State of Play: Blockchain

1. THE BATTLE FOR THE INTERNET

Maybe the Internet is fundamentally flawed. Like a marble column, with a single blow to the heart of the stone, the webbed masterpiece could explode into dust.

90% of data on the Internet has been created since 2016.[1] We upload family photos to a photo-sharing app; save travel plans on a travel app; store recipes in a recipe app. Almost every app we use asks us to save our debit or credit card details at some point. We trust others to keep our data secure, but there is no way to verify who else is accessing our data online. As soon as our data is uploaded, we cede control.

In the wrong hands, a little piece of data can go a long way. The attack on Equifax, a credit-scoring firm in the US, earlier this year compromised the account details and social security numbers of 143 million Americans.[2] Most of this data has already been sold to other black-market firms who will use that commit fraud.

As more and more of our data is stored in blackbox central databases, the success rate and scale of these data breaches will continue to scale. According to Karthik Swarnam, AT&T Vice President of Security Architecture, "Cybercrime damages are expected to rise to $6 trillion annually by 2021."[3] Enough successful attacks, and our trust in the internet will crumble.

But a fringe community of Libertarian programmers and activist hackers believe they have found a solution to restore our trust in the Internet, and they are introducing a paradigm for transacting online in the process.

For decades, a concerned community of computer scientists have been quietly working out a new system, resilient to the hammer strike that could render today's networks meaningless in a matter of moments. Their Holy Grail was a self-regulable, secure and decentralised network, capable of withstanding even the most pernicious threats: a malicious attack to a central node, or worse, a central authority going rogue and corrupting the network from within.

What began as a passion project of tech diehards has transformed, with breathtaking speed, into a movement that is sweeping through the digital community, touching off a surge in new ventures, investments and innovations that, if realised at scale, have the potential to fundamentally change how we interact with the Internet.

How did an idea pioneered by anti-authoritarian punks and championed by drug dealers, become the darling of governments, banks, and global corporations?

The story of Blockchain is the story of a persistent human quest for trust, autonomy and safety.

2. DOWN WITH THE BANKS

Threats to our data in the ether world parallel a more tangible threat that has dogged society for much of our modern history: the worth of money.

Throughout time, the mechanisms of commerce have been defined by social contracts enforced by a central authority. The King issues coins that ascribe a certain value to things, trade is regulated and, for the most part, people's individual fortunes are secured. But, who is to say if your coin is still valid if the rules change? You stockpile a treasure, and wake up one day to find the King is dead and your fortune is valueless.

> *"All money mankind has ever used has been insecure in one way or another." - Nick Szabo* [4]

To find a solution to our Internet problem, the cryptocurrency pioneers of the 1980s and 1990s began by first trying to solve our money problem. The hunt was on for a new currency that would be internationally recognised yet independent of the fortunes of the realm.

THE QUEST FOR THE ANTI-BANK

The first step towards a decentralised currency system was to find a means to make the exchange of money anonymous again.

Cash is a private exchange of a mutually-agreed value between two parties. Although you could withdraw cash from a bank, and the receiving party may in turn deposit the cash into another bank, the details of the purchase itself remain private. But with the rapid adoption of credit and debit cards, banks have quickly become repositories not just of money, but also for data on how we spend our money. When we transact digitally using a debit or a credit card, our financial data is no longer private: we are entrusting the details of that exchange with our bank, the credit card company and our friend's bank.

A method for private digital transactions would return the benefits of cash, with the speed and convenience of credit.

In 1983, David Chaum introduced the first model for eCash, a digital payment system that retained the privacy benefits of cash. The eCash system allowed users to store bank-verified digital money on their home computer, and to use that money to pay for goods or services from participating merchants. The new system was able to "blind" the relationship between the withdrawal and payment transactions, achieving the same level of privacy as traditional cash transactions.[5]

But Chaum's eCash system, along with similar schemes piloted during the mid-1990's by *CyberCash*, *Digital Equipment (Compaq Computer)* and *IBM,* fell short of the goal of an anonymous and decentralised currency system. To the consumer, the functional benefit of eCash was unclear. To the tech world, the system was still overly reliant on a central authority, since the bank remained singularly responsible for verifying each transaction. [6]

Meanwhile, a radical concept for the future of truly independent digital money was emerging.

THE CYPHERPUNKS

Whereas Chaum's eCash sought to transform fiat money into digital cash, the pioneers of cryptocurrency were pushing an even more revolutionary idea: creating a fungible currency for a purely digital community, de-linked from any federal monetary system.

> *A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. Traditionally these services have been provided by the government or government sponsored institutions and only to legal entities... I describe a protocol by which these services can be provided to and by untraceable entities.*

In a seminal essay published in 1998, Wei Dai, an intensely private computer engineer associated with Microsoft, described an anonymous cryptocurrency system backed by a distributed peer network that could facilitate both the creation and the exchange of digital "b-money." [7]

Dai was a member of the Cypherpunks, a loosely organised community of digital privacy advocates committed to realising the ideal of a decentralised and anonymous monetary system. Counted among their number were Adam Back, Hal Finney and Nick Szabo (who also briefly worked with Chaum at *DigiCash*, the successor to eCash). Building on each other's innovations, the Cypherpunks contributed essential pieces to the puzzle of a fully-realised cryptocurrency. [8]

The foundation for Dai's currency system was proposed by Adam Back a year earlier, in 1997, through a modification of the cryptographic principle of Hashcash.

Hashcash was conceived in 1992 by Cynthia Dwork and Moni Naor as a means to cryptographically secure email messages. The program appends a difficult-to-solve but easy-to-verify mathematical puzzle to the header of an email. The puzzle must be solved prior to sending the email, and solving it proves the sender has enough interest in the message being delivered to take the time to complete the puzzle.

Back's modified interpretation of HashCash applies the same principles, but uses the puzzle as an incentive, rather than a deterrent. According to Back, users could earn digital currency by solving the hash puzzles appended to pending transactions, earning at a rate corresponding to the time required to solve the puzzle. Worth is proportional to effort: a gold bullion is more valuable than a penny because it is harder to make.

Dai theorised a mechanism similar to Back's Hashcash in his concept of "b-money," a currency that could be created by anyone with a computer:

> *"Anyone can create money by broadcasting the solution to a previously unsolved computational problem. The only conditions are that it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual. The number of monetary units created is equal to the cost of the computing effort in terms of a standard basket of commodities." - Wei Dai*

Still, Dai's proposal lacked the technical details to implement his theory. Without the means to turn idea into reality, interest in the pursuit began to wane. By the early 2000's most had given up hope on the cypherpunks' dream for a cryptocurrency utopia.

3. I'VE BEEN WORKING ON BITCOIN

CRASH AND BREAKTHROUGH

The cypherpunks were motivated by the conviction that establishing a distributed and independent monetary system was essential to a secure and peaceful society.

As the world careened into the 2008 Financial Crisis, cypherpunk's interest in devising an alternative currency system sparked again. This time, after a nearly decade marinating in the technology hive-mind, a fully-fledged cryptocurrency system emerged — at the climax of a global financial meltdown.

On October 31st, 2008, one day after the chief of Merill Lynch resigned in the wake of revelations that the investment bank was exposed to $7.9 billion in bad debt, an email from Satoshi Nakamoto with the subject line, “Bitcoin P2P e-cash paper” was sent to a mailing list of cryptography enthusiasts. [9] [10] [11]

The brief email described a new peer-to-peer digital currency system that utilised several of the foundational concepts pieced together by the cypherpunks nearly a decade earlier: no central authority or mint, peer-to-peer authentication with hashcash and anonymous participation.

> *“I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.” - Satoshi Nakamoto, October 31 2008*

Within three months, on January 9th 2009, Nakamoto released Version 0.1 of the Bitcoin software, launching both the software and the first units of the Bitcoin cryptocurrency, also called bitcoins.

WHO IS SATOSHI NAKAMOTO?

An aura of mystery surrounds the creator of Bitcoin. Satoshi Nakamoto is most probably a pseudonym of the person (or group of people) responsible for inventing the technology. Multiple investigations have failed to reveal Satoshi Nakamoto’s true identity, although some suspect the inventor may be one (or several) of the cypherpunks who lay the groundwork for the Bitcoin system he pioneered.

Dai and Nakamoto exchanged emails in August 2008, several months before the publication of the Bitcoin whitepaper; Back and Nakamoto also allegedly emailed during that time. Hal Finney was the first person to use the Bitcoin software after Nakamoto launched it, and the first person after Nakamoto to mine bitcoins. And Nick Szabo began publicising his renewed efforts to build “Bit Gold,” a system with striking similarities to Bitcoin, in the spring of 2008, yet went inexplicably silent after Nakamoto’s October announcement. More notable coincidences surrounding the birth of Bitcoin link Nakamoto to at least half a dozen other crypto-pioneers. [8] [12]

There is greater consensus behind Nakamoto’s motivations. Like many of the cypherpunks, Nakamoto displays a distinctively Libertarian slant, characterised by a mistrust of centralised authority and a desire to establish a financial system free from state regulation. The first mined bitcoin — known as a Genesis Block — contains a message from Nakamoto that directly references the ongoing financial crisis: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.” [13]

The message, entered in the comment section of the first bitcoin block, quotes a headline from The Sunday Times of London. *“Chancellor Alistair Darling on brink of second bailout for banks. Billions may be needed as lending squeeze tightens.”* The reference has been taken as a critical commentary on the state of the financial markets. [14]

To Satoshi Nakamoto, the cypherpunks, and early Bitcoin adaptors, the 2008 Financial Crisis marked the demise of an outdated global financial institution, and heralded the entrance of a new breed of monetary exchange for the digital age.

A QUESTION OF TRUST

Bitcoin was not the first attempt at a digital currency. Various digital currency projects had already been born and passed into obsolescence — including eCash and b-money — long before Nakamoto introduced his digital coin.

The success of any private currency hinges on trust. Participants need to believe that others will accept their coins in exchange for goods or services, and that the goods received will be worth the value exchanged. People will avoid a marketplace if its merchants are known swindlers.

Anonymous cryptocurrencies face an even higher hurdle. By design, purchase records are private and buyer and seller identities are kept anonymous. Cryptocurrencies are seen as a haven for fraudsters, money launderers and drug dealers.

To earn public trust, bitcoin would need to do more than prove its coins are reliably redeemable. The platform would also need to demonstrate that the moral and ethical benefits of participation outweigh the risks associated with an anonymous digital currency.

E-GOLD: A CAUTIONARY TALE

One year before the release of bitcoin, the public witnessed the fall-out of a years-long effort by the Federal government to dismantle an earlier digital currency, E-Gold.

Driven by a conviction that the United States should never have left the gold standard, Douglas Jackson, a practicing oncologist and amateur economist, decided it was time for a “radical rethink of money.” With support from a software engineer, Jackson programmed, designed and launched E-Gold in 1996, introducing an anonymous, nationless currency backed by gold.

By 2005, E-Gold had grown to more than 3.5 million customer accounts in 165 countries, with 1,000 new accounts opening every day. E-Gold was second only to PayPal in the online payment industry.

But the dark side of an anonymous currency exchange would soon land Jackson behind bars. International criminals were using E-Gold for money laundering and to anonymously bank funds to finance their operations. Between 2003 and 2005, the FBI and the Secret Service used E-Gold to arraign a number of high-profile financial criminals. Jackson collaborated with the FBI until his own arrest in 2007, on federal charges of money laundering, conspiracy and operating an unlicensed money transmitting business. [15]

> *“Jackson’s radical dream, his goal of upsetting the economic status quo and overturning the government’s monopoly on money, is what really got E-Gold targeted.” — Richard Timberlake* [15]

In November 2008, less that one month after Satoshi Nakamoto introduced bitcoin to the cyperhpunk community, Douglas Jackson was sentenced to “36 months of supervised released — including six months of house arrest and electronic monitoring, and 300 hours of community service,” and handed strict guidelines requiring E-Gold to adhere to all regulations for money transmitters should it ever re-launch. [15]

It took E-Gold most of a decade to gather enough traction to earn the attention of federal regulators. Bitcoin’s fortunes turned when, after five years of relative anonymity, the US government once again turned its eye to the emerging cryptocurrency markets.

BITCOIN GOES TO THE HILL

On paper, Bitcoin should have shared E-Gold’s fate. Like E-Gold, Bitcoin was the passion-project of a fervent anti-bank idealist. Like E-Gold, Bitcoin developers spent much of its early life shoring up vulnerabilities and fixing glitches. And, as an anonymous, international, digital currency, bitcoin quickly became the coin of choice for criminals and black market traders.

But in U.S. Sentate hearings on the future of cryptocurrencies held in late 2013, testimony from financial regulators, law enforcement and federal officials signalled a surprising new openness to digital currencies.

Autumn 2013 had been a particularly fraught season for Bitcoin. In October, the FBI seized over 170 thousand bitcoin when they shut down the infamous Silk Road digital black market. That same fall, hackers forced two bitcoin exchanges, in Australia and Hong Kong, to shutter their stores. [16]

The two Senate hearings scheduled for November 18th (the US Senate Committee on Homeland Security and Governmental Affairs) and November 19th (the US Senate Committee on Banking, Housing and Urban Affairs), should have been cause for concern among bitcoin investors. But rather than call for the shuttering of the platform, this time government officials offered a cautiously positive outlook.

Jennifer Shasky Calvery, the director of the Financial Crimes Enforcement Network (FinCEN), chose her words carefully. “Digital currencies could be used for money laundering, but … this is no different from other financial instruments,” she said. Her measured testimony was a significant about-face from the federal ruling against Jackson six years earlier.

Ernie Allen, president of the International Centre for Missing and Exploited Children, suggested there was “broad-based agreement on its potential for social good.” Even the Chairman of the Federal Reserve, Ben Bernanke, offered that digital currencies “may hold long-term promise.” [17]

> *“[Digital currencies] may hold long-term promise.” - Chairman of the Federal Reserve Ben Bernanke, November 2013* [17]

The gulf between the technologists and the policymakers on capitol hill had narrowed, and government regulators, who for decades had monitored the growth of the Internet from the sidelines, were now signalling an embrace the technology for its potential in service to the public good.

Earlier that year, FinCEN, which is a division of the United States Department of the Treasury, issued the first significant guidance for persons creating, obtaining, exchanging, accepting and transmitting digital currencies. The document, which clearly defines the roles of the user, exchanger and administrator of digital currencies and the financial reporting requirements for each, paved the way for open discussions on how best to regulate bitcoin. [18]

With the cautious blessing of the US government, bitcoin was poised to enter the mainstream. Now only one roadblock remained: the banks.

The major banks and financial institutions followed bitcoin’s emergence with wary skepticism. Bitcoin’s decentralised exchange and stateless currency was a direct challenge to the traditional banking model. And the Bitcoin market was notoriously volatile; bitcoin could fluctuate in value by as much as 50,000% in a single day. Investors were understandably wary.

Still, Bitcoin had a solution to a problem that had been dogging banks and exchanges for years. International trades can take up to three days to settle on a public market: Bitcoin trades were clearing in a matter of minutes.

The banks wanted Bitcoin’s technology to improve their own processes. Meanwhile Bitcoin activists needed a signal from the banks that would gain Bitcoin the legitimacy and trust it needed to smooth its volatile exchange.

Soon, major global financial and technology institutions were toying with Bitcoin and examining the mechanisms that allowed the distributed financial network to operate as it did.

And it was in underlying logic of Bitcoin — the Blockchain — that banks, governments, and start-ups saw the true potential for a digital re-awakening.

4. UNDER THE HOOD

The mining and exchange of a cryptocoin works like this:

Step 1: Mining.

Assuming you don't have access to a faucet, or USD $4,000 to buy a bitcoin today, your participation in the exchange starts with "mining" bitcoin, as if you were mining for gold to take with you on a shopping trip.

Bitcoin is mined exactly as described by Wei Dai in 1998. Once your computer is connected to the bitcoin network through a bitcoin wallet, you can start mining. Mining happens any time a bitcoin transaction is requested on your network. In order to complete the transaction, a unique hash needs to be assigned to each request. To create that hash, every computer connected to the network races to solve a short math problem. The first computer to solve the problem - which generates the unique hash - receives an amount of bitcoin proportional to the complexity of the problem. The harder the problem is to solve, the more bitcoin you get.

Step 2: Setting up your wallet.

Now that you have some bitcoin, you probably want to spend it on something. First, you need to set up your wallet. Your wallet is a unique ledger assigned to you and protected through a public key infrastructure to keep your identity anonymous. The ledger tracks how much bitcoin you, and everyone else on your network, has to spend, by recording every transaction that has ever made. Functionally it is similar to the ledger of an old chequebook, except that it is readable by everyone on the network.

Step 3: Requesting a transaction.

With your wallet full of bitcoin, you're now ready to spend. Every exchange of bitcoin begins with a transaction request. When you request a transaction, a new "block" is created (like a new row in your chequebook) that contains all of the details of the transaction. Just like when you were mining for bitcoins, your block is assigned a unique hash.

Step 4: Verifying a transaction.

Once your block is created, each participant in the network verifies that all of the details for the transaction are correct. This is done by comparing the hashes of all of the previous transactions on the ledger (for example, when you first deposited money in your wallet).

This is the step that ensures you have enough bitcoin to complete the transaction, and that the party you are transferring funds to is able to receive them.

Step 5: Performing the transaction.

Once every computer in the network verifies the transaction, it is cleared to proceed. The funds change accounts, and the public ledger is updated accordingly.

Step 6: Storing the transaction data.

When you began you transaction request, you created a new block that stored all of the details of the transaction. As soon as your transaction is completed, that block gets added to the public ledger. That ledger is viewable by everyone in the network, and it is made up of all of the blocks of every transaction that ever happened on that network.

Because each block is linked to a unique hash, the ledger cannot be altered: if someone were to go in an try to change the details of a past transaction, the hash changes (because the data changes), and as a result, that block and all following blocks become invalid.

In this way, the exchange network is not only anonymous (using public key infrastructure) and decentralised (each participant in the network verifies each transaction), it is also tamper-proof.

This public ledger of connected blocks containing every transaction details is called the *Blockchain*, and it is the undergirding technology on which the Bitcoin system operates.

BEYOND BITCOIN

When the banks finally lifted the hood on Bitcoin, they discovered a powerful new protocol that could fundamentally transform how their institutions utilised the Internet for transactions.

Blockchain adds an extra layer of security for all participants in an ecosystem. Rather than rely on one centralised repository, Blockchain's decentralised model distributes decision-making power across a wide network of connected machines. To launch an attack, a malicious actor would need to divide his attention to overwhelm 51% of the network's distributed nodes, rather than focusing his efforts on a single main gate.

Blockchain's distributed ledger also enhances trust among participants on the network, which could include other banking institutions or customers themselves. Blockchain's hash protocol ensures that no record that has been stored on its ledger can be altered. Changing any data on the ledger would result in a new hash being created, which would invalidate the entire chain after the record in question. With an unalterable ledger, all participants in the network can be sure that the each transaction has proceeded exactly and only as recorded.

Because the Blockchain ledger stores all historical transaction data on a distributed network, the requirements to complete a transaction can be verified near-instantly. If Bill previously gave Sue $5, and now Sue wants to give $3 to Evan, Evan's and Sue's banks don't need to each independently go and check if Sue has $3 to give: as soon an Sue begins the transfer request, all of the parties on the network verify that Sue is able to send the money (and that Evan is able to receive it), by checking the Blockchain ledger. As soon as the request is verified, the value changes hands.

Using the Blockchain, banks could cut trade processing times from 3 days to 3 minutes or less. Once they understood what the Blockchain could do, the banking world sat up and began to take notice.

In March 2015, Nasdaq OSX, which oversees the Nasdaq stock exchanges, announced that it would begin testing a system that used bitcoin's Blockchain to oversee stock trades on the Nasdaq

Private Market, a separate market for private companies. By managing pre-IPO trades on the Blockchain, CEO's would be able to see in an instant who is buying and trading their stock. Before Nasdaq's pilot, pre-IPO companies were still tracking this kind of data on Excel spreadsheets. [19]

Nasdaq's move highlighted a growing interest in the Blockchain from the banking and technology sector. By the end of the year, over a half dozen financial and tech industry heavyweights — IBM, Cisco, the London Stock Exchange and J.P. Morgan among them — were experimenting with building their own Blockchains. [20]

> *"Bitcoin is like MySpace... it is paving the way for the Facebook or Twitter of Blockchain" — James Angel [19]*

Bitcoin's Blockchain is revolutionary, but it is also imperfect. James Angel, a professor of finance at Georgetown University, compares Bitcoin to MySpace. While bitcoin as a currency is deeply flawed, according to Angel, its underlying technology can be adapted to fundamental change how the financial sector. Bitcoin's Blockchain set the ball rolling, but it is more likely that another platform will emerge as the true giant.

Inspired by the Bitcoin Blockchain, IBM and Digital Asset Holders — called DAH for short, a start-up founded by a former JP Morgan executive — began work on their own Blockchain as part of the Open Ledger Project, supported by Linux. They dubbed their blockchain "Hyperledger." [20]

In keeping with the Linux ethos, Hyperledger is open source: although IBM has contributed the bulk of the code for the blockchain ledger, it is freely open and editable to others. Still more important for the future of blockchain, Hyperledger is also a distributed ledger and machines from many different organisations can participate in the network. As Marley Gray of Microsoft puts it, "Blockchain is essentially worthless within a single organisation. You have to have parties that are not yourself." [20]

> *"Blockchain is essentially worthless within a single organisation." — Marley Gray, Microsoft [20]*

By the close of 2015, with blockchain being embraced by governments, banks and the technology industry, it became clear that Bitcoin was just the first use case of a technology that held the potential to radically transform the Internet.

SMART CONTRACTS

As interest in blockchain grew, developers began exploring the system's potential beyond financial transactions.

Although initially designed for monetary exchanges, it quickly became clear that the technology could be used to oversee the exchange of any contract of record. The title deed of a new home, the sale of a used car, the execution of a will, a driver's license — even a ballot vote.

Not only can a blockchain record the exchange of these contracts in an indelible ledger, it can, through a decentralised network, automatically execute contracts and eliminate the need of the middleman.

Take for example the purchase of a new home:

In most jurisdictions, finding your “dream home,” though you might search for months, only gets you to the starting line. Most buyers will take out a mortgage, which means you will need to have your mortgage loan pre-approved from the bank before making an offer, and that bank will require a credit score from a 3rd party credit-rating firm. You will likely be closing with a real estate broker, not the current home owner, so once an offer is made the validation process will proceed in duplicate, with the brokers and bankers on each side of the transaction filing forms and reports. And there are any number of inspections that you, as the new owner, have the right to request. These inspections will need to be approved, conducted, and recorded. When you finally reach the settlement stage, your local government will step in to record transition of ownership. Then begins the process of registering for various utilities, phone lines, Internet, cable, updating your address with the postal service, updating your voting address and updating your address for food delivery apps.

A real estate application on blockchain, utilising self-executing smart contracts, can condense this process to just a handful of steps, with banks, brokers and the local government participating on a decentralised blockchain network with a distributed ledger.

ETHEREUM AND THE WORLD COMPUTER

Smart Contracts are open ended; almost anything that can be transacted can be represented by Smart Contract. The closest parallel to a Smart Contract is a website. Websites are used for the exchange of information, and all website developers follow a certain protocol when programming their sites. But the actual information on the site is infinitely variable.

Whereas Bitcoin restricted itself to one type of Smart Contract, for the purpose of the exchange of bitcoins, the team behind Ethereum saw an opportunity to develop a blockchain that would support any potential transaction on a peer network. The language on which Ethereum is built is Turing-complete — meaning Ethereum capable of doing just about anything that can be expressed in a computer program. And because Ethereum rests on a blockchain, the history of every transaction is stored on an enormous, distributed computer: the Ethereum Virtual Machine (EVM). [21] [22]

> *“Ethereum is literally a computer that spans the entire world.”* — Haseeb Qureshi *[23]*

Ethereum has opened ignited a surge of interest in Smart Contracts, and the supporting ecosystem of tools required to build Smart Contracts on the EVM. Ethereum’s value has skyrocketed over the last 6 months. [24]

Driven by Ethereum, the blockchain ecosystem is witnessing a transformation that has the potential to eclipse what happened when the launch of Mosaic in 1993 sparked an explosion of interest in the World Wide Web, which grew from 26 websites to 1 million in the space of one year. [24]

THE INTERNET OF TRANSACTIONS

Blockchain is not a “new” Internet, nor is it trying to “replace” the Internet. By deploying a decentralised, hash-based protocol with an indelible ledger, blockchain is offering a powerful alternative to the Internet processes that have become routine to us since the widespread adoption of the World Wide Web.

By combining centralised servers capable of storing massive amounts of data with a graphical user interface that allowed humans to easily read and interact with that data, the World Wide Web ushered in an Internet of Information that fundamentally changed the way we access and store information.

Blockchain has the potential to effect the same revolution, but for transactions. If its potential is realised correctly, we could trade stocks, buy homes, and play fantasy football on the blockchain with the same security and ease with which we watch cat videos on YouTube.

5. THE AGE OF BLOCKCHAIN

The dream of a self-regulated, secure, decentralised network sparked as an idea in the 1980's, grew into a quest in the 90's, was finally realised in the late 2000's, and truly came into its own by 2016.

Bitcoin is no longer the only blockchain platform with wide-scale adoption. A comprehensive blockchain ecosystem has emerged astonishing momentum in the past five years. According to Blockchain specialist and VC Josh Nassbaum, "the speed of blockchain's growth is the fastest that any area of technology has taken off." [25]

THE BLOCKCHAIN ECOSYSTEM

To illustrate the scale of blockchain's impact, Nassbaum has identified a Blockchain Project Ecosystem spanning eight major categories and 43 sub-categories that captures the depth and breadth of the blockchain ecosystem. [25]

Currencies.

Bitcoin was the first cryptocurrency to use the blockchain. Since then, many more start-ups have entered this category to improve on the initial work of Bitcoin, or to create tailored products for specific use cases. Companies active in the blockchain Currency category can be roughly segregated in to three sub-groups: Base Layer Protocols, for projects such as Bitcoin that codify currency exchange protocols; Payments, for projects like Ripple, a currency exchange and remittance network, that focus on the transfer of funds; and Privacy, for projects that are providing anonymous, untraceable cryptocurrencies. [25]

Developer Tools.

Blockchain was introduced on the back of Bitcoin, but since then a diverse category of Developer Tools has emerged, populated by companies and consortiums who are building and refining the tools required to actually deliver game-changing blockchain applications. As Nassbaum puts it, "In order for many of the blockchain use cases we've been promised to come to fruition, such as fully decentralized autonomous organizations or a Facebook alternative where users have control of their own data, foundational, scalable infrastructure needs to grow and mature. Many of these projects aim at doing just that." [25]

Ethereum and Hyperledger lead the Smart Contract sub-group, and are the tip of the iceberg for a deep and entwined category, with each sub-group enhancing or supporting the other. Other Developer Tool sub-groups that Nassbaum identifies include: Scaling, Oracles, Security, Legal, Interoperability, Privacy and DAGs (a variation on the technology that uses a "tangle" or "block-braid" rather than a blockchain). [25]

Fintech.

Fintech on blockchain is the natural outgrowth of a number systems, each with their own currencies, that are required to work together. The projects under this category serve to facilitate the exchange, lending and investment of different cryptocurrencies. Sub-groups under the Fintech category include: trading and decentralised exchange; insurance; lending and funds or investment management. [25]

The insurance and lending sub-group are particularly interesting, as Nassbaum points out, for their scalability. Blockchain networks enable greater differentiation of individual risk potentials, leading to cost savings, that should in theory pass on to customer. And, since blockchain ledgers are unalterable, users can be confident their individual histories haven't been tampered with. [25]

Sovereignty.

Projects in the Sovereignty category are turning to blockchain to address privacy concerns for highly sensitive data on the cloud. Centralised servers that store user data are prime targets for hackers. Blockchain's distributed database provides a more secure alternative for some data sets. (The Blockchain is not mature enough to handle such projects at scale yet, but is very effective at securing data on a smaller scale). Sovereignty projects can be clustered into seven sub-groups, each addressing a specific data type: user-controlled; governance; VPN; communication; identity; security and stablecoins. [25]

Value Exchange

While the Currency and Fintech categories profile blockchain applications for currency exchanges, the technology is able to support wide range of transactions between people or parties, without the need for a relationship or trust between those parties. Blockchain facilitates the exchange of both fungible and non-fungible goods, and this category identifies projects in both spaces. [25]

Blockchain is being deployed for the exchange of non-fungible value with projects in the content monetisation, data, marketplaces and social sub-groups. Blockchain projects for the exchange of fungible goods can be classified under six sub-groups: file storage, computation, mesh networking, energy and video. [25]

Shared Data

In traditional shared data exchanges, the aggregator of the data is the one who benefits the most, and rarely passes that value on to the individuals and companies who own the data. Shared data is also difficult to aggregate and verify between multiple parties, creating a significant barrier to entry where only the biggest players can capitalise on the benefits. [25]

Blockchain lowers the barrier to entry by giving autonomy to data owners that allows them to "take their data with them," as they engage with other parties for whom their data may be useful. For example, a seller who as built up a reputation for quality over many years in a single market, can open business in a new market and carry his reputation with him on an immutable blockchain. Blockchain also allows for the democratisation of data-collection, enabling a wide network of participants to add, annotate and build insights from data. Contributors whose data has proven the most useful can be incentivised through tokens which increase in value as the organisation grows. [25]

Projects currently underway to leverage blockchain technology for shared data are divisible into 5 sub-groups: Internet of Things, supply chain and logistics, attribution, reputation, and content curation. [25]

Authenticity

Blockchain's verification protocols and indelible ledger are a cryptographic means of ensuring that a datum or product (like a movie ticket) is what it says it is and will remain that way for an infinitely long time. Products that are susceptible to fraud can benefit from the Blockchain to guarantee their integrity. Recent projects in the Authenticity category have focused on two sub-groups: data and ticketing. [25]

From the speed with with the blockchain ecosystem has grown, and the scope that it already spans, it is clear that this is a technology that, in some form, will soon have a tangible impact on how we interact with and transact data on the Internet. [25]

The value exchange use cases alone are an invitation to image just what is possible when we reimagine every transaction as an opportunity to introduce the blockchain into our daily lives. Specific use cases from banks, Governments, and cutting-edge start-ups show what changes are already taking shape. [25]

THE BANKS

Since Nasdaq OSX's first overtures on bitcoin's blockchain in 2015, dozens of financial institutions have begun experimenting with the emerging technology.

> *"66% of banks will have commercial-scale Blockchain operations by 2020" - IBM*

In 2016, IBM issued a report predicting that 15% of global banks would implement Blockchain by the end of the next year (2017), and that 66% of banks would have Blockchain operations in commercial production and at scale by 2020. [26]

Bond Transactions (R3, 2016).

In September 2016, the US-based fintech start-up R3 announced it had successfully completed a pilot for bond transactions on blockchain. The platform deployed smart contracts to enable the trading, matching and settlement of US Treasuring Bonds, as well as automated coupon payments and redemption.

The project utilised Intel's blockchain technology and was carried out in partnership with 8 banks, including HSBC and State Street, with support from the US Treasury. [27]

Utility Settlement Coin (UBS, 2017).

Led by UBS and supported by the UK-based blockchain company Clearmatics, a growing network of European banks have teamed up to roll out a "Utility Settlement Coin"(USC), a type of crypto-coin that is convertible at parity with the currency denomination of any bank deposit. The system, which aims to be operational by 2018, would facilitate the near-instant digital exchange of fiat currencies, with the USC functioning as a digital equaliser. Spending a USC would be the same as spending the real currency it is paired with. [28]

Cheque Chain (Emirates NBD, 2017).

Emirates National Bank of Dubai (Emirates NBD), a leading banking group in the Middle East region, announced a unique blockchain pilot in the spring of 2017. As a developing region, many of the bank's customers still prefer to transact via cheque. Rather than enforce a new consumer behaviour, Emirates NBD is piloting an integration for blockchain that allows customers to continue to write cheques, but enables the bank to instantly store the cheque data on the Blockchain as soon as the cheque is deposited. Once a digital copy of the cheque is made — usually after it is deposited into a cheque deposit machine (CDM) — the bank reads the details of the cheque and stores it on the "Cheque Chain," creating an indelible record of the transaction. [29]

BOUNDARY-CROSSING START-UPS

The iconoclastic nature of bitcoin drew start-ups in droves. Much of the infrastructure around bitcoin today — including dedicated trading websites, international event organisations, and print publications, not to mention the volume programmers rolling our new applications — did not exist before 2013.

Between 2012 and 2013, venture funding of bitcoin and blockchain start-ups surged from $2.13 million to $95.05 million. Over the next two years, funding grew an eye-popping 726% — hitting $690.18 million by the end of 2016. [30]

As the technology matures, start-ups are tackling more than just financial applications, as Nassbaum's Blockchain Ecosystem demonstrates. Shipping and logistics, Art and even HR are among the industries about to encounter blockchain solutions.

Provenance (Shipping, Retail, Art).

One feature of blockchain, its ability to maintain indelible records, has proven itself particularly relevant to merchants concerned with validating the origin of the products they buy and sell. The fight against counterfeit products consumes the entire value chain, from brands and buyers to port authorities and customs officials. Provenance, a start-up based out of South East Asia, has built a blockchain application to leverage the indelible ledger to validate product "proof of existence," and track the history and origin of goods.

The start-up has proven particularly boon to luxury brands, who are turning to Provenance to help remove counterfeit goods from the market. Provenance is proving the applicability of blockchain technology for wide-ranging, non-financial implementations.

Industry watchers are keen to see Provenance take on the Art world as well, where advancements in technology have led to a surge of counterfeits, creating a pressing need to tell truth from fiction. [31]

Educhain (Education).

In the Education space degree or certification issuance and attestation is a surprisingly time consuming process requiring multi-step approvals and signatures. Smart Contracts on the blockchain present an opportunity to automate the issuance of certificates attest achievements through its distributed ledger.

Educhain, a Canadian start-up that recently won second place in the Dubai Blockchain Challenge, is providing a solution for educators, students and governments to remove current roadblocks surrounding the issuance of certificates, such as diplomas. By utilising the blockchain, Educhain is improving student experiences while reliably verifying the authenticity of a certificate for academic institutions and governments. [32]

Colony (Organisation Management).

Perhaps the most profound applications of blockchain, however, will come from challenging the very nature of how we work. To explore what work will look like when the potential blockchain is realised, concept artist Jack du Rose designed a though-experiment that utilises both blockchain and artificial intelligence to manage a decentralised, autonomous organisation of real human beings.

The concept, called Colony, examines what happens when humans are removed from organisation management, and instead left to focus on creative endeavors. By deploying AI to manage tasks and initiate smart contracts, Colony creates a space for people to come together to work and create - on time and on budget - without pesky humans messing up the process.

Colony is a perfect storm of emerging technology and a thought-provoking look at what blockchain might accomplish in society when we realised the potential of the Internet of Transactions. [31]

BOLD GOVERNMENTS

Government's interest in blockchain, which could be surprising given the technology's anti-establishment origins, seems to be the fulfilment of a prediction by Brad Peterson, who led the blockchain project at Nasdaq OSX. While developed markets with centuries of financial inertia to overcome may be slow to adopt the Blockchain, he said, countries in the developing world, unhindered by institutional legacies, could "jump straight to the Blockchain."

By moving certain government functions to the blockchain, where all transactions are publicly recorded and validated, governments have been able to weed out the corrosive influence of corruption and increase public trust. For large bureaucracies, blockchain is also proving efficient at streamlining processes and removing the paperwork burden that frustrates citizens and drains government resources.

> *In March 2017, there are over 100 Blockchain pilots in progress, planned or announced by more than 30 government agencies on six continents.*

From effectively zero in 2013 to over two dozen today, government agencies across the globe are actively pursuing Blockchain implementations to introduce greater security, efficiency and speed into all manner of government transactions. According to a recent report from Deloitte, there are as many as 64 government Blockchain pilots in progress across the globe, and another 50 pilots announced and planned. [33]

Dubai, United Arab Emirates.

Blockchain has proven particularly attractive to younger countries without a backlog of bureaucratic precedents to overcome. No where else is this trend more apparent than in the United Arab Emirates, where the federal government and the local government of the Emirate of Dubai have embraced the technology whole heartedly.

The Dubai Future Foundation, a government think-tank charged with imaging and creating the future of the city 10 to 50 years ahead of schedule, was instrumental in the establishment of the Global Blockchain Council in early 2016. The Council is made up of heavy-hitters from the technology sector, the banks, and major industry players from a wide swath of backgrounds, including Emirates Airlines and Nasdaq Dubai. It was established to exchange knowledge on blockchain pilot trends and policy development and service as a catalyst to blockchain development in the region.

Within nine months, Dubai announced its own Blockchain strategy, led by the Dubai Future Foundation and the Smart Dubai Office, with a vision to bring 100% of all applicable government transactions onto the Blockchain by 2020. Dubai's blockchain project will be successful when, in the words of the Crown Prince of Dubai, Sheikh Hamdan bin Mohammed, "In 2020, the Dubai government will celebrate its last paper transaction."

> *"In 2020, the Dubai government will celebrate its last paper transaction." His Highness Sheikh Hamdan bin Mohammed, Crown Prince of Dubai*

According to some back-of-the-envelope calculations, Dubai stands to save up to 5.5 billion AED every year by moving document processing to the blockchain by 2020. That is the equivalent of delivering the cost of one Burj Khalifa — the world's tallest building, located in downtown Dubai — in savings to the economy, year on year.

To transform its vision into reality, Dubai is pursuing blockchain implementations across all sectors. The government operates three accelerator programs — Dubai Future Accelerators, the Dubai Blockchain Challenge, and the Dubai Smart City Accelerator — that are bringing international start-ups to Dubai to test and run blockchain pilots from and for the city. [34]

As of March 2017, the United Arab Emirates had announced 7 blockchain projects, the most in the developing world. [33]

By October 2017, one year after the launch of its strategy, Dubai showcased its first blockchain pilot, an application to streamline land title transfers, at the annual GITEX exhibition. The system, which was developed in partnership with Smart Dubai, who is working with IBM and Consensys to implement their blockchain projects, uses blockchain to provide a secure database that records all real estate contracts, including lease registrations, and links these with the local utility authority, the telecommunications system, and various property related bills. The platform, which is also linked to residents' Emirates ID and residency visas, enables tenants to complete transactions electronically, and from anywhere in the world. [35]

Ghana.

Although a young nation, the United Arab Emirates has consistently demonstrated an openness and commitment to innovation that is on par with the United States, the UK and Singapore. But the benefits of Blockchain extend beyond countries with well established technology infrastructure or a robust knowledge economy.

As much as 90% of agricultural lands in Ghana are undocumented and unregistered. The Land Commission of Ghana, which is responsible for regulating land ownership and titles, is widely viewed as ineffective, and land disputes are common place among all participants in Ghana's real estate market, from mining organisations and real estate developers to local subsistence farmers.

Bitland, a non-profit NGO headquartered in Ghana, has turned to blockchain to build a trusted and indelible record of title statuses for unprotected land owners. Bitland is creating a redundant record of land ownership, providing citizens and farmers, as well as larger corporations, with a trusted certificate validating their possession, should it be required in the event of a dispute.

Bitland is helping Ghana leap-frog decades of technology infrastructure development and entrenched bureaucratic processes to deliver value, security and speed to its citizens with the Blockchain.

Inspired by the early success of its initiative in Ghana, Bitland is now building its own cryptotoken wallet and Land Registry Blockchain to extend blockchain technology at scale to all African nations. [36]

Estonia.

Blockchain technology adapted at scale by governments can have a profound impact on citizen's daily lives, both within and beyond the public sphere. In Estonia, an early champion of the technology, citizens can access health records stored on the blockchain to gain visibility on who else has seen or accessed with medical history. [37]

Estonia made waves a few years ago by rolling out an e-Citizenship program for all Estonian citizens (and anyone else in the world who was interested in joining the former Soviet-bloc country's digital experiment). Estonian's e-citizen IDs were secured with Public Key Infrastructure, a system for double-blinding user identities that it is integral to the blockchain: Public Key Infrastructure enables anonymous participation in a network.

As blockchain technology emerged, Estonia moved quickly to integrate their existing infrastructure with the blockchain, becoming the first nation to to implement blockchain at a country level. Estonia designed the KSI blockchain to make sure networks, systems and data are free of compromise, while retaining 100% data privacy.

Estonia's KSI Blockchain is now available in 180 countries.[38]

6. HTML FOR THE 21ST CENTURY

Interest in the blockchain has continued to accelerate dramatically in recent months. Major technology trade shows, including the Consumer Electronics Show in Las Vegas and the Smart City Expo and World Congress in Barcelona, featured panels on blockchain for the first time in 2017.

Blockchain venture capital investment reached $107 million by Q1 2017. The aggregate cryptocurrency market cap reached an all-time high of $25 billion in Q1 2017. [39]

In 2017, industry heavyweights completed a significant pivot towards blockchain. PwC (Vulcan Blockchain), Microsoft (Project Bletchley), JP Morgan (Juno and Quarom), IBM (Hyperledger and IBM Blockchain), Accenture and Deloitte entered into the Blockchain market with meaningful stand-alone project this year. [40]

Blockchain has reached the peak of the Garnter hype-cycle. [41]

With interest in Blockchain at an all-time high, but real-world successes still scarce, the technology has a long road ahead before the public can reap the benefits of widespread adoption envisioned by Blockchain evangelists.

THE DAO, PARITY AND THE RISKS OF BEING HUMAN

A favourite line of Blockchain evangelists is that the platform is "tamper-proof." Early adopters of Blockchain have praised the platform as "the most secure solution" for managing vast amounts of data. Others have pointed the use of public and private key infrastructure as a meaningful solution to secure individual's data privacy.

While Blockchain is capable of doing all these things, blockchain is not a fool-proof system, and as blockchain gains more attention, the rate of hacking attempts will also increase.

Two landmark attacks again the Ethereum network serve as a apt reminder that the blockchain, in spite of its massive decentralised databases and indelible ledger, is ultimately a human endeavour and not infallible.

Ethereum is a popular digital currency that uses the Blockchain to record transactions, described in smart contracts, in a giant decentralised network. Smart contracts on Ethereum function in a similar manner to traditional computer programs, except they follow the rules of the blockchain.

One of these programs was The DAO, or Decentralised Autonomous Organisation. The DAO facilitated venture funding for pre-approved companies. These companies could submit proposals for funding to The DAO, and investors would vote on whether or not to approve the request. Once 20% of investors approved the request, funds would be transferred automatically to the company's wallet. In case an investor wanted, for whatever reason, to leave the organisation, the program's developers built in a "splitting function" to allow investors to withdraw from The DAO and regain the capital they had leveraged when signing up: the DAO raised an equivalent to $150 million in its first month. [43]

The DAO was hacked less than two months after it was formed. Hackers exploited a bug in the "splitting function" to drain over $70 million in funds from The DAO in a matter of hours. The Ethereum community was able to stop the attack by re-writing the rules of the platform to permit a transaction to be reversed. (Part of 'indelible' is 'irrevsrervible'). [43]

In a separate attack, hackers were able to withdraw $30 million from Ethereum users by exploiting an error in the code for a digital wallet in the Parity smart contract that allowed hackers to re-program wallets in their name, then simply withdraw all of the funds within that wallet. The attack was stopped, but the money could not be returned. [23]

Neither attacks were caused by flaws in Ethereum or in the blockchain. Mistakes were made in the coding for a particular program, and maliciously exploited. Security is hard. Attackers only have to be successful once; defenders have be be successful every time, against every possible attack. And on a distributed network like Blockchain, the risk is even higher: an attack on one ledger is an attack on every ledger. [23]

So, what can we do?

Being indelible means that, once a piece of blockchain code it out there, it is in the world to stay, along with any mistakes, bugs or vulnerabilities built into it. Just as blockchain smart contracts have introduced cutting-edge cryptography, blockchain programmers will need to introduce cutting-edge programming languages that are as resistant as humanly possible to error and attack. [23]

Blockchain programmers are among the smartest and most dedicated in the world, but there is still a lot to do if this technology will truly transform how we transact on the Internet in the coming future.

BLOCKCHAIN FOR EVERY ORGANISATION

If all goes according to plan — and there's no reason to expect it won't — blockchain will be embedded within nearly every organisation on the planet in the next decade. [45]

Business, by definition, is the exchange of goods of services in fulfilment of a contract. Blockchain can regulate every step of that equation. Every step of a business life-cycle, in any sector, can be enhanced by smart contracts on blockchain.

Smart contracts in the music industry can be deployed by artists to ensure their IP is protected, and to make sure they receive payment for the work whenever an album or song is downloaded. The British recording artist Imogen Heap has emerged as a blockchain pioneer and evangelist, working to introduce the benefits of an indelible ledger and self-executing smart contracts to the music industry. [46]

Through smart contracts, musicians can automatically receive payments for a song and, as Heap has done, automatically share royalties with everyone who contributed to the making of the song.

Blockchain is also being explored as a legal and mutually remunerative reincarnation of Napster. Through its distributed network and ledger technology, blockchain can support an open, peer-to-peer music library that simultaneously allows fans access to all of their favourite music, and enables musicians to get paid for their work.

In the Art world, blockchain can be deployed to open a digital market for investors and artists, simultaneously assessing and validating the worth of an artwork, and recording the exchange of possession between artist and buyer. And as forgery techniques become even more advanced, blockchain networks can be deployed to verify an artwork's origins, helping would-be investors differentiate between an original Monet and an Artificial Intelligence copy.

Experts are also exploring use cases for blockchain in the more mundane field of Human Resources, where the Blockchain ledger could present a welcome alternative to the often time-consuming process of verifying references for new hires. With an employee's work record and referrals stored on a blockchain ledger, hiring managers can quickly asses a candidate's fit for a role. [45]

Self-executing contracts on the blockchain can also dramatically reduce payment turn-around times for client work. Companies in service, design and consulting fields who have entered into a smart contract with a client can receive payment for services within moments of the client signing a delivery note. Blockchain can transform a mind-bogglingly inefficient process, where payments take a *minimum* of 30 days, to payment within seconds. And, because the contract terms and transaction history are permanently stored on the blockchain, the audit trail is tamper-proof.

Businesses sizes should investigate the potential role of blockchain for their organisation, and be ready to embrace the technology as it matures. Mass adoption will come sooner than you think.

A CLOSING DOSE OF REALITY

The Internet existed for nearly a decade and a half before the World Wide Web was invented in 1989.

Like Blockchain, the Web itself remained staunchly the domain of academics, technology firms, computer geeks, and open-minded governments. Then, in 1992, the first multimedia graphic browser, Mosaic, blew the hinges off the door to the Internet. [47]

Within a year, the World Wide Web grew from 24 websites to over 1 million. Netscape launched in 1993. AOL rolled out its iconic CD-rom campaign in 1994. By 1995, 16 million people were using the Internet. By 2000, that number had soared to 361 million. Today, 3.8 billion people are online. [48]

The World Wide Web has become so ubiquitous that most people confuse the platform with the Internet itself.

Mosaic transformed the World Wide Web by making it visually appealing and easy to use for the masses, and in so doing rewrote how we live and interact with the world. Will Blockchain ever achieve the same degree of influence on our daily lives?

Today, the blockchain interface is still largely code-based. While governments, start-ups and banks have gotten involved, it is still in the domain of computer science experts, much like the early 1990s on the Internet before the World Wide Web took off.

Unless a new user-friendly experience for Blockchain emerges it is unlikely that the technology will ever reach such global prominence as the Web. Although the team behind Ethereum is trying, the platform's interface is still a nearly-entirely code based interaction. While Smart Contracts might eventually achieve a user interface more akin to a web page or mobile app, Blockchain itself will never attain the same level of visibility to the average user as the World Wide Web.

For all its acclaim, blockchain is a closer kin to html, the standard markup language for creating web pages and web applications. Most people recognise it, some use it, and a few know what it is truly capable of. And that is probably fine.

Whereas the value of the Web is understood through the opportunities it has created, the value of blockchain will be most strongly be felt through what is reduces in time, effort and resources. The challenge of the blockchain revolution is not: “What do we do with this thing?” but rather “What do we do with what this thing takes away?”

If payment schedules for creative agencies are reduced from 30 days to 0, what happens to the accountants?

If a musician can share new music directly with fans on a peer-to-peer Smart Contract, what will become of iTunes?

If Dubai does achieve 5.5Bn AED savings per year, what will they do with that money?

These are the questions that society will need to tackle in the coming years.