Chapter 1
Global Business Requires Global Infrastructure

"We have the means by which we can create a truly global society. The institutions of this global society can be created by our endeavours. That global ethic can infuse the fairness and responsibility that is necessary for these institutions to work, but we should not lose the chance in this generation, in this decade in particular… to create global institutions for the environment, and for finance, and for security and for development, that make sense of our responsibility to other peoples…"

Gordon Brown
Former UK Prime Minister
21 July 2009

In my first article for the Tomorrow Today Global blog, I opened with a statement referencing our approach to "**the singularity**"*; an abstract moment in time when all of humanity's endeavours reach their peak, and we are, in essence "at one" with all of our creation's technological abilities, abilities which would then exponentially surpass anything we were capable of before. In the same breath, I also suggested that the effects of another phenomenon, namely *globalisation*, are daily taking their toll. Famed inventor and futurist Ray Kurzweil has statistically predicted** that the technological singularity will occur in 2045. If he is correct, it is very likely we will experience this singularity before we experience true globalisation.

I hope I am wrong in the latter statement, because I believe "true globalisation" is humanity's destiny. The only reason geo-political nation states exist in a world of infinite information communications is to protect the egos of those who rule them. Egos that every so often get challenged by equally opposing egos. (Of course, I understand the immense complexities that are involved in geopolitics, and this is a drastic simplification).

By now, we should be living in a world of "the free movement of person" in the same way an American citizen can travel (and work) between Cincinnati and Ohio without any need of a passport. But alas, I fear the egos of world leaders will prevent this natural humanitarian progression for decades to come, and if not them, the conservatives among us might. And before you argue me on this, think about why walls around ancient cities existed, and then consider why those walls no longer exist.

And so, it is very likely the singularity will indeed happen before true globalisation. And if that is the case, then there is probably not much need to write the rest of this book. We can all continue in our archaic ways of face to face and home language trade without the need to prepare ourselves for a better way. A way that unlocks the vast resources awaiting the 3 billion global citizens currently living in poverty. The singularity will be our answer in 2045, at which point we can sit back and allow artificial intelligence to automatically create solutions before our very eyes while we sip pina coladas. Much the same way we sip our coke whilst

our microwave cooks our dinner at the single touch of a button. (Forgive the enthusiastic optimism).

But of course, there are two very obvious points still on the table:

1. There are still well over two decades until that moment. That's a lot of globalisation yet to take place.
2. Ray Kurzweil and his fellows may very well be wrong.

In which case, it's probably best we prepare ourselves and our companies for the inevitable globalisation of our societies and economies.

How do we prepare for true globalisation?

In the above excerpt, former UK Prime Minister Gordon Brown stated back in 2009 that we have the means to create a truly global society. The means already exist (and ironically, according to him, existed back then!) It behooves us as leaders therefore to explore these means astutely.

We can prepare for globalisation by understanding these means, and technologies, that will advance and empower it. And while this book is unfortunately not one about the philosophy of globalisation, it is one about a specific technology that I believe will advance the process.

Blockchain Technology: An important cog in the globalisation machine

It is quite remarkable that Gordon Brown made the statement that he did in 2009. Because only 6 months prior, in some backend garage of tech geeks, a person (or group of people) began running the code of the world's first blockchain. Bitcoin was the very first cryptographically secure digital money solving the problem of double spending. It was underpinned by an entirely new technology now known as "blockchain".

In this short book, we will briefly explore what the technology is and how it works, how it can contribute to globalisation, and more specifically (and perhaps more importantly to you) how you and your business can benefit from the technology, more than a decade since its invention.

A Global Economy Is Better

Now, let us briefly return to the topic of globalisation… Consider the following: Where would you rather do business? In New York City or in Hobart Bay, Alaska? London or Otago? (No disrespect to my Alaskan and New Zealand readers!) Of course, the natural answer is the bigger city. This is of course why urban migration is such a hot topic at government planning conferences. People want to do business where the money is, and so migrate en masse from their sparser places of living to larger economic hubs.

For millennia, cities have grown based on their geographical location in relation to trade. Cape Town was a convenient stop-off point for those travelling to and from The East. Rome was perfectly positioned for trade on the banks of the Tiber river. San Francisco and Johannesburg both had an abundance of gold ore discovered in the 1800's. In more modern times, cities have grown purely based on economic performance. Interestingly, in this post-modern era, I believe we will see a rise of smaller city-states whose progressive economic policies will position them as favourites among businesses seeking favourable regulatory and taxation policies. Singapore and Hong Kong have already achieved this, while the likes of Malta, Estonia and Isle of Man are positioning themselves now as favourites for a future global economy.

It is estimated that, at the time of writing, the world's GDP sits at $80 trillion per annum. In the same way that any ambitious business person would endeavour to open an office in a global hotspot like New York or Hong Kong, business people would most certainly want a piece of an $80 trillion pie. Globalisation allows any one of us the opportunity to partake in this economy, and no longer be limited by the much smaller economies within our borders. Simply put: A global economy is better for business.

And hence: A global economic infrastructure is paramount to this new global economy. The internet has laid the foundation for this infrastructure, and now, another significant layer is being constructed as I write this: Blockchain.

**The term "singularity" is more technically used to define scientific and mathematical points which become undefined and infinite, and no longer observe the standard behaviours of science. But it was first used as a term to describe a moment in time when technology would exponentially surpass humanity's abilities by the early 20th century mathematician John von Neumann, this "moment" has since become known as the "technological singularity".*

***Ray Kurzweil, The Singularity is Near, pp. 135–136. Penguin Group, 2005. "So we will be producing about 1026 to 1029 cps of nonbiological computation per year in the early 2030s. This is roughly equal to our estimate for the capacity of all living biological human intelligence ... This state of computation in the early 2030s will not represent the Singularity, however, because it does not yet correspond to a profound expansion of our intelligence. By the mid-2040s, however, that one thousand dollars' worth of computation will be equal to 1026 cps, so the intelligence created per year (at a total cost of about $1012) will be about one billion times more powerful than all human intelligence today. That will indeed represent a profound change, and it is for that reason that I set the date for the Singularity—representing a profound and disruptive transformation in human capability—as 2045."*

Chapter 2
What is Blockchain?

After that Tomorrow Today Global article I referenced in chapter 1, I received a few queries asking me how “Bitcoin” could help in people’s business. At first I was a little confused as to why I was receiving queries about a subject I didn’t even mention in my article, but after engaging with my enquirers, I realised that a number of people still hold to the misconception that “Bitcoin” and “blockchain” are synonymous.

I remembered an article that Forbes published in 2018 outlining the number 1 misconception with blockchain is this very misunderstanding I was being enquired over: That Bitcoin equals blockchain.

Bitcoin versus Blockchain:
Bitcoin is the Gold, Blockchain is the Spreadsheet

The truth is: Bitcoin **doesn’t** equal blockchain. Saying that the two are synonymous would be like saying “spreadsheets” are synonymous with “gold”. While spreadsheets help in the accounting of gold, the two are entirely different entities. Apply that to our scenario; and think of blockchain as the spreadsheet, and gold as bitcoin. It’s a very easy and helpful parallel. Blockchain is the type of spreadsheet that keeps Bitcoin’s record, and in the same way that a spreadsheet can be used to account for absolutely anything you can imagine, blockchain can be applied to just about the same.

While I am a believer in Bitcoin itself (which is a conversation for a few beers in a London pub - or at least perhaps the topic of my next book), when I refer to “blockchain” I am not referring to “Bitcoin”, I am referring to the technology that was invented in order to make Bitcoin work. And when that technology was invented, the creators accidentally (or perhaps purposefully) created a new technological framework for global businesses to operate on.

It is important to note though, that the first blockchain was introduced with Bitcoin, thus making it quite difficult to accurately explain blockchain, and certainly its origins, without referring to Bitcoin at some point. For the sake of helping you grasp a firm understanding of this remarkable technology, in the next few paragraphs I will be referencing Bitcoin a fair amount. Whether you believe in Bitcoin’s feasibility and value to society or not, it is impossible to recognise blockchain as an important technology without acknowledging Bitcoin’s role in its invention.

There is little doubt that blockchain is a significantly important technology in society's future. This future could be one where Bitcoin does or doesn't exist, but blockchain as an infrastructural technology most certainly will. With the likes of Facebook, IBM, Microsoft, Amazon, Walmart, HTC, Samsung and even Apple all investing heavily into blockchain technology in recent years, it is fair to say that this is a technology that is here to stay.

Blockchain versus Distributed Ledger Technology (DLT): A Colloquial Conundrum

The next colloquial challenge you may encounter as you journey into discovering more about this decentralised technology is differentiating between the term "distributed ledger technology" and "blockchain". Much like someone entirely ignorant about the technology may confuse the term blockchain with bitcoin, someone with a little more understanding may get confused between the terms DLT and blockchain.

This technology is so nascent that I have found it fascinating to watch even its etymology evolve and take shape as culture adopts its more favoured colloquialisms. Terms like "crypto", "cryptoassets", "hodl" (instead of "hold"), have all taken root when in many cases these words are incorrectly implemented (or downright misspelled!)

The same goes for the actual overarching reference to the technology's framework. According to a UK government tech report, the first distributed ledger was in fact Bitcoin's blockchain in early 2009, and that is likely why the term "blockchain" has become the standard for referencing this form of decentralised network. As you will learn in the forthcoming paragraphs, decentralised finance was being developed for decades before Bitcoin and its blockchain came about, and the idea of a "distributed ledger" had been toyed with many times before.

Only Satoshi Nakamoto's invention however finally solved the numerous problems decentralised finance posed. After the publication of the open source code, the idea of distributing a ledger on peered servers became viable. Some developers deployed distributed ledgers that did not necessarily need the "proof of work" algorithm required to secure their network, which in turn meant miners did not need to wait for blocks to be mined, thereby allowing for the data to be stored continuously rather than in a "chain of blocks" (these are terms you will also learn later in this chapter).

These forms of more simple decentralised databases are today known as "DLTs", which stand for "distributed ledger technology". A blockchain is a form of a DLT, but not all DLTs are a blockchain. Most technologists are in agreement that DLTs are slightly less secure than your standard "proof of work" blockchain.

Back to my point about etymology: Blockchain became such a buzzword in 2017 that the term was etched into the niche of decentralised finance and computing, and, as mentioned, has now become the overarching term when referring to the industry as a whole. So while I aim to set about simplifying an explanation of the technological framework of "blockchain", there may be some overlap into "distributed ledger technology" (this is particularly so in the

chapter about “self sovereign identity”). But again, the industry has now widely come to accept the term “blockchain”, and those implementing it in corporate dialogue will most likely be understood by the beginner and IT specialist alike.

It is however important to comprehend the distinction for an accurate holistic understanding of this complex subject.

Let’s just recap and summarise this etymological conundrum:

1. Blockchain and Distributed Ledger Technology (DLT) are technically two different types of networks.
2. A blockchain is a type of distributed ledger, but not all distributed ledgers are blockchains.
3. Distributed Ledger Technology was made possible by Bitcoin’s invention in 2008/09, and was slightly modified to create a cheaper and more energy efficient decentralised solution.
4. Blockchains are widely accepted to be more secure than “non-blockchain type” distributed ledgers (blockchains require more energy).
5. The term “blockchain” has become the widely accepted and agreed upon colloquial reference when citing the overall technology involved with decentralised and distributed networks.

With these points in mind, let us now explore how blockchain came to be, and delve into what the technology actually entails. I wish you luck...

Blockchain’s Origins

In the original Bitcoin white paper published by a pseudonymous “Satoshi Nakamoto” in September 2008, you won’t find a single mention of the word “blockchain”. Nakamoto uses the words “blocks” and “chains” frequently in order to describe the network, but the term “block chain” was actually first used in a 1997 cryptography mailing list about “hashcash”, an early foundation that Bitcoin’s creator used in the development of their protocol.

The term eventually became a commonplace noun as early Bitcoin users downloaded the entire history of the Bitcoin database and would refer to it as the “blockchain”. And because Bitcoin was open source code, the term “blockchain” then became synonymous with the network infrastructure underpinning all other cryptocurrencies developed after it, and it has stuck ever since.

So What Is Blockchain?

Hopefully my metaphor of gold and spreadsheets gave you some idea as to what we’re dealing with here. As mentioned, blockchain is very similar to a spreadsheet, but with two fundamental differences:

1. It is immutable
   Meaning it is unchangeable.
2. It is decentralized
   Meaning it has no central point of failure in the event of a network crash or for hackers to exploit.

Therefore: Blockchain can be explained simply as: An immutable, decentralised network database.

Sounds a lot like the internet, right? Indeed. The internet has opened the world of decentralisation, and paved the way for a far more democratic global society. But all that data still needs to be stored somewhere. This is traditionally a job for centralised servers. The first sign of decentralised data storage was peer to peer download sites, where multiple users shared their media files with friends on the internet. But these users weren't incentivized to keep sharing their data, thus making it an unreliable form of data sharing. Users had to trust other users to continue sharing their data.

Blockchain, on the other hand, takes that need for trust away.

Once data is secured in a blockchain network, we can trust that the data will remain there for us to access later. Whether that data be a ledger of transactions (in the case of cryptocurrencies like Bitcoin), a list of asset registries, or even coded computer applications (as we will explore later).

It is also important to note here that a key missing ingredient to my definition is the use of the term "cryptography" or "encryption". Obviously that's where the terms "cryptocurrency", "cryptoassets" and "crypto" come from. It is the root of where this all started. Many, if not all, of the software developers involved in the very first blockchain were all developers in the field of cryptography, and were working on encrypted methods of transmitting money without the need for a third party. I left it out of my definition in order to keep the definition as simple to remember as possible, and believe that the term "immutable" in essence covers the encryption involved with blockchain, because without strong encryption methods, it would be impossible to have an immutable database.

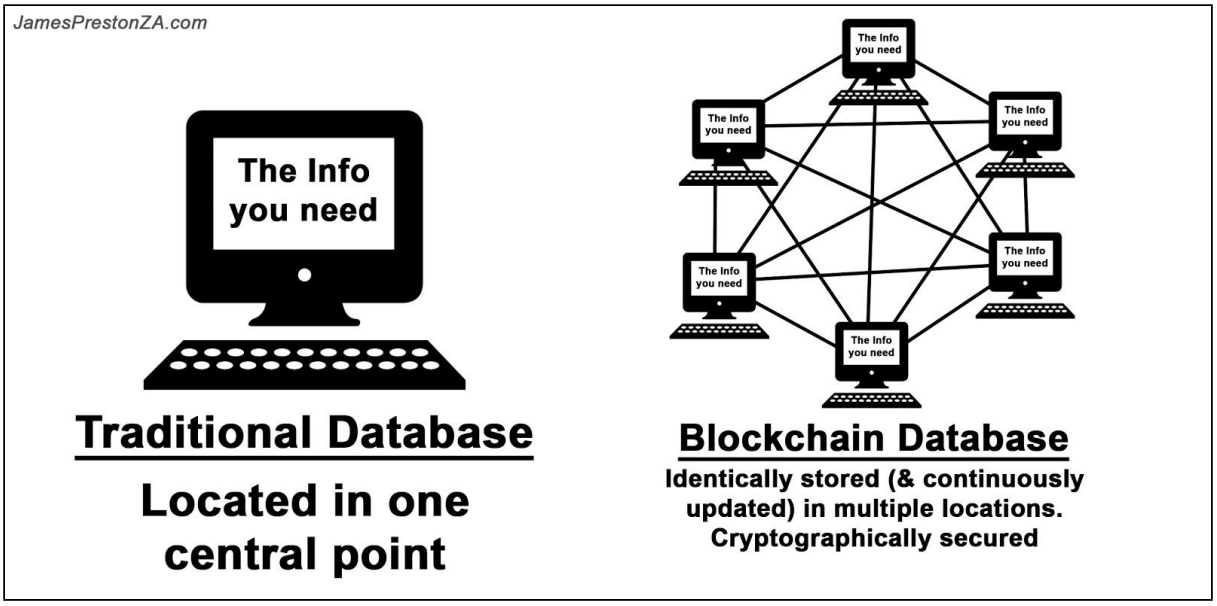
GETTING TECHNICAL

To further comprehend the "noun" of a blockchain, I'd like to unwrap a few more of the technical aspects that make up the word and entity "blockchain". While this is meant to be a short eBook to help you consider the possible benefits of blockchain specifically for **your** business, I want to provide a basic foundation to understanding blockchain technology so as to equip you in your journey of discovery. If you don't feel the need for such equipping, feel free to skip to the more relevant sections that may benefit you directly.

Nodes in Consensus

Let's start this short technical exploration with this below diagram:

Figure 1



This gives you a visual idea of a blockchain when compared with a traditional database on a central server. A traditional database is hosted by one, central point. A blockchain on the other hand is, in essence, a network of identical servers, each connected to each other. Talk about taking the interwebs to a whole new level! As you will see in the later screenshot of a live blockchain network, it is mind boggling to think that over 8000 computers can all be connected with **each other**!

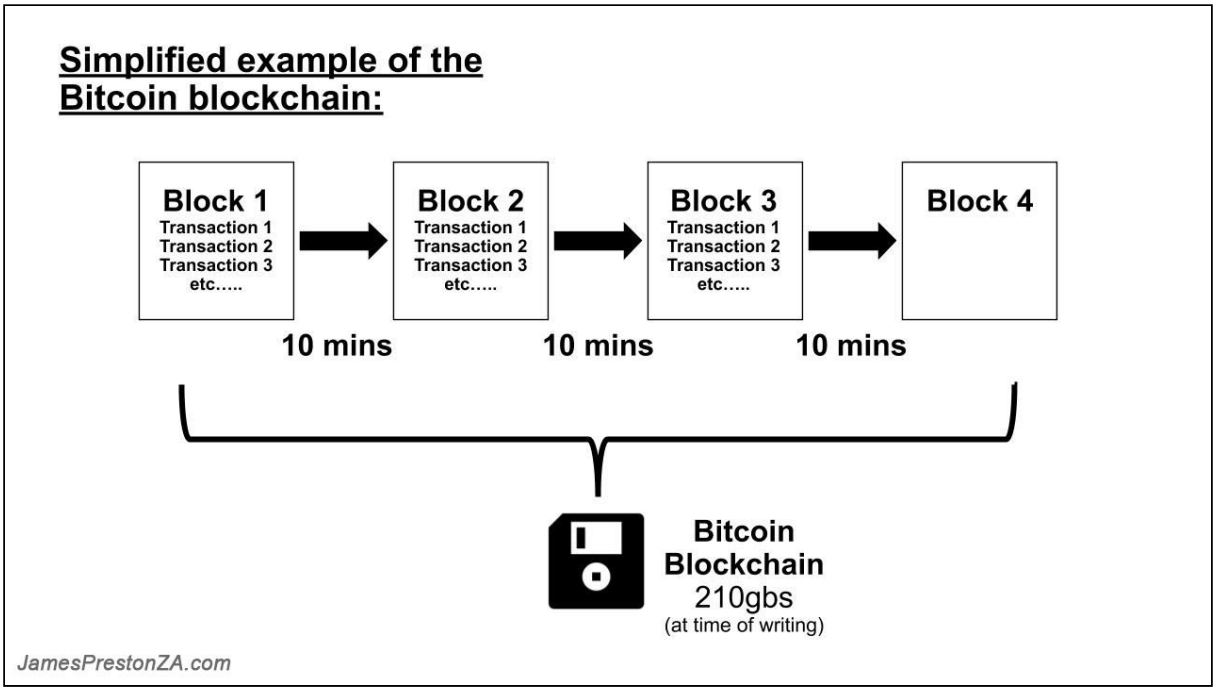
These computers, or "servers", are called "**nodes**". They are simply computers hosting that specific blockchain, and part of a blockchain's protocol is that every node in the network must be in perfect consensus with each other, hence the above diagram's explanation of data being "identically stored". It is this feature that gives blockchain its security as a large database, each computer on the network needs to see a mirror of its database on every other computer connected to it (node) in order to enter a new piece of data. Each new piece of data is entered onto the network of nodes at exactly the same time, and once the data is entered, registered, and confirmed, it is entrenched into the database forever.

This constant network "consensus" of nodes (or computers) means that a hacker would have to hack into every single node at exactly the same time. And even if they were successful, failsafes can shut off even a single node from the network, making it the "original copy", and able to be used to restore the original data to the entire network once it is secure again. You see, this consensus-based distributed form of databasing means there is no single point of failure for critical information.

Chains of Blocks

A blockchain is by representational definition, a "*chain of blocks of information"*. That's where it gets its name from. To help explain this point, let's take a look at the Bitcoin blockchain…

Figure 2



The Bitcoin inventor/s designed a database that is constantly creating new "pages" of information (in Bitcoin's case, every 10 minutes). These "pages" are called blocks. In these blocks, each Bitcoin transaction is irreversibly recorded. You can think of these blocks in the same way you'd think of a spreadsheet book, each block is like a new page in the book. These blocks are chained together using cryptography, and hence, we have what has now become known as the "blockchain". (This spreadsheet reference helps you understand why we encounter the term "ledger" frequently in this industry).

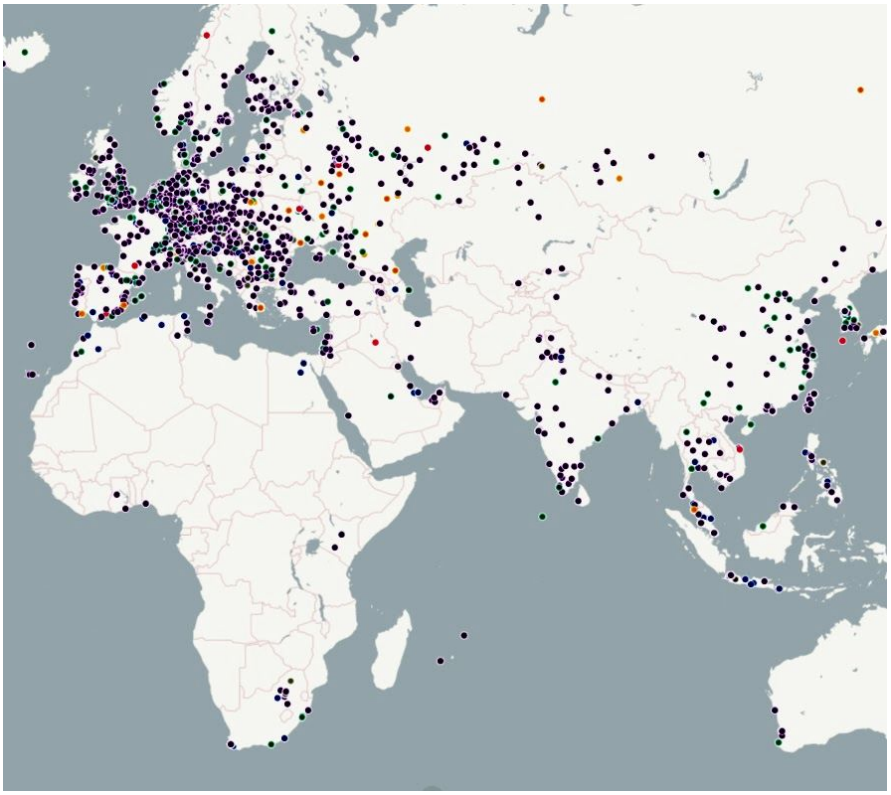
Now, as mentioned earlier, developers can in essence store any information in a blockchain, not just a record of transactions like the Bitcoin blockchain. "Ethereum" is one such example. You may have heard about Ethereum in the news or media, and that's because its relating digital token, the "Ether", is the second largest cryptocurrency by market capitalization. The Ethereum blockchain is quite different to the Bitcoin blockchain, and was designed with a number of distinctions, mostly, the fact that it stores computer code instead of just financial transactions.

With the decentralized, immutability of the Ethereum blockchain, software developers are able to write what has become known as a "smart contract". Although I will elaborate on this in Chapter 8, this is code which is able to execute securely and automatically without fear of malfeasance. Software developers are able to do this because their code isn't being stored on a centralized database, but instead on a decentralized database.

At the time of writing the Ethereum network had approximately 8650 nodes supporting it. Some very clever developers have built visualisations of these blockchain networks like the

Bitcoin and Ethereum blockchains, allowing us to see, in real time, where in the world these networks are distributed. Using a Carto map by Carlos Matallín, I can show you exactly where Ethereum's nodes are located in Africa, Europe and Australasia:

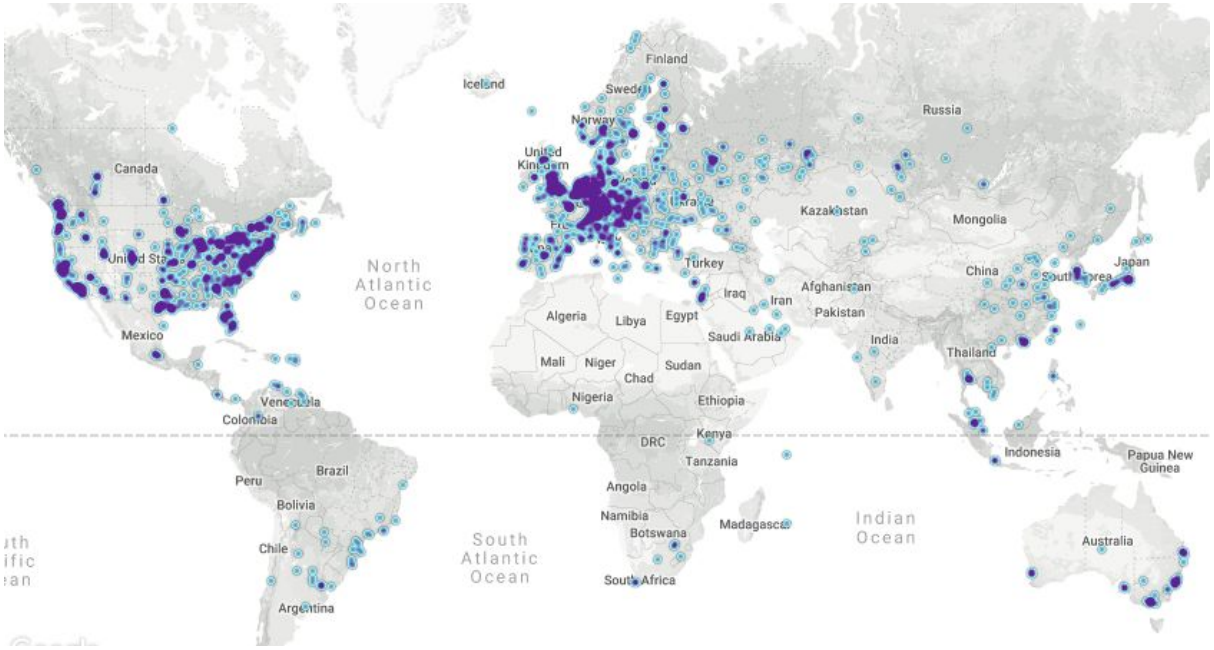
Figure 3



When you look at it visually like that, it isn't difficult to see why this is the future of computing. Already with over 8000 nodes running the entire blockchain identically, and supporting the network, Ethereum is incredibly secure. The more nodes supporting the network, the more secure it is.

For the sake of comparison, we can see in the below screenshot of the website Bitnodes.earn.com, that Bitcoin has a similar number of nodes located all over the world, which at the time of writing was 9593 nodes...

Figure 4



What I've done here is provide you with a visual representation of a blockchain network in operation, in real time. Now I'd like to discuss the incentive-based design of the "proof of work" algorithm, and how that impacts the energy consumption debate.

Proof of Work, Electricity, Immutability, and Changing The Blockchain

By now I am hoping you understand that a blockchain is essentially an "unchangeable" database. I'd like to confuse you a little here (if you weren't already confused!) by throwing a small spanner into the works: Technically the database **is** actually changeable.

But before you throw your iPad or smartphone away along with this eBook in protest of confusing network infrastructure and its terminology, I'd like you to track with me...

A blockchain's database is changeable in the same way it is "technically" possible to fly to the surface of the sun; the engineering required to get to the sun is too great an endeavour and the cost massively outweighs the reward.

The same goes for a blockchain database. Technically, it is possible to edit the database, but the computing power required to do so is supremely greater than the financial reward for simply supporting the network. The inventors of blockchain ingeniously implemented an incentive system for supporting the network that would not only reward network supporters, but also drastically disincentivize malicious actors.

At the time, they integrated a technology called "proof of work" to their invention, which required computing power, and therefore energy (in the form of electricity), in order to contribute to the network. The use of the proof of work algorithm has been discussed at length as a strong criticism for Bitcoin and other blockchain-enabled cryptoassets and the

like, and while I believe it is overstated and out of context, it is important to note that an alternative algorithm was put forward by a software developer in 2012 called “proof of stake”. This algorithm uses similar incentive structures to secure a decentralized network, but without the need for computing power as its source of security, instead network supporters (or “nodes” as discussed earlier) simply require a minimum balance of the blockchain’s digital token in order to support and contribute to the network, and in turn be rewarded with further digital tokens. This algorithm is still being developed and is yet to prove as secure as the proof of work algorithm, but I mention it here for you to take note of the fact that software developers are cognizant of the energy consumption challenge, and are working to find solutions. For some insightful reading about energy consumption in the blockchain industry, read this article by blockchain entrepreneur and climate change activist, Christopher Jospe.

While software developers are fast exploring the most energy efficient methods to secure decentralized databases, the proof of work algorithm remains the best mechanism by which we can rest assured that a blockchain network is indeed unchangeable. It’s also important to note that the energy consumption of proof-of-work based cryptoassets like Bitcoin is poorly reported on and often with strong bias, and as we know in this new world order of “fake news”, presenting information with such bias will often sell you more clicks, be careful of this bias!

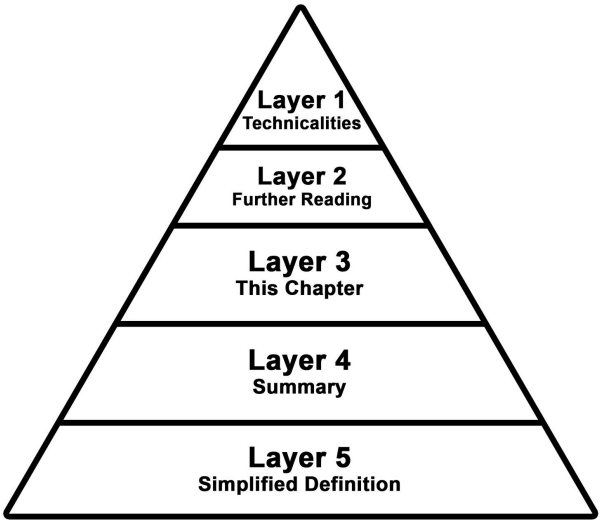
Conclusion

And with that we come to the conclusion of your introduction to blockchain technology. Hopefully you don’t feel confused and overwhelmed. I am confident you have already been somewhat exposed to blockchain somewhere along your journey, and my hope is that this chapter has helped further solidify exactly what it is that the tech does, and how it works.

In summary, and in helping you digest what you’ve just consumed, I’d like to put this all into perspective by introducing five layers of understanding…

Figure 5

Layers of Understanding:



Layer 1 is the actual technicalities of blockchain technology necessary for software developers and technicians to comprehend.

Layer 2 would be further reading devoted to the topic of blockchain.

Layer 3 is this entire chapter.

Layer 4 is then a summary of this chapter into the following sentence:

A blockchain is an immutable, decentralised database distributed on multiple computers anywhere in the world called "nodes", who all support the network using a cryptographic "proof of work" (or stake) algorithm.

This leads us perfectly into the even more simplified definition that we looked at earlier as the final layer, **Layer 5:**

A blockchain is an immutable, decentralised network database.

Chapter 3
In What Ways Can Blockchain Help Your Business?

Now that we've spent an exhaustive amount of time looking at what blockchain actually is, let's start to explore some of its actual benefits. Why is the technology so hyped, and what is so revolutionary about it? Well, there are a number of ways to answer that question, and a number of reasons your business should at least be exploring the *possibility* of blockchain adoption.

There is little doubt in my mind that blockchain has become one of the most hyped technologies of modern times due to its direct link with financial value. The price speculation of Bitcoin, Ether, Litecoin and the myriad other cryptocurrencies is what has given its underlying tech an incredibly helpful boost. It has been quite a fascinating thing to watch; these hype and doom, bust and boom cycles, where mainstream media praise cryptocurrency as the answer to the world's problems in one breath, then condemn it to the doldrums of useless tech in the next. Financial value, or money, makes us humans do very strange things, and it is this aspect that has given blockchain tech a unique position among so many of its counterparts of recent history.

Does this mean the tech is actually useless? Not by a longshot! I am merely commenting on its fascinating treatment by the media and public. The tech is without doubt a marvel, and one that should be explored in every way possible by all businesses. I have written about tech, business, and socio-economics for the last 12 years, and have met some incredible people on my journey. But I have never met such intelligent minds as the minds of those in the blockchain industry. These minds have been building our vehicles, designing our smartphones, and coding our operating systems, quite happy to go about their daily lives without the fanfare of public interest. But when many of them discovered the treasure trove of technological prowess of blockchain, they couldn't help but get involved.

It is unfortunate that there are a few what we call "Bitcoin maximalists" in the industry who relegate blockchain tech to a simple cog in the wheel of their saviour Bitcoin. These critics are narrow-mindedly stuck in the worlds of their favourite muse, and a simple broadening of their minds to listen to some of the most intelligent thinkers on the planet would shake them out of their parochial ways. Thinkers like boy prodigy and Ethereum co-founder Vitalik Buterin, featured in this TechCrunch conference session with equally impressive thinker Naval Ravikant, or genius mathematician and blockchain engineer Charles Hoskinson, or CEO of blockchain startup Lightning Labs and Harvard Law doctor Elizabeth Stark. While, as mentioned, I am a believer in Bitcoin, I believe relegating its underpinning infrastructure "blockchain" to a side note is unwise.

Blockchain is still a remarkable marvel. It would seem though, that is has become in recent years somewhat of an overhyped marvel. But it nevertheless behooves us as leaders to explore this marvel, and acquaint ourselves with it, and look for opportunities whereby it could be utilized.

As it currently stands, the primary reasons businesses are exploring and in some cases adopting blockchain technology are as follows…

1. **Efficiency**
2. **Security**
3. **Cost reduction**
4. **Transparency**
5. **Financial remittance**

Thanks to its secure infrastructure, blockchain allows for many intermediaries to become redundant. These intermediaries ensure stock is released accurately, money gets delivered to its intended destination, logistics are legally handled correctly, accounts are in order, etc. The list of different kinds of intermediaries is comprehensive, and if a company can remove the need for them, they can of course **cut costs** significantly. A company may only do this if they are guaranteed that the replacement infrastructure would indeed perform as **securely** and perhaps automatically as intended, but in many cases the cost reductions and **efficiency** improvements are so significant that the R&D is worth the investment anyway.

In addition to this, the **transparency** of a blockchain means that businesses, staff, suppliers and officials can be held to account in ways never before available. How this works itself out as companies grapple with the idea of making their affairs public will be interesting to see, but with forward-thinking companies like Buffer already releasing their financials to the public on an annual basis, public accountability could reach new heights, and the ideals of a far less unequal society could well become a reality. A reality that blockchain's inventor/s had hoped for.

In the example of Buffer used above, auditors would have had to compile those financial records before they are confirmed as legitimate. Had Buffer been using a blockchain-enabled accounting system, those records would have been readily available without the need for an intermediary's verification. This utility for blockchain is still some way out from being fully realised and implemented, but it is now a very real possibility for the future.

And the final primary way that businesses are exploring blockchain is currently the most obvious: **financial remittance**. Businesses are already utilizing international, cross-border settlements within a matter of minutes using a whole host of different blockchain options. Whether that be Bitcoin or more traditional currencies now tokenized as digital currency. As I allude to later, JP Morgan have already created their own cryptocurrency to ensure secure payment transfers for their institutional clients, no matter where they are in the world.

But what about <u>your</u> business?

Can your business benefit from this marvel?

Well, that depends on two factors. **How big is your business? And what industry does it play in?**

Blockchain is, at the time of writing, only a 10 year old technology. And so it is still a rather niche environment within which to find affordable yet reputable software companies able to build bespoke products. For this reason it is unfortunately a rather expensive undertaking, which many times eliminates small to medium businesses from this market.

As with all business: It comes down to 1) “how much of a need is the solution” versus 2) “the cost of implementing it”. If the need is greater than the implementation cost, then you need to make the investment. But if the cost is greater than the need, most small to medium businesses can get away without the technology until it becomes more widely available.

And it won’t be long until it is more widely available. With IBM, SAP, and Microsoft all working on enterprise blockchain solutions, we will see more cost-effective products on the market within the next 5 years or so, but until then, the “need verse cost” scenario is going to be the big debate in small to medium business boardrooms. I would advise SMEs that are looking at blockchain to consult with a local computer engineering consultancy in tackling this debate, in order to get an expert opinion on your specific needs.

Larger companies

What about larger corporates? Well, if your company has a hefty R&D or even IT budget and is able to allocate at least $200,000* to a year’s worth of IT implementation costs, and would like to use those funds to both improve your operation from a cost-cutting/efficiency point of view and from a cybersecurity point of view, then certainly, I would indeed recommend exploring blockchain.

Granted, an additional $200,000+ can be quite a bump off the bottomline, but the benefits can be enormous. Besides the cost-cutting, efficiency and security benefits, the marketing and PR spin in our current tech climate can be worth its weight in marketing budget gold. Just throw in “AI” along with your new blockchain development into your communications and the local journalists will be dubbing you the next “Apple”!

Let’s Dive In

With all that said, it’s time to take a look at some of the areas where blockchain tech is indeed helping businesses become more efficient, safer, securer, faster, or more accountable. I have identified 11 specific areas where blockchain could be of benefit to you and your company:

Rated by two things: Level of development and readiness for deployment. And level of necessity to improve the industry.

I will separate each specific area into a unique chapter in this book, for the sake of reference, but in some cases, their idea is fairly self-explanatory, so you will find some chapters are far shorter than others, where elaboration is required. I have based the order of the list on both current adoption rates and actual technological capability to responsibly go to market. IE. The first on the list is a technological use-case that has already been adopted with great success, while the last on the list is either still in prototype phase or is just too buggy to be widely adopted.

I may be linking directly to some companies already developing these tools, in order for you and your company to contact them direct should you be intrigued by the possibilities they offer. **But a link here is in no way an endorsement, and most certainly not an advertisement.** They are purely companies I have reported on in the past, and worth at least getting in touch with. If you would prefer more options, or wish to verify a potential blockchain dev company, you're welcome to contact myself or my team.

Chapter 4

Potential Blockchain Use Case 1: Supply Chain Efficiency

The supply and value chains of business have fast become the go-to application for blockchain technology. As a modern society, we've become so far removed from the food on our plate or shoes on our feet that we are stunned when journalists expose the time and distance the products have traveled to get to us. These lengthy delays and distances provide enormous challenges for regulators, especially when it comes to tracking specific shipments in disease tracking or malfunctions.

As I wrote in an article for Tomorrow Today Global, Walmart faced this exact challenge when E. coli broke out in as many as 11 states of the USA in October 2018, and even affected Ontario and Quebec in Canada. Many of the victims reported buying lettuce from Walmart, the world's largest grocer (and company by revenue), which left their execs with the gargantuan task of locating the source of the outbreak. That task took 3 weeks.

As you can imagine, lettuce sales practically dried up in those 3 weeks, and the weeks following. Only when Walmart were able to release a statement declaring their success in finding the outbreak's source, and subsequent containment of the outbreak and affected lettuce, did people begin trusting lettuce again. It turned out, Walmart had already been in talks one of the world's leading blockchain development projects, Hyperledger.

Hyperledger is a branch project of the Linux Foundation, the non-profit foundation that supports the open source development of Linux and its software projects, Hyperledger being one of them. Hyperledger itself being a non-profit, open source software project, is supported not only by the Linux Foundation, but also by software giants such as IBN, Intel and SAP. When you dig into the history of these projects and companies, you see just how deep the blockchain rabbit hole goes.

I've had the privilege of interviewing Brian Behlendorf, the Executive Director of Hyperledger for our blockchain news website, and I can tell you, as a former Director of the Mozilla Foundation, CTO of the World Economic Forum, and Director at the Apache Software Foundation, he ranks right up there as one of those incredibly intelligent minds I was speaking about in Chapter 3. Brian joined the Hyperledger Project in May 2016 after being deeply inspired by blockchain technology's promise, and has already been involved in some incredibly exciting projects. There is no doubt that their Walmart project is their highest profile project to date yet.

When the executives at Walmart analysed the disaster of this Romaine Lettuce E. coli infection, they knew exactly who to turn to for a solution: Hyperledger. Having already done much of the analytical legwork in their consulting with Walmart before the outbreak, Hyperledger were able to have an entire blockchain system that integrated IOT (Internet of Things) devices ready for roll out, and ready to prevent such a supply chain traceability delay from ever happening again. Within a month, Walmart's food exco sent out a letter to each and every supplier of leafy green vegetables contracted to the retailer saying "they had one calendar year to register on their newly designed blockchain database – or else lose their contract". It was that serious.

Walmart and Hyperledger's respective software engineers had run trials of their traceability blockchain product, and found that they could reduce the source search time from 3 weeks to 2.2 seconds. Yes, you read that correctly, 2.2 seconds. Can you imagine how much quicker lettuce could have been back on the shelves of even the affected areas had Walmart traced the E. coli-infected lettuce within 2.2 seconds? Revenue would barely have been impacted.

Walmart aren't the only bigshot company integrating blockchain in their supply chain tracking. Just this week, America's largest Tuna canner, Bumble Bee Foods, announced that they would be tracking their entire supply chain of Tuna on SAP's newly developed blockchain solution; eventually even giving customers the full supply chain route of the very can of tuna they just purchased. Talk about transparency. Maersk and MSC Shipping companies along with Alibaba are all high profile companies rolling out blockchain tech to bring their supply chain management into the 21st century.

But why is it that blockchain is better for supply chain efficiency?

What makes it better than standard databasing systems? It has to do with what we opened up with: Globalisation. 100 years ago, our supply chains were much smaller and entirely different to the bureaucratic monsters we're faced with today, where there is a pressing need for a technology that offers us greater trust and better efficiency.

Traditional databases and ERP (enterprise resource planning) systems just cannot offer this security, transparency, and efficiency in one holistic package. They may be efficient, but they'll compromise on security and transparency.

With blockchain, we're able to eliminate the bias so common in today's opaque supply chains, where not only contractors are found protecting their reputations, but staff and managers are as well - as they only provide the information they know their clients and superiors want - often eliminating the truth, or at least misrepresenting it.

Let's take a look at the four primary reason why companies are turning to blockchain for supply chain management:

1. **Improved Security**
   The immutability, decentralization, and cryptographic design of a blockchain ensure that the data is far more secure than traditional systems. Added to this, the decentralized nature of the database coupled with its potential for smart contract implementation (as outlined in Chapter 11) makes auditing the supply chain vastly easier and cheaper.

2. **Transparency**
   As discussed, various touchpoints throughout a supply chain can enter data almost automatically (especially when integrated with IoT* devices), leaving no room for editing or deletion. Just like in Walmart's letter to their contractors, companies can roll out a blockchain system across their entire supply, adopting a "take it or leave it" approach, completely eliminating the temptation for contractors and staff to act dishonestly.

3. **Scalability**
   Because a blockchain is based on decentralized networking, like the internet itself, and due to its infrastructure, you can have almost any number of participants across

the network. There is no concern, and certainly no cost factor, with adding more participants to your network, and in fact, it is encouraged as it enhances security.

Blockchain tech is perfectly to suited for supply chains to scale their tracking procedures, but isn't ready (yet) for larger data storage scaling. Due to each node on the network required to store the entire blockchain on its harddrive, actual data is limited to a single node's capabilities, and the larger storage required, the harder it becomes for nodes to join the network. Anything above 1 terabyte (1000 gigabytes) for a blockchain is pushing the feasibility limits, although, as computing advances, these sizes will increase. There are also new advances in blockchain tech itself, with the likes "sharding" and "sectioning", whereby some nodes don't have to download the entire blockchain, because of course, if a chain is half a decade old, it is very likely that those earlier years of data are, in essence, superfluous to the network.

So, when I talk about scaling here, I am referring to the ability for supply chains to scale their traceability & tracking network, as scaling of blockchains themselves is still a work in progress, and not quite yet required for blockchain's current usability cases.

4. **Innovation Opportunities**
   Thanks to the entirely decentralized architecture of the tech, there become a myriad of opportunities for different departments and contractors to innovate their processes. They could introduce new approval gateways, new auditing steps, automate key processes of their specific functions, even introduce new ways of incentivizing, rewarding or penalizing participants in their process.

   The technology allows for a whole host of innovation opportunities, and I always strongly encourage companies to foster innovation, and so if your company does adopt blockchain, especially for its supply chain process, it is highly recommended that you allow your IT teams or those who take an interest in tech to experiment with how they can improve the network. Remember that the Light Bulb, Cellphone, and even Blockchain Tech itself, were all results of experiments by curous thinkers.

As you can now see, supply chains, especially complex ones, have fast become the perfect place for blockchain to provide its service. No other databasing system offers this kind of data security and transparency. Not only will indexing your supply or value chain on a blockchain mean it remains immutably secure, but it can be accessed within minutes should a product ever need to be traced and isolated. And the best benefit of all: Contractors, suppliers, company divisions, and the like, can't tamper with the data.

And while some old school critics will say that traditional databases perform better than blockchain databases for supply and value chains, this is only true for entirely centralized ones, which most supply chains are not. In an increasingly complex global economy, most are distributed across numerous departmental, international, company, and even industry

borders. You simply cannot achieve the security, efficiency, and transparency that blockchain tech provides with a traditional database.

So where can your company get started with putting your supply chain on the blockchain? I would argue that your first port of call should be IBM, as their work with the Hyperledger team has been industry formational, and they already have an impressive portfolio of clients. Microsoft have an equally impressive offering, while Openledger can offer very similar standards at slightly lower rates.

***IoT: Internet of Things devices. Small, independent devices that are connected to the internet and can log and track data directly to a network in real time.**

Chapter 5

Potential Blockchain Use Case 2: Democratic Voting Systems

On a cold Winter's morning in 2003 in Schaerbeek, a small district just outside Brussels in Belgium, a young woman named Maria Vindevoghel thought she had started a Belgian revolution. The former airplane cleaner was now a vocal candidate for the Belgian Communist Party, a party with little going for it according to pre-election polls. But on the day of the country's national elections, in that district's voting station, she received over 4096 votes alone. Enough to potentially give her a seat in Parliament.

But there was a problem. Her result was impossible. 4096 was more votes than the number of registered voters at that station. Fortunately, it was this anomaly that raised the alarm bells.

Belgium were experimenting with digital, computerised voting for the first time, and had it not been for the anomaly of Vindevoghel's votes numbering more than actual voters, she may have just snuck in under the radar. But history didn't go her way that day, and the IT specialists of the Belgian federal government immediately began an investigation.

They came to an astonishing conclusion: The 13th bit in the computer's memory had flipped from "off" to "on", launching Vindevoghel's votes from a dozen to 4096. The 13th bit in a computer's memory registers 2 to the power of 12, giving you 4096. The cause of this "bitflip" will boggle your mind: It is officially recognised as being the result of a "cosmic ray", a cosmic particle from outer space, striking that "bit" in the computer's memory at the very moment a voter voted for the Communist Party candidate, Maria Vindevoghel.

While a "bitflip by cosmic ray" is an extreme scenario, it does highlight the fragility of digital voting systems. The numerous voting systems employed by governments globally are regularly questioned and doubted due to the ease with which malicious attackers could affect an election result. This ease lies in the centralised nature of the digital data storage. No matter the level of security, if the data's encryption and digital security protocols are breached, malicious hackers could have a field day. Not to mention if administrative officials with access to the data were compromised through bribery or other sinister means.

These risks caused the German government to doubt the integrity of digital elections, and even issue a decree in 2009 stating that all digital voting systems should have the ability to be audited by any user in an easy-to-understand manner. For this reason, most German elections are still cast on paper ballots.

Blockchain-based voting systems may well be able to solve many of these problems: They are not only significantly more trustworthy, but they are also notably more secure. Once a vote is entered, it is registered across all the nodes on its network, who record it in agreement. Any inaccuracies, errors or suspicious activity will be rejected by that network, and flagged as such until technicians can investigate the problem, all while the remainder of the distributed network continues to operate without a problem. The results can also be easily verified and audited without risk of compromise.

Such blockchain-based voting systems are already being rolled out for public use. In the 2018 November mid-term elections in the USA, some votes were cast on such a system. Permanent residents of the State of West Virginia that were serving in the US military were able to register and vote via a blockchain-secured, biometrically verified smartphone app (an app only accessible using a biometric like a fingerprint or facial recognition). The trial was so successful, the city of Denver applied the technology to their municipal elections in May 2019 with outstanding results, as did the State of Utah. The convenience of allowing eligible voters residing overseas to vote on their smartphones caused voter turnout to double! Being able to secure a mobile-based voting system is a revolutionary step in the progress of democracy.

Taking Blockchain To The Boardroom

Such progress is not limited to public elections. It is in the corporate environment that such technology should interest you. Securing shareholder's voting rights should be a top priority for private and public companies alike. William Baldwin, a senior Investing Writer at Forbes, makes a strong case for the need of corporate democracy reform. He highlights the reality that most public company shares are held by exchange traded funds, and not by the shareholders themselves, thus denying these shareholders the opportunity to vote on matters that are important to them, such as climate change. Roger Aitken highlights exactly the same problem in the UK.

It is in this very arena that blockchain presents an enormous opportunity. Not only does the technology offer a far more secure and efficient form of shareholder democracy, but as we will discuss in Chapter 10, the technology can then facilitate dividend payouts as well. It is very likely that shareholders of the future will be voting for new directors and company policy from the comfort of their own home or office via a blockchain-secured app on their phone or computer. This app would also incorporate the reception of quarterly dividends.

Convincing Arguments

Attorneys, scholars, business consultants, and numerous others from across industry are seeing blockchain as a significant tool for 21st century business. Professor David Yermack of the NYU Stern School of Business & Economic Research concluded in a January 2017 research paper that "shareholder voting would become much more reliable and less costly" thanks to blockchain. In the 2019 edition of the University of Pennsylvania's Journal of

Business Law, Spencer Nord concluded that blockchain “provides an opportunity to reform an otherwise chaotic and complex system of ownership that leads to voting inaccuracies and increased costs to corporations.” And a group of law professors penned a paper for Oxford University titled “Blockchain and Public Companies: A revolution in… corporate governance”, and in it they unravel the benefits of blockchain-based corporate governance in public companies, and call for regulation in order to bring the technology to market.

University Journals aren’t the only publications where you will find convincing arguments for blockchain-based corporate governance. Attorney Fiammetta S. Piazza wrote in the Penn State Journal of Law & International Affairs that “the blockchain can achieve a progressively relevant status as a corporate governance tool,” although she did admit that its transparency could have unexplored consequences on company share prices. While IBM published an article in July 2019 highlighting the challenges of proxy shareholder voting, and how blockchain can help.

I have little doubt that corporate governance will be empowered and underpinned by blockchain technology in the near future, and in light of this, companies that implement the tech sooner rather than later will find themselves with an edge over their competitors in both adoption and executive management. And these arguments are already moving from theory to practice, as large corporates such as SWIFT are already running trials of the tech for their corporate governance.

The exciting thing about this industry is that tech startups are working hard to provide these solutions for such innovative companies, making its introduction achievable. Software companies like VOATZ and Govurn have already been contracted by government and private companies alike, and are able to provide surprisingly affordable solutions. Citizen Data’s Netvote is in the final stages of an available product, providing “tamper proof votes on the blockchain”. Netvote also believe that blockchain has the unique ability to incentivize voting, thereby reducing voter absenteeism.

Even famed cryptographer David Chaum, the inventor of Bitcoin’s precursor, Digicash, is working on a cryptographically secure voting system called “Elixxir”, and published a number of papers in the late nineties and early 2000’s outlining his vision for democracy “on the blockchain”: Visit his publications page on his website, sorted in alphabetical order, and look for the “Scantegrity” papers for further reading here.

I believe that blockchain based democracy will be an integral part of our future. I am confident that its use will see more shareholder involvement in public companies, and more voter engagement on the political landscape. Its benefits will provide the public with more confidence in the democratic structure, as companies and governments become more transparent, more accountable, and in turn, less corrupt.

Chapter 6

Potential Blockchain Use Case 3: Cross-Border Value Settlement

As emphasised in my introduction, globalisation is removing the borders of trade that have impeded international business for so long. The ability for value to be securely transferred and settled across borders within a matter of minutes will truly revolutionise the way the world does business. Corporates today have to pay hefty fees to third party institutions and wait out lengthy settlement delays which can cost billions of dollars if a foreign exchange market fluctuates during the transaction. Granted, there is much legislation yet to be introduced in order to safeguard various stakeholders (we are seeing such legislation being rolled out as I write this book), but blockchain technology allows for almost instantaneous cross-border transactions without the need for third-party settlement institutions.

Utilising blockchain for international value settlement is arguably what the tech is being used for the most at the present moment. People and businesses are doing business transactions in Bitcoin, Ether, Ripple, Litecoin every second, and sometimes worth billions of dollars at a time. While much of it is based on investment speculation, what is important to consider is that these transactions are entirely borderless - ie. there is no jurisdictional legislation impacting the transaction whatsoever.

Bringing The Tech Inhouse

But rather than attempting to transition the world's economy onto an entirely new monetary system based on cryptocurrency markets, blockchain developers are also bringing the tech to the current monetary system. While some purists would argue this defeats the point of cryptocurrency's invention, that argument is outside of the purpose of this book. While I believe there is certainly space for an entirely new asset class such as cryptocurrency/cryptoassets, we must keep in mind that this asset class has introduced a technology that is equally as disruptive. This technology is allowing corporates, banks and even governments to create a secure, virtually unhackable value transfer system that is indeed borderless and global, and virtually instant, bringing the global economy into the 21st century.

What the technology allows is the ability for institutions to create any kind of digital token that could represent any conceivable asset: A country's currency, a precious metal, or even a basket of investment assets. So instead of transferring US Dollars into Bitcoin for example, companies can exchange their US Dollars for a blockchain-based digital token representing the US Dollar. This token can then be instantly transferred to a wallet anywhere in the world within minutes, while remaining 100% pegged to the value of the US Dollar.

Current Banking Inefficiencies

VISA published a paper in 2006 highlighting the inefficiencies of the then global trade infrastructure. In the paper, VISA's Professor Yoon S. Park states that "cross-border payments are intrinsically inefficient"* due to two primary factors:

1. A lack of a global payments standard.
2. Banks being designed with local legislation in mind without considering international trade.

In other words: Because each country's regulatory framework has unique nuances, as well as the fact that there is no international standard for big banks to adopt and adhere to, one bank in one country can process payments in one way, while another bank in another country can process payments in an entirely different manner.

This can cause immense bureaucratic headaches for two companies in different countries wanting to do trade with each other, especially if their banks don't employ the same payment protocols. With this in mind, Professor Park shares the following example:

"*A British company making a U.S. dollar payment to a Korean company transfers the necessary dollar amount from its U.S. correspondent bank to the Korean company's U.S. bank account in the U.S. If the Korean company does not maintain an account at a bank in the U.S., the funds are transferred to the Korean company bank's correspondent bank in the U.S.*"*

Such an example gives us a small insight into the bureaucratic nightmare that is international trade. And because of this bureaucracy, payments are either:

1. Tediously delayed
2. Or immensely expensive

And in many cases, they are both.

With cross-border trade doubling every decade, and (as repeatedly mentioned) with the world's economies becoming increasingly global, a solution to this headache is urgently required. While the last century saw organisations such as SWIFT, BIS and the IBAN organisation facilitating most of this cross-border trade, we are now seeing a host of international FinTech startups providing alternative methods. But the reality is: These startups are simply implementing innovative methods of the same process. They are disruptive companies employing traditional technology.

Blockchain technology elegantly solves the problems of cost, speed and security for cross-border payments, and the big banks have already started to see this.

JP Morgan for instance created their very own blockchain-enabled cryptocurrency in February 2019. Aptly titled the “JPM Coin”, the cryptocurrency allows for the virtually instantaneous transfer of value in US Dollars (as described above) between their various banking jurisdictions like North America, Australia, Europe, etc.

Not long after the launch of JPM Coin, the banking giant in partnership with Accenture were recruited by the progressive governments of Canada and Singapore to develop an innovative cross-border value settlement solution. The partners got to work building an effective service on their open source “Quorum” and “Corda” blockchain software, and within a few months were ready to run live trials. The first transaction took place in April 2019, and the SGD$105 exchange was the first recorded transfer of value between two sovereign states settled on a blockchain.

My home country’s central bank, the South African Reserve Bank, identified blockchain technology as a means for international trade early on. By as early as 2014, the “SARB” were one of the first central banks to publish a position paper on the technology, with the December 2014 publication providing important insight for FinTech startups building in the space.

The SARB weren’t just out to merely pontify. Less than 3 years later, they began work on “Project Khokha” whereby each major retail bank in the country partnered with the regulator to create a blockchain based settlement solution that could be transacted on anywhere in the world. The project was built using the Ethereum network, with the assistance of key Ethereum software development company “ConsenSys”, who had already worked on such projects as the Singapore Government’s “Project Ubin”, and was able to process South Africa’s entire banking daily transaction volume in under 2 hours.

With the vast amount of FinTech companies already providing international payment solutions, there are understandably a number of critics. But after numerous international, large corporate-backed case studies, the technology has proven itself to be cheaper, faster, more secure, and even effective in the prevention of money laundering.

To date (August 2019), over 44 government central banks around the world had been reported by the World Economic Forum to be trialling blockchain technology, and it is now no longer a case of “if” we ever use blockchain technology in international trade, but “when”. The future is coming fast, and I posit that major banks will have international settlement products built with blockchain tech by at least 2024.

It’s important to note that these international blockchain transaction trials did not involve the popular cryptocurrencies covered in the media today. They were digitised versions of the national currencies in question, secured by blockchain tech. For those in the financial sector looking to make use of blockchain-enabled international value transfer, my suggestion would be to get in touch with Ripple Labs. They have trusted working relationships with many of the world’s leading banks, and are building an impressive international value transfer network.

Chapter 7

Potential Blockchain Use Case 4: Tokenised Securities & Fractional Asset Ownership

Asset ownership is one of the world's great challenges. The world is divided by the "haves" and the "have nots". The "have nots" are always looking for new ways and opportunities to get their foot in the door in their journey to becoming a "have". Economists will tell you that some of the most effective ways of achieving this is by investing in equities, bonds, or real estate. The trouble however is that these traditional investment vehicles can be restrictive because of a) the bureaucracy to purchase them, or b) they're just too expensive to begin with. These two restrictions are the primary reason many in the lower demographic of the middle class (and below) never get round to opening such investment accounts and beginning their savings journey - thus the cycle of "lack" very often perpetuates itself (not to mention the high, wealth-robbing fees of packaged investment funds).

The system's bureaucracy is understandably necessary because it prevents fraud and corruption in these markets, and ensures legitimate purchases are made and ownership is correctly allocated, while dividends are adequately distributed.

Blockchain makes a strong case for providing a solution to this bureaucracy however due to the fact that ownership allocation and dividend distribution can be securely done with minimal third party involvement - thereby lowering the cost.

Thanks to blockchain's immutable "finality", transactions are forever secured - meaning that when an asset has been allocated to a specific party, that party in question can rest assured it belongs to them. If they own the "private key"* allocated to that specific asset, it's as good as theirs. Dividends would work using the same principle: A public address would be registered with each investor, and dividends would be distributed to these public addresses based on the percentage of investment each investor holds. That distribution can happen at the few clicks of a button (when set up by the financial team of the distributing holding company/fund) and securely sent to many thousands of investors within minutes.

Fractional Ownership

These benefits of less bureaucracy and faster dividend distribution are only two of a few benefits to what the technology can bring to this space, eventually making "tokenised" shares and securities more attractive than traditional stocks, the biggest benefit of all is the ability to fractionally divide assets into much smaller parts, thereby making them more affordable and even easier to invest in.

Think about a property worth $1 million… Billions of people on earth can only dream about buying property in that price range. But using blockchain tech, that $1 million property can be split up into multiples of even millions, with each fraction digitally tokenised as a percentage ownership (IE. 1000 tokens could equal 1% share in the property).

This is similar to Bitcoin today (February 2020): Many people make the comment to me that they have missed the Bitcoin boat, and they could either never justify spending over $8000 on a digital, high-risk asset, or that they just don't have that kind of money ($8000). But here's the kicker: Bitcoin can be denominated into 100's of millions. Just like the US Dollar is denominated into units of one hundred called "cents", Bitcoin can be denominated into one/one hundred millionth called a "Satoshi". This means investors can buy one one hundred millionth of a Bitcoin for less than $1, and they get to partake entirely of its economy.

Based on this mathematical ability to denominate assets into fractional percentages combined with the reduced bureaucracy, the barrier to entry for millions of people is drastically lowered, making our global economy even more accessible, not only to a vast array of new investors, but to a myriad of companies and entrepreneurs looking to raise capital. The technology is already being put to good use in a number of cases, most notably with the recent launch of a tokenised property investment portfolio by USA real estate firm Red Swan.

Growing The Global Cryptoasset Economy With Cryptoasset Exchanges

Additionally, blockchain-empowered digital tokens become much easier to transfer internationally, meaning that they can be bought and sold on numerous markets. Cryptocurrency exchanges trading Bitcoin, Ether and numerous other cryptocurrencies, have become huge business in the blockchain industry, creating multiple new tech "unicorns" generating billions of dollars in monthly revenue on trading fees. There are hundreds of these exchanges all over the world that are fully licensed and regulated, many of whom have been active for over 5 years with a proven track record of transparent governance and quality service.

While in such a nascent industry, there have obviously been a handful of bad actors maligning the name of cryptocurrency exchanges, but as the industry has evolved we have seen more and more reputable exchanges rise to the top and eventually gain the trust of even top central banks and licensed Venture Capital firms.

These cryptocurrency exchanges experience phenomenal numbers. While there are over at least 100 fully regulated, credible and trustworthy crypto exchanges globally, the Top 20 alone have a combined hourly liquidity of $464.8 million. To simplify that metric: That number is the combined value of buyers and sellers on those 20 exchanges at a given moment. While it doesn't yet rival the enormous liquidity of traditional stock markets, you can clearly see just how significant the cryptoasset economy is.

This kind of liquidity gives entrepreneurs and companies easy access to a truly global economy. By simply reaching out to these accredited exchanges, companies can have their tokenised assets listed on many of them simultaneously for palatable listing fees, unlike the sizeable costs involved in listing on a traditional stock exchange like the NYSE or NASDAQ. Of course there are still multiple regulatory accreditations required for such companies to make their “securities” legally compliant in many countries, but these legal costs are far less than those of traditional stock exchange listing fees. Not to mention the fact that many jurisdictions do not have such heavy-handed securities legislation as large economies like the USA, where the SEC are extremely tight-fisted with how US citizens can invest their money.

And while accreditation with the SEC is actually not such a difficult hurdle to overcome, there are already progressive economies recognising that digitised securities are a fantastic way for their citizens to get their foot on the ladder of wealth-creation investing.

ECONOMICS 101: Understanding The Difference Between An Asset And A Currency

While on the topic of exchanges: Most of the cryptocurrencies on those crypto exchanges are unfortunately only speculatives tokens, and hold little to no underlying value except for perhaps their scarcity and fungibility (their ability to be traded anywhere with anyone). This is why most of them are called crypto “currencies” and not crypto “assets”, because they act like the currency of a country: They simply allow you to trade with other people. They are a form of trade.

The US Dollar and the myriad other “fiat” currencies are not necessarily underpinned by the strength of their economy. Instead they are carefully regulated by their national central bank’s inflation and economic policies. I say “necessarily”, because of course the strength of their economy does impact the demand to buy or sell the national currency - a strong US economy drives the value of the US Dollar for instance - but holding a US Dollar does not give the holder any direct benefit, besides the stability (or strength) of its value.

This is the same with Bitcoin and many of the other leading cryptocurrencies. Holding Bitcoin will not give you any direct benefit, besides the strength of its value. Granted, holding Bitcoin will allow you to trade internationally just like holding the US Dollar will allow you to trade in more places than just your home country (if it is not the US), but besides that utility of the currency, the holder does not benefit directly. This is what a currency is: A tool for trade.

Assets however are of course more than just tools for trade, they have more benefits than just the strength of their value. IE. Wheat can be eaten or used in multiple food applications, while also being traded. Gold can be used in electronic manufacturing or jewelry design, while also being traded. The same goes for oil, gas, water and numerous other assets known in the realm of economics as “commodities”.

This is why most investors don’t classify currencies as an asset class. Assets instead provide the holder with inherent value. This is why I prefer the term “cryptoassets” over

“cryptocurrencies”. Cryptoassets refers to the entire economy of cryptographic digital tokens, while cryptocurrencies is far more restrictive.

(On this note: Many cryptocurrencies are a little more “asset” than they are “currency” because they have two additional benefits to the holder: A limited supply [thus the value will grow over time as demand increases], and their blockchains can be used for more than just the storing of the token’s accounting ledger - like Ethereum’s blockchain that is used to store smart contract code, giving utility beyond just finance.)

But besides those two benefits, there is not necessarily a direct benefit to the user for holding a cryptoasset like Bitcoin. Whereas, a digitised company share on the other hand gives the user the benefit of voting rights on the company’s board as well as paying out dividends.

These digitised shares are what we call “Security tokens”. I sincerely believe this is the future of cryptoassets. We’ll cover Security Tokens in a bit more detail in Chapter 10.

Evolution of Traditional Stock Markets

The evolution of digital assets has been an amazing journey: Accounting ledgers could be recorded on computers therefore creating digital records of value in the 70’s. Money eventually became almost entirely digital in the early 2000’s as the internet and technology advanced. Blockchain technology allowed for the transfer of value without the need for centralised third parties in the 2010’s. And now, in the 2020’s, we are seeing blockchain-empowered, dividend-paying securities rolling out to dozens of cryptoasset exchanges all over the world.

Traditional stock markets like the NASDAQ, London or Tokyo Stock Exchanges etc. all began moving their accounting of shares from paper format to digital, beginning with the launch of the NASDAQ in 1971. (Fun fact: Did you know that one of the last companies to digitise their shares was the Walt Disney company in October 2013? Their paper shares had in themselves become a hot commodity being emblazoned with famous Disney characters and an etching of Walt Disney himself.) These electronic shares are recorded in central servers and carefully accounted for by the accounting software of each respective exchange. This is still labour intensive, bureaucratic, and invokes hefty security costs.

It therefore becomes obvious that traditional stock markets will eventually move to a blockchain-like infrastructure for their already digitised shares. While the first evolution was that of paper to digital starting in 1971, we are now seeing the next phase of centralised digital shares evolving into more decentralised, blockchain-empowered digital tokens. This evolution is already well underway with the Swiss Stock Exchange rolling out their blockchain infrastructure and Deloitte in Europe predicting a full blockchain enabled token economy some time in the future.

Could it be possible that traditional stock exchanges be eclipsed and made redundant by entirely digital cryptoasset exchanges like Binance, Huobi, Coinbase and the like? I think it's possible, but I wouldn't put my head on a block for it, as of course those legacy exchanges have the favour of their central banks and national governments. What I personally do think is more possible: We will see these legacy exchanges become more and more digital, eventually becoming simply competitors to these new and emerging crypto exchanges.

Conclusion

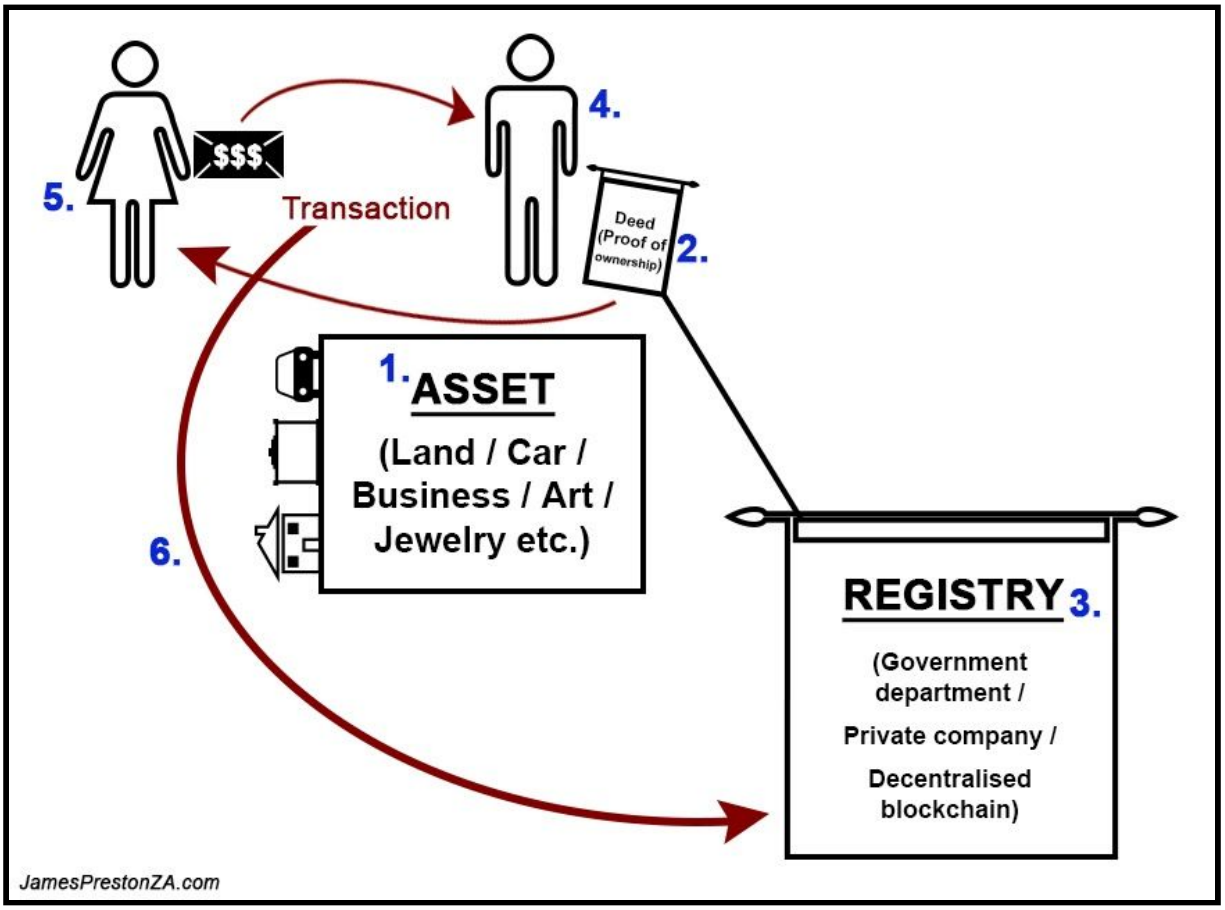
The technology for digitised company shares that give voting rights and pay out dividends, or fractional shares in assets like property or other businesses, is available and already being used by innovative companies today. The tech is being regulated in progressive jurisdictions like the Isle of Man and Singapore, and the markets are being traded with billions of dollars every single hour. Emerging exchanges that are entirely digital make it easy for anyone in the world to invest in these new digitised and tokenised shares, with the future of finance being built right before our very eyes.

The tokenised security is indeed in the future of finance. The Polymath platform is quite possibly the best platform with which to begin your company's journey of exploring a security token, but please ensure you have knowledgeable consultants assisting you in the process.

Chapter 8

Potential Blockchain Use Case 5: Asset Registries

We'll open this chapter up with a simple diagram to illustrate how useful blockchain technology can be to asset registries…



In the economy of assets, there are essentially 6 components:

1. The asset itself: A plot of land, a car, a piece of art, a business, a commodity, jewelry etc.
2. The Deed: This is the document that proves current ownership of the asset.
3. The Registry: This is simply the location where a record of the deeds (ownership provenance) is stored.
4. The current owner of the asset.
5. The new owner of the asset (or willing buyer).

6. The transaction of value in exchange for ownership of the asset, and thus transfer of the deed.

This seems like an incredibly simple way to understand ownership of assets, but the bureaucracy involved to ensure fraud and theft does not take place has become so lumbersome that most asset registries are ripe for disruption.

Enter blockchain.

By now, you should start to see the benefits of blockchain in the application of what should be a simple process. You would have noticed that at point 6, I labeled the storage of the registry as numerous options. This is because there are indeed numerous options for registry authorities to choose from when it comes to handling the important job of their administration.

Many authorities will likely keep their centralised server-based systems coupled with paper documents. In most of these cases where digital and paper coexist, the paper documents can be seen as simple “receipts” that prove ownership of an asset. These documents can be reprinted by the governing authority as and when necessary if the owner produces the correct identification documentation (very similar to our Digital ID explanation in Chapter 5). However, just because someone has the “proof of ownership” document (vehicle’s logbook, house’s APN number etc.) in their possession, it does not mean that they necessarily have the rights to the asset, as their identity needs to match the identity listed on the proof of ownership document.

It should be a fairly simple process, but in many countries this process has become overly bureaucratic and wrought with administration - drastically driving up fees and time required to process such changes.

The digital storage of the proof of ownership is currently done on standard, centralised servers, similar to those of big banks with high security and encryption methods. This is fine and understandable, but again, many technologists will argue: Blockchain just provides a higher level of security in the protection of the information, while also providing interoperability options for public services to read certain aspects of the stored data securely, which would improve multiple processes surrounding the industry in question (real estate, automotives, etc.), processes such as insurance, loan finance, utility services, and the like.

Practical Outworking

Here are a few ways that blockchain technology can assist in these processes. The first one is that of the provenance document itself (title deed etc). The details of the provenance document could be stored in a unique encrypted wallet on a blockchain, only viewable by

The adoption of the technology in government asset registries is going to take far slower than it will in the public sector, but there are already numerous examples of certain public departments around the world taking the bold step. Australia seem to be the most innovative of the government jurisdictions in this sector, with a number of examples to showcase. The Australian government released a detailed report in late 2019 of their plan to deploy blockchain technology in various government departments, with the New South Wales Land Registry the first to use the technology in their new “eConveyancing” system which went live before the report was even released.

ViVA Ventures and Medici Land Governance Company were asked by the government of Tulum in Mexico to migrate their existing land records onto a blockchain-based system in 2019, with the aim of accurately measuring tax requirements and thereby driving collection for the municipality.

Chapter 9

Potential Blockchain Use Case 6: Smart Contracts: Reliable Automation At Scale

The ability to automate the execution of a contract's conditions is already one of the most explored (but not most developed) uses for blockchain technology. The reliability of secure and robust decentralised blockchains allows for applications to automatically execute certain commands based purely on data. These commands can be executed with confidence that the data won't lie, and even if the application executed the command in error, the error will be there for all to see, not covered up in hope of protecting its reputation. A machine doesn't have that kind of selfish ambition (not yet, anyway).

This kind of execution is based on what is known as a "smart contract", a term originally coined by cryptographer and later Bitcoin contributor Nick Szabo in 1994 - long before Satoshi Nakamoto invented Bitcoin.

A smart contract is essentially a computer program that can facilitate the performance of a contract without the need for third party involvement, which of course makes such programs perfect fodder for being stored on decentralised blockchains - in fact, much of what we have written about leading up to this chapter actually involves these "smart contracts".

These smart contracts get written and tested, and then deployed to a software blockchain (as opposed to a financial blockchain) such as Ethereum, Neo, or EOS among others. What this technology now means is that companies can confidently write applications that read "input data", and execute certain commands based on that data (known in software development as an "IF THEN" rule) **automatically**, knowing this software cannot be edited or infiltrated, while remaining transparent for all parties to scrutinise.

While these automated "smart contracts" could easily be deployed to standard centralised computer servers such as Amazon Web Services or Microsoft Azure instead of a blockchain, the opacity of the data on these servers coupled with their single point of failure problem is why many developers are turning to software blockchain platforms instead. Additionally, the more centralised a software application is, the higher the fees are to utilise it. Open source permissionless blockchains provide significant security and transparency at a fraction of the cost.

In cases where important transactions and activities are happening between separate individual parties, the code implementing these activities needs to be trusted by all those parties involved. It therefore makes sense that this code be transparently run off an immutable data server like a blockchain, giving these parties the ability to scrutinise not only

the code itself, but the entire record of activities that have taken place to date, while also trusting that the code is as secure as possible.

These blockchain platforms mentioned above are known as “DApp Platforms”. A “DApp” is a “decentralised application”, and many software engineers believe that DApps are going to play an important role in the future of the internet’s infrastructure.

While these DApp platforms wrestle with how to scale the size of their blockchains (numerous software applications and their records are obviously much larger than simple financial ledgers), lightweight DApps are already successfully operating with much acclaim by even skeptical technologists and engineers. I am going to bring to your attention three areas where smart contracts are being seriously considered with vast potential. The first (copyrights) is still extremely nascent, but the following two are robust enough to already have products deployed in the market.

1. **Copyrights Protected On The Blockchain**

Copyright laws have always been very difficult waters to navigate. In the world of digital media consumption, such navigation has become even more difficult. Thousands of digital platforms are continuously playing thousands of pieces of art by thousands of different artists; whether they be authors, musicians, filmmakers or even graphic artists, they all try to make a living off their craft, but trying to police the actual payout of these artists’ royalties has become a nightmare in the digital age.

Smart contracts are a possible solution in the fight for equal royalties distribution. While there are many blockchain startups working on copyright solutions, arguably the most notable is actually a music distributor: Innovative distributor Ditto Music based in the UK say they’re tired of seeing hundreds of thousands of dollars go to the wrong place regularly, and believe that a common dataset for all music data should be shared by music distributors. Their CEO believes that the solution lies in blockchain technology.

Ditto have created a blockchain solution called “Bluebox” that will keep a register of all the sheet music from their thousands of musicians. The long term goal is that any music playing service like a radio station or streaming service would pull the data from their blockchain-based music database, and when there is a match, the music playing service would automatically register an amount to be paid to the identified artist using a smart contract. This creates a trustless and automated system whereby artists can rest assured that they will get paid fairly for the use of their music,. With contracts in place with the likes of MGM and Sentric Music already, it would seem this project is one of the more advanced royalty distribution platforms in the market.

Meanwhile, Microsoft have also seen the promise of the technology for digital rights, and have partnered with Ernst & Young to produce a solution. Grace Lao, Microsoft’s GM of Finance, says that “the complexity of digital rights and royalties is the perfect problem for blockchain to solve, because the technology can handle the unique nature of each contract between rights owners and licensors efficiently, with an audit trail for each participant.”

While this use case for smart contracts is still a few years out from adequate integration into the media industry, it shows significant promise of what is possible with the technology.

2. BRAVE: A New Internet Browsing Experience

In the same way that blockchain tech is helping artists get a fair share of their royalties, the technology can be used to distribute revenue streams in a more even manner. The internet today is skewed toward those building the internet, not the users. The best media designers build addictive websites that people can't stop clicking on and coming back to, sell the ad space at a premium, causing the advertisers to distract these users to clicking on **their** content, and the only people that see a return are the advertisers and the media platforms.

If there were some way to build an internet that shared the value of user attention with the actual user, we would see much more responsible media platforms being built. One famous internet developer believes he has such a solution to the internet's current mess…

Brendan Eich is an engineer famous for co-creating the Mozilla Firefox internet browser. As someone with intimate experience with consumer internet-browsing habits, Eich saw the problem of the consumer-centric internet not long after Mozilla Firefox was launched. Banner advertising on websites was fast becoming an invasive experience, turning good reading into a maze for users to try and navigate. This problem was exacerbated when advertisers began taking advantage of "cookies" and user-tracking technology, allowing the adverts to become even more personalised.

Eich became passionate about providing a solution, and so began the journey of building a private internet browser, "Brave". Launched in Nov 2018, Brave automatically blocks ads, limits cookies, does not record user activity on its servers, and has a built-in smart contract based economy: That of the "Basic Attention Token", or "BAT".

The Brave browser aims to make the consumer the focal point of the internet, not the advertiser with all their invasive techniques. Brave have designed a micropayment ecosystem, whereby users get paid for the adverts they **do** see, as well as being able to contribute to monthly news subscriptions (like NY Times or Wall Street Journal) on a "per article basis".

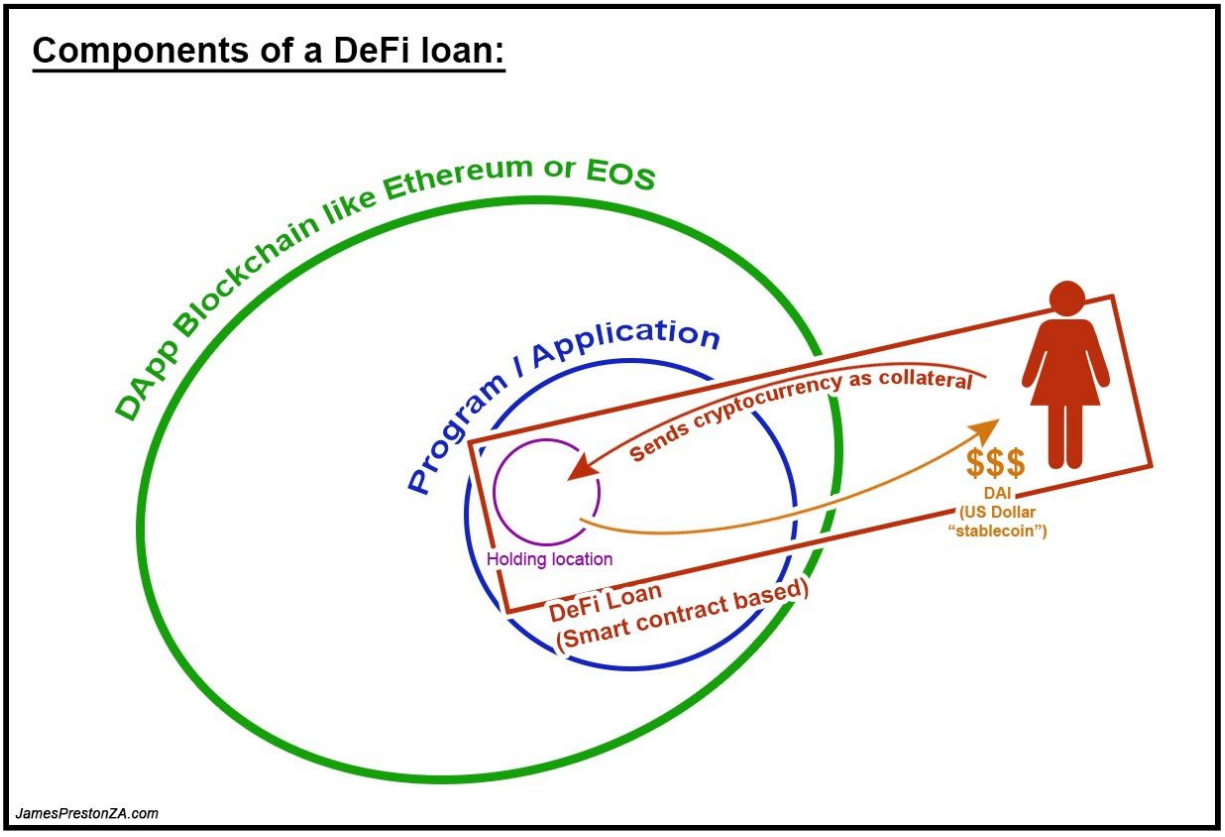
Here's how Brave's ecosystem works: Advertisers set up campaigns with Brave, and these campaigns get strategically placed to be seen by users. The Brave team then enter a number of conditions and rules of these adverts into a smart contract running on the Ethereum network, and when a user sees an advertisement from one of these campaigns, the smart contract reads the data of how long the user saw the ad for, if they clicked on it, etc. and automatically pays the user out a small percentage of BAT, the browser's native cryptocurrency. These payouts average 70% of the actual ad revenue, highlighting just how user-centric Brave want to make their ecosystem. The usage and viewership statistics of these ad campaigns will be recorded on Ethereum's blockchain, allowing verifiable and trustworthy (but user-private) data for the advertisers.

Launching with 800,000 users in November 2018, the browser reached 3.5 million users in its first year. By January 2020 it was being utilised by 10 million people, and had advertising contracts with the likes of Intel, Amazon and Pizza Hut.

3. DeFi: Decentralised, Automated Financing Options

While Brave is one of the more sexy utilisations of smart contracts (that is actually being put to good use), automated financing has recently grown to become the largest space for the DApps industry. Known as “DeFi”, which stands for “Decentralised Finance”, these smart contracts allow users to free up capital by putting up their cryptocurrency as collateral in an automated loan.

While the term “DeFi” encompasses all forms of financing options, the one being most utilised in these yet nascent stages of cryptocurrency is that of the “collateralised debt position” (CDP). Using complex financial and mathematical structures, developers have created programs running on smart contract platforms like Ethereum that allow users to send their cryptocurrency to a “holding location” and automatically receive a certain amount of US Dollar value in return in a smart contract based loan.



In order to further explain the above, and to illustrate how a smart contract system can simplify a complex financial product, let’s go through a step by step example...

While DeFi can be operated on any smart contract platform, the most popular by a very far margin is the Ethereum network. There are two tokens involved in a DeFi loan running on the Ethereum network: ETH (Ether) and what is known as a “US Dollar stablecoin”, usually DAI. Both of these cryptocurrencies are available for purchase on the many popular and reputable exchanges mentioned in chapter 7.

So we have ETH and DAI, and in our example, we have a woman called Daniella, and her son called Marco, try to see if you can follow along…

1. Daniella is a cryptocurrency investor, and was holding 100 ETH as one of her high risk cryptocurrency investments (cryptocurrency is a high risk asset). She was always going to hold that ETH for the long term, so for the next year or two it wasn’t going to “do” anything for her (besides perhaps growing in value).

2. Daniella’s 22 year old son Marco wants to buy an eCommerce store on Shopify Exchange, as he is trying to earn extra income while at University. So, Daniella decides to leverage some of her ETH.

3. She puts 50 of her ETH into a DeFi loan position (the “collateralised debt position”) using the “MakerDAO” protocol.

4. The smart contract only allows her to take out a maximum of 66% of the value of her collateralised ETH. At the time, each ETH token was worth $100, so her 50 ETH was worth $5000 in total. To reduce the risk of a liquidation of her assets* (the ETH), she takes out 50% of the value instead of 66% (the closer you are to 66%, the more chance you have of your loan being liquidated in order to fund the automatically-running protocol).

5. Once everything is in place, Daniella clicks “agree”, and 50% of her ETH value is automatically paid out to her in the DAI token (a US Dollar “stablecoin”), let’s just call it $2500 instead of DAI 2500 for the sake of understanding.

6. Daniella can pay back this amount whenever she feels like it, at an annual interest rate of 8% (at time of writing - these interest rates are automatically adjusted according to the price of ETH).

7. Daniella is now sitting with DAI 2500, while 50 of her ETH are locked up in a separate wallet controlled by the smart contract - the code (viewable for all to see) has no access to these funds, besides the strict conditions of paying back or liquidating the collateral (another important example of why secure blockchain technology is the best suited infrastructure for this kind of application).
   Daniella then moves her DAI tokens to a large cryptocurrency exchange, and sells it for Bitcoin. She then sends that Bitcoin to a “fiat/crypto” exchange like Coinbase, Luno or Bitstamp, where she sells that Bitcoin for real US Dollars, and withdraws that USD into her Wells Fargo bank account.

Steps 5 to 7 all took a few minutes, while the US Dollars arrived in Daniella's bank account the following day.

8. Now Daniella has an extra $2450 (after a few fees) in her Wells Fargo bank account. She transfers this to her son Marco's bank account, who purchases the eCommerce store from Shopify Exchange for $1900. In return, Marco gives his mom a 40% stake in the business. It is agreed that the additional $550 be used for some extra marketing of this new online business.

9. After 6 months and some great work by Marco, the business has generated a total of $1000 in net profit, and Daniella's son pays his Mom $400 as her part of the profit-share. The business is now worth $7000 according to Shopify Exchange's data, and Daniella's son decides to buy his mom out so he can go alone, and pays his mom $2800 in order to get his 40% equity back.

10. Daniella now has a total of $3200 after 6 months. All the while, the price of ETH had continued to rise, and at $140 per token Daniella's 50 ETH are now worth $7000.

11. Daniella thought it was a good time to close the loan, and worked out that her 8% per annum interest fee would be $100 (if she closed the position after 6 months, the fee would be 4% because it was closed after half a year, thus half the interest rate is charged). This makes the total DAI owed back to the smart contract $2600.

12. Daniella deposited $2650 into her Coinbase cryptocurrency account, again, $50 to overcompensate for fees.

13. The next day, when the money reflected, she bought Bitcoin with that $2650, and sent the Bitcoin to a cryptocurrency exchange where she could buy DAI. 10 minutes later she was able to buy $2600 worth of DAI.

14. She sent the DAI (her original $2500 + the $100 4% interest) back to the Ethereum address where her DeFi loan was sitting, and immediately her 50 ETH were unlocked and back in her own ETH cryptocurrency wallet.

15. In 6 months, Daniella had collateralised her 50 ETH that she was always going to hold anyway, and made $700 for a few clicks, while also helping her son set up an online business. She also didn't lose out on the growth in ETH's value, because she got the full 50 ETH back, which were now worth $7000 as opposed to $5000 6 months ago.

    This is the power of collateralised loans when used wisely and correctly.

A **liquidation of a Collateralised Debt Position is when your locked up ETH is lost. When the price of the ETH token causes the value of your locked up ETH to go below 150% of the DAI you have been loaned, the smart contract will automatically sell your locked up ETH to*

the market in order to protect its operation and the market. However, you are not obligated to return the DAI you borrowed, as the sold ETH acts as the collateral.

The point of all this is not to show you how collateral can be leveraged for your economic empowerment, instead it is an example to highlight the power of automated executions in computer code - a smart contract. There was not a single person involved in checking Daniella's collateral, verifying who she was, or counting the correct amount of DAI is paid out and vice versa when she paid it back. All of that was done automatically by the mathematical equations run (and then executed by) the code. This code sits on the Ethereum blockchain, so it cannot be adjusted or edited unless the large community of open source developers agree.

All interest rates, liquidation rates, amounts paid out, are all automatically adjusted based on numerous data points, allowing for complete self-service in not only absolute confidence, but anonymously as well.

Smart Contracts: A Key Backbone in our Technological Future?

This DeFi example shows exactly how powerful smart contracts are, it also highlights why immutable, transparent and decentralised blockchains are so important for such power. If there were a central point of failure and it were taken advantage of by a malicious actor, millions of dollars worth of cryptocurrency could be stolen.

The network infrastructure of big banks (like Wells Fargo or JP Morgan) actually has a number of central failure points. If they were breached, it could mean bankruptcy for millions of people. But to secure these vulnerabilities, the banks deploy billions of dollars in security technology in order to give them and their customers absolute peace of mind. These billions of dollars are felt every day by the average consumer, who pays exorbitant fees for a simple transfer and has to wait sometimes days before that transfer is complete. An immutable, decentralised, network database means consumer security remains extremely high, but fees are kept to the bare minimum.

It has been argued by many DApp developers that blockchains were made for smart contracts. These incredible decentralised lines of code allow for automation in almost anything that can be connected to the internet: Your TV, your car, your smart watch, a ship, a shop, a house or a fridge. Any device that transmits data into "the cloud" has the potential to be utilised by a smart contract.

In the same way that DeFi utilises the data of ETH prices and loan values, other smart contracts can utilise the data of flight times or delivery notifications, allowing for secure and reliable execution of the next step in the process entirely automatically.

Other areas of industry where smart contracts are either being experimented with or have already been introduced are automated flight insurance, crowd-sourced household and asset insurance, and even online role-playing games where users work for and get rewarded

in cryptocurrency. Most of these are still in their extreme infancy, but are already revealing how the technology could reduce costs and increase efficiency without compromising trust.

The first smart contract platform Ethereum was only released to the public on 30 July 2015, over 6 years after Bitcoin was released, highlighting just how nascent this vertical of blockchain tech really is. In these early stages, there will be many trials, errors, and failures along the way, but when you see the automation of the already successful applications like we've seen above, you see just how powerful the technology can be.

There is very little doubt that smart contracts are going to play a considerable part in the future of commerce, and are one of the most powerful features of blockchain tech. If your business relies heavily on contracts being fulfilled and honoured before work, goods or payments are released, then automating this process by placing the various rules and conditions on a DApp blockchain could be an important move in positioning yourself for the future of work.

Chapter 10

Potential Blockchain Use Case 7: Digital Identity

There is a strong case to be made that Identity is the biggest and most consequential challenge facing the digitised society within which we now live.

In order to comprehend the need for a blockchain-like solution in this arena, we must grasp the philosophical nature of the problem. So indulge me as we examine the problem at hand before exploring the solution...

Our identities are made of all kinds of unique facets: the physical look of our bodies and faces, the construction of our DNA, the sound of our voice, the design of our eyes, the shape of our fingerprints, the way we walk and act, our handwriting, our intelligence, who our parents and family relations are etc. All are physical attributes of our identity, otherwise known as “biologically measured metrics”, or “**biometrics**”.

Then there are **reputational** attributes of our identity: What we own, who we know, what we know, what we have achieved, where we were born and where we now live. These reputational attributes are infinitely complex: How we drive, where we drive, how we use the internet, where we used the internet. It is these more complex sums of our reputation that create an infinitely unique identity about us that poses a far-reaching problem: It is a form of our identity that we don’t *necessarily* own.

This is why identity is a significant philosophical problem. Who owns our identity? The obvious answer is that each individual should own their identity. After all, my fingerprint cannot belong to anybody else, my voice, my eyes, all the biological attributes of who I am that no-one else can have in their possession. It is uniquely within my realm of ownership, and is physically impossible to be stewarded by anyone else.

This is why slavery and equal gender rights are such importance issues. Who owns a human being? The answer should be quite simple: We each own ourselves. This is the core principle of identity that is millennia old: It is undeniably ours.

But in the post-modern age, as we have crafted a very complex web of reputational identity, we have unintentionally (and unwittingly) lost control of that which has been uniquely ours for thousands of years. This complex problem has become exponentially exacerbated in the digital age. Before the age of the internet, our reputational identity could fairly easily be scratched out and restarted by moving to a new state or country by gaining new citizenship, opening a new bank account, etc.

A Question Of National Security?

Of course, this is what criminals and fraudsters have done for centuries. But here is where we come to the crux of the argument: Law enforcement agencies have long argued that this reputational identity is important to their cause of catching such criminals, and thus their ability to monitor such reputations is necessary for the safety of society.

One could argue that these law enforcement processes were merely gathering evidence in order to adequately bring such criminals to justice. We bought into this argument (or at least accepted it) in the pre-digital age, and in fact didn't think too much of it. But as the world has become infinitely connected in the information age, this dialogue should be taken a lot more seriously - instead though, law enforcement agencies are using the same argument for an entirely different time, and an entirely different set of data; data that should remain the property of the individual.

It is fundamentally a human rights dialogue: Who owns your identity? You or someone else? At face value it's an extremely simple response: You do. And that means every time someone needs a record of your identity, you should know about it. Think about the pre-digital age: Law enforcement agencies or government bodies would need to physically get a photo of you, a fingerprint from you, a DNA sample, your body measurements, etc. And each time, you would know about these samples, and you trust these agencies and bodies to safeguard such information.

In the digital world, not only is your reputational identity being recorded without your consent, it is being done without you even knowing it.

This has become an historic human rights problem.

If our identity belongs to us, it should be a fundamental right that every aspect of this identity remains within at least our knowledge, let alone consent.

Granted, there are far more rudimentary human rights challenges that still face society that must be equally addressed. But we cannot fight one on one end of the spectrum while ignoring the other. Both are to be addressed with equal severity.

The Blurred Progression Into Digital Reputational Identity

An important challenge in this digitised reputational identity crisis is the way in which we arrived here: Unintentionally.

Because the internet is entirely unchartered territory for civilisation, there was no framework to adopt in policing it. Instead, the best and most profitable ideas won. And yes, you guessed it, those ideas were pretty much best capitalised by Google and Facebook. Yes, Amazon, Apple and other tech "decacorns" have created equally impressive titans, but Google and Facebook designed their business model around the capitalisation of reputational identity. And it all started so innocently (in Google's case, anyway).

The Rise of Google

Google was a great idea. Quite frankly: A phenomenal idea. An idea so great and powerful I would argue they wholly deserve their near-trillion dollar market capitalisation. The idea? To archive the entire internet. Simple, profound, and extremely helpful.

This archive obviously meant that users of the internet could visit this website in order to search the entire archive; Google had made the internet “searchable”. It didn’t take long for the brilliant engineers to realise a powerful opportunity they had created as a by-product of their genius invention: Internet users began using this archive in search of websites they specifically needed, and this meant Google could sell the top search positions to the highest paying bidders. And on a fateful day in the year 2000, “Paid Search” was born, allowing advertisers to target their market with scalpel-like precision.

It seemed harmless at the time. But when internet developers realised the power of a 1994 invention “the cookie”, a little piece of data stored on your computer each time you visit a website, they saw just how precise this targeted advertising could get.

This realisation happened in the late nineties, and wasn’t properly capitalised on until 2007, when Google made their first acquisition in the advertising space: That of a tech startup who were tracking people’s internet activity. So as you can imagine, 2000 to 2007 is actually a fair amount of time for paid search to become a harmless addition to our internet experience. Within seven years, the majority of internet users had accepted paid ads as part of the Google product.

As this “cookie technology” progressed and became more widely introduced, the ads simply became more targeted. There was no “internet police” or regulatory body monitoring how these companies, now gargantuan tech powerhouses, should be operating. And the internet was such a precious tool (freely accessible infinite information!) we humans naturally made it part of our everyday lives. And so the cycle continued in the early 2010’s. Every website (and page) we visited was inserting cookies on our computers, being used to target us with even more specific advertising.

We actually thought it was quite neat: Ads that we wanted to see, instead of spam that meant nothing to us like what we had become accustomed to on TV.

Then came Facebook.

The Facebook Monster

By the time Google was tying up their acquisition of the AdTech company in 2007, an extremely intelligent and crafty young software engineer from Harvard was seeing his creation take the world by storm. Facebook had replaced MySpace as the social network of choice, which in themselves were new and exciting concepts.

Do you know what the difference between Mark Zuckerberg's Facebook and Tom Anderson's MySpace was? Zuckerberg, like Google, had realised the potential of targeted advertising. And there was no more powerful form of user data than that of a highly engaging social network. To this end, Zuckerberg set out to build the most engaging social network possible. A feat he achieved pretty much from the get go.

Users couldn't get enough of it, and because the idea of user data had barely been considered, let alone dialogued, we all kept handing our data over with each and every click. Soon, ambitious politicians recognised the powerful tool hyper-targeted advertising was. In 2008, Barack Obama's marketing team utilised the engagement of Twitter to attract and win over younger voters, setting a precedent that other politicians desired to emulate, which they did the world over.

By the time Brexit's referendum had passed and Donald Trump had won the USA Presidency, it was too late. Our reputational data had become a prodigious tool being used to manipulate us.

We, collectively, all of society, had become the slow cooked frog, not noticing the slow rise in temperature that started with fairly innocent paid search ads in 2000 and progressed into a belly-up mess of dead flesh 16 years later.

Entire inquisitions were launched. Documentaries were made. Policies were written. But it was all too late. The tools that we used every single day had become such an innate part of our everyday lives that the companies who owned them knew we wouldn't give them up. They knew that we would gladly hand over our reputational identity in return for the use of their extremely well designed dopamine-releasing tools.

So while millions of pages of policies were written and billions of dollars of legal fees were paid, the only thing that changed was that we now had to give consent to these software giants using our reputational identity. Think about a drug addict: If all they needed to do was to tick a box and hand over every piece of information about themselves in order to get the next hit of their favourite drug, even if it meant that fundamentally their human rights were being handed over, do you think they'd tick that box? Of course they would. Every. Single. Time.

Dramatic

You may think this is an unnecessarily dramatic indictment on these software companies. Afterall, manipulation of user data is nowhere near as bad as deliberate withholding of government aid to the starving, or child labour in Somalia, right? Well, that's why I started with the elementary understanding of our identity belonging directly to us, and no one else. It is a fundamental human right. And if these human rights are not protected, how much more abuse will we as society willingly consent to, even if it is by simply turning a blind eye?

If my user data is part of the fundamental make-up of my identity, then it is blatant misuse for private companies to store that data without my consent, let alone compensation, and a compounded gross abuse for that data to be used in manipulating my actions.

This foundation is important for us to understand why reputational identity needs a better solution in the Information Age.

Giving The Data Back To Trusted Owners

Trust is a big word in the Information Age, it's why blockchain has become such an important topic: Public blockchains are essentially "trustless", they don't require trust. But there is a serious reality we must be aware of: There is essential data that needs to be stored somewhere in order to give us as individuals a place in our home countries/jurisdictions. Things like our birth dates, gender, names, race, all need to be recorded and assigned to a specific number: Your social security, identity, or passport number.

These are important pieces of data essential to our operation within our societies. We trust our governments to protect this data and only use it for their own recording purposes. While at face value it may not be ideal for our governments to hold such important data about us, we all recognise that it is important for civil responsibility.

But this is where the data should stop.

Ideally, there should not be any other party that stores such important information about us. We have trusted governments for thousands of years to protect our identity records, and we should not be trusting anyone else. Today however, we are trusting our banks, phone service providers, clothing stores, grocery outlets etc. with our data (bearing in mind we don't have an alternative unless we don't want a bank account, cellphone, or clothing account).

This is all before we address the digital reputational identity problem online! Besides our governments, we have dozens of physical consumer-facing outlets storing our personal data, and openly using it and selling it on in order for us to be marketed to. Not to mention the fact that the more entities that hold our data, the more chance we have of that data being stolen by malicious hackers. This fundamental citizenship data should be stored in one place, not by every entity with whom we have an account.

Private Personal Information (PPI) And Solving How We Get Verified

This fundamental citizenship data is known in the forensic and legal sectors as "Private Personal information", or "PPI". While there are a few technologists in the blockchain and SSID industries who argue that blockchains provide a good platform for this PPI to be stored, the majority prefer the idea that PPI should be kept off of a blockchain, because blockchains are fundamentally transparent, and having that PPI data (which is immutably stored on the blockchain) accidentally or even purposefully accessed by unwarranted users would be a nightmare. (There may be a blockchain solution for the **storage** of PPI in the

future, but my study of the industry points to the alternative I present here. I am open to technological development in the years to come proving me wrong).

Instead of blockchains providing the **storage** solution of our PPI, they can provide a **verification** solution. But likewise, instead of each entity with whom we have an account storing our PPI, these entities should simply be verifying us and our credentials (like credit history etc.) using a digital key, something blockchain technology can provide.

While perhaps not ideal, but exponentially better than our current system, it is widely agreed that our PPI should only be stored with single, centralised holders, such as a government or corporation with whom we transact. IE. Our citizen data should be stored with government, our bank account data should be stored only with the bank in question, our clothing account data only with the outlet in question, etc.

Instead of all these data points, such as spending habits, income level, credit history, speeding fines, being shared among large organisations to create this perfect profile for marketing companies, these data points can stay with each organisation and never have to leave. There will be a lot of data mining and marketing executives reading this squirming in their seats as they read it, but as extensively described above, our reputational identity is fundamentally ours to own, and thus we should own the right to approving (or not) its release and use to other organisations.

A silver bullet to the head of the PPI "recording monster" is simply to *prove* our PPI to each organisation with whom we transact *without* that entity knowing the PPI itself.

Each time you open a new clothing, bank, or medical account, sign a new lease agreement, or buy a new asset, you need to provide copies of your PPI such as ID documents, drivers license, proof of address and bank statements. These items give the corporations surety that you are who you say you are, and you do indeed qualify for the product you are applying for. **In a "self sovereign identity" scenario, you would not need to hand over that PPI to any of these organisations at all.**

Instead, you control who gets to see your PPI, how many times they see it, when they see it, if they see it at all, and what each organisation does with your identity when they do see it. Each "pull" of your PPI is recorded on a blockchain, and is verifiable by, or at least notifiable to you.

How It Works Practically

Every individual on record is assigned a digital identity made up of a private and public key, linked to their PPI on government record, and linked to their unique biometric attributes (fingerprint, face, etc.). The most secure option to generate and store these keys is with a blockchain.

Individuals can then access and manage their digital identity using an in-browser application on the internet or on their smartphone. A separate and unique physical device like a thumb drive could potentially serve the same purpose of managing digital identities, but practically doesn't seem to provide the best user experience (users don't really want another device to look after and protect, and carry around with them regularly).

The in-browser or smartphone application is accessible using a biometric signature, where all of the individual's PPI is viewed, and a history of each verification request sent to the user's public key is displayed. This gives the individual peace of mind not only because they know which organisations are trying to prove who he/she is, but also because those organisations will never know their actual PPI.

Think about it: Every universal human citizen is identified by only a handful of numbers. In your home country it could be an ID or Social Security number. When you travel abroad, it could be a passport number. But instead of giving that number out to organisations to assign you an identity with that organisation, you would give your "public key" to that organisation.

So What Is A Public And Private Key?

I realise that up until this point we haven't discussed public or private keys. This is because we haven't needed to discuss how a blockchain transaction takes place, we have only discussed how blockchain networks are actually built and supported.

A public and private key belongs to the "wallet" of a single entity, this could be an individual, a group, or a company. Each wallet has a public and a private key. The public key is how information is sent to the entity's wallet, and the private key is how the entity accesses that wallet. Let's use the world's largest blockchain, Bitcoin, as an example: A public key on the Bitcoin network is where people can send Bitcoin to. A private key on that network is how the owner of that public address spends the Bitcoin inside that wallet.

These keys are made up of a large string of alphanumeric characters generated by the encryption algorithm of the blockchain. Take a look at the example below:

Private key (used to access and spend the Bitcoin):
L47ke1NDKcK82YZkoL6JYzVsJUSRSS2mW5q6rx5JGvQgBh19mtbo

Public key (used as an address to send Bitcoin to):
19wkwEaLsfW4Jg7uURQvypbErLxgTsz85z

The private key is to be kept safe and secure at all times, because if anyone gets their hands on it, they will be able to access and spend all of the value inside of it. And if your mind, new to blockchain technology, is thinking "if all I need to do to spend the Bitcoin inside a wallet is to guess that private key, then why don't I invest time in doing some guessing?" Well, the odds of guessing a private key on a standard public blockchain are 1 in 115 quattuorvigintillion. A quattuorvigintillion has 75 zeros in it. To give you some perspective: The odds of winning the average lottery is 1 in 14 million, a million only has 6 zeros in it. For

further perspective: There are approximately 115 quattuorvigintillion atoms in the universe. Guessing a private key is like randomly choosing the correct atom out of every single atom in the entire Universe.

Now, let's get back to our SSID example...

Practical Example

Let's take this knowledge of public and private keys, and our practical understanding of Self Sovereign Identity so far, and apply it to an example similar to what we did in the DeFi chapter. For the sake of continuity, we will use "Daniella" as our subject person again.

1. Daniella really likes a new bank on the market, "Future Bank", and decides she wants to open an account with them. She logs onto their website, and clicks on "open new account".

2. A dialog box asks her to enter her "SSID (self sovereign identity) public key", which she does.

3. The bank's system automatically pings the digital wallet associated with that public key, and without actually seeing any of the information inside that wallet, is able to verify she is a local citizen, is in good credit standing with her current bank, but does generate a request for full names and her address for billing purposes.

4. This sends a notification to Daniella's phone, where she accesses the SSID wallet via biometric fingerprint. The notification tells her exactly what the bank wants to verify and see, and she approves the request.

5. Future Bank's systems automatically approve Daniella because they're able to verify that she meets all of the criteria, and even offers her a credit limit on a new credit card, based on the risk profile her current bank has listed her as (again, this information is only accessible when another entity asks for it, which needs to be approved by the individual).

6. A new bank account number is automatically generated for Daniella, and sent to her public key. Now Daniella can access this bank account number in her SSID digital wallet, and transfer cash into it, or give the account number to new clients etc.

7. Even paying at grocery stores is done using the NFC technology (the same tech used in chipped bank cards) inside her smartphone, which is associated with her SSID digital wallet.

Daniella never had to enter her private key, because that was previously setup when she first downloaded the application. Now that her phone has associated her private key with her

fingerprint and face ID, she is able to access the SSID digital wallet application using those biometrics without ever having to enter her private key.

When she upgrades to a new phone, she would do the same thing: Download the application, enter her private key, and all of the associated accounts are immediately accessible.

Where Is All The Information Stored?

1. The primary and general citizen data is stored in the centralised facilities of Daniella's national government, and is associated with her unique private key.

2. This private key, along with an associated public key, is generated on a trusted blockchain network (companies like Sovrin and Uport are doing proven, successful work in this field).

3. Each individual corporation, government organisation, and even individuals, all store only their associated information with Daniella on their servers/facilities. Info such as bank statements and credit history is stored by the bank, driving license details are stored by the Roads Authority, grocery account details are stored by the grocery outlet, rental agreements are stored with the landlord on their own computer, etc. These entities only access Daniella's SSID wallet to verify the existence and good standing with the other entities, they cannot access the data itself. And each time they do access and verify Daniella's wallet, she knows about it.

This is very likely the future of our identity data. While it could take decades to become widely adopted and used, with a few iterations along the way, this fundamental process empowered by blockchain verification is a clear starting point of where the industry is likely headed. There is no need for our data to be recorded and duplicated by hundreds of different organisations. Each organisation should only store the data they need for their own purposes, and we should know if that data is ever requested by another organisation - we should also have the power to approve, deny or report such requests.

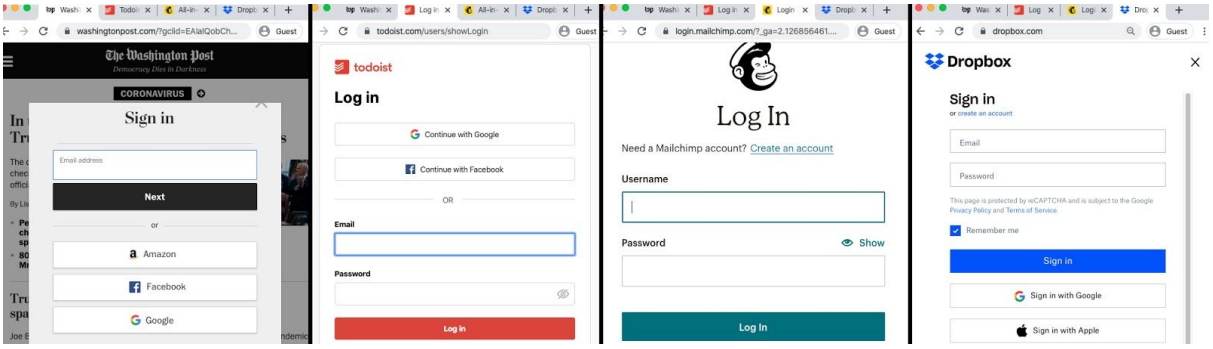
Applying This To The Internet

This technology that clearly makes sense in standard scenarios such as opening a bank account, should also be used in our use of the internet. The unfortunate reality of the current state of the internet is that Google, Facebook and Apple dominate the web almost entirely. Most websites these days create user accounts for their websites, this is not only to track data, but for less sinister uses such as capturing your contact data so they can keep in touch with you with regular newsletters and promotions etc.

The problem of course, widely discussed earlier in this lengthy chapter, is two fold:

a) These websites are storing “cookies” on your computer so as to remarket to you later.
b) It is highly likely that they are selling the data they have on you to other companies.
c) They offer “sign in” options via Facebook, Google, or Apple. This gives these companies even more insight into your internet usage, and more data for them to use in marketing to (and manipulating) you.

I did a quick test on my own internet browser to see what options various websites give me in logging into their platform. I checked four companies that I personally use regularly: The Washington Post, ToDoist, Mailchimp, and Dropbox - A news site, a productivity app, an email marketing company, and a cloud storage company. As you can see in the below screenshots, of the four companies, three of them offered me login options via Google (75% of the random sample) while two of them offered me login options via Facebook (50%). The odd one out was Mailchimp who only offered login via email. Granted, it’s a weak dataset and I’m not drawing any conclusions about the amount of internet websites that require login via these Social Media companies, but it does give a very raw idea of how Facebook and Google have dominated the internet.



The reason internet companies such as the above offer login via Facebook, Google and other accounts is because it is an easier “user experience”. The idea was first introduced in the late 2000’s, and was sold as a simple solution so users didn’t have to remember a different password for each website they visited - bear in mind that at the time, many websites didn’t require you to login at all (like the Washington Post, CNN, or NY Times for instance).

Much like digital ads on Google and Facebook, this form of logging in became so much easier that almost everyone adopted it, and slowly but surely it became the standard method by which users entered (and even registered for) various websites. Once again, a slow cooked frog scenario. This form of logging in allowed for even greater user profiles that contributed to the voter manipulation scandals of Brexit and the 2016 USA election among others. It allows for Google and Facebook and other companies who offer the service to gain even more valuable information about us, and create razor sharp profiles of who we are.

An SSID option gives us the easy user experience, but without any of the user data infringements whatsoever. A user could login with a credential associated with their SSID,

the service in question like the Washington Post or Dropbox would simply notify the user's SSID wallet that a login was made, and grant access to the user and create a profile around them. This profile is associated with the user's SSID, none of the information inside the SSID wallet is ever released to the service (unless they ask and the user allows for it - in which case the user could be compensated with a small amount of a cryptocurrency), and all the data generated by the service such as their reading habits, their interests, their location, would remain secure because that data is associated with the SSID and releasing to a third party would require a notification sent to their wallet.

This is the age of Self Sovereign Identity that many computer scientists, software engineers and even philosophers and policymakers are working towards. I believe it will be an age we will see in our lifetime, as it is the next frontier of the internet.

Gary de Beer, a South African software engineer who is recorded as one of the first users of the internet in South Africa, pioneered internet infrastructure for his corporation in the mid nineties because he saw it as the next stage of technological innovation. Three decades later he now believes that Self Sovereign Identity, empowered by blockchain and distributed ledger technology, is the stage that naturally follows.

"Huge internet companies have become honeypots of aggregated, specific data about every one of us," de Beer said in a short interview with me for this book. "We should have agency over this data, and should have the right to terminate services and revoke our consent to the ownership of it."

Like Gary, along with thousands of people around the world, I believe we will see an internet that offers us such agency some time in the future, and very likely later in this decade (2020's).

A future where our identity belongs to ourselves, and is sovereign from any other organisation, is arguably one of the most important futures blockchain technology can provide us.

- - - - - - - - - - - - - - - - - - -

For further reading on this deeply technical and philosophical topic, I would highly recommend a presentation by Australian Computer Scientist John Phillips explaining Self Sovereign Identity in an easy-to-understand way. Special thanks to Gary de Beer, one of South Africa's very first internet developers and now arguably the country's leading SSID experts for his assistance in my research, along with his recommendation of Mr Phillips' work.

Some exciting working examples of Self-Sovereign Identity already being deployed include:

- *TruuID in the UK, eliminating exhausting identification paperwork for new doctors in the medical field.*
- *MemberPass and CU Ledger financial service products.*

- *The South African Financial Blockchain Consortium's partnership with the country's leading bank ABSA to improve security and speed in new bank account applications.*
- *The African Union's plan for a digital identity platform to allow for easier cross-border trade in the African Free Trade Area.*
- *KIVA, in Sierra Leone, a United Nations project that has built a national digital identity platform.*

Companies that can assist in the building of Self-Sovereign Identity products include the Linux Foundation's Hyperledger Indy and Aries, the Sovrin Foundation, Cambridge Financial Blockchain, Evernym Software, and uPort (an Ethereum based identity platform).

Chapter 11

Potential Blockchain Use Case 8: Company/Project Fundraising Through An ICO or STRO

This is arguably the most widely adopted utility for blockchain at the moment. You are probably well aware of the “ICO” craze that swept through mainstream financial media in 2017, whereby every user and their dog was investing in the next ICO, all driven by hype the fear of missing out. User X invested half a bitcoin into Project Y and their half q bitcoin was now worth 100 bitcoin. The reality is though: In the vast majority of cases, User X invested in an ICO and got lucky in an early and unprecedented “bull market”.

For those that don’t know what I’m talking about: An ICO is an “initial coin offering”, very similar to an “initial public offering”, or “IPO”. As I’m sure you’re well aware, in the traditional IPO: A company will register with an official stock exchange such as the New York Stock Exchange, Hong Kong Stock Exchange or the NASDAQ stock exchange, in order to allow public investors to buy stock options (or shares) in the company. Through an almighty rigmarole of administrative and legal process, the shares will be listed on a certain day, at a starting price based on a number of factors such as projected earnings etc. That share price will then fluctuate from moment of listing, and the lucky ones that got in early on a good company usually make some decent return on their investment in due course.

An ICO, Initial Coin Offering, on the other hand is based on a similar principle, except without much regulation. A project could create a whole bunch of cryptographic digital tokens just like Bitcoin (because Bitcoin was open source - its source code and intellectual property available for free), and put them up for sale to whoever wanted to buy them. Once launched and distributed, these tokens would then trade on cryptoasset exchanges (as mentioned, there are hundreds of them) and people would trade and speculate on their price.

Many of the founders behind the numerous blockchain projects that ran an ICO argued that their “coin” was necessary for the functioning of their blockchain ecosystem, in other words their token had utility. But in actual fact, another more established cryptocurrency could have been implemented into their ecosystem. Many of these founders were clutching at straws as they attempted to explain the reasons their ecosystem needed its own unique digital token. This may have been the case for some of these ecosystems, but it certainly was not necessary for each and every blockchain.

Most of these digital tokens aren’t underpinned by the company’s health and do not offer any form of dividend, nor any voting rights to the company’s operations. IE. They are in reality nothing like shares in a real company, and are pure speculation.

Having said that though, a few companies **have** taken the responsible approach and created distributed dividends and voting rights to token holders (ie. each token is equal to a percentage share in the business), but these companies are unfortunately in the extreme minority in the cryptoasset industry. This is what you get in an unregulated landscape. As someone who thrives on innovation and emerging technology, I have actually enjoyed watching the evolution of this unregulated landscape and its Wild West nature, but I am also keenly aware of the damage it has done to many immature investors by unscrupulous scam

artists (it's the reason I started SA Crypto's news portal, to help self-regulate the industry with responsible journalism).

The Security Token

These more responsible companies took the "STO" route instead of the easier "ICO" route. As touched on in Chapter 4, an STO stands for "Security Token Offering". Unlike an Initial Coin Offering, which could be a distribution of digital coins/tokens that are not directly related to a project or company's performance, a Security Token **is** in actual fact directly linked to company performance.

The SEC (Securities and Exchange Commission) is the USA's regulatory body for investment firms, helping to protect investors. They of course have clamped down pretty hard on cryptoasset companies within the US, and for this reason, Americans are not allowed to invest in a lot of the cryptoassets and currencies on the market, or even open accounts on certain cryptoasset exchanges. The SEC deems that a security is a share or token that is directly linked to an entity's performance. For example: When Tim Cook announces that Apple will roll out a new feature on the iPhone, its share price may go up. In this case, an Apple share is a security.

While the SEC has not *officially* labeled any cryptoassets a security as yet, based on this definition (called the Howey test) many cryptoassets actually are securities. Bitcoin is not a security because there is not one single entity representing it, therefore there is no way to anticipate what its performance could be, and, it did not start by raising funds. But many others, with central figures and leading personalities overseeing their projects, are indeed securities.

Promising Avenue To Raise Funds

Today, now a number of years on from the "ICO craze", the market is starting to show signs of maturation, and a lot more companies are thinking how they can raise funds responsibly without fleecing their investors. This means giving value to their investors, and while an ICO is still a potential option for a lot of companies to raise fairly quick and "easy" funds from a global pool, and is still being adopted as a form of fundraising by some in the industry, it is the STO that is fast becoming the industry's chosen method to raise capital.

Let's take a look at the basic outline of the process required to raise funds using the cryptoasset framework and what goes into kicking off an STO or ICO…

1. **Choosing the desired format: ICO or STO**

   The first thing a company looking to raise funds with these methods in mind is determine which format most suited to their needs. Choosing the avenue of ICO or STO depends on a number of factors such as how fast a company wants to raise funds, how much regulation and administrative process they are willing to go through, how much of the company's control they are willing to hand over, etc.

It also depends on where the company is based. The USA's SEC regulation now restricts ICO investment significantly, so companies there or those wanting to attract USA investors would be better off running a registered STO instead of an ICO.

After all the evaluation, the company may even come to the conclusion that the traditional IPO market is actually better suited to their needs. I have drawn up a comparison chart that looks at the differences between an ICO, STO and an IPO - and this gives a basic idea of which offering is better suited for certain companies at varying stages.

2. Technological framework of offering

Once a decision on format has been made, and assuming the company have decided upon an STO or ICO, the next step is choosing the technological infrastructure. There are numerous blockchains upon which such offerings can be built, with some more suitable than others.

Ethereum is the go-to choice because of its size and network support. Ethereum, as explained in earlier chapters, is built as a "smart contracts" platform, and thus tokens can be written onto its platform easily with all kinds of algorithms associated with these tokens: Such as supply amount, company share percentage, etc.

Ethereum has become the largest smart contract platform because it was the first, and thus has grown a lengthy and credible history, and has proven itself to be reliable in the deployment of such smart contracts for thousands of different companies.

Ironically though, while size is arguably Ethereum's strongest suit, it is also one of its weakest. Due to the size of the Ethereum blockchain's database of smart contracts, transactions and code, it has become fairly congested. This congestion has given rise to numerous alternatives that have also proven to be considerable players in the market.

One such player is Cardano (not the polymathematician from the 1500's but the blockchain network named in his honour). The Cardano platform was founded by one of the co-founders of Ethereum after some disagreements in protocol design, and is arguably one of the best alternatives to the Ethereum platform because of its similarities.

Other alternatives that are worth considering are EOS, Stellar, NEO, and RSK, the latter being the first smart contracts platform integrated directly with the Bitcoin blockchain.

3. Choosing the structure of the offering

There are two primary things to decide upon when running a token offering:

a) **Format of investor payment**
This refers to how investors make their contribution to the offering (ie. the payment gateway). Many token offerings only take Bitcoin, some only take Ether (this is common if the offering is being run on the Ethereum blockchain), some take Bitcoin, Ether and traditional currencies like US Dollar. Some only take traditional currencies, but this is uncommon because it alienates the numerous cryptoasset enthusiasts, the very market that such offerings appeal to. It is advisable that companies running a token offering set up a payment gateway that accepts at least two cryptocurrencies and a few traditional currencies.

b) **The type of sale**
This refers to the actual structure of the offering itself. There are two primary routes that companies take when running a token offering: One is to set early stage prices, and the other is to run a "dutch auction" style offering.

While many (including investment bankers) prefer the idea of setting a starting price, it's important to note that at the end of the day: The market will decide the price. A company's executives may believe that their value should be "3x", but when their shares go public, the market decides that their value is actually closer to "1x".

So while setting a starting price can be tempting because it helps in goal setting, it should be noted that in-depth company analysis is required to set a **fair** price so that the market's response reflects that price accurately.

Alternatively the dutch auction style can be more beneficial in the long term, because the company running the offering may only reach a certain amount of investors, and thus the price starts out low, and as the wider global market cottons on to the investment potential (if there is any), the price naturally rises as the investor pool rises - basic supply and demand economics. This also helps with company expectations, because more often that not, companies don't raise as much as they initially expected.

In both instances however, it is important that companies take into consideration various rounds of investment. Many of us would be familiar with the numerous rounds of Venture Capital funding, such as angel, pre-seed, seed, series A and B, etc. It is similar with token offerings: Companies usually set private sales, semi-public sales, and public sales. This is easier to set when a company has chosen the initial starting price of their token, because each round can be cheaper than the next thus earlier stage investors have an advantage.

It becomes more of a mathematical challenge in a dutch style offering, because it is difficult to determine the value of the token after only one or two rounds, it is only after the offering has been completed that the value of the token can be determined. This is why a dutch style offering requires an experienced tokenomics mathematician to assist in the formula of the auction. While I can recommend one such mathematician, others can be found using traditional Google and LinkedIn searches.

4. **Legal compliance**

It is extremely important that legal counsel is sought in the design of a token offering business plan. Operating in the business space is frought with regulation, and can land (and has landed!) a lot of businesses and executives in a lot of trouble. Ensuring one is on the right side of the law in structuring their offering is of paramount importance.

While basing the offering from a progressive jurisdiction like Cayman Islands, Seychelles, Malta or Isle of Man, I highly recommend any company seeking to run a token offering consult their legal partners for advice on moving ahead, just to ensure they are protected in the event of regulator or investor backlash. There are also numerous legal firms worldwide who offer consulting for digital token investment law.

5. **Taking the offering to market - Building the narrative**

Now that the foundation has been built, with the format, the software platform, the style of the offering, and legal partners all selected and put in place, the offering is ready to go to market. This is where a lot of companies get it wrong: For two reasons: They are either market their offering too well and don't have a good enough product, and eventually face significant public outcry, or (and this is more common) they have a remarkable offering but have no clue how to tell the world about it, and therefore don't raise anywhere near enough money as they were hoping.

A single experienced marketing consultant can do wonders for companies without such experience, because they can help build the story of what their product will actually do, why it will make money as a business in the future, and therefore why investors should contribute to the offering. This is the most essential part of the "take to market" strategy. Without the narrative of what a product is and why investors should part with their money, a company can't sell it. A company just has to get these two things right (what and why), believe in them (don't do it if you don't believe in it!), and they can achieve impressive results.

Once the what and why narrative has been settled upon, it's just a case of "how" it gets taken to market. Will the company invest heavily in paid marketing? Will they

use “growth hacking” tactics and cheaper PR? Will they go to institutional investors, retail investors, or both? How much marketing budget will they set aside to reach these investors? All these decisions need to be made with some kind of marketer’s input, and agreed upon before launching the offering.

Once agreed, it’s off to the races. Launching the offering, and seeing how the market responds to the company’s story.

6. **Operation after the offering**

   An important stage in the life of a token offering is what happens after the investment rounds have ended. Unfortunately, many companies in this industry hit astonishing numbers, and the founders splashed their new found cash in extremely irresponsible ways. As they say “money makes funny”. This resulted in neglecting the project itself as the founders went on celebrity roadshows, and no winter savings for coming bear markets, and eventually to the closure of hundreds of companies that successfully raised staggering amounts of money.

   What happens after the offering, whether it is deemed a success or not, is absolutely critical. If too little was raised, companies can still bootstrap their way to a successful entity and raise the value of their token. And arguably more importantly: If the offering was a success, the company must follow through with regular communication with their investors, payouts of blockchain-based dividends (if it was an STO), regular shareholders meetings with digital streams and voting options for investors, and of course successfully hitting deadlines on the roadmap.

   With consistent hard work, I have seen obscure companies rise to remarkable prominence as they proved to the tech world that they have a product that solves a problem well and is therefore profitable.

The great thing about raising funds through this method, is that it is available to anyone. Whether a company is 500 staff strong, or just an ambitious individual at home alone looking for ways to “kick start” their business, anyone can truly do it. The only thing someone needs is to be able to reach enough people (with disposable funds) and convince them their offering is worth investing in.

I like the thought of an ICO or STO, because there isn’t a lot to lose, depending on budget of course. If a company has a large R&D budget and wants to experiment with this, there is much to gain. But if a company watches every penny, and doesn’t believe in this form of fundraising, then there is far too much at stake.

If a company wants to be part of the fourth industrial revolution, can hustle up a bit of cash for software development and marketing, and has an appetite for risk, then this is certainly something worth exploring.

For those keen on exploring this form of fundraising, I would highly recommend this article by Fitzner Consulting about how to run an STO, and this guide by Cointelegraph on how to run an ICO. And if you do ever go ahead with ICO or STO, please contact me with feedback, because I would love to hear about how it went, especially if this book inspired you to do it.

Chapter 12

Potential Blockchain Use Case 9: Automated Insurance

The insurance industry is perfectly poised for blockchain disruption. So much so, that PWC claimed in a research paper in 2019 that 100% of surveyed insurance groups planned on integrating the technology into their systems by 2021. Big auditing and researching firms such as KPMG and Deloitte have all come out recently with consultation papers explaining their understanding and stance on the technology in the insurance industry, and like PWC believe it will be widely adopted in their technological infrastructure in the near future.

Professor Dan Ariely, the Chief Behavioural Officer at Lemonade Inc, one of the leading insurance startups in the world today, rightly states the following about the current state of the insurance industry:

“There is an inherent conflict of interest in the very structure of the old insurance industry. Every dollar your insurer pays you, is a dollar less for their profits. So when something bad happens to you, their interests are directly conflicted with yours. You’re fighting over the same coin. Basically, if you try to create a system to bring out the worst in people, you would end up with one that looks a lot like the current insurance industry.

Conflicts of interests encourages us to embellish our claims. That increases distrust, making the process painful and frustrating, and that vicious cycle continues to spiral. Before you know it, premiums go up, while getting paid becomes a nightmare.”

Ariely and Lemonade Inc set out to build an insurance company from the ground up back in 2017, and they immediately went to blockchain for the underpinning framework. Unfortunately it must be noted that the technology was not mature enough for their ideals, and they had to abandon it as part of their tech stack a year later in order to adequately meet their growth goals. It is expected that the technology would have developed sufficiently by 2021 so as to be more widely utilised for industries such as insurance.

But how would blockchain benefit the insurance industry?

As suggested by Professor Dan Ariely, fraud is one of the biggest challenges that insurance companies face. In the UK for instance, the association of British insurers believe that insurance fraud costs their industry approximately $2.5 billion (USD) every year - an industry primed for disruption for “trustless”* disruption! Wrapping policy data into a smart contract is arguably one of the best ways to reduce and hopefully eliminate such fraud.

It is quite feasible that insurance fraud will eventually be a thing of the past. Imagine: Each policy's terms and conditions written into a smart contract, and when a claimant meets the required criteria, they will be paid out *immediately*, without the need for investigation or even verification, because the verification criteria will be written into the smart contract before the policy is even taken. Now, there may of course be issues in the early days whereby fraudsters *might* find loopholes in the infrastructure, we have to accept that this is part of the innovation process: not absolutely everything can be considered on its first engineering attempt. It will only be through trial and error, and continuous protocol updates, that the system will be 'loophole free'. But this is a small price to pay in the quest for zero insurance fraud and cheaper insurance.

Just consider all boundary-pushing technology: The Apollo missions. The Space Shuttle. Virgin Galactic. Self-driving cars. The list could go on. All technology is rigorously tested before going to market, but even then, the technology still requires improvement. This is the natural course of evolution.

Even blockchains are regularly being updated as they get rigorously tested by their community. At the time of writing (19 August 2020), the Ethereum blockchain is currently on version 1.9.19, which is its 174th update to its code since its release in 2015. The Bitcoin blockchain is on version 0.20.1, which is its 236th update since its code was originally released in January 2009.

Back to insurance security… Insurance companies long for the day that their policies are watertight and secure. And smart contracts on the blockchain are a significant solution to bring such security.

Applying blockchain to the insurance industry is going to take some time to get right, because there is so much regulation and value involved in the ecosystem. But there are pioneering companies already offering policies backed by smart contracts. Lemonade Inc., mentioned above, have an almost entirely automated claims process for household insurance built using state of the art artificial intelligence, coupled with a unique business model. They have experimented extensively with smart contracts, and have announced they will most certainly be using the tech in future offerings.

Inmediate is a Singaporean startup building an entire insurance platform on the blockchain, available for corporate insurers to simply plug into. If you're in South East Asia in the InsureTech industry, scheduling some time to see this team is highly recommended.

Black Insure are an ambitious European InsureTech startup who not only want to revolutionise the way consumers interact with their insurance companies, but they want to give the consumers a piece of the pie as well.

Everledger are already one of the most established blockchain companies around, with a diverse portfolio of smart contract applications, the most famous of which being their diamond and precious gem offerings. Using a smart contract, Everledger are able to verify a precious gem's authenticity, and thus insure it adequately and quickly.

Again, as mentioned, the availability of this kind of InsureTech to the consumer is going to infiltrate the industry slowly. The key benefits of blockchain in the industry are:

- Less bureaucracy in both the client onboarding and the claims process
- Quicker, eventually instantaneous payouts
- Insurers can rest assured that fraudulent claims will become almost impossible, and thus are only paying out legitimate incidents
- This will mean much cheaper premiums for the consumer

I would highly recommend those in the insurance industry to begin consulting with respected blockchain tech experts and prepare for the future of insurance today.

"Trustless" is a fairly new term associated with blockchain and DLT. It derives from the feature whereby the network doesn't depend on the intentions of its participants, who could be malicious **or honourable. In a traditional network, we trust that the central authority holding all our data are a) not malicious, and b) have done everything they can to prevent malicious actors from threatening our data. In a trustless network like a blockchain, we don't depend on the central authority (like a Google or Amazon), we instead confidently rely on the decentralized network underpinned by its code. Malicious actors are simply rejected by the network entirely.*

***At time of writing: 19 August 2020*

Chapter 13

Potential Blockchain Use Case 10: Contracted International Worker Payment

Remote Work: Opening Up A Global Workforce Of Billions

The internet, along with its modern applications of the 21st century, have made it possible for a vast array of jobs to be conducted from anywhere in the world. Thanks to Zoom, Skype, Google Hangouts, Slack, and of course high bandwidth internet, employees and freelancers alike can continue building products with their teams from the comfort of their own homes. It has been forewarned by many trend analysts, including the team at Tomorrow Today Global, that remote work will be the job location of choice for more than half of the workforce by 2025, and the Covid-19 Coronavirus Pandemic highlighted just how important being able to work and manage a business from home actually is.

While many company executives scratch their heads at the challenges they perceive related to remote work, many other progressive execs see the potential to tap into a far wider pool of talent, potentially for even cheaper. Remote work is another hot topic of our globalisation dialogue, and with it comes the challenges of cheaper workforces in economies where currencies are more powerful than others. We have seen how India has become the hub of outsourced software development due to the strength of the US Dollar in comparison to the Indian Rupee.

This of course can wreak havoc on the Western software development workforce, but I would argue (as would many trend analysts) that the forces of market economics must take their course. Which is exactly what they did when the internet allowed India to rise into a dominant software dev hotspot. The trend of Western companies outsourcing their code to India began in the late nineties, and within a decade it was the “thing to do”. With so much code being written offshore, it didn’t take long for highly qualified students from Stanford, Harvard, Caltech and the like to accept lower pay in order to get work. The market somewhat equalised. I say “somewhat” because the quality of code was, and is, higher by the law of averages, and therefore many Westerners are able to charge a premium. But if you want cost-effective; India remains to this day a place for incredibly affordable software development, while perhaps not being the most polished.

But Indian software development for Western companies is only one example of an entirely new trend that has now exploded in the post-Coronavirus era. The internet truly has created a global workforce, and this makes it so much easier to find affordable talent for companies and entrepreneurs to build anything they want at a fraction of the cost. Entrepreneurs and company execs only need to tap into the millions of “gig workers” offering their services on websites like Upwork, Fiverr, Freelancer, or Guru, many of whom are working in the West.

I have hired at least three dozen freelancers from websites like the above while working both for myself as an entrepreneur, as well as when I was the Marketing Manager of a medium-sized corporation with a staff of eight people in my care. I have also worked as a freelancer myself earning extra income offering my services as a voice over artist to companies all over the world, so have fairly intimate knowledge of the gig economy from the perspective of both sides of the table.

It doesn't matter what you do or even who you work for. If you need to get a project done, tapping into a global workforce of millions instead of going through the process of trying to hire the right person can save you hundreds of hours and thousands of dollars. A global workforce empowered by the internet has changed our economies forever.

But how does this workforce get paid?

I have given this framework to lead into the point of this chapter: **International payments for this global workforce.**

With a fairly vast array of experience in freelancing, I can confidently attest that cryptocurrency is by far the most common and accessible form of value transfer on offer in the market today. Its closest competitor is PayPal, but the internet payments giant is limiting for many recipients because the process to withdraw funds out of their PayPal accounts into their native currency is too technical, laborious, and expensive. While it may be instant, it most certainly is not the most effective.

Cryptocurrencies like Bitcoin or Ether are easily exchanged into local currencies because there are a handful of cryptoasset exchanges in most countries, whereas in many cases PayPal withdrawal services are only offered by a single bank, if at all (for instance: Here in South Africa, only one of the top ten banks offer a PayPal withdrawal service, while there are six regulated cryptocurrency exchanges where cryptoassets can be exchanged for South African Rands and withdrawn to any of the local banks).

A Practical Example

Paying someone in cryptocurrency is incredibly easy, and in some ways simpler than a traditional wire transfer…

1. Employers can either use their credit cards on many of the main international cryptoasset exchanges (like Binance, Coinbase, or Bitstamp) for immediate conversion of their national fiat currency into cryptocurrency - or deposit national fiat currency into these crypto exchange accounts via local wire transfer, and purchase the cryptocurrency once it reflects.

2. Then, all the employer needs to do is take the public key (as discussed briefly in Chapter 5 about Digital Identity) of the worker's cryptocurrency wallet, and type it into the recipient section of a new transaction on the exchange, add a note, ensure the

public key is correct, and hit “send”!

Voila!

3. Of course there will be a verification via Google’s 2fa (two-factor authentication) or via email, and in some cases, the public key (recipient’s public address) will need to be pre-approved/whitelisted before this transaction takes place. Such a pre-approval is as simple as what I have just described, and when the transaction takes place, it is simply a case of selecting the pre-approved/whitelisted address from a drop down menu.

4. Depending on which cryptocurrency is used, the amount will reflect and be spendable in the recipient’s wallet within any one of 5 seconds (Ripple), 30 seconds (USD Tether or DAI), 5 minutes (Ether), 20 minutes (Monero), or an hour (Bitcoin) - these processing times are all dependant on the construction of the cryptocurrency’s blockchain, and each have been constructed with various factors taken into consideration.

Widespread Adoption

The ability to pay someone internationally without requiring overwhelming paperwork and not needing to jump through administrative hoops has caused dozens of companies all over the world to employ staff and contractors based on Bitcoin or Ether salaries (Ether being the native cryptocurrency of the Ethereum network). Cointelegraph, the world’s leading blockchain news outlet (think “Bloomberg for blockchain”), pays all its writers in Ether. These writers are distributed all over the world, from Russia to Australia to Argentina and beyond. The onus is then on the writer to declare that income in their own personal tax returns.

The majority of freelancers I have worked with are very happy to be paid in one of the top cryptocurrencies for their services, and many of them prefer this form of payment.

As with so much in the cryptoasset and blockchain industry, this form of commerce is still extremely nascent, but is becoming more popular by the week. Various regulations and price volatility have hindered its adoption, but the trend is clear: **A cryptocurrency-based remote work economy is fast approaching.** As more cryptocurrency exchanges open around the world, and as more people become comfortable with how cryptocurrencies work, the regulation will follow (here in South Africa one of the big banks recently launched a cryptoasset custodial wallet). The volatility is no longer an issue, as stable coins like “US Dollar Tether” or “DAI” are now widely accepted cryptocurrencies in a myriad of crypto wallet services and exchanges, meaning that workers can receive the benefit of being paid in US Dollar value, but with the speed and global accessibility of cryptocurrency.

Convergence of Global Technologies

The convergence of remote work and cryptocurrency is an inevitable one, and we will eventually see a platform showcasing this convergence at scale, at which point there will be

an exponential growth in the remote work economy. In more recent years, many platforms have been restricted by local regulation in order to protect local economies. One such example is the world's largest freelancing network Upwork creating a division between the international economy and the USA economy. Before the division, freelancers and employers would meet based purely on their needs and skills. But after the intervention by regulators, American employers would only be matched with American freelancers, thereby removing international freelancers from the US economy; a regulation brought about because American freelancers complained about losing work to their international counterparts (obviously because their counterparts were cheaper).

But regulation can only prevent the inevitable for so long. As international trade becomes much easier and more accessible through blockchain-enabled cross border payments, and platforms arise that integrate such payments, the global market of remote workers will once again equalise the labour markets.

Already there are a handful of blockchain focused platforms connecting employers and employees where cryptoasset payments are accepted. While Crypto.jobs and Proof of Talent are well-positioned to disrupt the recruiting industry with their focus on the global cryptoasset economy, incumbents like AngelList, Glassdoor or even freelance sites Upwork and Fiverr could easily shoot to become tech unicorns if they successfully navigated the tricky waters of regulation and were able to integrate cryptoasset payments for work done on their platform.

As has been exhaustively stated in this book: Along with the internet, Blockchain provides the next significant layer of infrastructure for a global economy. With high speed internet and all the tools we need for creating great products on our laps, borders are becoming redundant. In a century (or perhaps two due to the slow response of nationalist politicians), it is very likely that our economies will evolve into a single economy of global talent, limited only by time zones. And there is no better financial technology to build such a single global economy than blockchain. There will be numerous cryptoassets changing hands for various reasons, with the likes of Bitcoin, Ether, US Dollar Tether, DAI, Monero, Ripple and Binance Coin all the likely winners in decades to come. But all are borderless and permissionless, and all are built with blockchain.