks. If it does not, then surely it will last a while longer. Or so states the Lindy effect. This chapter is a collection of arguments about why Bitcoin will eventually become worthless.

Accountability

"Those who run the network should be held accountable for offering a platform."

Governments do not like what they cannot control. Especially when it comes to money, there needs to be accountability when things go wrong. Bitcoin, by design, is not this. No Bitcoin company can be shut down and no CEO, which can be held responsible. Instead, accountability lies with the people using the system. Decentralized systems like Bitcoin are by default neutral and with that censorship-resistant. Individuals should be responsible for their actions.

Complexity

"You need to be an expert to understand and use Bitcoin."

The best kind of technology is the one which is invisible, and nobody even needs to think about how to use it. Complex solutions may work well for machines, but humans may struggle with it. If Bitcoin is not usable for everyone in daily life, it prevents or even excludes people to adopt and use it. Unlike many people currently using Bitcoin may believe, the average person who is not familiar with Bitcoin does not need to know everything about it. No matter where people live, ideally, they only need to know the basics of Bitcoin. Maybe in the future, nearly every household has a smart device which includes a Bitcoin node to validate transactions. But for the next decade, it is perfectly fine if people do not completely understand how the Bitcoin network operates. All they need to know is that Bitcoin can be used with ease, always works as expected, and can be trusted as money for those with a small and large budget. Even children know how to use it. Like the Internet, all new technologies need some time to adapt to daily use without people even needing to think about how it works.

Cryptography

"Quantum computers will break Bitcoin's cryptography."

SHA-256 and ECDSA are considered very strong currently, but they might be broken in the far future. If that happens, Bitcoin can shift to a stronger algorithm. Yes, eventually, this could happen. But quantum computers are currently not yet capable of doing this. Meanwhile, multiple new solutions are being explored to become quantum resistant.

Denial of service (DoS) attacks

"The more decentralized the Bitcoin network becomes, the slower it becomes when put under stress."

Sending lots of data to a node may make it so busy it cannot process normal Bitcoin transactions. Bitcoin has some denial-of-service prevention built-in but is likely still vulnerable to more sophisticated denial-of-service attacks.

There are many measures taken in the current Bitcoin Satoshi client to protect itself from DoS attacks. A more extensive list can be found in the references. But to give some idea, here are some measurements. A lot of traffic is prevented by not forwarding orphan-transactions/blocks, double-spend transactions, the same block, transaction, or alert twice to the same peer. Nodes that misbehave are banned for a certain time (24-hours default), and a DoS score is kept for peers that send messages that fail to comply with the rules. To further prevent DoS attacks, there are protocol rules to limit and restrict the amount of information. Examples are restricting the block size, size of each script, number of expensive operations, and signature checks. A DoS attack could paralyze single or multiple nodes, but attacking every Bitcoin node at the same time is very difficult.

Energy consumption

"Bitcoin consumes more energy than an entire nation like Denmark."

Energy consumption for mining has a high correlation with bitcoin value (exchange rate). Because variable costs of mining are dominated by electricity prices, the economic equilibrium for the mining rate is reached when global electricity costs for mining approximate the value of mining reward plus transaction fees. So the higher the value of one bitcoin, the higher the value of mining rewards and transaction fees, the higher the energy consumption of the bitcoin network in the long run. More efficient mining gear does not reduce the energy use of the bitcoin network. It will only raise the network difficulty cheaper energy linearly increases mining energy use of the bitcoin network. The same

conclusions apply to all proof of work-based currencies. The energy which is used for mining is essential for its extreme security, neutrality, and immutability. But it also stimulates miners to turn to renewable and even wasted sources of energy if they want to stay profitable.

Exclusion

"Governments will criminalize people using Bitcoin."

Banning Bitcoin will only result in an increased focus on privacy protection, driving it more into uncontrolled illegality. Additionally, it will migrate people and companies from their country to become profitable somewhere else.

Fifty-one percent attack

"When a single entity or group of entities control fifty-one percent of the hashing power, they will be able to control the Bitcoin network."

An attacker that controls more than 50% of the network's computing power can, for the time that he is in control, exclude and modify the ordering of transactions. This allows them to reverse transactions and confirmations for any transaction that had previously been seen in the blockchain while he's in control. But also prevent some or all transactions from gaining any confirmations or prevent some or all other miners from mining any valid blocks.

But what the attacker cannot do is reverse other people's transactions without their cooperation (unless their coin history has been affected by a double-spend), prevent transactions from being sent at all (they'll show as 0/unconfirmed), change the number of coins generated per block, create coins out of thin air, or send coins that never belonged to the attacker.

With less than 50%, the same kind of attacks are possible, but with less than 100% rate of success. For example, someone with only 40% of the network computing power can overcome a 6-deep confirmed transaction with a 50% success rate. It's much more difficult to change historical blocks, and it becomes exponentially more difficult the further back you go. As above, changing historical blocks only allows you to exclude and change the ordering of transactions. If miners rewrite historical blocks too far back, then full nodes with pruning enabled will be unable to continue, and will shut down; the network situation would then probably need to be untangled manually (e.g., by updating the software to reject this chain even though it is longer). Since this attack doesn't permit all that much power over the network, it is expected that rational miners will not attempt it. A

profit-seeking miner should always gain more by just following the rules, and even someone trying to destroy the system might find other attacks more attractive. Probably the most likely scenario where this attack would be employed would be for a government to try to get control over Bitcoin by acquiring a majority of hashing power (either directly or by enforcing rules on private miners within its borders). Then this government could use the transaction-censorship power listed above to do things like: Prevent any transactions spending "stolen" coins, effectively destroying those coins. If the coins are stolen, then there is a risk that this action will be accepted by the Bitcoin community, but this would set a very damaging precedent. If it becomes possible for coins to be blacklisted in this way, then it is a slippery slope toward blacklisting of other "suspicious" coins. Prevent all transactions from unknown people, so everyone has to register with the government to transact. The appropriate response to any long-term attack by miners is a hard fork to change the proof-of-work function. This fires all existing miners and allows new ones to replace them. Miners are only part of the network. If their powers are abusive, the Bitcoin community will turn against them with countermeasures such as a hard-fork and continue with miners who remain neutral.

Flood attack

"Overloading the network with transactions will render the network useless."

It is easy to send transactions to yourself repeatedly. If these transactions fill blocks to the maximum size (1MB), other transactions would be delayed until the next block. This is made expensive by the fees that would be required after the 50KB of free transactions per block are exhausted. An attacker will eventually eliminate free transactions, but Bitcoin fees will always be low because raising fees above 0.01 BTC per KB would require spending transaction fees. An attacker will eventually run out of money. Even if an attacker wants to waste money, transactions are further prioritized by the time since the coins were last spent, so repeated attacks by spending the same coins are less effective. An attack would soon become very expensive if the only goal is to fill the network with on-chain transactions. But if the fees remain expensive for a long time, people will soon turn to alternatives such as the lightning-network.

Fractional reserve bitcoin

"Custodians holding bitcoin for customers will hand out, I-owe-you's for bitcoins that they do not 100% own."

This probably says more about people who trust their assets to intermediaries — those who do not are fully aware of the saying; Not your keys, not your bitcoin.

Governance

"Bitcoin needs to be regulated."

Blockchain is great at rule enforcement but does not provide at all for rule-setting. This lack of governance makes implementing innovations slow and painful. Moreover, power may get concentrated in the hands of a few (miners, in the case of Bitcoin). Regulating bitcoin is near impossible. What they can regulate are the gates between bitcoin and fiat currencies because those are centrally controlled by companies that need to abide by the law. By doing so, the effect is that these laws and regulations slow down adoption and use it for good use. And when stores stop using them because of too much recordkeeping and regulation, it will drive bitcoin unnecessary more into the illegal territory.

Hedonic adaptation

"People only invest in bitcoin on the false promise of getting rich quick."

Hedonic adaptation, also known as hedonic treadmill, is the observed tendency of humans to quickly return to a relatively stable level of happiness despite major positive or negative events or life changes. In other words, people desire big changes like the bitcoin price going up and getting rich, will not change their happiness. Greed is driving people's expectations and making them unhappy when because they feel entitled to get rich. We can redesign this by changing the mindset of people. Bitcoin is not making you rich but only offers financial sovereignty. Even if it does, then it won't make you happier. Just focus on other sustainable aspects that will make you happy, like building relationships or learning new things. There is no single reason why people get into Bitcoin. Many who join are not interested in price, but simply seek like-minded people or the opportunity to bring value to something bigger than themselves.

Illegal content

"Once illegal content is written on the blockchain, it will forever be there."

It is illegal in some countries to possess/distribute certain kinds of data. Since arbitrary data can be included in Bitcoin transactions, and full Bitcoin nodes must normally have a copy of all unspent transactions, this could cause legal problems. However, Local node policy generally doesn't permit arbitrary data (transactions attempting to embed data are non-standard), but steganographic embedding can still be used, although this generally limits storage to small amounts. Various ideas have been proposed to limit data storage in the UTXO set further (but are not currently being seriously considered for deployment). What is called illegal

content in one country, is called free speech in another. If people disagree with the content, they can choose to ignore or selectively show on-chain content.

Intermediaries

"It is in the best of interest that people use intermediaries to protect them from irreversible mistakes."

Working without intermediaries is cherished by a core group of Bitcoin enthusiasts. The mass audience, however, dislikes having no rights, no recourse, no guarantees, no legal coverage, nothing. They just want secure, reliable, and hassle-free access to their money and a help desk to call when they lose their password. People will still have a choice if they trust themselves more or less than an intermediary — something which they didn't always have before Bitcoin.

Liquidity

"Low liquidity and low volume will lead to market manipulation."

If bitcoin is banned and there are no accessible markets to exchange, then the liquidity will suffer. Although liquidity does not say everything about the quality of Bitcoin as a technology, it does need to be used to be interesting. The price will always go down or up to its value. Markets will always balance out depending on supply and demand.

Manipulation

"In an unregulated market, the rich control it."

Market manipulation. Abuse. Whales. As the years go by, Bitcoin is becoming more decentralized, and the influence of rich individuals is becoming less and less.

Maturity

"Bitcoin is still an early experiment."

Although Bitcoin exists for nearly a decade, the code still hasn't been promoted to a 1.0 release. The question is if this ever will happen at all. This does not imply that Bitcoin is unstable or immature. But it is typical in the blockchain space where many developments such as sidechains, the lightning network, and scripts are used in production but are officially still labeled as "beta." In other words, the possibilities of the system make it so that nobody isn't 100% sure that things cannot be broken, misused, or hacked. It may take another decade before people

accept bitcoin. Meanwhile, it is slowly becoming more practical and accessible every year.

Misinformation

"Bitcoin is only used by criminals for conducting illegal activities."

If education is the way to help people make better decisions and take action, misinformation is the opposite of this. Misinformation comes in many forms. In some cases, the cause is related to a lack of education and understanding. In other cases, the information is not related to facts, but people's opinions or the interpretation of information. The worst kind of misinformation is related to propaganda. This approach has the core focus to send out one narrow perspective of information to brainwash people as if this is the only logical truth. Common places where misinformation is found, are social networks and mainstream media. Their main focus is always to get as much attention as possible. And one way of getting attention is to spread fear into people's minds. Most of the news and articles nowadays are dominated by negative news. Every time the bitcoin price reaches an all-time high, the media has its attention and focuses on the negative aspects. Recurring arguments come back, such as waste of energy, unregulated, used in criminal activities, and so on. The best way to stop misinformation is to focus on education and the successes of the past. Make information transparent, factual, and freely accessible. And these aspects just happened to suit Bitcoin just perfectly. The facts tell a different story. Bitcoin is more transparent than the creation of fiat debt or money laundering paper bills.

Non-fungibility

"When bitcoins used in illegal activities are be banned, they lose their fungibility."

Related to compliance, when governments discriminate against the origin of bitcoins, then some will lose their fungibility. This path is a tricky slope. Take the example of drug traces on fiat paper bills. Eventually, nearly all bills will end up with tiny amounts of drug residue on them after coming in contact with other bills. The same principle applies to bitcoin. The more bitcoins will be labeled as 'tainted,' the more these bitcoins will be mixed with 'untainted' bitcoins until eventually, every transaction will contain some satoshi's used previously in a transaction labeled as illegal. Some argue that 'virgin' bitcoins will have a premium price because they are newly minted by miners. But what they forget is that the 'virgin' bitcoins of miners not only contain a coinbase transaction (new bitcoins) but also older transaction outputs from existing bitcoins that have been transacted. Therefore even 'virgin' bitcoin can never 100% pure. Practically, it is

extremely hard to exclude certain bitcoins from the rest. In the future, privacy protection will only make it more difficult.

Ossification

"Bitcoin code is becoming ossified. Unable to adapt and too rigid."

If people expect Bitcoin to change faster than it does, then they are free to fork it and modify whatever they want. If people value stability, they accept the current approach.

Privacy & anonymity

"Only criminals need more privacy and anonymity."

Privacy is a tool to protect individuals. But like any tool, it can be used for good or worse. But for governments, privacy is a double-edged sword. Swing too far to one side, and we end up with a big-brother system that captures and processes every single move and transaction of the individual, eventually influencing and the lives of their citizens. Swing too far, the opposite side and individuals can exploit their anonymity by abusing the rules. There are a plethora of reasons why governments do not like Bitcoin. But most fears are related to not following the rules like tax-evasion, purchase of illegal drugs, or financing criminals and terrorists. So far, Bitcoin is not fully anonymous, and many "illegal transactions" (depending on the country) can be tracked and monitored. However, some governments already declared 'privacy coins' as illegal and may not be bought or sold within that country. Some exchanges already decided not to include them or even delist privacy coins. If Bitcoin developers decided to enhance Bitcoin's privacy features, be it Mimblewimble, ZK-snarks, or another variant, Bitcoin may obtain the illegal status as well. The future of privacy will remain one of the important aspects of Bitcoin, which deserves further attention and development. Unlike any other financial system, Bitcoin is open and immutable. Tracing a coin's history can be used to connect identities to addresses. Once identities have been coupled to bitcoin addresses, then this can be dangerous once this information becomes publicly known. Already people have been attacked and killed because people found out that they possessed bitcoins. That is why people need to be protected. The freedoms we have in one country is not always shared in another country. Only if we treat everybody equal, can we be all be free?

Regulation

"The bitcoin market needs to be regulated to protect investors."

Do we need more regulatory guidance? Its decentralized nature makes it difficult to regulate. Governments and regulators may never come to like decentralized financial networks at all. A negative event, such as a price crash followed by public outcry, could trigger a regulatory crackdown. Companies operating around the edges need to stay compliant with rules and regulations. They need to do KYC and AML checks. They would have compliance officers who need to trace back the history of bitcoins and perform risk assessments if they were involved in illegal activities, according to national guidelines. Globally, countries are forming new regulations that apply to cryptocurrency possession and trading. The things that can be regulated will be regulated. That which cannot will not.

Scalability

"Bitcoin is unable to scale to what is needed for global payment transactions."

In the early years of Bitcoin, there was little network traffic, and transactions were free or nearly free. But as network traffic increased, Bitcoin had reached its first limitations and could only handle about 4.6 transactions per second. This forced people to pay higher transaction costs or wait longer for their transactions being accepted by miners. This situation where the Bitcoin system was no longer fast and free, is probably the most frequently mentioned argument why some people say that bitcoin could never be a good global currency. Compare this to the thousands of transactions per second that can be processed by credit card providers. Or even Alibaba, which can process hundreds of thousands of transactions per second. The Bitcoin network is currently clogged, and the current level of transaction fees (average $8 in November 2017) makes it very unattractive for small payments. Consider the blockchain trilemma, which contains security, speed, and decentralization. Second-layer solutions like Lightning Network. Zero-layer or network layer solutions like bloXroute. There are multiple ways in which bitcoin can scale. However, not every transaction may appear on-chain.

Security vulnerabilities and bugs

"It will only be a matter of time before bitcoin will be hacked, due to its open nature."

Loss of funds due to double-spending. Hash rate, centralization of mining. They can change the rules. It's possible but unlikely that a newly discovered bug or security vulnerability in the standard client could lead to a blockchain split or the need for every node to upgrade in a short timespan. For example, a single malformed message tailored to exploit a specific vulnerability, when spread from node to node, could cause the whole network to shut down in a few hours. Bugs

that break user anonymity, on the contrary, have been found, since the pseudo-anonymity property of Bitcoin has been analyzed less. Starting from version 0.7.0, the Bitcoin client can be considered a mature project. The security-critical sections of the source code are updated less and less frequently, and those parts have been reviewed by many computer security experts. Also, Bitcoin Satoshi client has passed the test of being on-line for more than three years, without a single vulnerability being exploited in the wild. See Common Vulnerabilities and Exposures for a detailed list of vulnerabilities detected and fixed. If people can hack the bitcoin protocol, then the world may see a whole range of worse problems with lesser securities.

Segmentation

"If one major nation like China disconnects, the network will split."

What if China disconnects itself from the rest of the Internet? We need to look at hash power for creating the largest chain. It is extremely likely that in this situation that information between the two chains will be synchronized. This way, the longest chain will end up as the winner.

Sybil attack

"Malicious people may exploit the network by adding many client nodes they control."

If an attacker attempts to fill the network with clients that they control, you would then be very likely to connect only to attacker nodes. Although Bitcoin never uses a count of nodes for anything, completely isolating a node from an honest network can be helpful in the execution of other attacks. There are some ways to exploit this state, such as refusing to relay blocks and transactions from everyone or relay only blocks that they create, effectively putting you on a separate network and then also leaving you open to double-spending attacks.

Bitcoin makes these attacks more difficult by only making an outbound connection to one IP address per /16 (x.y.0.0). Incoming connections are unlimited and unregulated, but this is generally only a problem in the anonymity case where you're probably already unable to accept incoming connections. Looking for suspiciously-low network hash-rates may help prevent the second one. Measures are being taken.

Transparency

"If bitcoin transactions decide to hide the amounts, it will make the system susceptible to hidden inflation bugs, and potentially break the scarcity of 21 million bitcoins."

Opt-in like Beam. Transparency is now being used against people. This also, to some degree, affects the fungibility of bitcoins, because some can be filtered out or not being accepted, which hurts the neutrality of Bitcoin. We need to find solutions that offer the best of both worlds. Trust the system through transparent verification of cryptography and increase the privacy of everybody.

Tribalism

"Toxic communities may split the community and prevent new people from getting in."

This happens when people advocate only one coin as the one true solution. Market price manipulation. Pump & Dump. ICO's. Paid/stupid YouTubers and social media experts. Media manipulation. Fear of missing out. Limited offers. How to redesign this? Instead of focussing on differences, talk about the aspects which are the same or which can be used together to strengthen both. Stimulate the creation of differences. More explorations will lead to more solutions, which will be beneficial to many more. Share knowledge, people, and code. We need to reward good behavior and ignore the bad.

Unencrypted wallets

"People unaware of hacking 101, run the risk of losing their money."

The wallet is stored unencrypted, by default, and thus becomes a valuable target for theft. Recent releases of the Bitcoin client now supports encryption to protect the wallet data, though the user must opt-in. New wallets vulnerable with old passwords via backups
An old copy of a wallet with its old password is often easily retrievable via an existing backup facility (particularly Apple Time-Machine): draining that old wallet, with its old password, drains the current wallet with the current password -- this is contrary to most non-technical users expectation of what 'change the password on your wallet' should mean following password compromise. An initial solution is to mandate (either in code or as expressed policy) that changing a wallet's password causes (or asks the user to cause) the creation of a new wallet with new addresses, and the sending of existing sums to them. Backed-up copies of the original wallet with the original password would then be empty, should they be compromised. On the downside, the password-changing process would potentially take much longer, cost a transaction fee or more, and - initially at

least - the new wallet is no longer backed up. On the upside, non-technical users won't find their wallets drained from security compromises they believed they had closed, nor be required to locate existing backups of a wallet to destroy them. Eventually, the good and secure wallets will drive out the worse, making the whole ecosystem safer because of natural selection.

Volatility

"People cannot handle the current market volatility and will leave forever."

While the value of "ordinary" money is managed by the central bank, Bitcoin's supply is fixed, and its value depends very much on demand, which makes it inherently volatile. Change and uncertainty scare most people because something, mostly outside of their control, affects them. See also loss aversion. Those who do leave probably entered bitcoin for the wrong reasons and lost more than they could afford.

Building on Bitcoin

Not everybody willing to contribute is a Bitcoin core developer nor aspires to become one. Fortunately, there are other things than the platform to help with and create. If not already, then soon, most development will not be spent on further developing the Bitcoin platform, but on the things around it. This chapter takes a look at some of the products, services, and activities within the Bitcoin ecosystem, excluding Bitcoin itself.

Banking services

Wherever money flows, banking services are likely to be a part of the process. As long as these services add value or reduce friction, people are more than willing to pay for them. Ideally, these services will become decentralized, removing the intermediaries and replacing them with a trusted system such as Bitcoin. But until the underlying systems are ready and tested, custodians will likely continue to play a role by offering promises of consumer protection and excellent customer service. Many of these services will fall under the category of decentralized finance, offering the services previously only provided by banks, but now integrating with and supporting a range of blockchain technologies.

Three popular financial services that will likely continue to exists are storing, lending, and bartering. The most common of these three is leaving cryptocurrencies under the custody of an exchange or a financial institution. Protecting customer funds has been a good enough reason for many people. But new players are just around the corner offering new services such as bartering and lending. Their business model is to use consumer funds to either gain interest or to provide fiat-pegged cryptocurrencies for collateral. In all situations, people need to trust these intermediaries for managing people's assets.

The future seems to be heading towards more decentralized finance. Smart-contracts, multi-sig transactions, and time-locks may likely become more mainstream and suitable for multi-party lending and settlements. There may still be third-parties offering simple-to-use products that facilitate these services. But the main difference is that these third-parties will no longer be in control over the assets. Instead, their role will be more of a marketplace for customized, peer-to-peer lending.

Central bank digital currencies

For many years governments perceived cryptocurrencies as speculative assets not suited for anything else than illegal activities. But it wasn't until Facebook (and partners) announced their plans for a stable cryptocurrency that made some

countries consider the impact of borderless digital money competing with the euro, dollar, and alike.

In the next decade, it is likely that central banks will investigate more about central bank digital currencies (or CBDC's) and how to upgrade their legacy systems with some features from cryptocurrencies. The question is what impact this will have on stable-coins and if these will remain relevant. Their future may depend on the differentiating factors that CBDC's are unlikely going to support.

Community development

People are social beings and seek to find other people of interest who bring value and happiness into their lives. With millions of users, Bitcoin brings people together. If nobody puts any effort into community development, then this might mark the end of Bitcoin as well. When a community grows, Bitcoin as an ecosystem will grow as well.

With more and diverse people joining a community, new rituals are formed and shared. These worldwide initiatives are already happening, such as Bitcoin pizza day, where people buy and eat pizza in remembrance of the first commercial bitcoin transaction. Or proof of keys, to create awareness for digital ownership. This yearly ritual where people jointly move their cryptocurrencies from exchanges and transfer them to an address of which they control the keys.

Healthy communities strive the most by stimulating inclusivity and diversity. Everyone should be equally treated and free to contribute in their ways. When communities strive to achieve specific goals collectively, it will bring people closer together and helps benefit everyone instead of small groups of individuals.

Decentralized oracles

Decentralized oracles promise to solve the problem of translating reliable, neutral data from outside the network to be used within. This approach should extend the use-cases for general smart-contracts where settlement relies on neutrally incentivized, independent parties, instead of trusted third-parties who might benefit from data modification.

Use-cases that may benefit significantly from oracles are supply chains. This way, blockchain solutions can keep track of the physical changes that happen to products and services and add this information to the blockchain. These changes can be handovers between different parties, or sensors that validate the conditions or state during an event or timespan. But who guarantees that the information put onto the blockchain is indeed correct? There needs to be a

certain level of trust for sending reliable information to an oracle. One approach is to verify the data by third parties and punish falsifying information. When designing for these kinds of use-cases, it is crucial to consider all touchpoints within the digital and physical domain from start to finish.

Making things tamper-proof is challenging. One of the most difficult challenges to solve is the reliability of information when it transitions from the physical to the digital domain (and back). "Garbage in, garbage out," is a pattern that is very applicable for oracles. If this problem can be solved, then it will open a lot of new opportunities. Right now, the best solution is to reward good behavior and punish bad behavior.

Decentralized organizations

Centralized authorities with power cannot be trusted to always act in the best interest of the community. Since most organizational structures are hierarchical, management at the top is responsible for making the most critical decisions for that organization. Decentralized organizations try to solve this problem by replacing decision making by a select few, to decision making based on transparent smart-contracts.

DAO's are independent entities that operate on the blockchain. These entities can be a group of people, autonomous machines, or both. Most decision making at this time is relatively simple and includes aspects such as voting, upgrades, or simple fund-management. The current approach seems to be a focus on doing one thing well instead of many complicated things poorly. One of the major concerns is security. The past showed us that a hacked smart-contract could have devastating consequences.

But with increasing confidence, DAO's will likely continue to mature and become applicable for an increasing number of uses. Instead of one big smart-contract, DAO's will most likely consist of multiple, modular smart-contracts with self-contained logic. This approach not only makes it easier to maintain but also to verify and test potential flaws.

Decentralized web

Centralized web-solutions can act biased or censor specific groups of people. Gone are the days where individual people review the quality of the content according to the platform's rules. Machine learning is taking over this process by scanning content and customer reports of inappropriate content. And although this may be a practical approach at scale, there are numerous incidents of incorrect content blocks by these large social media companies. The

decentralized web tries to solve this problem with a combination of tools needed to host unstoppable and uncensorable websites.

Solutions such as NOS, Elastos, IPFS use these to build their platform.
One of the problems is adoption. The gap is too large. They try to tackle all, but people often only need part of a solution.

It's too early for complete solutions. Instead of tackling everything, there might be opportunities in building bridges instead. Standardization might help to make things as easy as plug-and-play.

Digital open marketplace

A place where people can find value and developers can collaborate and reuse third-party services to combine them.

Decentralized exchanges

People need to be in control over their private keys. Centralized exchanges are riskier targets for attacks from hackers.

Exchanges are needed to onboard people into bitcoin. They need to offer solutions such as buying, selling, and trading.

People don't like KYC. Give some additional examples of how to redesign this, and why. What is the role of exchanges? Education or custodians?

Educational systems

There is a lack of neutral, unbiased educational systems that help people learn about blockchain technologies such as Bitcoin.

Where do people start when getting familiar with Bitcoin? Is it the bitcoin.com or bitcoin.org website or perhaps Wikipedia? Most likely, people will start off Googling the word, which leads to millions of search results linking to news articles and exchanges. The question is, how can we explain what Bitcoin is as a starting point and from there gradually and safely onboard them. The goal is to give people the right information to not only make the right decisions but also give them the tools and skills to take action.

Gateways

The blockchain ecosystem is exploding. There are thousands of cryptocurrencies listed on coinmarketcap.com at the time of writing. Many of these currencies

share an underlying blockchain infrastructure, but many are deployed on their own blockchain with unique features. Implementing different blockchain protocols offers particular benefits for users of the system, so various blockchains are created to suit their creators goals. Variety in design creates a healthy, scalable, and resilient ecosystem, but creates its own problems. Disparate blockchains are isolated environments and transferring value between them is difficult. We currently rely on centralized exchanges which can be slow and expensive. Creating programmatic connections between blockchains to ease transfer of value is an important factor for mass adoption of these systems. A two way pegged gateway allows users of a blockchain to deposit the native cryptocurrency of a blockchain and receive the cryptocurrency of another blockchain on the other network. A classic example of this system is BTC Relay, which acts as a peg between Bitcoin (BTC) and Ethereum (ETH). Holders of bitcoin can send BTC to a Bitcoin address, thereby releasing a certain amount of ETH on their behalf on the Ethereum blockchain.

Interesting things may happen when bitcoins can be used to run smart contracts on more flexible blockchains such as Ethereum.

Help and care

Too much seduction, too little prevention.

There are too few social programs where people with problems caused by cryptocurrencies can turn to — especially the care for people when things already went wrong.

Professional help such as addiction centers. Companies involved should at least devote a percentage of their gains to alone or collaboratively support professionals able to help people get their lives back on the rails. Doing good and showing well is also good for your reputation. Help existing professionals with their crypto knowledge.

Those who have problems or those who see others struggling should safely and securely be able to access information about help & care. Remove as many obstacles and barriers as possible.

Heritage planning

People die. And when they have nothing planned, their heritage may become lost forever. What is your plan if you end up in a situation where you are unable to explain that you own crypto assets. Do you have something planned for this?

Wallets and private keys. Writing a will. Telling at least one person about it. How is your next of kin able to access your assets? Crypto inheritance planning book.

Incentivized economy

People need an incentive in order to get them to act. When micropayments can be integrated into everything, people are incentivized to contribute.

Think about getting paid to report or solve bugs, get tipped by writing high-quality content. People and machines are paid by the outcome they produce. Let people and machines get paid for every second of the service they provide.
Micro-transactions should be fast and cheap.

Multi-channel integration

Solutions better match the products people are already using in their day-to-day lives. Products only aim at one thing. But is this enough?

Although I expect that wallets will become feature-rich portals to products and services, they will not be the only interface to use cryptocurrencies. In the first phases, it is more likely that there will be a blend between the old and the new world. This means that existing mobile apps and desktop software will likely integrate bits and pieces of cryptocurrency support into their products. The first attempts will be ugly, like plug-ins or stand-alone apps. But eventually, it will be much more seamlessly integrated into the existing user interface.

Are people able to pick and choose? Or do they use only 10% of their tools? Then more variations will appear in more shapes and sizes. Payments via smart-watches, credit & debit cards, or other IoT devices that are in one way or another connected. Most are owned and controlled by people. But eventually, more devices will be connected autonomously at scale and controlled by local governments or groups of investors.

Productivity

Removing financial intermediaries implies fewer people needed. Will fire people. More efficient.

Replacing financial trust

Removing financial intermediaries. Trust bitcoin and blockchain.

Replacing cash

Fewer paper bills.

Smart payments

Money can be made flexible by everyone. One of the problems of traditional digital money is that only banks are able to get creative with processing money. But with Bitcoin, it is now possible for everyone with some programming skills to create new smart payment services, which were not possible yet.

One example is micro-payments, which allows transactions smaller than 1 cent. Through the use of the lightning network, it is now possible to send the small amounts or satoshis with little to no fees. Building on top of this, people can create business models based on smaller units of measurements. Imagine paying someone per second of their time, per every word that is written, every milligram of food, or every meter that a vehicle has driven.

With bitcoin, you would need to authorize the payment monthly every single month, which is a huge hassle for most people. In the future, we might be able to use a smart contract for recurring payments, but we're not there yet. For now, Patreon represents the best option for this kind of ongoing fundraising. A consistent, recurring stream of income allows me to budget and plan for the long term.

Stable coins

This might be a good intermediate transition from digital fiat currencies to bitcoin. Their lives are already suited for stable prices. Bitcoin as a currency is not yet this.

The world still used euro and dollars as a medium of exchange. Stablecoins might be a step between bitcoin and fiat. Familiarity - Global Coin - Libra. GDBC. Putting myself in Facebook's position, what you are saying is what I would do if I were them. Right now, more then 95% isn't ready for Bitcoin, but I am sure they would love to use a stable coin like GlobalCoin for daily usage. People will sacrifice their privacy (usage) for convenience. I would bet that GlobalCoin might even see a higher daily usage than Bitcoin because it is much more related to what they know FIAT currency is, without major price swings.

Will it help or hurt global adoption? I believe it might be a stepping stone to bypass banks via companies they already use. Does the majority of people care about decentralization? Bitcoin pegged stable coins.

Token governance

People are emotional beings. Governing this via tokens and contracts may be helpful for sustainable businesses.

One thing Ethereum is good at is governance via smart contracts. Young startups are blowing ICO cash like it is nothing. It would be in the best interest of owners and shareholders if more decision making would end up in smart contracts. Token holders can have some control on how well their investments are spent by the founders. Spend slowly instead of fast and dying. Or prevent scams.

Unstoppable markets

Supply and demand create new and existing markets. Decentralization creates something that cannot be turned down easily. In the future, this might apply to a lot of technical aspects such as domains, file storage, or hiring CPU power to perform some tasks.

In most cases, buying, lending, or ownership of certain products and services is not illegal. The crux, however, is in the way of using it. Freedom of speech is often seen as a greater good. But expressing hate and violence is crossing the line of what humanity as a whole finds acceptable. So, where the technology may be neutral by itself, putting this to bad use may lead to some questionable situations in the future.

Since much of this is new and laws are often not created yet, how should we deal with this? Who will be responsible when an actor uses technology for bad things? Or can we help designers and developers create better software? Some guidelines, like the core principles, should help already. Transparency, decentralized control, and the open-source nature of code and documents make sure that the community as a whole can see and interact along the way.

Are the creators responsible for keeping out bad actors? Can they be held accountable when damage is done or when people die? How can we prevent situations like Ross Ulbricht and the Silk Road? (6). Do we want a future wherein developers pro-actively and protectively remain anonymous when creating software? Another approach designers are familiar with is to create filters. Filters can be used to block malicious or age-restricted content. Filters can be customized based on laws and regulations. Ignoring them is, therefore, done intentionally by the user. This is just one simple example. And more solutions and discussions need to take place in the future.

Wallet apps

Apps on your own computer. Web-apps are light wallets, online, and browser-based.

Why is it a good solution? - The quality and diversity are too diverse. Focus on standardization and good design. Short term: Language: wallets should be available in more languages other than English. Especially for developing countries.

Wallet custodians

Exchanges
risks & rewards
no keys
protection
https://medium.com/guarda/%EF%B8%8Fcustodial-vs-non-custodial-wallet-s-%EF%B8%8F-benefits-of-light-wallets-87cf701054d1

Wallet hardware

Ledger, Trezor, KeepKey, Samsung smartphone.

Wallet of paper & steel

Quite a lot of people prefer to store their private keys and mnemonic seed phrases as a back-up on physical materials such as paper, steel, or other materials. Paper wallets are what the name implies, generated wallet addresses, and keys to be printed on paper. This makes them easy for gifting or storing funds offline. Those who receive this gift can import the private key or seed phrase at any time into a compatible wallet app for sending and receiving transactions.

When choosing to create or use a non-software wallet, there are some considerations to keep in mind. The most important choice is the material of the wallet. Paper wallets are relatively cheap to create and well suited for gifting or as a back-up for a few years. However, paper and ink are more likely to lose their quality over time. In addition, the paper does not cope well with water, heat, smoke, or fire. A more expensive option, which is more durable, is a wallet made of metal.

How should we redesign this?

- Stimulate offline generation of keys
- Give warnings when generating online and why this is more dangerous.
- Include instructions and explanations on the printed wallet itself
- include trusted software wallet links which work well with the paper wallet
- Do not create legacy addresses by default but generate Segwit instead.

- Allow advanced options for generating legacy addresses.
- Explain possible import problems when generating addresses.
- Most paper wallet generators only come in small sizes, hard to read.
- They do not consider importing them into safe bitcoin wallet apps for use.
- When used for gifting, they should look more fun — customization like birthday cards.
- Include an area to write down the amount.

Wallet of the mind

Easy to remember and easy to lose.

Don't trust, verify

Use these references to double-check the information written by this author.

1. "Bitcoin Design Principles - IDEO Lab presentation by Andreas M. Antonopoulos," youtube.com/watch?v=Ur037LYsb8M
2. Bitcoin whitepaper, "Bitcoin: A Peer-to-Peer Electronic Cash System," bitcoin.org/bitcoin.pdf
3. "The Five Pillars of Open Blockchains," youtube.com/watch?v=qlAhXo-d-64

Glossary

This quick glossary contains many of the terms used in relation to bitcoin. These terms are used throughout the book, use this for a quick reference.

address

: A bitcoin address looks like 1DSrfJdB2AnWaFNgSbv3MZC2m74996JafV. It consists of a string of letters and numbers. It's really an encoded base58check version of a public key 160-bit hash.