THE BUILDING BLOCKS OF TRUST

AJ Huxtable-Lee

Industry Research Project | Word Count: 14,050

MA Digital Experience Design 2018 | Hyper Island

Special Thanks

This journey through the Industry Research Project, and also the MA Digital Experience Design programme at Hyper Island has been an exceptional insight into my chosen career as a designer. It would not have been possible without the help, support and guidance of some incredible people.

First and foremost; my wife, Siân. The help, patience, advice, wisdom, guidance, laughs and fun you've given me have made all the hard work, late nights, grit and determination worth it. I couldn't have made it without you. Thank you.

Next, the Hyper Island MCR team; Tash, Catherine, James, Kathryn, Sarah and Vikki. Thank you all for allowing me the opportunity to explore the crazy world of design and Hyper Island. It has been an immense journey and one that I shall never forget. Thank you.

To all the industry leaders who have shown me an insight into their world, shared their stories and tips, probed my thinking and given me valuable feedback along the way. Thank you.

To my supervisor, CJ, who has given me things to think about, inspired me and pointed me in the right direction when I've hit a wall in what to do next. Thank you.

To the Hyperbees, Crew UK 18. I can consider myself to be incredibly lucky to have met you all and completed this journey together with you. When I started this programme I never knew how close we would all become, but we've some had great times and created so many memories. I can't thank you all enough for accepting me into your crew, but I mean this from the depths of my being. Thank you.

To my mum and dad who have supported my decision to move away (again) to pursue my career ambitions. It really helps to know that I have the support of my family when I need it most. Thank you.

Special mention to John and Mo who have put a roof over my head and have shown incredible patience and support while I have completed this industry research project over the past 18 weeks, on top of their continuous assistance throughout the programme. Thank you.

Finally, to everyone who has taken part in this project, by giving writing advice, tips, conducting interviews, feedback, help and their time to help me complete this project. Thank you.

Contents

Abstract

Data has become integral to the digital services we use today. Nearly all apps and services require the submission of our personal details in order to use them. There have even been some suggestions that data will become the next currency. However, there have been an increasing amount of data breaches, most notably, the Cambridge Analytica scandal that was shown to have influenced the American Presidential election.

Blockchain technology has emerged as a potential technology for people to protect their data from recurrences through the use of self-sovereign identity platforms. While development of sustainable services that utilise blockchain technology is still in its infancy, designers are beginning to concern themselves with the user experience of how such a service would work.

Emerging technologies and innovations have been shown to go through a ‘life cycle’ of adoption before it is absorbed into the mainstream. At the beginning of this life cycle is a degree of trying to determine how trustworthy a new service is.

This paper aims to explore and understand how trust can be built into the foundations of new services and innovations to speed up and aid the process of widespread adoption. An experience design process will take a human-centred approach to understand, define, develop and iterate a model that can be used by design teams to build trust into their product or service. This model will then be tested by designers and users, and conclusions and future steps will be drawn up based on their feedback and insights.

01.

INTRODUCTION

Introduction

"Today, individuals in developed nations are hard-pressed to avoid the influence of technology" (Carbone, 2015, p.526). Such influence does not often come without some price to pay. In the 21st Century, that price is usually paid in the form of the user relinquishing personal data to whoever is the supplier of technology, whether that be Facebook, Google, Apple or almost any other digital service that requires an account. Although each service requests the same information - often intimate information such as names, date of birth and telephone numbers, to name a few common requests - the individual's right to protect it remains unclear (DeVries, 2003, p.288). Users have the choice to opt out of information sharing, but doing so regularly means the user cannot use the service until they agree to do so. Examples of this include accepting cookies on websites, sharing certain attributes of information like email addresses when signing in to a website via social sign-on and even blocking web adverts through the use of an ad-blocker.

Since the Cambridge Analytica scandal came to light in March 2018, trust in large corporations has fallen. A report by Edelman found that although global trust in institutions had risen by a single percentage point between 2017 and 2018, trust levels among the general population globally remained in the 'distruster' level (48%) (Ries et al., 2018). Blockchain technology, the underlying technology of the cryptocurrency 'Bitcoin', has surfaced as a potential means of protecting personal information that removes the 'middleman' of who looks after our data. Although the technology is still in its relative infancy regarding its wider use, there is currently a lot of hype around blockchain; therefore, expectations may exceed the reality (Zile and Strazdina, 2018, p.12). With new technologies, come new challenges and blockchain is no exception; some of these challenges include scalability, the integrity of network participants, distribution of computational power, reaching of consensus, preserving the confidentiality of users and safety of the used encryption algorithms (ibid.). While I do not disagree with the above challenges, I believe that Zile and Strazdina have missed off another significant challenge; trust.

I believe that there is a general scepticism of blockchain, which I will be using as a hypothesis; it has been greeted with unconditioned enthusiasm by libertarians and, alternatively, with great suspect and aversion by other economists (Krugman described Bitcoin is 'Evil') (2013, as cited in Corradi and Höfner, 2018, p.193). As with most things, there will always be those who advocate new technologies and those who oppose it. Jimmy Song, a venture partner at Blockchain Capital, says "Blockchain is not going to solve [all problems]" (Griffith, 2018). While I agree to some extent that blockchain cannot - and should not - be used to solve all problems, I believe its use in business, if done correctly, can address a lot of the concerns raised from those who responded to a survey; this will be detailed later in the paper.

This paper aims to explore if my hypothesis holds any truth. I will be putting recent learnings from the Hyper Island Digital Experience Design programme into practice from an Experience Design perspective. I will not be focusing on particular products; instead, I will be looking more into the experience users go through before adopting new technologies, with a specific focus on the emerging technology of blockchain and self-sovereign identity. Successful designs must offer more than products or services, caring for holistic experiential dimensions
(Berger and Pain, 2017, p. S4691).

Through a literature review, qualitative and quantitative research, this project will investigate what considerations a user has before deciding to adopt new technology. In addition, the research will discover what prevents people from doing so and understand the current perception of blockchain among the general population. I will explore what the experts in their field believe inhibits widespread adoption of technologies and combine those insights with the opportunities that arise from questioning designers in the blockchain space to understand the challenges they face.

From the qualitative and quantitative research, I will synthesise the findings and pull out key insights and themes. Based on my findings, I will develop and iterate a prototype that I believe will help address the issue of trust when developing new products and services that design teams can use when ideating for their next product or innovation.

The goal of the prototyped model is not to help design teams create the best feature or service, but to take a step back and consider what it would take for new users to begin using their innovation in the first place. This goal is based on an assumption – that will validated later in this paper – that the wider majority of people have a misunderstanding of blockchain technology and only associate it with Bitcoin, which has been claimed to have been used for "nefarious" (Amadon, 2018) activity in the past.

Research Questions

I came up with a set of loosely framed research questions that were used to enable me to diverge and explore my chosen topic from conducting my research and writing my literature review. I was able to converge by synthesising my research to come up with a more enhanced and tightly framed question which allowed to me adjust the scope of my work, before ideating possible solutions and creating a prototype.

- **What is the general perception of blockchain in wider society?**

- **How do we build trust when designing the onboarding experience for new adopters of blockchain?**

- **How might we make self-sovereign identity socially acceptable?**

Research Methodologies

This project was conducted over the course of 18 weeks, and all data was collected and conducted by myself through primary and secondary research. “Good research generates dependable data, which is derived through practices that are conducted professionally and that can be used and relied upon” (Blumberg, Cooper and Schindler, p.14). The research was generated through a variety of methods. An online survey was used to gather quantitative insights to understand common needs and concerns of end-users. Conducting in-depth interviews with designers helped me to understand the considerations and challenges that design teams face when developing new products and allowed me to dig deeper by asking further questions based on their answers.

The Design Council’s double diamond process was used as the guiding framework as this is the model used through the Digital Experience Design programme while studying at Hyper Island. The double diamond provides a stable, easy-to-follow process which enabled me to keep track of where I was during the project and allowed me to consider my next moves based on my understanding and experience of using the model.

In-depth interviews were conducted with designers and blockchain developers and were reached out to via LinkedIn or through the Hyper Island network.The people who participated in this project were:

- Jonny Howle, Product Designer at uPort (Consensys)
- Brian Amadon, Co-Founder of Designers in Blockchain
- Mark van der Net, Tech Lead in the CTO office, Decode Project, Amsterdam
- Sarah Baker Mills, Head of Design at Consensys
- Javier Tarazaga, CPO & Co-Founder of Superblocks
- Anonymous Blockchain Developer
- Gabriel Melo, UX Designer
- Pedro Marques, Product Designer at Personio
- Albert Zikmund, Interaction Designer at frog
- Jamie Bolland, user testing;
- Melissa Ma, user testing
- Karina Solari, user testing
- Rheya Hemrajani, user testing

As was expected, these interviews provided me with a lot of insights and opportunity areas to focus on with my prototype. The prototype was initially developed and sent back to my interviewees via email for feedback, which was then taken and iterated on. Being unable to test my prototype with designers face-to-face was difficult and frustrating, but express consent was still obtained from each interviewee.

Finally, I will draw up conclusions from the whole project and reflect on it before outlining my future intentions.

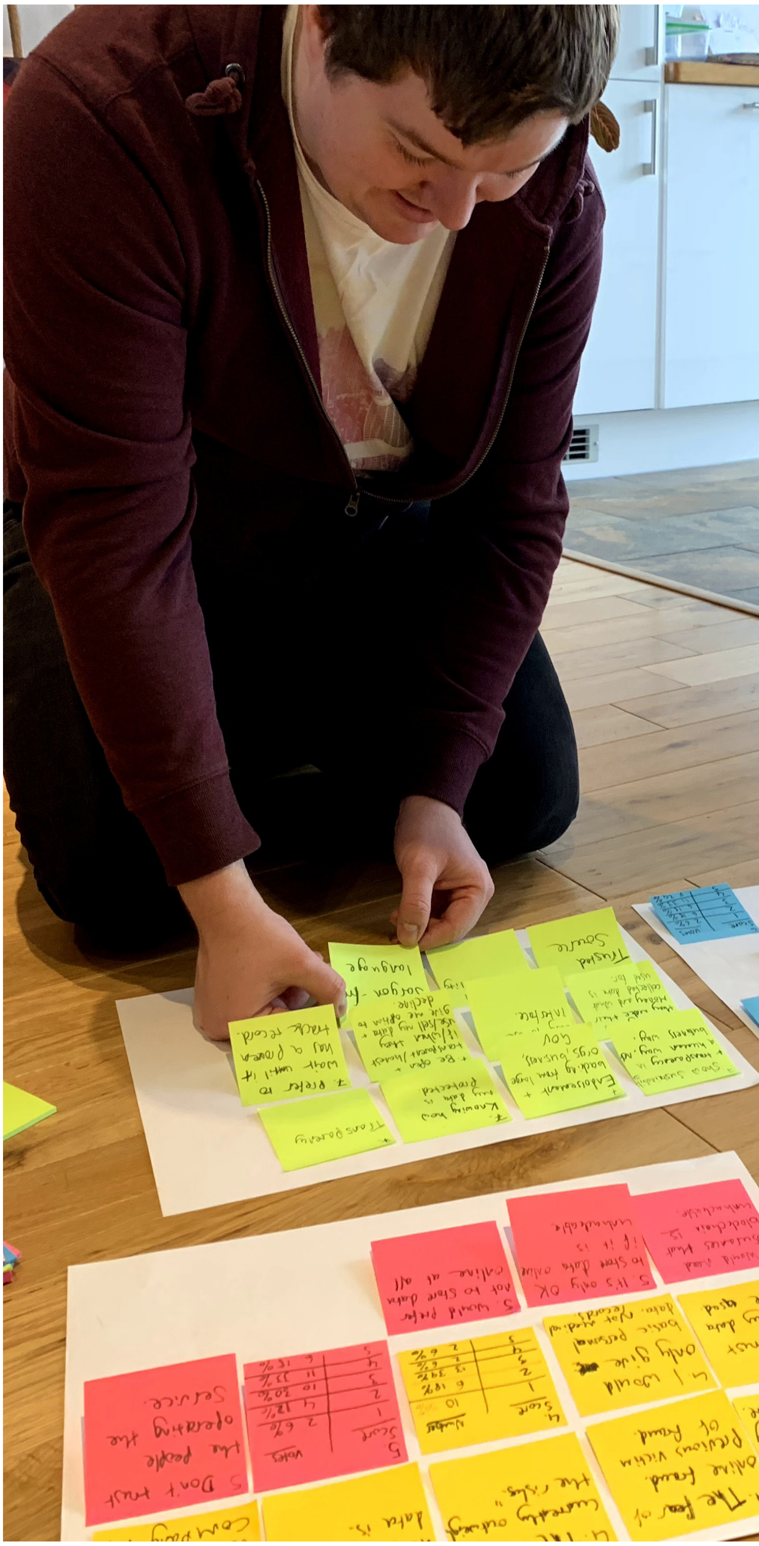
Limitations of Study

While it was recommended that the project be completed while working with a design team, I was unable to secure placement within a design team. However, the Hyper Island network is vast and far-reaching, so online feedback through emails, social media platforms and video-calling from designers from all backgrounds and professions allowed me to make the necessary iterations to my prototype. While not ideal, it still proved vital for the progression of my work.

All knowledge of the topics in this paper has been gathered throughout the course of this project, and while a substantial amount of reading has been conducted, I know there is a vast amount of knowledge still to be gained which simply was not possible to gather within the timeframe of this project.

Similarly, all knowledge of blockchain has been gathered through the research conducted during the writing of the literature review and by talking with the participants of my interviews. I know that blockchain technology is complex and although I feel I have grasped a basic understanding of how it works, I do not claim to be an expert in the field.

Due to my rural location, interviews with experts had to be conducted through the use of online video calls. An unstable internet connection sometimes prevented the use of my webcam, so it was difficult for me to have any face-to-face rapport with my interviewee.



Downloading research and synthesising the insights and opportunity areas from interviews (Personal archive, 2018)

Terminology

Design Process: As I will be conducting this research project through an Experience Design lens, the term "the design process" should be read similarly. I intend for the design process to mean "from an Experience Design perspective".

Distributed Ledger Technology (DLT): DLT is another name for blockchain. It is based on the idea that each participant has access to a shared ledger. (Ølnes, Ubacht and Janssen 2017, p.356) The thinking behind DLT is to have an open, universally accessible ledger which provided a solution to the problem of establishing trust in an unsecure environment without relying on a third-party (ibid.).

Blockchain: The technology at the focal point of this research project is used broadly to cover the underlying technology behind the likes of Bitcoin and cryptocurrency, and should not be taken to refer to any cryptofinancial aspects unless otherwise stated.

Self-sovereign identity (SSI): SSI refers to the practice of using blockchain technology to manage digital identities in a secure, untamperable way. The thinking behind the idea is that users will use SSI services only to verify the information that needs verifying without providing further, unnecessary information.

Designer: The term 'designer' can be used to describe many aspects of the field of design. In this paper, it should be taken to read as a designer currently operating in the blockchain space, unless stated otherwise.

SEED Phrase: The SEED phrase is a set of words consisting of 12-24 English words that allows access to a user's blockchain account in the event of a loss of access to the account. The loss of a user's SEED Phrase can lead to a permanent loss of the account, including all assets associated with the account, such as finances or digital identity.

02.

LITERATURE REVIEW

Personal Data and Trust

In the age of digitisation, we, as users of more and more digital products, have almost grown accustomed to handing over our personal information to various companies, organisations, agencies and governing bodies. If one were to total up the number of websites, apps and services they have signed up to with various usernames and passwords, it would probably be in the hundreds. How many of those websites have different or unique usernames and passwords? Forbes believes the figure is around 27 (Cicchitto, 2017). Usernames allow individuals to build an online persona or identity, so it is no surprise to see a pattern in the kinds of usernames and passwords that individuals choose. Perhaps also unsurprisingly, research suggests that 81% of cyber attacks are based on weak or stolen passwords (Liedke, 2018). The emergence of a social login has provided users with the option to access an account through their social media authentication and authorisation, with 73% of users preferring social login over traditional login methods (Cicchitto, 2017). According to this statistic, it would suggest that users would choose convenience over security. If one's social media account had been hacked, then all of the associated accounts would also be compromised.

Personal conversations over time and throughout this project have suggested that although we allow permissions for these digital products to gain access to the requested data - usually our names, email address, friends list and date of birth - we are not happy about it. Given the number of data breaches of the companies and organisations that hold our data - 'securely', apparently - it is hard not to understand why. Most recently, it was announced that Facebook "gave unfettered and unauthorised access to personally identifiable information (PII) of more than 87 million unsuspecting Facebook users to the data firm Cambridge Analytica" (Isaak and Hanna, 2018). This access was used to push the presidential election campaign of Donald Trump and also the Leave campaign for Britain's exit from the European Union (EU), both in 2016. Since then, trust in businesses and organisations has fallen, with only 46 per cent of UK consumers now willing to provide businesses with their data (Jay, 2018).

Perhaps the most high profile case of data misuse was back in 2013, when Yahoo announced that it was involved in what became the largest data breach in history, when three billion user accounts were stolen in an attack that not only saw names and email addresses being compromised, but dates of birth, passwords and even security questions and answers too. This breach of data knocked an estimated $350 million off the company's sale price at a crucial stage in negotiations with Verizon (Jay, 2018). In the UK, Butlin's, Dixons Carphone, Thomas Cook and even the British Government have fallen foul of substantial data breaches, which have exposed the personal details of millions of people and perhaps even more staggeringly, details on how to obtain security passes to government buildings and communications with MI5 and counter-terrorism officials (Cook and Archer, 2018).

These instances of data breach came at a time when digital data handling was covered by the Data Protection Act 1998, in the UK at least. This act, which stipulates how data handlers and controllers should use personal data, has since been updated with new, stricter policies under the EU General Data Protection Regulation (GDPR), which came into effect in the EU on 25th May 2018. Under the new Data Protection Act 2018, any breaches of data must be notified within 72 hours of the breach occurring and companies may be fined up to 4% of GDP or €20 Million (whichever is greater) (EUGDPR.org, 2018). These new measures should now put more pressure on companies to act with more care, lest they find themselves staring down the barrel of a very significant financial fine.

While these new measures are certainly a step in the right direction, they still do not provide any reassurances to the public that their data is being stored and used appropriately. There have been an increasing number of data encryption specifications like HTTPS, 256-bit encryption and even emerging encryption tools like Honey Encryption, which aims to deter hackers by serving up fake data (that resembles the actual data) for every incorrect guess of key code (Bradford, 2018) to the point that attackers won't be able to tell what is and isn't real (Feinberg, 2014). These are all certainly ways of ensuring that data stays encrypted, but what is to say that the centralised bodies and agencies responsible for looking after that data are doing so responsibly? "In today's digital world, it is hard to judge what's authentic, where information has come from and who has had a hand in changing it. We have no practical way to know what to believe, and our trust in the institutions that govern our lives is crumbling" (Müller, 2018). Research suggests that, due to increasing data breaches across the globe, people are less likely to hand over their data in the future (Fadilpašić, 2016). Companies, including the likes of Facebook and Yahoo, now have to rebuild the trust in their user base.

In his Ted Talk, *Blockchain: Massively Simplified,* Richie Etwaru (2017) suggests there is a 'trust gap', claiming that the gap is increasing between consumers and commerce. One particular area that Etwaru talks about is identity fraud, where in the US in 2017, there were a reported 1,579 data breaches, resulting in an estimated 158 million Social Security account numbers and 14.2 million credit card numbers (Tatham, 2018) being exposed to fraudsters. In the UK, there were over 300,000 cases of identity theft (Samee, 2018). Although there are plenty of ways for companies and people to encrypt personal data, there will still always be a looming opportunity for hackers and fraudsters to target that data, as long as it held centrally by a third party organisation, such as Google, Facebook or a user's bank. It could be argued that it is simply no longer acceptable for our data to be held by third parties and the onus must be shifted on to the user to store and manage their data for themselves. In this regard, the search for new tools and technologies for business models development is vital (Babkin, Golovina, Polyanin, and Vertakova, 2018, p.1).

“The blockchain emerged as a novel distributed consensus scheme that allows transactions, and any other data, to be securely stored and verified without the need of any centralized authority.” **(Karame and Capkun, 2018)**

Blockchain

It is perhaps an alignment of the stars then that there have been technologies looming on the horizon that may be the solution to this problem. Distributed Ledger Technologies (DLTs) - commonly known as blockchain - offer a new way to secure and store data. DLTs can be described as ‘an electronic ledger where the information that is written (normally events or transactions) has been processed and agreed by a number of distributed nodes [computers], once they have achieved consensus’ (Garcia, 2018).

Consensus, in this case, is a process where everyone on the network verifies a transaction. Since 2009, people have been using blockchain technology to trade a digitised cryptocurrency known as ‘bitcoin’ securely. Bitcoin was developed in 2008 by a person, or persons by the name of Satoshi Nakamoto (the identity of Nakamoto has never been revealed) and was described as a ‘peer-to-peer version of electronic cash, which would allow online payments to be sent directly from one party to another without going through a financial institution’ (Hopkins, 2018, p.248). Users (known as ‘miners’) are rewarded with bitcoins through the computational processing of mathematical equations to verify transactions from other users. The more complex the mathematical equation, the more computer processing power required and the bigger the reward.

Blockchain will supercharge artificial intelligence and IoT to make everything from supply chains to digital identity management smarter and more secure (Accenture, n.d.). What makes the prospect of blockchain an excellent suggestion for digital identity management is the fact that it is untamperable. To simplify Garcia’s words about DLTs, information can only be altered once it has been agreed by everyone on the blockchain ledger, meaning any attempts by would-be hackers and thieves to change that information for their own gains would be thwarted almost immediately. “At the core of blockchain is the ability to create a global database (extended from a ledger/list) which is immutable (not changeable by anyone after the fact), transparent, and trusted — even when the parties who write to it are not trusted by each other” (Sidhu & Fred-Ojala, 2018).

Blockchain’s strength lies in its immutability. Once a block is created, all the information of the preceding blocks is contained in the new one, including the ‘hash’. In the context of bitcoin, hashing is the function of taking a series of inputted data (a transaction, for example) and turning it into an output of a fixed length via an algorithm known as SHA-256 (Blockgeeks, 2018). Simply put, ALL information that was in the previous block will be taken into the new block, meaning anyone can see what information was added to that block and when. ‘This creates a chain of blocks from the first (genesis) block to the current. This makes it computationally impractical to modify information once it is in the chain because all subsequent blocks should also be regenerated’ (Baars, n.d., p. 4).

Delving deeper into how a blockchain can be used to store personal information is a relatively new arm of blockchain known as ‘self-sovereign identity’ (SSI). As the name might suggest, SSI ‘is the notion that we all are the makers of our own identity, online and off. Because they do not rely on any centralised authority, self-sovereign identity systems are decentralised, mirroring the way identity works in real life’ (Windley, 2018). While SSI would not give complete control to the user, it would define the borders within which decisions are made and outside of which the user negotiates with others as peers (ibid.).

Where the onus falls on to individuals to look after their data is that no one owns a blockchain ledger, in the same way, that no one owns the internet. However, the internet is public, and anyone can write on to the internet. These ledgers are transparent when made public and are time-stamped whenever an amendment is made to a record. The option to be able to see any amendments made of a record must be considered as a step in the right direction for users to know who has handled their data and when. For an individual to be able to see all this information whenever they want without having to put in an information access request should be seen as a way of bridging the previously mentioned trust gap.

That said, getting the masses to trust this new technology in the first place remains just one of the many challenges that lie ahead for blockchain and its branching technologies.
It could be argued that the idea of providing our most personal information to millions of other users in the form of blockchain nodes (computers on the blockchain) is, on the face of it, a worse proposition than merely handing it to third parties who are protected by strict data protection laws. So how does a new technology that is high in complexity become absorbed into society and adopted as the default?complexity become absorbed into society and adopted as the default?

Case Study: Estonia

Image Source: Worksup.com (2018)

Case Study: Estonia

When one considers looking to a country for the nationwide adoption of a new digital system, it could be argued that Estonia is not the country that would immediately spring to mind. The world's most literate but least religious country (Smith, 2018) might be home to only 1.3 million people, but it was the first country in the world to introduce online voting back in 2005. Numerous online public services including digital identification, digital signatures, electronic tax filing and online medical prescriptions have put Estonia at the forefront of states aiming to modernise their public sector while providing transparent governance (Vassil, 2016, p. 1). Digital identification is now compulsory for all citizens and in 2014, was used around 80 million times for authentication and 35 million times for digital transactions (ibid.). Not bad for a country 6.7 times less populated than London.

So, how did a whole country adopt such a new way of life? The method used by Estonia is perhaps best likened to Everett Rogers' proposed idea of technology diffusion, described as a sequence of steps in an innovation decision process (Rogers, 1962). In his book, Diffusion of Innovations (1962), Rogers stated the process included gaining knowledge of the technology, being convinced of its usefulness, and deciding where to implement it (Vassil and Solvak, 2016, p. 60).

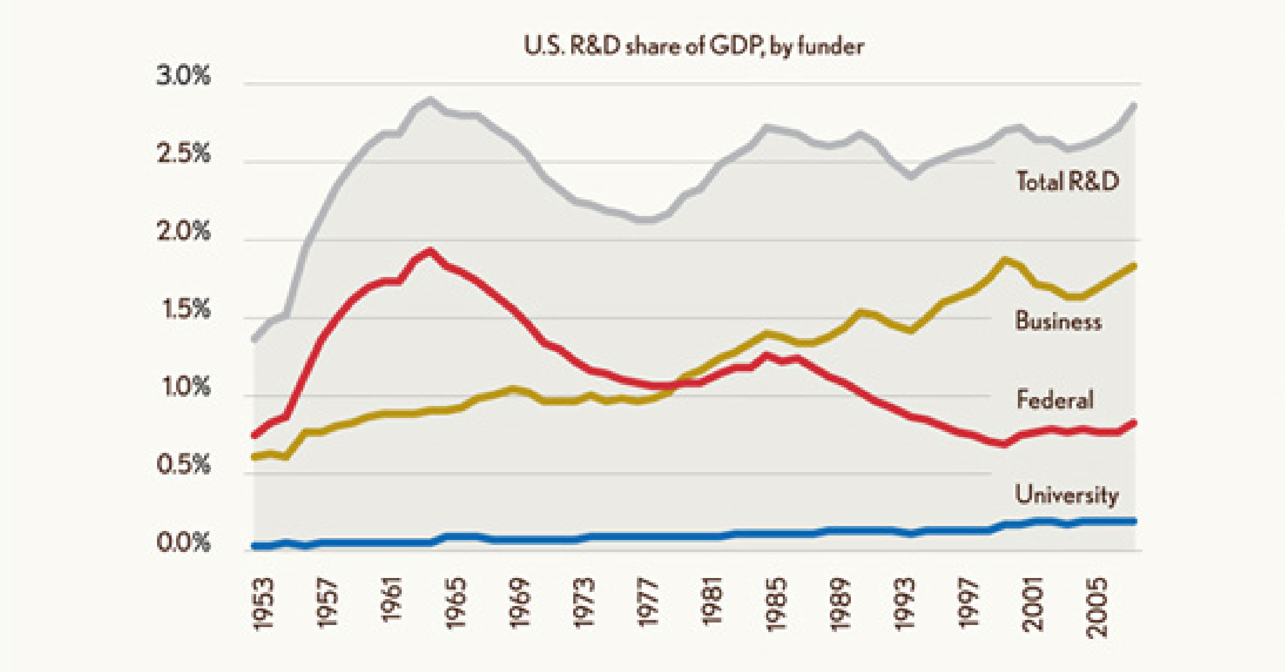


Fig. 1: Chart showing the amount of investment into R&D in the United States over a period of fifty years. This government investment has often been said to have contributed to the US's position as the world's largest economy (Council on Foreign Relations, 2016).

Empirical evidence generates a positive correlation between technological innovation and economic performance (Lumen, n.d.). Massive government investment in research and development (R&D) for innovations during the 1970s is hypothesized to be a central driving force in the steady economic expansion of the U.S., allowing it to maintain its place as the world's largest economy (see Fig. 1) (Lumen, n.d.; Council on Foreign Relations, 2016). This evidence points to a general trend in successful innovations, attributed to the so-called 'Technology Life Cycle' (TLC). The Technology Life Cycle shows the trend of a new technological innovation adoption as a line that starts low during the R&D phase, peaks to a high point during the adoption of the early majority before its decline into obsolescence (Duretec and Becker, 2017) as innovations are researched again (see Fig. 2).

Implementation of the process involved introducing it a small subgroup of society who are open to trying new technologies known as early adopters. From there, the process of adoption spreads to other subgroups (early majority, late majority and laggards), i.e. diffusion, which Rogers said is reminiscent of a bank-run, where the number of people adopting the technology is dependent on the number of previous adopters (Rogers, 1962, p. 206).

If the concept of diffusion of e-voting was to continue right through to adoption by laggards, both the cost - not only financial, but the need

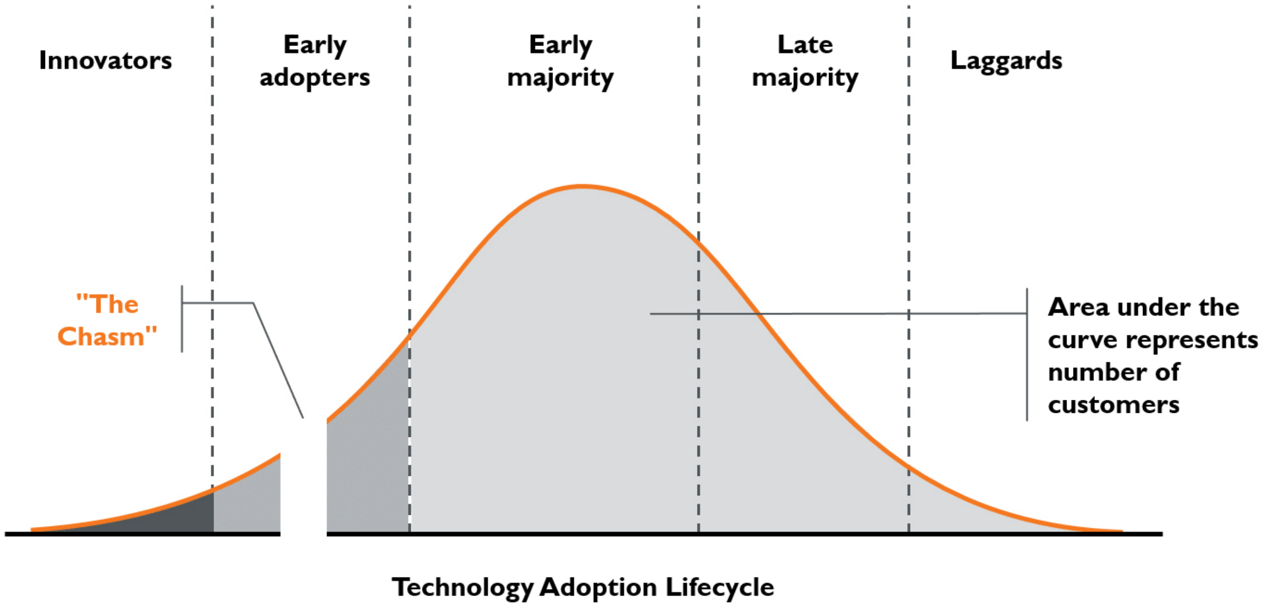


Fig. 2: The Technology Life Cycle. The grey section under the line represents number of customers. (Heigel, n.d.).

to come to terms with the higher complexity of the new technology and the need to evaluate relative gains compared to the previous solution (Vallis and Solvak, 2016, p.61) - and benefits of adopting such technology had to be addressed. Those labelled as early adopters are generally more tech-savvy, open to the ideas of new technologies, younger and better educated, meaning that any barriers that were erected during use would not be as big an issue. For the laggards, however, the benefits of using e-voting had to be visible quickly, lest there be a plateau of adopters. Any system needs to be sufficiently well designed and easy to use in order for successful diffusion to happen. (Vallis and Solvak, 2016, p.87) Choosing to e-vote should be more convenient, faster and provide a more accessible option as voters would not need to visit a polling station.

Research shows that around one-third of Estonia now votes online (Vallis and Solvak, 2016, p.64). As the graphs in Fig. 3 show, apart from a drop in the number of e-voters during the 2014 European Parliamentary election, growth and use of e-voting has risen year-on-year. While the work conducted by Vallis and Solvak showed what a ‘typical e-voter’ looked like for the first three elections - including age, technological savviness and education, among others - their research shows that distinguishing the socioeconomic background of new first-time voters became steadily more difficult in subsequent elections. Put simply; it was becoming increasingly difficult to determine whether uptake of e-voting was being done by the early or late majority or laggards. From this research, it can be concluded that the full-blown diffusion of e-voting [had] taken place (Vallis and Solvak, 2016, p. 67).

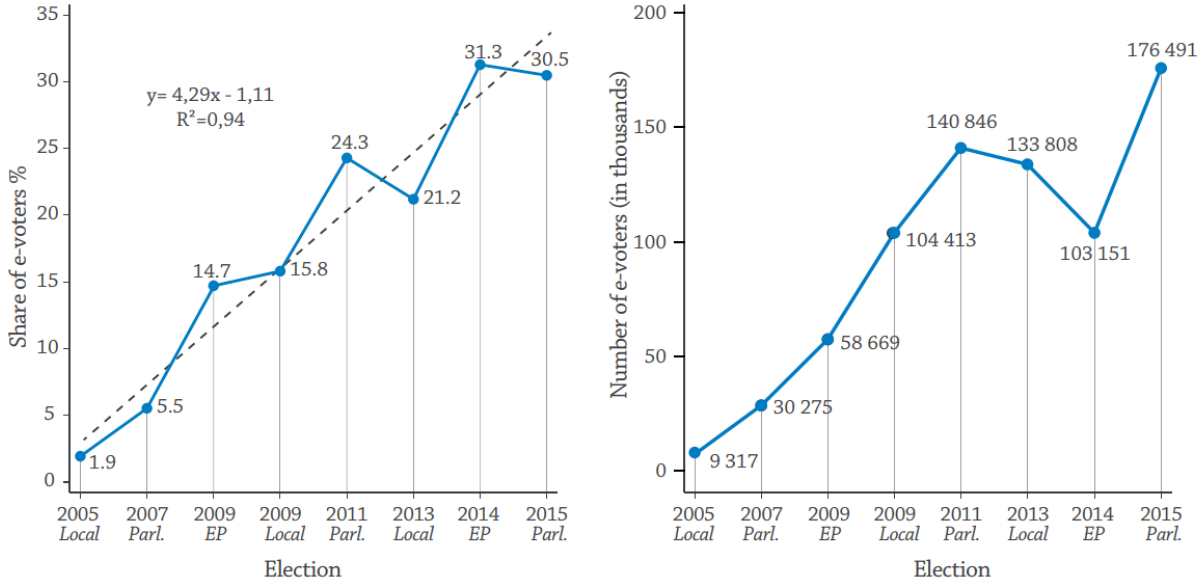


Fig. 3: The relative share and absolute number of e-voters.

(Vallis, 2016, p. 4)

The study in Estonia's online voting and digital identity for all citizens provides optimism that with the correct approach, even the smallest, least populous of nations can bring in a new era of digitisation to the wider majority of its citizens. Estonia also plans to adopt blockchains in a range of areas such as an e-residency project (which allows foreign citizens to establish a business within Estonian jurisdiction) and healthcare (Kshetri and Voas, 2018, p.96). Being able to set up a new business within a new country or monitor one's health in real time without the hassle and complexity that often comes attached should provide a great incentive for more countries to adopt blockchain technology.

If this were to happen in a larger, more populated country with a greater economy - where, admittedly, the margins for error are greater - would diffusion be faster and more widespread? Using the United Kingdom as a starting point, which sector would work best for implementation to begin? Sectors such as the health, banking and employment sectors all pose great suggestions, but other factors need to be taken into consideration first. Which demographic needs to be targeted first? How much would it cost for a new digital system to be implemented on a broader scale? What is the current view on blockchain across a wider population? Moreover, how does one go about making self-sovereign identity socially acceptable?

These considerations are just a selection of what must be kept in mind when proposing a new solution to the public and businesses if the UK is to keep up-to-date with digitisation.

Designing for Trust

Although the idea of untamperable digital identities as an alternative to numerous usernames and passwords sounds ideal, making it easy to understand for people to take it seriously, to begin with, remains an initial challenge. The success of digital identities - or more specifically, self-sovereign identities on the blockchain - depends on adoption by not only highly skilled and interested users but everyday people who are trying to do their jobs, purchase goods, or just have fun (Baker Mills, 2018a).

What is needed here, as is the case with many projects in modern design, is the need to focus on user needs through human-centred design. IDEO's vision of human-centred design is that of a process and a set of techniques used to create new solutions for the world (UBC, n.d.). Defining 'real' problems through a human-centred approach (that is, concerns that are currently having an impact on how people live their lives) that blockchain can tackle is a challenge that continues to elude designers. "Blockchain is a hammer, and everything looks like a nail. How to communicate the value of blockchain is both a demonstrated value (so, solving a problem) and a marketing/storytelling issue" (Baker Mills, 2018b).

Further, once a problem has been defined, making the product easy to use and follow for the user is something that does not appear to be a challenge that has been cracked so far. It could be argued that there is too much focus on simplifying blockchain for the user. Instead, the focus should be on making the steps the user goes through a more natural user experience like any other product, rather than a forced experience because the product is built on blockchain technology.

From an experience design point-of-view, it simply does not make sense, nor will it do anyone any favours to blindly launch products and services into society in the hope that the general public will start using them. A user's journey through a product or service needs to be intuitive and straightforward without confusing them. The needs and desires that have been uncovered through user research should be shown to have been addressed in the products. There does not appear to be much academic research on user experience (UX) design in the blockchain space. This comes at a bit of surprise, given the amount of academic research on UX design in general. However, it could be argued that regardless of the field that a UX designer is working in, best practices in design should still apply.

Users have proven that they are unwilling to invest time or money in security improvements (Dhamija, 2008, p. 25) and this is especially true for services that do not immediately prove to the user why they should be using one product over another. Referring back to the works of Rogers (1962), he outlined five characteristics that influence a person's decision to adopt or reject an innovation (On Digital Marketing, n.d.):

Relative Advantage - How improved an innovation is over the previous generation. In other words, how is this product or service better than what is currently out there?

Compatibility - The level of compatibility that an innovation has to be assimilated into an individual's life. Rogers refers to the ease of integrating an innovation into an individual's everyday life.

Complexity – If the innovation is too difficult to use an individual will not likely adopt it. Possibly the biggest challenge in promoting blockchain to the wider public is making it simple to understand. Failure to make it as accessible as possible will likely fail a broader societal adoption.

Trialability – How easily an innovation may be experimented with as it is being adopted. If a user has a hard time using and trying an innovation this individual will be less likely to adopt it. How can people try out an innovation without committing to it long-term?

Observability – The extent that an innovation is visible to others. An innovation that is more visible will drive communication among that person's peers and personal networks and will, in turn, create more positive or negative reactions. (Rogers, 1962, pp. 15-16) How can the broader population see it in action?

If designers can follow these five characteristics when designing for their users, it could go a long way to ensure that the needs and desires of the users are being addressed and the product or service does not become another innovation that is shelved shortly after its release.

In his book, *Managing Innovation Adoption: From Innovation to Implementation* (2014), Majharul Talukder talks about the need to avoid innovations falling foul of 'shelfware syndrome', a term coined to describe software productivity packages sitting idle on bookshelves without being utilized by the individuals for whom they are intended (Talukder, 2014, p.2). While the exact terminology might be slightly off in terms of general innovations, the thinking behind the idea remains critical. People need to trust a product, organisation or even new technology to be able to take it off the shelf and use it.

Steven Drozdeck and Lyn Fisher talk about trust in an equation (Fig. 4) in their book *The Trust Equation* (2003). When applied in principle, the amount you trust someone is the sum of how credible you believe they are on a subject, how reliable they've proven themselves to be over time, and how authentic you think they are as a person or organisation, divided by how much you think they're acting in their own self-interest (Firstround.com, n.d.).

The perception of self-interest is an intriguing consideration as individuals will have their reasons and motivations for using a service or product. It is undeniable that there are some individuals whose intentions could not be considered 'good intentions' and there will undoubtedly be those within the blockchain arena. There will always be users who find creative ways to crack the most sophisticated and secure security measures. There will always be a weak link, and if new technologies are used by people who perhaps might not understand the best practices regarding personal security, then there will be those who seek to exploit that lack of understanding. It can be argued that those users with bad intentions can be attributed with the sowing of seeds of mistrust among the wider public. This mistrust, especially when potentially the most intimate of personal details are at risk of attack, could be enough to keep self-sovereign identities on the shelf.

$$\text{Trust} = \frac{\text{Credibility} + \text{Reliability} + \text{Authenticity}}{\text{Perception of Self Interest}}$$

Fig. 4: The Equation of Trust (Drozdeck and Fisher, 2003)

In conjunction with Rogers' five characteristics, the equation of trust can be utilised in blockchain design teams to build trust in users. The equation can be broken down thus, according to Anne Raimondi, COO of Earnin:

Credibility: Credibility in this case could be exhibited in how well blockchain has performed so far in terms of its security, how it has been used, who has adopted it, how it has developed over time and the kind of language it uses. Currently, it could be said that language remains something that can be improved.

Reliability: Ethically, reliability is the characteristic that provides a user with the peace of mind they seek with regards to how safe blockchain is. If blockchain can be shown to be consistently reliable, accountable and responsive, I believe it should go a long way to closing the trust gap.

Authenticity: When applied to blockchain, it needs to be clear to the user that the app or service is working in the best of interests of the user and not the service's supplier. It needs to say and do what it says it will do. This implies that the app or service will provide transparency.

Perception of Self-Interest: The denominator in the equation of trust is perhaps the most difficult for blockchain to portray to the user. Raimondi describes it as, "The greater the perception of self interest, the lower the trust between people. Alternatively, the more someone appears to be doing work for the benefit of the team, end user, or a higher goal, the easier it is to trust them (Raimondi, n.d.)." The blockchain technology in itself will not be looking to gain from the user, but the agencies and platforms the user is subscribed to might be. The user will need reassurance from these agencies and platforms that there is an agenda that benefits the majority and not the singular.

It could be argued that in order to reduce the level of complexity in understanding blockchain, more needs to be done to make end users feel like they have a better grasp of the benefits of the technology. If one were to put this into an analogy, it could be that the average member of the public does not know the intricacies of an online bank transfer or how an email works, but they know how to use them and the benefits of using them. This can be likened to counterfactuals.

In their paper, *Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR*, Wachter, Mittelstadt and Russell talk of opening a "black box" (2018, p.3) of explanations relating to the 'right to explanation' in the GDPR law. They argue that "building trust is essential to increase societal acceptance of algorithmic decision-making" (Wachter, Mittelstadt and Russell, 2018, p.4). The same thinking also holds true for blockchain. However, counterfactual explanations do not attempt to clarify how decisions are made internally (2018. p43) and explanations of [blockchain] need not hinge on the general public understanding how [distributed ledger technologies] function (ibid.).

“Design ethics has remained under-developed despite an increasing relevance in the Anthropocene, when many novel ethical issues and problems are anticipated to emerge from man-made artifacts and systems.” (Chan, 2018)

Ethics

As with most projects where humans are the subject matter, ethics play a vital role in ensuring the product or service is right. However, with emerging technologies - blockchain and digital identities in particular - there appears to be a distinct lack of academic research on where the question of ethics sits in this field. Of course, common sense and logical practices still apply with regards to abiding laws and upholding personal virtues if an individual or business is to use new technology - or any technology, for that matter - with the best intentions. This might mean not using a service fraudulently by obtaining another individual’s personal details without authorisation, uploading indecent content on to the blockchain or inciting hatred, abuse or violence against another person(s). It goes without saying that there are many more considerations beyond the ones listed here.

However, ethical considerations must also fall to organisations that use blockchain to ensure a repeat of the Cambridge Analytica scandal does not happen. For those organisations and businesses that have had privacy problems in the past who are looking to utilise blockchain to store user data, it could be argued that this technology provides a second chance at building, maintaining or even enhancing their reputation in the business world. However, it must be done correctly, for the right reasons and with the correct procedures in place.

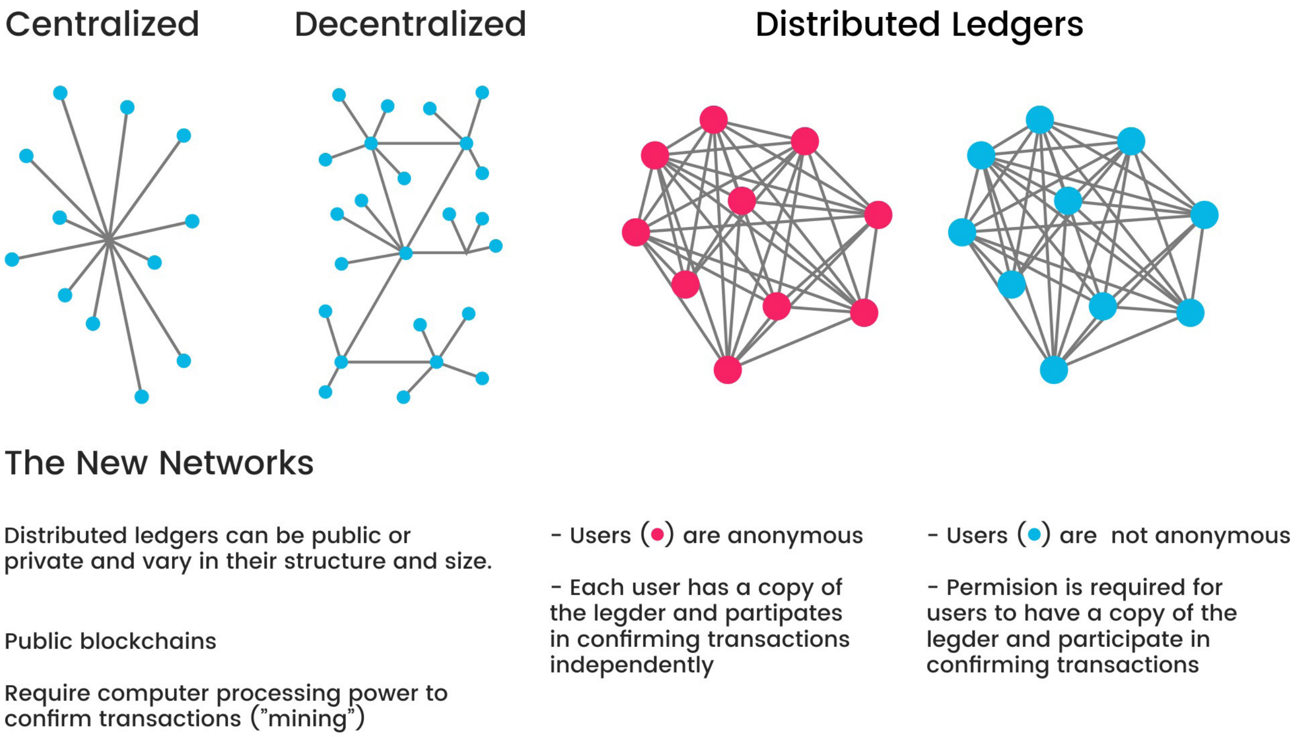
This all sounds like the obvious is being stated, but sometimes it is required to avoid falling into the same security pitfalls as before. However, who decides what is ethical and what is not? Sometimes, ethical problems are open-ended, perhaps even messy, in that there is rarely if ever, a uniquely correct solution or response (Whitbeck, 2011 as cited in Kirkman, Fu and Lee, 2017, p. 2). Of the options available at the time, some might merely be unacceptable while the remaining options could push the decision to be made on a ‘lesser of two evils’ basis, dependant on how much the advantages of each option outweigh the disadvantages.

Perhaps then, the answer lies in more businesses and individuals learning about the intricacies of human-centred design, where ethical considerations and empathy for the end user build the foundations of the methodology. Marc Steen talks of making the ethics of human-centred design processes explicit so that the people involved can become more aware of these ethical qualities and can incorporate them consciously and reflexively in their practices (Steen, 2014, p. 390). By bringing the characteristics of the human-centred design process to light, participants can make conscious ethical decisions and over time, turn that decision-making into a habit.

The financial implications of managing data in its current state might also be an incentive for businesses to look to blockchain. Research suggests that businesses are spending around $1 billion a year on data management and a password reset costs around $70 (Aitken, 2018). Max Di Gregorio of PricewaterhouseCoopers references a Santander FinTech study which suggests 'distributed ledger technology could reduce financial services infrastructure cost between US$15 billion and $20 billion per annum by 2022, providing the possibility to decommission legacy systems and infrastructure and significantly reduce IT costs' (Di Gregorio, 2017). These figures are a huge carrot to be dangled in front of many businesses and while nobody likes spending more than he or she needs to when there is a cost-effective alternative available, the reasons for wanting to utilise blockchain for data management have to stretch beyond simply saving money.

While looking at the reasons for using blockchain in the broader sense, it is also essential to take a step back and look at blockchain from the other side of the argument; is the technology even good for humanity? If one were to read into the security and decentralisation of Bitcoin and Ethereum, the two largest platforms that currently use blockchain technology, it was discovered that the top four bitcoin-mining operations had more than 53 per cent of the system's average mining capacity per week. Meanwhile, just three Ethereum miners accounted for 61 per cent (Orcutt, 2018).

There have been suggestions on how to avoid a small minority holding a majority rule of the technology, including an as yet untested hypothesis revolving around consensus protocols that do not rely on mining or permissioned systems that require permission to join (ibid.). However, this raises the question of who has the authority to grant or deny that permission. Also, how will the system know the genuineness of a validator? Permissioned systems will also require power to be held by specific people or bodies of people, which goes against the very idea of using a blockchain in the first place. There is also an energy consumption factor that is concerning climate-conscious people across the globe. The computational processing power required to process bitcoin transactions pose a serious threat to the global commitment to mitigate greenhouse gas emissions (GhGs) pursuant to the Paris Agreement (Truby, 2018 p.399). The amount of energy required to power blockchain transactions is equivalent to that



The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions (”mining”)

- Users (●) are anonymous

- Each user has a copy of the legder and partipates in confirming transactions independently

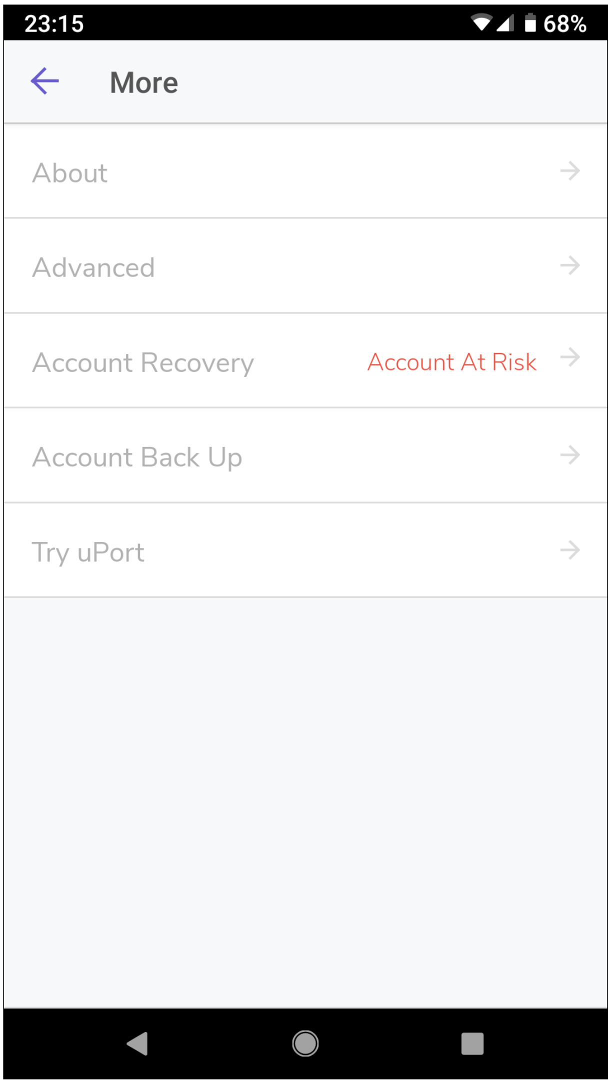
- Users (●) are not anonymous

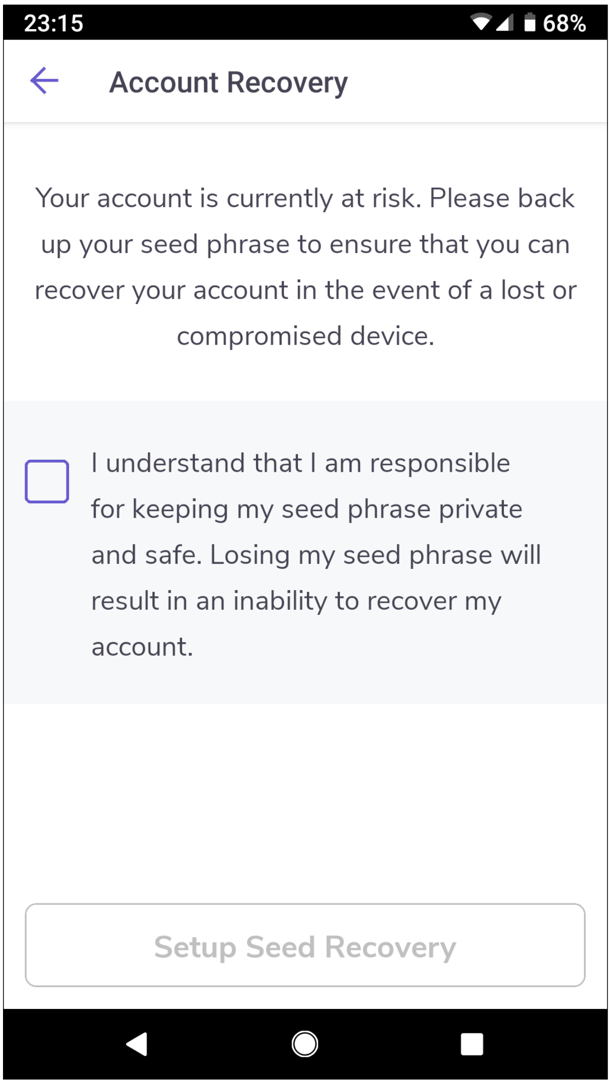
- Permision is required for users to have a copy of the legder and participate in confirming transactions

Fig. 5: The variations of blockchain network, showing centralised, decentralised and distributed ledgers. (Rosic, 2016)

required to power the whole of Denmark and even the processes involved in a single Bitcoin transaction could provide electricity to a British home for a month (ibid.). The figures around the actual energy cost of bitcoin mining vary across the Internet and scientific literature, but there have been suggestions that it ranges from 10 Megawatts (MW) right up to 3-6 Gigawatts (GW) (Vranken, 2017, p.5). For comparison, 1 MW can power up to 650 residential homes (Hagadone, 2015). This comes at a time when the Intergovernmental Panel on Climate Change (IPCC) have issued a warning to countries that we are not doing enough to reach our target of 1.5°C warming (IPCC, 2018), and the world is already experiencing an increase in extreme weather, such as localised flooding, hurricanes, longer, hotter days and increased rainfall. Using blockchain technologies on a larger scale will only add to this climate change and might speed up the level of global warming to dangerous levels.

Another ethical consideration is the recovery of one’s account on the blockchain. Account recovery of data stored on the blockchain would be a huge factor in turning people away from using blockchain in the public domain. Users struggle to remember usernames and passwords they have set themselves; how will they manage to keep track of a randomly generated alphanumeric key? The uPort mobile application (Fig. 6) even goes as far as placing absolute responsibility on the user to look after their ‘SEED phrase’, a recovery phrase involving a list of randomly generated words that the user is advised to write down on paper, so as not to store them digitally. Finding the delicate balance of account ownership and account security is just one more challenge to be added the already long list of seemingly endless challenges blockchain designers face.





Your account is currently at risk. Please back up your seed phrase to ensure that you can recover your account in the event of a lost or compromised device.

□ I understand that I am responsible for keeping my seed phrase private and safe. Losing my seed phrase will result in an inability to recover my account.

Fig. 6: Account recovery process from the uPort mobile application.

(Personal archive, 2018)

"On the Internet, nobody knows you're a dog."

Paul Steiner's famous cartoon that plays on the anonymity of Internet users.

(Steiner, 1993)

Final Thoughts

This literature review has delved into some of the many facets of the distributed ledger technologies (DLT), commonly known as blockchain. Through my reading, I have discovered that, while the potential of blockchain and self-sovereign identity is huge, understanding the complexity of the technology remains a sizeable challenge.

The literature review has also explored the reasons for and against using emerging technologies in blockchain and self-sovereign identities as a method of storing and controlling personal data. It has highlighted the many challenges and hurdles that are in place for designers to tackle when starting their design process. Blockchain and self-sovereign identity offer significant improvements and opportunities to the management of personal data, but as the technology is still in its infancy, it does not come without its risks. Control and ownership of personal data can be entrusted back to the user, but that user must have a sense of tech savviness to be able to keep a record of the account recovery methods in place by some of the existing SSI platforms, such as uPort.

Moreover, while blockchain and distributed ledger technologies are touted as being untamperable and unhackable, the more creative people who wish to harm have already found ways around the immutability of the technology. Looking into how Estonia has introduced digital identities for all its citizens provides optimism that it is possible on a wider scale. Estonia might not be the country at the top of many people's lists of countries leading the charge into digital identities, but their successful nationwide adoption of e-voting provides a blueprint for more countries to follow suit.

Further, the risk to the environment through the cost of computational processing power to verify blockchain transactions cannot be ignored, especially at a time when there is a global crisis affecting our climate.

However, while these risks exist, perhaps the biggest challenge that remains is building trust. Designers must find a way to close the trust gap if blockchain and its associated technologies can be rolled out to not only the early adopters but the mainstream as well.

The next part of the paper will go through the design process to look into how designers can break down the barriers to make this exciting, yet profoundly complicated technology more straightforward to understand on a wider scale. Then, using the insights and opportunity areas gained from interviews with experts and users, I will narrow my findings down into an intervention that will be prototyped, tested and iterated on.

03.

THE DESIGN PROCESS

This chapter will outline the tools used to answer the research questions and hypotheses from an experience design point of view while analysing the research gathered throughout the process. The research will primarily be conducted through field research in the form of qualitative and quantitative research, such as interviews and an online survey. The research questions and hypotheses I am looking to answer are:

How might we make self-sovereign identity socially acceptable?

How do we build trust when designing the onboarding experience for new adopters of blockchain?

Insights from the Literature Review

The five key insights to be taken from the literature review are:

- Before a wide-scale adoption can be achieved, there must be trust in the technology or product;
- There is a user preference to convenience over security with regards to account log-in details, such as usernames and passwords;
- Blockchain explanations are often complicated and can potentially scare users away;
- The added value and benefits of blockchain need to be made more explicit to the user, rather than trying to explain how the underlying technology works;
- Transparency is key. People want to know what happens to their data when third parties take control of it.

For a new technology to be adopted by the mainstream, there must be a degree of trust from those who would be considered the end users. A typical inhibitor for adoption during this early phase is the lack of a common vernacular (Gisolfi, 2018). Knowing why users trust or distrust [blockchain] can provide important insights into system features that can help build and stabilise trust (Hole, 2016, p.66).

I hypothesise that there is currently a lack of trust in this relatively new technology among those people who are not in the blockchain space because it is too difficult to explain. Recent interviews with designers have highlighted this as a common problem, with one interviewee saying that blockchain is not currently easy to explain in "under thirty seconds" (Amadon, 2018) which in turn, makes it difficult to explain to new users. Referring back to Everett Rogers' five characteristics of innovation adoption, 'complexity' provides a suitable hurdle to tackle; "If the innovation is too difficult to use an individual will not likely adopt it" (Rogers, 1962, p.15). This notion of complexity can be found in the way users choose their passwords, preferring to choose convenience over security.

Research shows that users would rather choose a single password that is easy to remember or use their social media login for multiple services, rather than have to manage a longer, more complex password that provides much more security. If a Facebook or Google user forgets their account password, they can go through the account recovery process. If this were to happen to a blockchain user, where the onus is on them to look after their account rather than a third party, the account recovery procedure is much more difficult because there is no centralised party to ease the user's concerns. The challenge of SEED phrase management is a user experience challenge that end users currently in the market are having to deal with (Howle, 2018).

It is essential to close the trust gap by showing users what they can do with blockchain, rather than scaring them off with additional explanations of how the technology works behind the scenes. An insight from an interview with a blockchain developer (whose identity is kept anonymous) was that blockchain works best when the user does not know they are using blockchain. Keeping the language around blockchain jargon-free and simple to understand should also do much to ease users into the world of blockchain.

The next step of the design process is to validate my hypotheses by interviewing experts and designers. The Double Diamond will be used as a model to frame the process to discover the challenges that design teams face when designing for blockchain and to uncover the overall perception of blockchain in the public space. While the likes of the d.school Design Thinking model (d.school, 2010) and the IDEO Human-Centred Design model (IDEO, 2015) are other models that can be used to provide a similar design process, the Design Council's double diamond model is the one most familiar to me.

Discover - Qualitative and Quantitative Research

The Double Diamond (Fig. 7) is a four-stage design process that is based on the notion that "a number of possible ideas are created ('divergent thinking') before refining and narrowing down to the best idea ('convergent thinking')" (Design Council, n.d.). This act of divergent and convergent thinking is where the double diamond gets its shape from. However, the Design Council propose that this diamond-shaped way of thinking occurs twice in the design process.

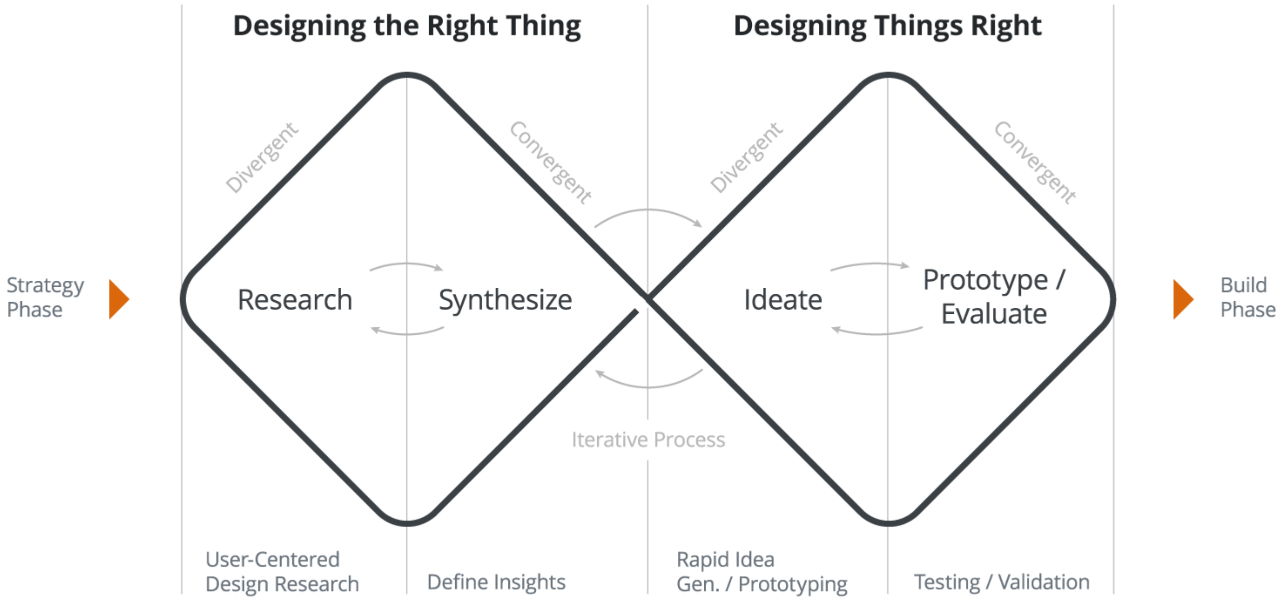


Fig 7: An adapted version of the double diamond that shows the stages where to design the right thing vs. designing the thing right (Stack Overflow, n.d.).

Teams begin by discovering what the problem is, through user research involving desk research, qualitative and quantitative interviews and surveys and immersive experiences. The second step is to define the problem further by narrowing the research scope through synthesising research notes and insights into a workable hypothesis or research question. Next, design teams develop a solution to their problem through rapid prototyping and various levels of fidelity user testing, iterating the design based on user feedback before delivering a refined solution or prototype to the client for testing.

Before I could move forward towards developing a prototype, I needed to understand what is currently providing a barrier for design teams when designing for blockchain. To do this, I spoke at length to several designers and developers who are currently working in the blockchain space. Interviews are among the most familiar strategies for collecting qualitative data (DiCicco-Bloom and Crabtree, 2006). In-depth interviews allow interviewers to pick up on hidden signals that might sometimes say what the interviewee's words do not, through eye contact, body language and even what they have on the desk in front of them. However, because of my current location, all interviews were conducted through online video calling, which did not afford me the opportunity to pick up on these signals.

It was ethically important to gain consent from each interviewee, to be able to use their insights and quotes in this paper. These were obtained in the form of a signed consent form that explained how their data would be used. In addition to in-depth interviews with designers, I sent out an online survey which received thirty-seven responses. Participants were told that their responses would remain anonymous, meaning I did not require them to provide their consent.

Mixing of qualitative and quantitative methodologies is not a new or unique phenomenon (Frels and Onwuegbuzie, 2013, p.184) because assessing the needs of the users and people that one is designing for “necessitates the consideration of multiple sources of data” (Powell et al., 2008, p. 293). Mixing both qualitative and quantitative data has allowed me to tackle the problem from two angles which has ensured that I could ‘design the right things, but design the things right’ (Stack Overflow, n.d.). This means that the solution I propose in this paper will be based on the insights and opportunity areas gathered by asking about the challenges that designers are currently facing while addressing the needs and desires of those who would end up using these innovative new products.

Analysing the Survey Results

From the thirty-seven responses to my online survey I uncovered several insights and commonalities between participants. The most significant percentage of participants (57%) were aged between 25 - 34, with the second largest contingent aged between 35 - 44 (24%). Seventeen participants were British (although some specified as ‘English’) which made up around 46% of participants. Designers and students made up the majority of participants (27% combined), while other occupations varied greatly. Over 75% of participants had heard of blockchain, but very few used it in the form of apps and services.

The online survey aimed to garner an overall perception of blockchain in the general public by asking this original set of questions;

1. How comfortable do you feel when sharing your personal data (including, but not limited to personal details, medical records, finance etc.) with third parties (such as Facebook and Google)?;
2. How comfortable would you feel storing your personal data on an unhackable, digital record network?
3. How comfortable would you feel having sole responsibility for looking after your personal data?
4. What would make you have trust and confidence in using a new digital service?

The wording on these original questions might have skewed the answers somewhat, which led me to believe a lot of the respondents might have focused too much on the inclusion of Facebook and Google. This could have influenced their answers. I wanted to make the message clear; however, this proved to be difficult without being able to explain in detail the reasoning behind the question, while at the same time keeping the answer short and concise. Therefore, I changed the first question halfway through the survey.

The participants were asked to rate how comfortable they were on a scale of 1 to 5, with 1 being 'very uncomfortable' and 5 being 'very comfortable' on the following questions. The below analysis will use the altered wording for the first question.

1. How comfortable do you feel when sharing your personal data (including, but not limited to personal details, medical records, finance etc.) with third parties?

Results for this question varied across the scale, with the majority of participants choosing between 1 - 3; 38% answered with a '3'. These results were interesting as it provided some substance to my hypothesis that people did not feel comfortable with sharing their data. Reasons for their scores included, "it depends on who the company is"; "I don't trust how my data will be used" and "I don't feel in control of my data anymore", with one participant who voted a '5' saying "the benefits currently outweigh the risks".

2. How comfortable would you feel storing your personal data on an unhackable, digital record network?

Results were more favourable to participants feeling more comfortable, with the majority (34%) answering '4'. However, many of the reasons why they chose these answers focused on the 'unhackable' part of this question; this was perhaps partially due to the lack of a shared vocabulary (Blumberg, Cooper and Schindler, p.445). The most common answers wanted to know how unhackable the service would be. From my perception of blockchain, I expected there to be a level of scepticism surrounding the security of blockchain and the reasoning to these answers does much to confirm this thinking.

3. How comfortable would you feel having sole responsibility for looking after your personal data?

35% of participants answered with a '4' followed by 24% of people choosing '5'. These results were somewhat surprising, as I did not expect participants to feel quite as comfortable with taking control of their data. However, this has provided optimism as it shows that people are willing to take on the responsibility if it means keeping it from being misused, although there were still many who questioned how much responsibility they would be in control of and raised concerns about what would happen if they lost access to it. These concerns were discussed in the literature review, and conversations with blockchain designers have told me that finding the answer to how users can alleviate these concerns is an industry-wide headache (Howle, 2018).

4. What would make you have trust and confidence in using a new digital service?

This question was more open-ended as I wanted to discover what particular traits people looked for in new digital services. Nearly 20% of participants mentioned transparency as something they look for which coincides with what Brian Amadon (2018) said in his interview with me. Other things included endorsements from companies or agencies, like the government, guaranteed unhackability, honesty, jargon-free language that talks “in a human way, not a business way” and a clear, easy-to-use interface.

Concluding the Survey

Synthesising the results from the survey shows that the most common demographic were British students or designers aged between 25 - 44. The consensus among respondents was that people did not feel overly confident in providing their personal data to third parties because of a loss of control of data, mistrust in how the data will be used, while some would only provide necessary personal details, dependant on who the company was. A word that came up often ‘transparency’. Organisations and businesses that use blockchain in the future must be clear and transparent in how they use data and the answers from this survey would suggest that this is a significant point of contention for users. This aligns with research found in the literature review that people are rapidly losing trust in those who would lay claim to our data.

The majority of respondents would prefer to store their personal data on ‘an unhackable, digital record network’ (i.e. a blockchain), providing they were assured of the technology’s unhackability. This would suggest that there needs to be some form of education regarding the potential and practicalities of blockchain, not necessarily in how it works, but to “show what the added value is for users over what they already have” (Van der Net, 2018). Van der Net’s point ties in with Rogers’ ‘relative advantage’ characteristic as stated in the literature review: “How improved an innovation is over the previous generation” (Rogers, 1962, p.15).

People would feel reasonably comfortable in taking responsibility for their own data but shared concerns about what this would entail and would require assurances that their data was safe and recoverable in the event of them losing account accessibility. These results raise a lot of ethical questions for designers to consider. For example, how much control do you allow an individual to have? What safety limits need to be put in place to ensure accounts can be recovered? How do they recover their seed phrase? “How to protect [...] the cryptographic keys that allow access [...] to blockchain applications remains a top concern for any organisation or individual interested in using blockchain to transact anything of significant value” (Boireau, 2018). These concerns would require blockchain applications to be reliable and provide sufficient usability for users to feel like there are steps available to help with account recovery. Conversely, it was suggested that it is “unethical to violate people’s trust” (Howle, 2018). The idea of ‘paternalism’, when designers “don’t provide the ability for users to make mistakes” (Howle, 2018), should be avoided to allow users to make their own decisions and ultimately, their own mistakes.

Define - Insights and Themes from Interviews

A critical piece of the Ideation phase is plucking the insights that will drive [the] design out of the huge body of information [...] gathered (IDEO, 2015, p. 81). Throughout the interviews I have undertaken I have asked each interviewee the same set of questions to provide a fair testing environment to allow for the clustering of any themes and insights. As each interviewee provided their answers to each question, it quickly became apparent that there were a certain number of themes that designers in blockchain face in the form of currently unsolved problems. However, both Mills and Howle expressed concern with the wording around my central research question, "How might we make self-sovereign identity socially acceptable?". Both were saying the connotation of something being socially acceptable meant people would be judged for using blockchain and self-sovereign identity technology (Howle, 2018; Mills, 2018b).

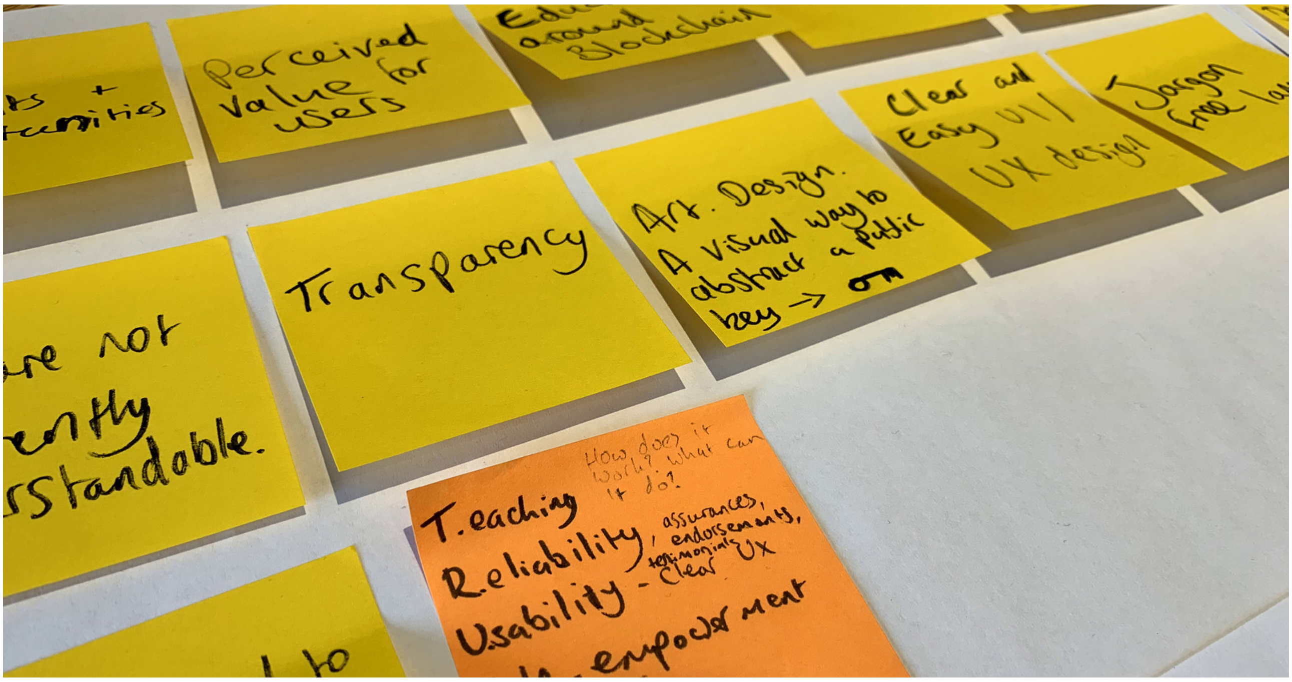
User experience (UX) and user interface (UI) design came up a lot in each interview, which corroborates with the results of the online survey. One point that Brian Amadon made was that "clear UX is important; If it's hard to use, it's hard to adopt" (Amadon, 2018), while Mark van der Net told me that "apps are not currently understandable" and there needs to be "a visual way to abstract a public key into a physical or material thing" (van der Net, 2018). Van der Net suggested that we can use visual design to make complex components of blockchain easier to understand by turning them into things we recognise, like a key icon can be used to describe a user's public key, for example (van der Net, 2018). However, there is some suggestion in the wider design space that "simplifying certain concepts can actually misinform or create confusion later" (Mills, 2017). I agree with Mills on the idea that visual iconography can sometimes be hindering, rather than helpful, and my suggestion would be that there is a mix of both text and icons to help with clarity on what an option does. An icon can sometimes clarify what something means by turning it into something more recognisable and vice-versa.

Many of the interviewees spoke of keeping apps and services transparent. One particular point that an interviewee made was for businesses to define what they would need to use blockchain for. If businesses are transparent with how they use data, it should help alleviate some of the concerns that many of the survey respondents had regarding what happens to their data.

However, there is a trade-off between transparency and confidentiality: the more information is shared, the more transparent the business will be, and the more potential for business secrets and confidentiality to be compromised (Wang and Kogan, 2018, p.1). There are two ways for businesses to use blockchain; public, or private (also known as permissionless or permissioned, respectively). If a business uses a permissionless blockchain, they provide the transparency that users are concerned about.

However, as Wang and Kogan point out, this means their rivals have full disclosure of pricing strategies, transactions and any other detail that would otherwise be kept out of public view. Full disclosure can be avoided by making the blockchain private, but this can also require an intermediary to look after the blockchain - which concentrates the operational risk in a single or several points of failure (Wang and Kogan, 2018, p.2), effectively negating the point of using a blockchain in the first place. Businesses will need to decide if the benefits of using blockchain outweigh the risks.

The interviews also revealed the need to integrate blockchain into existing processes without having to create something new from the ground up. If services can be developed with blockchain so that there could be a seamless transition from a service that does not currently use blockchain to one that does, can facilitate the early stages of trust. What these interviews revealed ties back into what Rogers (1962, pp.15-16) was referring to in the context of 'trialability' and to a lesser extent 'observability'. If a user can continue using a service with enhanced security features without really noticing a difference, it can be argued that the user is 'trialling' and 'observing' those security features without having to make a conscious decision. However, in the name of transparency, users must be notified that their data is being held on a blockchain so they can make an informed decision on whether to continue using the service or not.


Perceived Value for users
Education around Blockchain
Clear and Easy UI/ UX design
Jargon free lan
Transparency
Art. Design. A visual way to abstract a public key → on
re not ently standable.
How does it work? What can it do?
Teaching
Reliability, assurances, endorsements, testimonials
Usability - Clear UX
empowerment

Synthesising the themes and insights taken from the interviews.

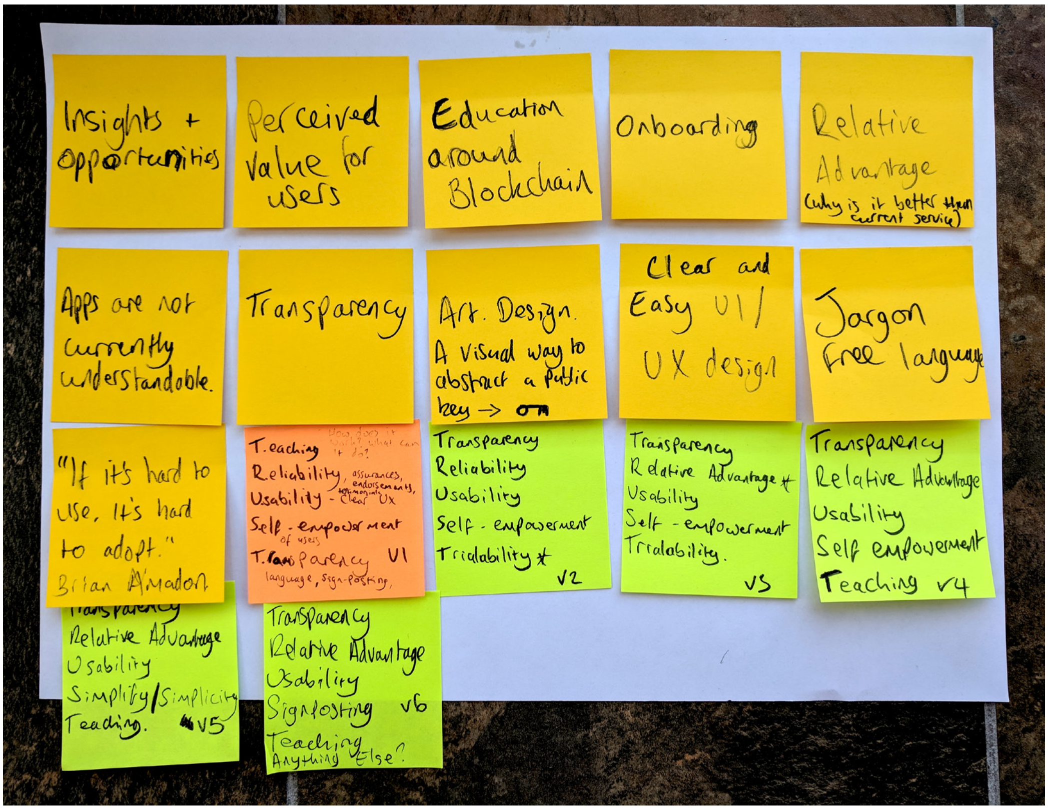
(Personal archive, 2018)

Develop - Prototyping the idea

By the end of the interviews, I pulled out the recurring themes and insights and began to consider how they could be taken forward. The themes I worked with were:

- Transparency
- Reliability
- Relative Advantage (or added value for users)
- Simplicity
- Self-Empowerment of users
- Usability
- Education of technology
- Onboarding
- Clear UX
- Jargon-free language

The interviews and literature review have changed the scope of my research questions. It has become apparent to me that, while I still believe that self-sovereign identity is an excellent technology to protect user data, it will not matter in the long run if nobody trusts it enough to use it. Trust needs to be built into all blockchain technologies and the related products and services. Therefore, the focus of my work has shifted to answering the newly formed research question, "How might we consider trust when developing blockchain products and services?".

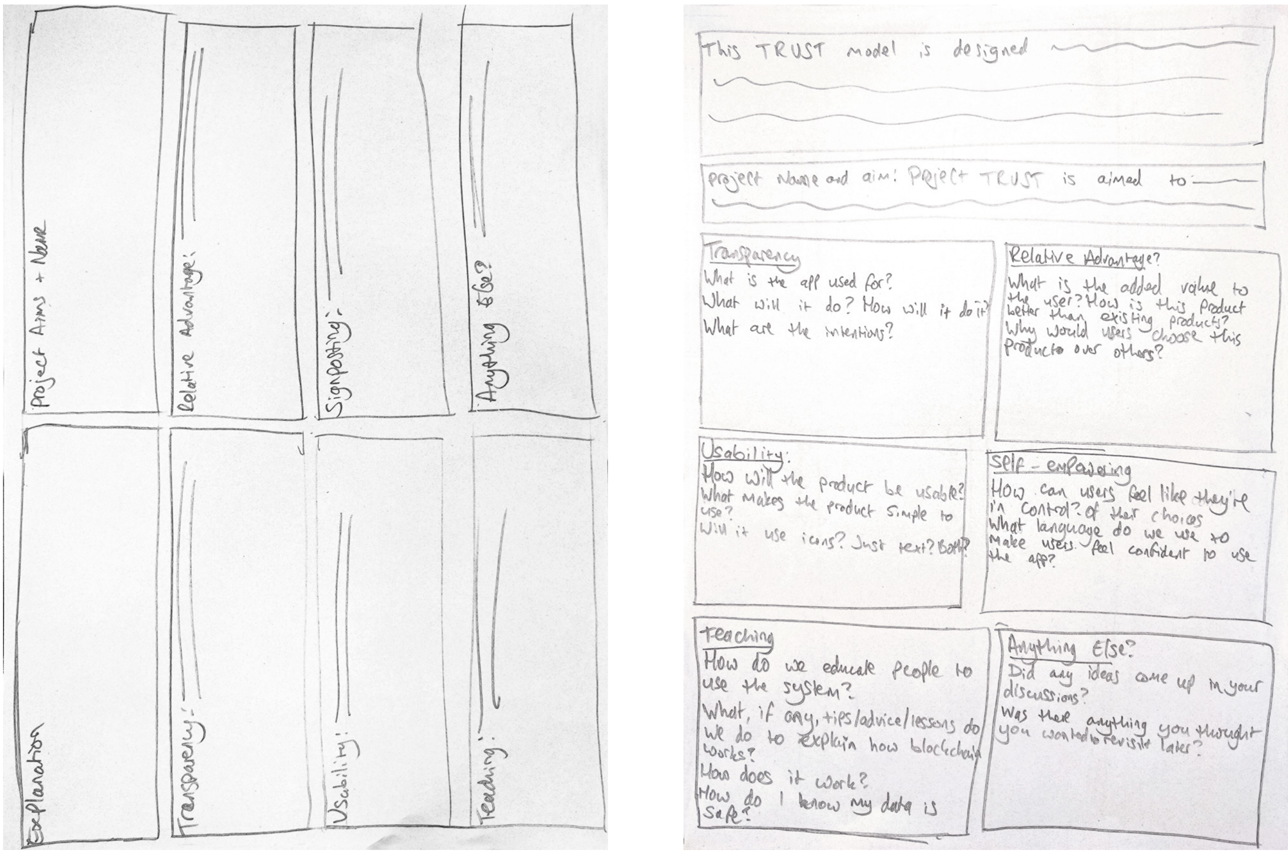

Insights + opportunities
Perceived value for users
Education around Blockchain
Onboarding
Relative Advantage (why is it better than current service)
Apps are not currently understandable.
Transparency
Art. Design. A visual way to abstract a public key →
Clear and Easy UI / UX design
Jargon free language
"If it's hard to use, it's hard to adopt." Brian A'Madon
T.eaching How does it work? what can it do? Reliability, assurances, endorsements, testimonials Usability - Clear UX Self-empowerment of users T.ransparency V1 language, sign-posting,
Transparency Reliability Usability Self-empowerment Trialability * V2
Transparency Relative Advantage * Usability Self-empowerment Trialability. V3
Transparency Relative Advantage Usability Self empowerment Teaching v4
Transparency Relative Advantage Usability Simplify/Simplicity Teaching. V5
Transparency Relative Advantage Usability Signposting v6 Teaching Anything Else?

Exploring the various configurations of the T.R.U.S.T. Model from the themes taken from interviews (Personal archive, 2018)

Using the above themes from my insights, I worked with several configurations of the characteristics in the model, and finally settled on: transparency, relative advantage, usability, signposting and teaching. These letters spelt out the word ‘TRUST’.

The first round of prototyping revealed that the format of the model did not flow correctly because of its landscape orientation. There also wasn’t any space to allow design teams to flesh out their ideas, so a whole new worksheet was developed to allow teams to transfer an idea from mind to paper quickly. The resulting prototype is the ‘Trust Ideation Worksheet’ which focuses on allowing design teams to come up with design concepts for new blockchain apps, products or services, with a view to ensuring that trust has been considered in the development of the product’s foundations.

The ‘Idea Building Blocks’ tool on the first page is developed as a way for teams to get ideas flowing. The model can be used to quickly give substance to an idea that blockchain design teams have. This will enable individuals to talk to their design team members about the thinking behind the idea, or to express ideas and give


Project Aims + Name
Relative Advantage:
Signposting:
Anything Else?
Explanation
Transparency:
Usability:
Teaching:
This TRUST model is designed
Project Name and aim: Project TRUST is aimed to:
Transparency
What is the app used for?
What will it do? How will it do it?
What are the intentions?
Relative Advantage?
What is the added value to the user? How is this product better than existing products?
Why would users choose this product over others?
Usability:
How will the product be usable?
What makes the product simple to use?
Will it use icons? Just text? Both?
Self - empowering
How can users feel like they're in control? of their choices
What language do we use to make users feel confident to use the app?
Teaching
How do we educate people to use the system?
What, if any, tips/advice/lessons do we do to explain how blockchain works?
How does it work?
How do I know my data is safe?
Anything Else?
Did any ideas come up in your discussions?
Was there anything you thought you wanted to revisit later?

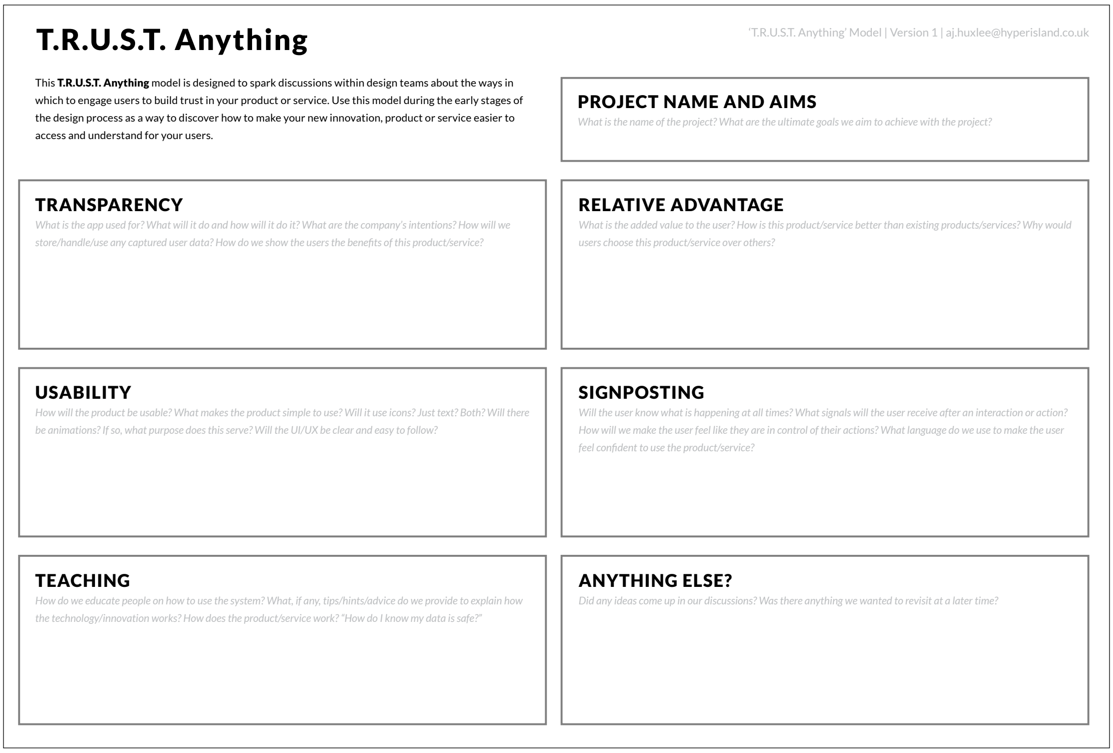
Low fidelity prototype in the early stages of ideation.

(Personal archive, 2018)

them some form while backing up why the idea is relevant to the project. It has been developed so team members can show what the purpose of the idea is and what problem it aims to solve.

The 'T.R.U.S.T. Model' on page 2 is about fleshing out how trust can be built into the idea by getting team members to ask questions. That idea can be iterated on further by discussing how to make it address some of the concerns that inhibit people's reasoning to trust a new product, based on results from the survey and insights gathered from interviewees. The 'T.R.U.S.T. Model' can be used to validate whether an idea would be good for target users, and by asking relevant questions around each of the idea's characteristics.

After the first iteration of the prototype had been developed to a point where I could gain further feedback, it was sent to the people I'd interviewed to get some external thoughts on its feasibility and if they thought it would work. Due to the location of my interviewees, all of whom were not based in the UK and spread across various time-zones, feedback had to be gathered remotely through emails and video calling. As a result, I was unable to test how the model would have worked within the context of a design brief, which I believe would have yielded much stronger feedback and would have enabled me to gain first-hand experience of seeing it being tested in-situ. Having to wait for responses from those asked was frustrating and meant the window for gaining feedback on the model shrank each day.



T.R.U.S.T. Anything

'T.R.U.S.T. Anything' Model | Version 1 | aj.huxlee@hyperisland.co.uk

This **T.R.U.S.T. Anything** model is designed to spark discussions within design teams about the ways in which to engage users to build trust in your product or service. Use this model during the early stages of the design process as a way to discover how to make your new innovation, product or service easier to access and understand for your users.

PROJECT NAME AND AIMS

What is the name of the project? What are the ultimate goals we aim to achieve with the project?

TRANSPARENCY

What is the app used for? What will it do and how will it do it? What are the company's intentions? How will we store/handle/use any captured user data? How do we show the users the benefits of this product/service?

RELATIVE ADVANTAGE

What is the added value to the user? How is this product/service better than existing products/services? Why would users choose this product/service over others?

USABILITY

How will the product be usable? What makes the product simple to use? Will it use icons? Just text? Both? Will there be animations? If so, what purpose does this serve? Will the UI/UX be clear and easy to follow?

SIGNPOSTING

Will the user know what is happening at all times? What signals will the user receive after an interaction or action? How will we make the user feel like they are in control of their actions? What language do we use to make the user feel confident to use the product/service?

TEACHING

How do we educate people on how to use the system? What, if any, tips/hints/advice do we provide to explain how the technology/innovation works? How does the product/service work? "How do I know my data is safe?"

ANYTHING ELSE?

Did any ideas come up in our discussions? Was there anything we wanted to revisit at a later time?

Initial ideation of the T.R.U.S.T. Model

(Personal archive, 2018)

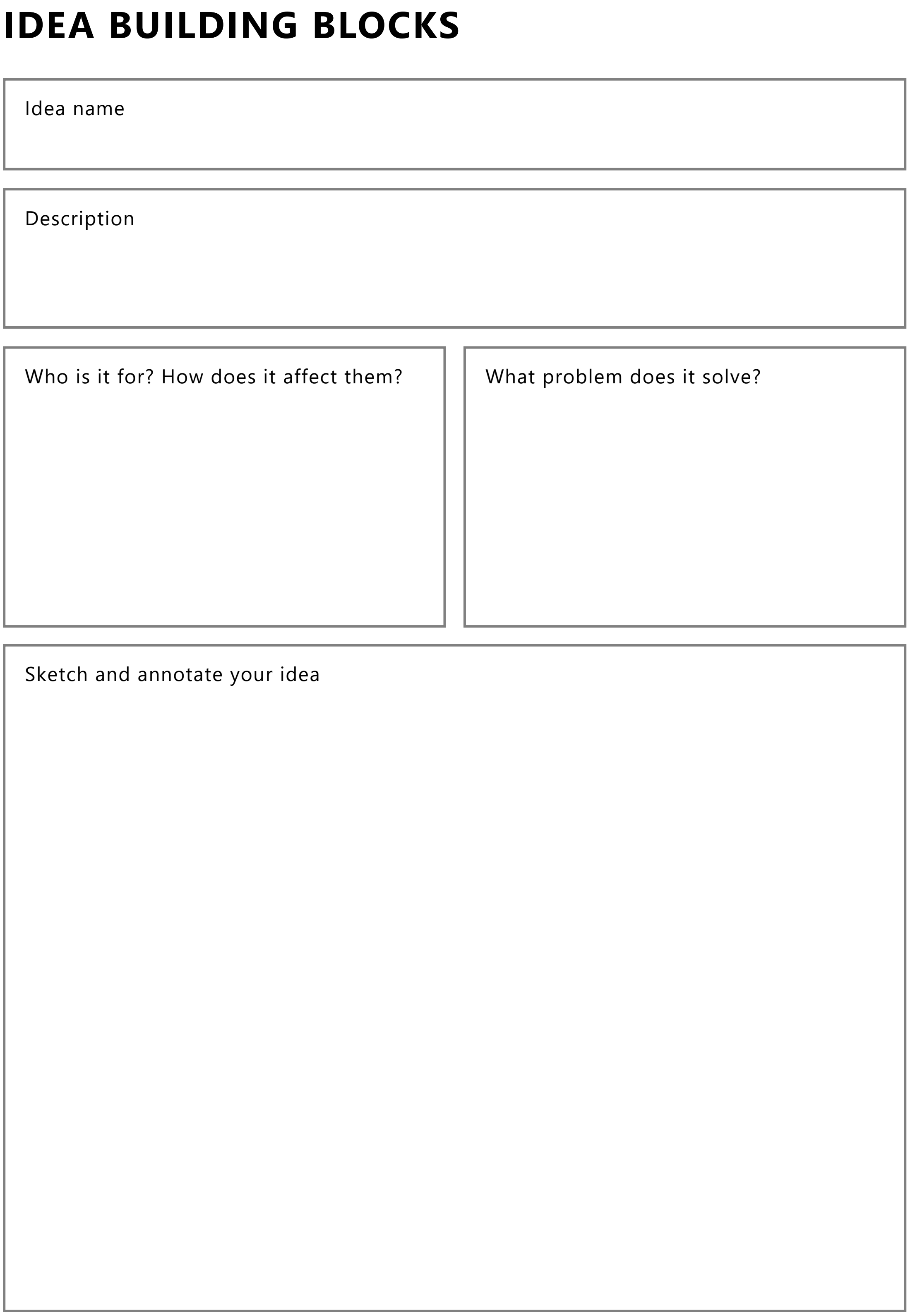
Deliver - Prototype Feedback and Iteration

Initial feedback on the prototype was positive. Respondents said the model made sense on first impressions. The instructions that came with the worksheet were clear, and the worksheet was “actionable” (Melo, 2018). Additionally, the canvas had been “developed into what designers/entrepreneurs are doing in real-life”, and will help guide “the development of new ideas” (Marques, 2018). The consensus around the model was that it functioned as a model that could be used for any idea or concept, and not primarily limited to blockchain products and services, which was pleasing. Javier Tarazaga, Co-Founder of blockchain development start-up Superblocks, said the model looked interesting and he would love to try it out in a design project.

However, interviewees all expressed concerns with the nature of the questions that had been provided on the ‘T.R.U.S.T. Model’. The questions provided in the prototype were designed to be example questions to help provide a bit of context on the kind of conversations design teams have around trust. For example, the ‘Usability’ section asks the question, “Will the UI/UX be clear and easy to follow?”, which Pedro Marques, Product Designer for Personio, pointed out that the answer from UX designers would always be ‘yes’ and went on to say “designers want to create a clear and easy to follow UX, but that’s the challenge, right?” (Marques, 2018). I did not anticipate this and amended the model to clearly express that these questions were examples only and provided design teams with a blank template to enable them to add their own notes.

Opinions were split on which of the two tools (Idea Building Blocks (“page 1) and T.R.U.S.T. Model (“page 2”)) worked best. Albert Zikmund believed the page 1 model was not as useful because of the existence of similar tools, while Marques believed the page 1 model was “a quite simple and straightforward representation of an idea/concept” (Marques, 2018). Conversely, Zikmund said, “The idea of the T.R.U.S.T. [model], feels very important. I believe that the technology is progressing so fast, there’s no time to think about the people that are using it” (Zikmund, 2018). All respondents agreed that the model could be used outside of the scope of blockchain projects because “any design process/product development cycle can use the model to give the team involved a better understanding of an idea. Plus, data security is something that is needed in every product, so I don’t think it is a blockchain-focused model” (Marques, 2018).

Gabriel Melo, a UX Designer, believed there ought to be a section for design teams to add in their own definition of what trust means. “There are many questions about many parts of an idea, and without a clear agreement on what the end goal is, it is easy for the discussion to lead to many answers but miss the point of the exercise” (Melo, 2018). Melo’s suggestion provided a valid point, and so the next iteration of the T.R.U.S.T. model was adapted to include a section for teams to define trust in their own words.



IDEA BUILDING BLOCKS

Idea name

Description

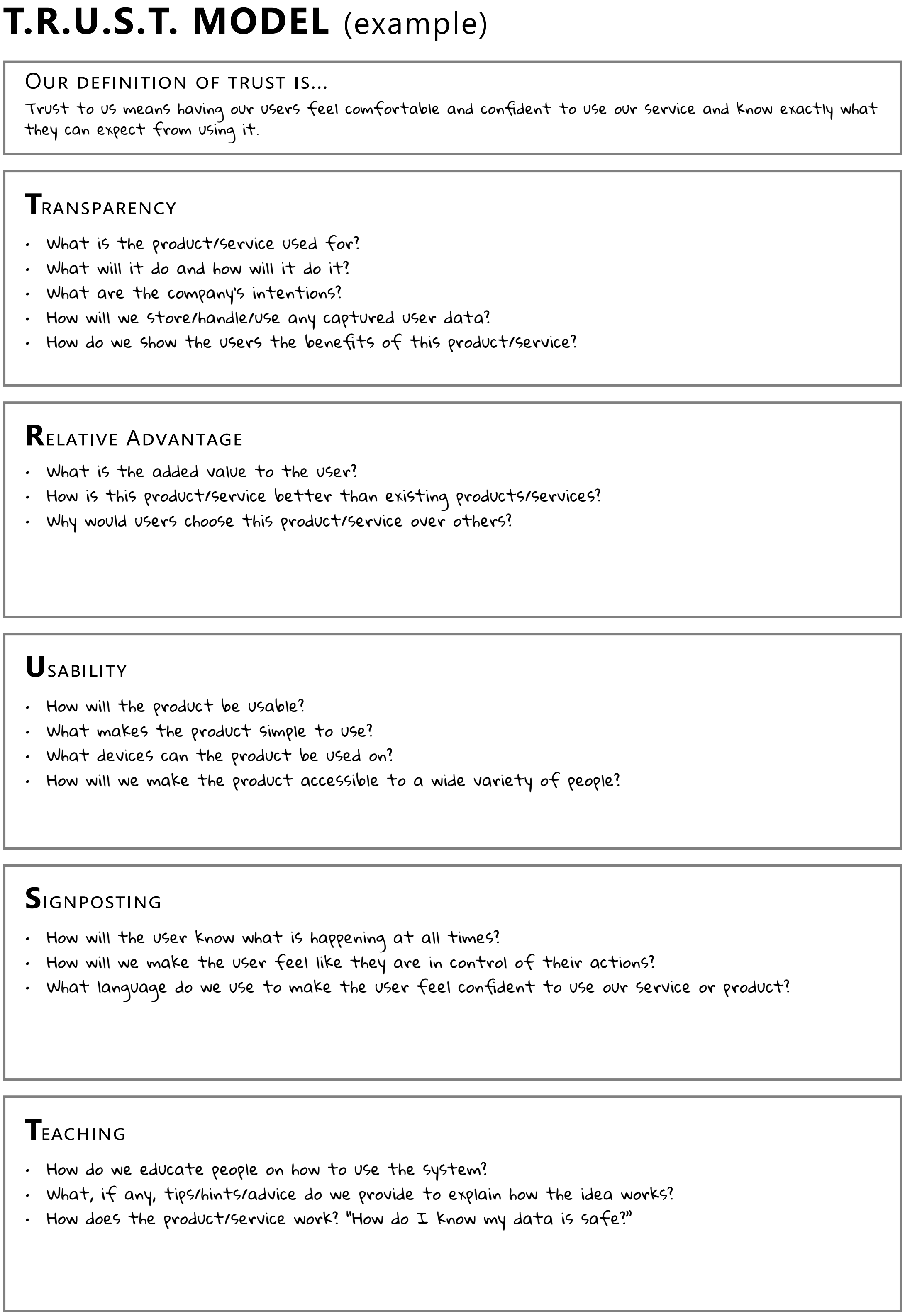
Who is it for? How does it affect them?

What problem does it solve?

Sketch and annotate your idea

Page 1 of the final version of the Trust Ideation Worksheet.

(Personal archive, 2018)



T.R.U.S.T. MODEL (example)

Our definition of trust is...

Trust to us means having our users feel comfortable and confident to use our service and know exactly what they can expect from using it.

Transparency

- What is the product/service used for?
- What will it do and how will it do it?
- What are the company's intentions?
- How will we store/handle/use any captured user data?
- How do we show the users the benefits of this product/service?

Relative Advantage

- What is the added value to the user?
- How is this product/service better than existing products/services?
- Why would users choose this product/service over others?

Usability

- How will the product be usable?
- What makes the product simple to use?
- What devices can the product be used on?
- How will we make the product accessible to a wide variety of people?

Signposting

- How will the user know what is happening at all times?
- How will we make the user feel like they are in control of their actions?
- What language do we use to make the user feel confident to use our service or product?

Teaching

- How do we educate people on how to use the system?
- What, if any, tips/hints/advice do we provide to explain how the idea works?
- How does the product/service work? "How do I know my data is safe?"

Page 2 of the final version of the Trust Ideation Worksheet.

(Personal archive, 2018)

User Testing

Once the model had been sufficiently iterated on based on designer feedback, I needed to validate if it had addressed some of the concerns expressed by the respondents to my earlier survey, looking at the general perception of blockchain from users. The prototype was presented to a sample of respondents who were asked to answer a new set of questions to see if their previous concerns had been addressed and if their opinions towards blockchain had changed. By including the original participants in the experience design process, I have ensured the human-centred aspect remains key by getting opinions from the people whose activity and experiences will ultimately be affected most directly by a design outcome (Iversen, Halskov and Leong, 2012, p.87).

Q: Have your scores to the above three questions changed? Why?

User responses were varied, which was expected, given the variety in the scores provided by each respondent in the survey. However, what was not expected was that respondents said their scores had not changed upon introduction to the model. It could be argued that a degree of trust in the model needs to be built up first before people's opinions change. Conversely, one respondent said that her opinions on blockchain have changed since she had read up on it more. This change in attitude towards blockchain is optimistic and shows that providing context and education around the technology in the first place can immediately ease concerns.

Q: If a product was developed with the five T.R.U.S.T. characteristics in mind, would this address some of the concerns you expressed in your previous answers? Why?

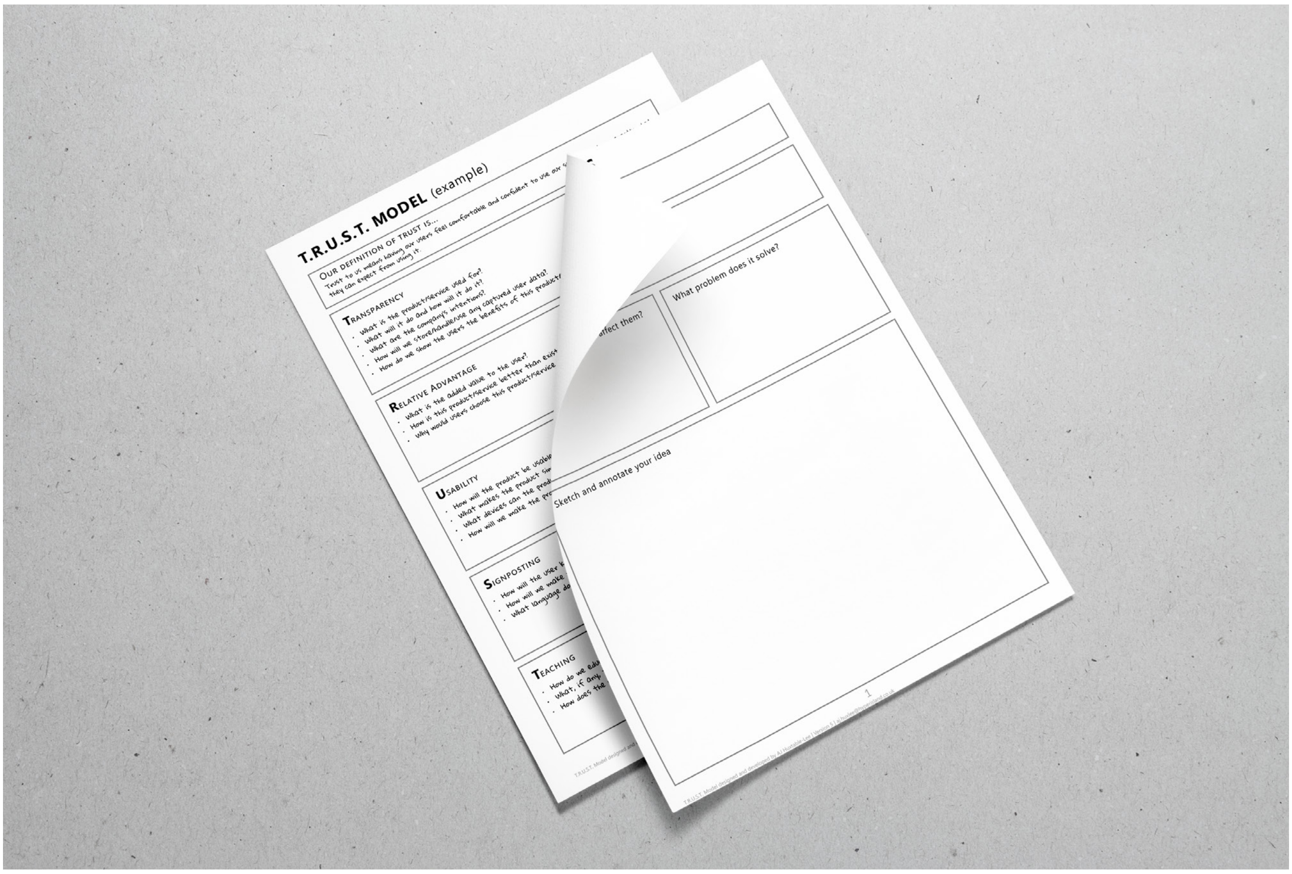
All respondents agreed that the T.R.U.S.T. Model would address some of their concerns as it would make design teams consider and be aware of some of the issues that could come up in a design project. Melissa Ma said, "When used successfully, can lead to better ideas that help teams identify and address important needs and concerns" (Ma, 2018). It is fair to say that design teams will come up with relevant questions based on the user research that will allow them the opportunity to build trust in their products. Jamie Bolland said of the model, "breaking down the elements of trust is much more useful than asking designers to simply consider "trust" in a more abstract way. I think that it's more likely to lead to successful outcomes" (Bolland, 2018).

Q: Does the model make sense from a user perspective?

All respondents believed it made sense from a user perspective as it took the user needs and desires into consideration. This provides optimism as it meant the human-centred aspect of the design had shone through and completed its task of building a product around addressing real issues rather than assuming the model is what was needed. It was also mentioned to make it clearer where in the design process the model should be used, or even if it was a model that could be referred back to throughout the course of the project (Bolland, 2018).

Q: Is there anything else you would change about the model?

Some of the respondents were concerned about how the T.R.U.S.T. Model values would be implemented into a product. In future revisions of the model, I believe it would be beneficial to explain that the model is best used to start conversations and raise awareness of the attributes that help make products trustworthy, rather than the model being a “comprehensive way to address all the intricacies of each question” (Ma, 2018).



T.R.U.S.T. MODEL (example)

OUR DEFINITION OF TRUST IS...
Trust to us means having our users feel comfortable and confident to use our s
they can expect from using it.

TRANSPARENCY
- What is the product/service used for?
- What will it do and how will it do it?
- What are the company's intentions?
- How will we store/handle/use any captured user data?
- How do we show the users the benefits of this product

RELATIVE ADVANTAGE
- What is the added value to the user?
- How is this product/service better than exist
- Why would users choose this product/service

USABILITY
- How will the product be usable
- What makes the product sim
- What devices can the produ
- How will we make the pro

SIGNPOSTING
- How will the user k
- How will we make
- What language do

TEACHING
- How do we edu
- What, if any,
- How does the

T.R.U.S.T. Model designed and

affect them?

What problem does it solve?

Sketch and annotate your idea

1

T.R.U.S.T. Model designed and developed by AJ Huxtable-Lee | Version 5 | aj.huxlee@hyperisland.co.uk

Final version of the Trust Ideation Worksheet.

(Personal archive, 2018)

04.

CONCLUSION

Conclusion

This project set out to explore ways that people can use emerging technologies to safeguard their data in the future in the wake of the Cambridge Analytica scandal and the process that people go through before deciding to trust and use those technologies. My feelings of frustration, helplessness and anger spurred my decision to dig deep into blockchain and self-sovereign identity technologies that are currently making waves in the digital world. However, from the conversations I had been a part of around blockchain, I had gathered the feeling that there was a sense of scepticism surrounding the technology. This was the basis for my first hypothesis which ultimately turned into the direction I wanted to take this project. I wanted to explore how to make self-sovereign identity 'socially acceptable'.

Answers from an online survey confirmed that there was a scepticism around blockchain, partly stemming from a misunderstanding of how the technology works. However, the literature review highlighted another problem in technology in general, particularly with new technologies and innovations. There are phases of adoption that the public will subconsciously go through when a new technology emerges, as shown in the technology life cycle (see Fig. 2, on page 19). The technology life cycle shows that adoption begins with early adopters in society and it would be beneficial to show my work to those known as evangelists, if I am to make further progress with my work.

Trust plays a key factor in the adoption of innovations and the more I researched, the more I came to realise that the nature of the technology is not wholly important as all technologies follow the same pattern of adoption. Insights from interviews continuously provided trust as a theme to explore and this discovery enabled me to shift the focus of my project to explore how we might consider trust when developing new blockchain products and services.

The 'Trust Ideation Worksheet' that I have developed has been put to the designers and developers I had previously interviewed and while there were some suggestions regarding the wording on the example questions and minor improvements, the general consensus of the model was positive. The designers told me they could see a use for it in projects in the future and it highlighted questions and considerations that are normally taken for granted (Tarazaga, 2018). Tarazaga also told me he would be looking to use the model in his next project at Superblocks, although nothing had been arranged at the time of writing and I suspect this will happen outside the timeframe of this project.

From a customer perspective, the T.R.U.S.T model has the potential to start conversations in design teams around building trust into products and services. However, as expected, there is still plenty of room for improvement and iterations. The outlook for the Trust Ideation Worksheet looks positive, but it remains to be seen how much of an impact it will have on the development of new products and services when used in a working environment.

Future Steps

I aim to continue developing the model outside the timeframe of this project by introducing the model to evangelists and early adopters of blockchain technology, as well as academics and experts that work in the field of trust. While I feel like the model is a good starting point to kick start conversations in the design process, I know there is room for further iterations and improvements. I also have a 'phase two' concept that I would like to explore that turns the model into a more tangible asset, through the development of 'blocks' that can encourage conversations around trust. Based on feedback from users and designers alike, I intend to adapt the prototype to be usable in other areas of design and not limited to only blockchain.

Additionally, I plan to publish my work with a view to collaborating with any designers or agencies that see the potential in my research. Before my work is published, I will seek consent from those who have participated in my research and act accordingly if anyone does not wish to be a part of the published work.

Reflections

What worked well?

Using a human-centred approach in an experience design process really enabled me to focus my thoughts and project structure. I feel the results of both the qualitative and quantitative research helped to shape the subsequent stages of my project. Without the answers from the respondents of my survey, I would not have had a basis with which to build my prototype, and the insights and opportunities revealed in the interviews provided the necessary themes to incorporate into the T.R.U.S.T. Model. I am particularly pleased with the direction my project went in after learning about Rogers' five characteristics that determine a person's decision to adopt or reject an innovation and the trust equation. I believe these two discoveries were my 'Eureka!' moments.

What did not work well?

Having to conduct all of my interviews and discussions through remote video calls and online communications was incredibly frustrating. Unstable internet connections, different time-zones and busy schedules meant there was a lot of waiting around for responses to my questions and requests. It is difficult to say how much of an influence this has had on my project, but if I had been meeting these people in person, then perhaps some of the answers or observations might have yielded different results. Additionally, not having the opportunity to embed myself in a design team meant I was not able to pick up valuable industry experience from working with teams and individuals, where I believe I would learned a lot.

What did I learn?

At the beginning of this project, I had almost no knowledge of blockchain and self-sovereign identity. I have learned a considerable amount about how blockchain works and the security behind it, as well as the concerns expressed by those currently in the field. I have also learned that there is an almost unconscious process that the majority of people go through when deciding on whether to adopt new technologies, based on Rogers' findings in his book Diffusion of Innovations and the Equation of Trust. I found it fascinating to dig deep into the fundamentals of trust in people and would like to continue to learn more about it going forward. Designing for trust was a new facet of the human-centred design approach that I will consider in future projects.

What would I do differently?

While I found the insights from designers and developers valuable, I believe it would have been even more beneficial to talk to people whose expertise is working with trust (Rachel Botsman, as just one example). Researching and reading about the various models and characteristics of trust is useful, but I believe talking to those experts in a one-to-one environment and being able to ask questions directly to them would have been incredibly fruitful. It would also have been beneficial to embed myself within a design team where the opportunity to test my model in a working environment could have had a profound effect on the feedback I received, the iterations I made and the working experience of using it in-situ.

05.

REFERENCES & FIGURES

Primary References and Interviews

All interview manuscripts are available on request.

Anonymous Blockchain Developer. (2018). Personal communication. *Interview regarding the challenges designers and developers face when designing for blockchain. Interviewee expressed their wish to remain anonymous.* [Interviewed on 13th Oct. 2018].

Amadon, B. (2018). Personal communication. *Interview regarding the challenges designers and developers face when designing for blockchain.* [Interviewed on 1st Oct. 2018].

Baker Mills, S. (2018b). Personal communication. *Email conversation regarding the challenges designers and developers face when designing for blockchain.* [Interviewed on 19th Oct. 2018].

Bolland, J. (2018). Personal communication. *User testing on prototype.* [Testing took place on 9th Nov. 2018].

Hemrajani, R. (2018). Personal communication. *User testing on prototype.* [Testing took place on 5th Nov. 2018].

Howle, J. (2018). Personal communication. *Interview regarding the challenges designers and developers face when designing for blockchain.* [Interviewed on 26th Sep. 2018].

Ma, M. (2018. Personal communication. *User testing on prototype.* [Testing took place on 4th Nov. 2018].

Marques, P. (2018). Personal communication. *Provided feedback on prototype.* [Interviewed on 27th Oct. 2018].

Melo, G. (2018). Personal communication. *Provided feedback on prototype.* [Interviewed on 27th Oct. 2018].

Solari, K. (2018). Personal communication. *User testing on prototype.* [Testing took place on 4th Nov. 2018].

Tarazaga, J. (2018). Personal communication. *Interview regarding the challenges designers and developers face when designing for blockchain.* [Interviewed on 25th Oct. 2018].

Van der Net, M. (2018). Personal communication. *Interview regarding the challenges designers and developers face when designing for blockchain.* [Interviewed on 11th Oct. 2018].

Zikmund, A. (2018). Personal communication. *Provided feedback on prototype.* [Interviewed on 31st Oct. 2018].

References

Accenture. (n.d.). Blockchain, *Accenture.* [online]. Available at: https://www.accenture.com/gb-en/insights/blockchain-index?src=LINKEDINJP&c=gb_gb_blockchain_10348988&n=psgs_generic_0818&gclid=EAIaIQobChMIiuvlsuvE3gIVBbftCh2YLQeUEAAYAiAAEgL5kPD_BwE [Accessed 8th Nov. 2018].

Aitken, R. (2018). IBM Blockchain Joins Sovrin's 'Decentralized' Digital Identity Network To Stem Fraud, *Forbes.* [online] Available at: https://www.forbes.com/sites/rogeraitken/2018/04/05/ibm-blockchain-joins-sovrins-decentralized-digital-identity-network-to-stem-fraud/#3bfa5cb215ed [Accessed 15th Sep. 2018].

Baars, D. (n.d.). Towards Self-Sovereign Identity using Blockchain Technology, *University of Twente.* [online] Available at: https://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf [Accessed 1st Sep. 2018].

Babkin, A., Golovina, T., Polyanin, A. and Vertakova, Y. (2018). Digital model of sharing economy: blockchain technology management. *SHS Web of Conferences,* [online] Vol. 44. Available at: https://doi.org/10.1051/shsconf/20184400011 [Accessed 27 Oct. 2018].

Baker Mills, S. (2017). Blockchain Design Principles, *Medium.* [online]. Available at: https://medium.com/design-ibm/blockchain-design-principles-599c5c067b6e [Accessed 15th Oct. 2018].

Baker Mills, S. (2018a). Designing for Blockchain: What's Different and What's at Stake, *Medium.* [online] Available at: https://media.consensys.net/designing-for-blockchain-whats-different-and-what-s-at-stake-b867eeade1c9 [Accessed 6th Sep. 2018].

Berger, E. and Pain, F. (2017). Model and Mobilise Imaginary for Innovative Experience Design, *The Design Journal.* [online] Vol. 20(1), pp. S4690-S4696. Available at: https://doi.org/10.1080/14606925.2017.1352967 [Accessed 27th Oct. 2018].

Blockgeeks. (2018). What Is Hashing? Under The Hood Of Blockchain. [online] *Blockgeeks.com*. Available at: https://blockgeeks.com/guides/what-is-hashing/ [Accessed 1st Sep. 2018].

Blumberg, B., Cooper, D.R. and Schindler, P.S. (2005). *Business research methods.* London: McGraw-Hill.

Bradford, C. (2018). 5 Common Encryption Algorithms and the Unbreakables of the Future, *StorageCraft Recovery Zone.* [online] Available at: https://blog.storagecraft.com/5-common-encryption-algorithms/
[Accessed 22nd Aug. 2018].

Boireau, O. (2018). Securing the blockchain against hackers, *Network Security.* [online]. Vol. 2018(1), pp. 8-11. Available at: https://doi.org/10.1016/S1353-4858(18)30006-0 [Accessed 11th Oct. 2018].

Carbone, C. (2015). To Be or Not To Be Forgotten: Balancing the Right to Know with the Right to Privacy in the Digital Age, *Virginia Journal of Social Policy & the Law.* [online] Vol. 22(3), pp.526 - 560. Available at: https://heinonline-org.ezproxy.tees.ac.uk/HOL/Page?collection=journals&handle=hein.journals/vajsplw22&id=570&men_tab=srchresults [Accessed 24th Oct. 2018].

Chan, J. (2018). Design ethics: Reflecting on the ethical dimensions of technology, sustainability, and responsibility in the Anthropocene, *Design Studies.* [online] Vol. 54, pp.184-200. Available at: https://doi-org.ezproxy.tees.ac.uk/10.1016/j.destud.2017.09.005 [Accessed 11 Nov. 2018].

Cicchitto, N. (2017). Why Do We Use Usernames And Passwords?, *Forbes.* [online] Available at: https://www.forbes.com/sites/forbestechcouncil/2017/10/31/why-do-we-use-usernames-and-passwords/#62ae86c71fda [Accessed 24th Sep. 2018].

Cook, J. and Archer, J. (2018). Telegraph investigation: Google search exposes sensitive files and emails from inside the government and the NHS, *Telegraph*. [online] Available at: https://www.telegraph.co.uk/technology/2018/07/21/telegraph-investigation-google-search-exposes-sensitive-government/ [Accessed 24th Aug. 2018].

Corradi, F. and Höfner, P. (2018). The disenchantment of Bitcoin: unveiling the myth of a digital currency, *International Review of Sociology.* [online] Vol. 28(1), pp. 193-207. Available at: http://doi.org/10.1080/03906701.2018.1430067 [Accessed 26th Oct. 2018].

Council on Foreign Relations. (2016). Keeping the Edge: U.S. Innovation, *Council on Foreign Relations.* [online]. Available at: https://www.cfr.org/report/keeping-edge-us-innovation [Accessed 22nd Oct. 2018].

Design Council. (n.d.). The Design Process: What is the Double Diamond?, *Design Council.* [online] Available at: https://www.designcouncil.org.uk/news-opinion/designprocess-what-double-diamond [Accessed 20 Feb. 2018].

DeVries, W. T. (2003). Protecting privacy in the digital age, *Berkeley Technology Law Journal.* [online]. Vol. 18(1), pp. 283 - 311. Available at: http://web.a.ebscohost.com.ezproxy.tees.ac.uk/ehost/detail/detail?vid=0&sid=05aa9353-8088-4236-9d1d-a224f1ec3850%40sdc-v-sessmgr03&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=9816605&db=bth [Accessed 24th Oct. 2018].

Dhamija, R. (2008). The Seven Flaws of Identity Management: Usability and Security Challenges, *IEEE Security & Privacy* [online] Vol. 6(2), pp. 24-29. Available at: https://ieeexplore-ieee-org.ezproxy.tees.ac.uk/stamp/stamp.jsp?tp=&arnumber=4489846 [Accessed 6th Sep. 2018].

DiCicco-Bloom, B. and Crabtree, B. (2006). The qualitative research interview, *Medical Education.* [online] Vol. 40(4), pp.314-321. Available at: http://doi.org/10.1111/j.1365-2929.2006.02418.x [Accessed 9 Oct. 2018].

Di Gregorio, M. (2017). Blockchain: A new tool to cut costs, *PricewaterhouseCoopers.* [online] Available at: https://www.pwc.com/m1/en/media-centre/articles/blockchain-new-tool-to-cut-costs.html [Accessed 15th Sep. 2018].

Drozdeck, S. and Fisher, L. (2003). *The Trust Equation.* 1st ed. Financial Forum.

Duretec, K. and Becker, C. (2017). Format Technology Lifecycle Analysis, *Journal of the Association for Information Science & Technology.* [online]. Vol 68(10), pp. 2484-2500. Available at: https://doi.org/10.1002/asi.23881 [Accessed 22nd Oct. 2018].

Etwaru, R. (2017). *Blockchain: Massively Simplified | Richie Etwaru | TEDxMorristown.* [video] Available at: https://www.youtube.com/watch?v=k53LUZxUF50 [Accessed 15th Aug 2018].

EUGDPR.org. (2018). GDPR Key Changes, *EUGDPR.org* [online] Available at: https://www.eugdpr.org/key-changes.html [Accessed 21st Aug. 2018].

Fadilpasic, S. (2016). Brands losing consumer trust over data handling, *ITProPortal.* [online] Available at: https://www.itproportal.com/2016/01/25/brands-losing-consumer-trust-over-data-handling/ [Accessed 22nd Aug. 2018]

Feinberg, A. (2014). Sneaky "Honey Encryption" Stops Hackers By Drowning Them in Phony Data, *Gizmodo.* [online] Available at: https://gizmodo.com/sneaky-honey-encryption-stops-hackers-by-drowning-the-1511718913 [Accessed 22nd Aug. 2018].

Firstround.com. (n.d.). Use This Equation to Determine, Diagnose, and Repair Trust. *FirstRound.* [online] Available at: http://firstround.com/review/use-this-equation-to-determine-diagnose-and-repair-trust/ [Accessed 11 Sep. 2018].

Frels, R. and Onwuegbuzie, A. (2013). Administering Quantitative Instruments With Qualitative Interviews: A Mixed Research Approach, *Journal of Counseling & Development.* [online] Vol. 91(2), pp.184-194. Available at: http://dx.doi.org.ezproxy.tees.ac.uk/10.1002/j.1556-6676.2013.00085.x [Accessed 9 Oct. 2018].

Garcia, P. (2018). Biometrics on the blockchain, *Biometric Technology Today.* [online] 2018(5), pp.5-7. Available at: https://www-sciencedirect-com.ezproxy.tees.ac.uk/science/article/pii/S0969476518300675 [Accessed 30 Aug. 2018].

Gisolfi, D. (2018). Self-sovereign identity: Unraveling the terminology, *IBM.* [online] Available at: https://www.ibm.com/blogs/blockchain/2018/06/self-sovereign-identity-unraveling-the-terminology/ [Accessed 1st Oct. 2018].

Griffith, E. (2018). WHEN THE BLOCKCHAIN SKEPTIC WALKED INTO THE LIONS' DEN, *Wired.* [online]. Available at: https://www.wired.com/story/when-the-blockchain-skeptic-walked-into-the-lions-den/ [Accessed 26th Oct. 2018].

Hagadone, Z. (2015). Megawhat?: How many homes can you power with a single megawatt?, *Boise Weekly.* [online]. Available at: https://www.boiseweekly.com/boise/megawhat/Content?oid=3433953 [Accessed 5th Nov. 2018].

Hasso-Plattner Institute of Design Stanford. (n.d.). *An Introduction to Design Thinking PROCESS GUIDE, Hasso-Plattner Institute of Design Stanford.* [pdf] Available at: https://dschool-old.stanford.edu/sandbox/groups/designresources/wiki/36873/attachments/74b3d/ModeGuideBOOTCAMP2010L.pdf [Accessed 10th Oct. 2018].

Hole, K. (2016). Building Trust in E-Government Services, *Computer.* [online] Vol. 49(1), pp.66-74. Available at: http://doi.org/10.1109/MC.2016.4 [Accessed 7 Oct. 2018].

Hopkins, D. (2018). Introducing Bitcoin, *Governance Directions.* [online] Vol. 70(5), pp. 247-252. Available at: http://web.b.ebscohost.com.ezproxy.tees.ac.uk/ehost/pdfviewer/pdfviewer?vid=1&sid=42b6dce5-d5bf-4f5e-a011-1aff545a611b%40sessionmgr103 [Accessed 3rd Sep. 2018].

IDEO. (2015). *Field Guide to Human-Centred Design.* 1st ed. [pdf] San Francisco, IDEO. Available at: http:// www.designkit.org/resources/1 [Accessed 28 Mar. 2018].

Intergovernmental Panel on Climate Change (IPCC) (2018). IPCC - SR15, *IPCC.ch.* [online] Available at: http://www.ipcc.ch/report/sr15/ [Accessed 5 Nov. 2018].

Isaak, J. and Hanna, M. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection, *Computer.* [online] Vol. 51(8). Available at: https://ieeexplore-ieee-org.ezproxy.tees.ac.uk/stamp/stamp.jsp?tp=&arnumber=8436400 [Accessed 21st Aug. 2018].

Iversen, O., Halskov, K. and Leong, T. (2012). Values-led participatory design, *CoDesign.* [online] 8(2-3), pp.87-103. Available at: https://doi.org/10.1080/15710882.2012.672575 [Accessed 2 Nov. 2018].

Jay, J. (2018). UK consumers' trust on businesses' data handling processes among the lowest in the world, *Teiss.* [online] Available at: https://www.teiss.co.uk/news/uk-businesses-customer-data/ [Accessed 21st Aug. 2018].

Kirkman, R., Fu, K. and Lee, B. (2017). Teaching Ethics as Design, *American Society for Engineering Education.* [pdf] Available at: https://peer.asee.org/teaching-ethics-as-design.pdf [Accessed 13th Sep. 2018].

Kshetri, N. and Voas, J. (2018). Blockchain-Enabled E-Voting, *IEEE Software.* [online] Vol. 35(4), pp.95-99. Available at: http://doi.org/10.1109/MS.2018.2801546 [Accessed 30 Oct. 2018].

Krugman, P. (2013). Bitcoin is Evil, *The New York Times.* Retrieved from https://krugman.blogs.nytimes.com/2013/12/28/bitcoins-is-evil/

Liedke, L. (2018). 100+ INTERNET STATS AND FACTS FOR 2018, *Web Hosting Rating.* [online] Available at: https://www.websitehostingrating.com/internet-statistics-facts-2018/ [Accessed 18th Sep. 2018].

Lumen. (n.d.). Technology and Innovation: Technology as a Driver and Enabler of Innovation, *Lumen.* [online]. Available at: https://courses.lumenlearning.com/boundless-management/chapter/technology-and-innovation/ [Accessed 22nd Oct. 2018].

Müller, T. (2018). Blockchain: From touch points to trust points, *Fjordnet.* [online] Available at: https://www.fjordnet.com/conversations/blockchain-from-touch-points-to-trust-points/ [Accessed 30th Aug. 2018].

Ølnes, S., Ubacht, J. and Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing, *Government Information Quarterly.* [online] Vol. 34(3), pp.355-364. Available at: https://doi.org/10.1016/j.giq.2017.09.007 [Accessed 28 Oct. 2018].

On Digital Marketing. (2018). 5 Factors of Technology Adoption Rates | *OnDigitalMarketing.* [online] Available at: https://ondigitalmarketing.com/learn/odm/foundations/5-factors-that-influence-technology-adoption-rates/ [Accessed 6 Sep. 2018].

Orcutt, M. (2018). How secure is blockchain really?, *Technology Review.* [online] Available at: https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/ [Accessed 15th Sep. 2018].

Powell, H., Mihalas, S., Onwuegbuzie, A. J., Suldo, S., & Daley, C. E. (2008). Mixed methods research in school psychology: A mixed methods investigation of trends in the literature, *Psychology in the Schools.* [online] Vol. 45, pp. 291–309. Available at: https://doi.org/10.1002/pits.20296 [Accessed 9th Oct. 2018].

Raimondi, A. (n.d.) Use This Equation to Determine, Diagnose, and Repair Trust, *First Round Review.* [online] Available at: http://firstround.com/review/use-this-equation-to-determine-diagnose-and-repair-trust/ [Accessed 7th Oct. 2018].

Rogers, E.M. (2003 [1962]). *Diffusion of Innovations.* 5th edition. Free Press, New York.

Ries, T., Bersoff, D., Adkins, S., Armstrong, C. and Bruening, J. (2018). 2018 Edelman Trust Barometer, *Edelman.* [pdf] Available at: https://cms.edelman.com/sites/default/files/2018-01/2018%20Edelman%20Trust%20Barometer%20Global%20Report.pdf [Accessed 24th Oct. 2018].

Samee, S. (2018). New report reveals record levels of identity fraud in 2017| Cifas, *Cifas*. [online] Available at: https://www.cifas.org.uk/newsroom/new-report-reveals-record-levels-identity-fraud-2017 [Accessed 22 Aug. 2018].

Sidhu, I. and Fred-Ojala, A. (2018). Future of Blockchain – A Berkeley Perspective, *Sutardja Center for Entrepreneurship & Technology.* [online] Available at: https://scet.berkeley.edu/future-blockchain-berkeley-perspective/ [Accessed 30th Aug. 2018].

Smith, O. (2018). 25 incredible things you didn't know about Estonia, *Telegraph.* [online] Available at: https://www.telegraph.co.uk/travel/destinations/europe/estonia/articles/amazing-facts-about-estonia/ [Accessed 1st Sep. 2018].

Steen, M. (2014). Upon Opening the Black Box and Finding It Full, *Science, Technology, & Human Values.* [online] Vol. 40(3), pp.389-420. Available at: http://journals.sagepub.com.ezproxy.tees.ac.uk/doi/10.1177/0162243914547645 [Accessed 15 Sep. 2018].

Talukder, M. (2014). *Managing Innovation Adoption*. London: Routledge, p.2. Available at: https://ebookcentral.proquest.com/lib/tees/reader.action?docID=1643843&query= [Accessed 11th Sep. 2018].

Tatham, M. (2018). Identity Theft Statistics, *Experian.* [online] Available at: https://www.experian.com/blogs/ask-experian/identity-theft-statistics/ [Accessed 22 Aug. 2018].

Truby, J. (2018). Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies, *Energy Research & Social Science.* [online] 44, pp.399-410. Available at: https://doi.org/10.1016/j.erss.2018.06.009 [Accessed 5 Nov. 2018].

UBC. (n.d.). Design Processes, *University of British Columbia.* [online]. Available at: http://dstudio.ubc.ca/research/toolkit/processes/ [Accessed 30th Oct. 2018].

Vassil, K., and Solvak, M. (2016). *E-voting in Estonia:Technological Diffusion and Other Developments Over Ten Years (2005 - 2015).* [pdf] Available at: https://skytte.ut.ee/sites/default/files/skytte/e_voting_in_estonia_vassil_solvak_a5_web.pdf [Accessed 29th Aug. 2018].

Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Current Opinion in Environmental Sustainability,* [online] Vol. 28, pp.1-9. Available at: https://doi.org/10.1016/j.cosust.2017.04.011 [Accessed 5 Nov. 2018].

Wachter, S., Mittelstadt, B. and Russell, C. (2018). Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR, *Harvard Journal of Law & Technology, 2018.* [online] pp.3-52. Available at: https://arxiv.org/ftp/arxiv/papers/1711/1711.00399.pdf [Accessed 6 Nov. 2018].

Wang, Y. and Kogan, A. (2018). Designing confidentiality-preserving Blockchain-based transaction processing systems, *International Journal of Accounting Information Systems.* [online] Vol. 30, pp.1-18. Available at: https://doi.org/10.1016/j.accinf.2018.06.001 [Accessed 14th Oct. 2018].

Windley, P. (2018). How blockchain makes self-sovereign identities possible, *Computer World.* [online] Available at: https://www.computerworld.com/article/3244128/security/how-blockchain-makes-self-sovereign-identities-possible.html [Accessed 1st Sep. 2018].

Zile, K. and Strazdina, R. (2018). Blockchain Use Cases and Their Feasibility, *Applied Computer Systems.* [online] Vol. 21(1), pp. 12 - 20. Available at: http://doi.org/10.2478/acss-2018-0002 [Accessed 24th Oct. 2018].

Figures

Fig. 1: Council on Foreign Relations. (2016). Keeping the Edge: U.S. Innovation, Council on Foreign Relations. [image]. Available at: https://www.cfr.org/report/keeping-edge-us-innovation [Accessed 22nd Oct. 2018].

Fig. 2: Heigel, J. (n.d.). What's Your Company's Three-Year Plan?, Sagence. [image]. Available at: https://sagenceconsulting.com/posts/whats-companys-three-year-plan/ [Accessed 22nd Oct. 2018].

Tallinn, Estonia: Worksup.com. (2018). 10 amazing savvy-technology facts about Estonia, Worksup [image]. Available at: https://www.worksup.com/10-amazing-savy-technology-facts-about-estonia?1 [Accessed 27th Oct. 2018].

Fig. 3: Vassil, K., and Solvak, M. (2016). E-voting in Estonia:Technological Diffusion and Other Developments Over Ten Years (2005 - 2015). [image] p. 4. Available at: https://skytte.ut.ee/sites/default/files/skytte/e_voting_in_estonia_vassil_solvak_a5_web.pdf [Accessed 29th Aug. 2018].

Fig. 4: The equation of trust. Drozdeck, S. and Fisher, L. (2003). [image]. The Trust Equation. 1st ed. Financial Forum. [Accessed 29th Aug. 2018].

Fig. 5: Blockchain networks. Rosic, A. (2016). What is Blockchain Technology? A Step-by-Step Guide For Beginners, Block Geeks. [online]. Available at: https://blockgeeks.com/guides/what-is-blockchain-technology/ [Accessed 11th Nov. 2018].

Fig. 6: Account recovery page from the uPort mobile application. Photo from personal archive, 2018.

Paul Steiner's famous cartoon that plays on the anonymity of Internet users: Steiner, P. (1993). "On the Internet, nobody knows you're a dog." [image] Available at: https://condenaststore.com/featured/on-the-internet-peter-steiner.html [Accessed 9th Sep. 2018].

Fig 7: An adapted version of the double diamond that shows the stages where to design the right thing vs. designing the thing right. Stack Overflow. (n.d.). Scaling Product Design Practice on a Growing Team [online] Stack Overflow. Available at: http://www.kurtisbeavers.com/so-design.html [Accessed 9th Oct. 2018].