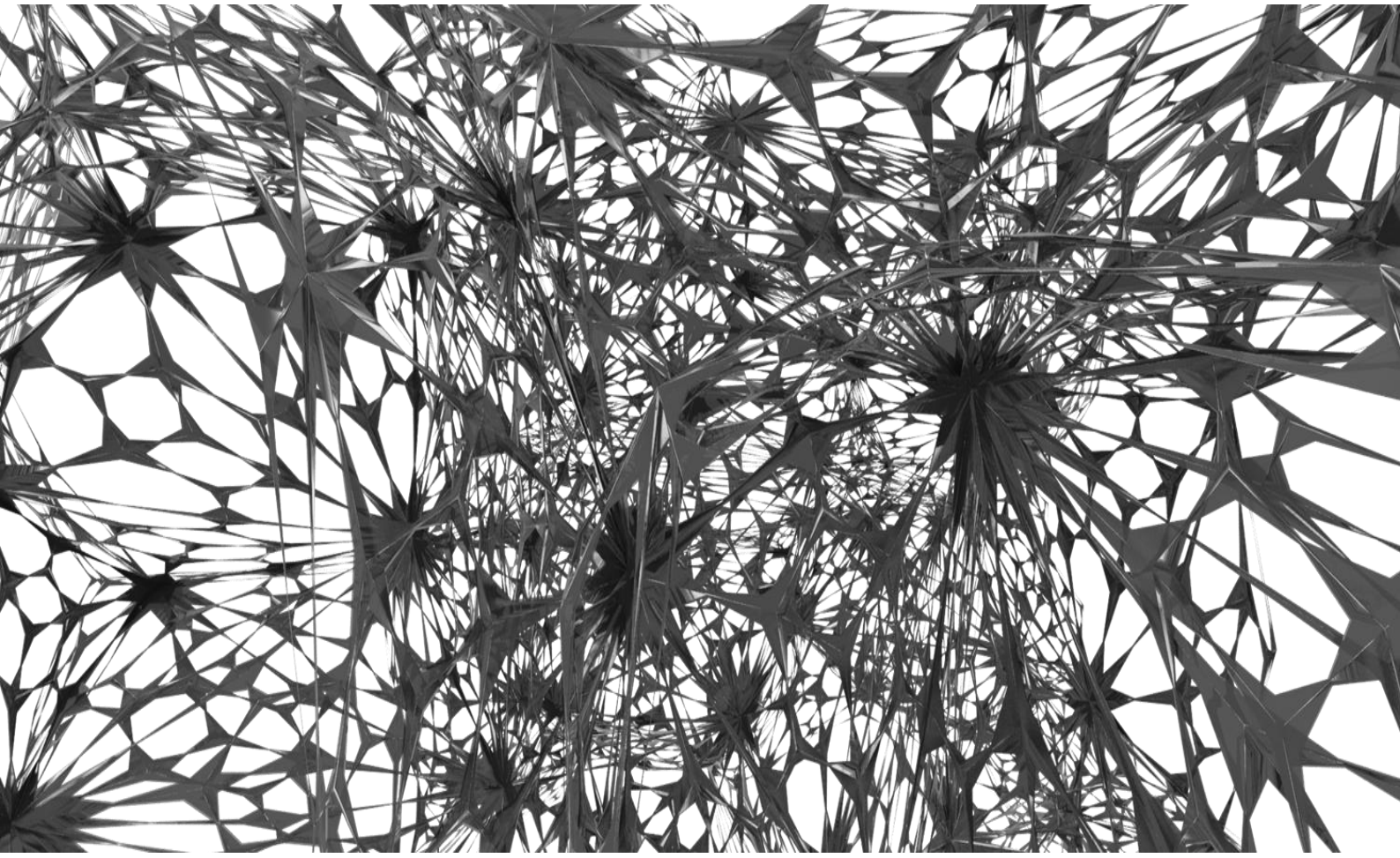
Chain Of A Lifetime:
How Blockchain Technology Might Transform Personal Insurance



December 2014

A Long Finance report prepared by Z/Yen Group

CHAIN OF A LIFETIME:

HOW BLOCKCHAIN TECHNOLOGY MIGHT TRANSFORM PERSONAL INSURANCE

Michael Mainelli and Chiara von Gunten

DECEMBER 2014

Z/Yen Group Limited
90 Basinghall Street,
London EC2V 5AY
United Kingdom

+44 (0)20 7562-9562 (telephone)
+44 (0)20 7628-5751 (facsimile)
hub@zyen.com (email)
www.zyen.com (web)

Cover image: adapted from **a complex network of rhizomes**
an image of the Institute for Advanced Architecture of Catalonia (www.iaac.net)
developed in the Masters in Advanced Architecture in 2013-14 by Boney Virendra Keriwala

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

Blockchain technology provides an electronic public transaction record of integrity without central authority. The transaction record is a ledger of all transactions that have taken place within a set protocol, recorded in a sophisticated, distributed data structure. The data structure is decentralised and shared by all nodes, i.e. computers, within the participating system or network. Cryptographic and problem-solving block validation prevents duplicate transactions, double-spending, and ensures ledger integrity. The blockchain does not require a central authority or trusted third party to coordinate interactions, validate transactions, or oversee behaviour. The blockchain can contain sets of documents and record assets. In short, a blockchain is a secure peer-to-peer ledger with storage, analogous to peer-to-peer music sharing systems such as Napster.

In January 2009 blockchain technology was first used publicly to help create Bitcoin, a cryptocurrency-based protocol. While Bitcoin is problematic both socially and economically, and there have been technical glitches with Bitcoin wallets, the blockchain technology has proven robust. In fact, as a demonstration of blockchain technology's robustness, Bitcoin has been superb, showing the technology to be proof against a wide range of attacks, from criminals to national security agencies.

Blockchain technology has wider applications than just Bitcoin or the other hundreds of cryptocurrencies using it. Blockchain technology can be applied in financial areas where a central, trusted third party has traditionally been used, trade reporting, depository receipts, escrow, trade finance, etc. Since 2009, blockchain applications that extend beyond currencies, such as smart contracts and decentralised autonomous organisations, have been developed and tested.

People use trusted third parties in many roles in finance, as custodians, as payment providers, as poolers of risk, i.e. insurers. Trusted third parties in finance provide four functions:

- validating the existence of something to be traded;
- preventing duplicate transactions, i.e. someone selling the same thing twice or 'double-spending';
- recording transactions in the event of dispute;
- acting as agents on behalf of associates or members.

If faith in the technology's integrity continues to grow, then blockchain technology might largely displace two roles of a trusted third party, i.e. preventing duplicate transactions and providing a verifiable public record of all transactions. Emerging applications, such as smart contracts and decentralised autonomous organisations, might in future also permit blockchains to act as automated agents.

This report explores the question "how might blockchain technology transform personal insurance?", along the way developing four themes that relate insurance and blockchain technology:

Figure 1 – Themes

Theme	Service
Identity	Authentication
Space	Transactions
Time	Debts
Mutuality	Communities

What if … you had a portable, secure, globally available store of personal data in a blockchain? You could have all of your health records or driving history available to share with trusted third parties at any time. You might hand over your health record to a new doctor or to obtain a life insurance quote, or share your driving history at an airport counter for a car rental insurance discount. Your personal data store might also have your biometric data, thus giving you the ability to prove your identity at any time.

Identity – blockchain technology and related applications could transform the way people manage identities and personal information. Blockchain-based identity schemes could empower people with personal data storage and management, permission frameworks for access by third parties such as insurance companies, and even distributed reputation ratings. Individuals would no longer need to trust centralised third parties to store or manage their information. Such applications could reduce identity and claim fraud, increase confidence in products, and lower rates thus increasing coverage. As blockchain technology expands the range of possible items that can be stored and recorded in a decentralised way, interesting applications could emerge in relation to accident or health data records, common data, and related notary functions. The concept of never losing data could materially alter the way society views identity, privacy, and security.

What if … the importance of regulatory boundaries diminished? With blockchain applications, insurance products could reach scale at both local and global levels. Further, insurance coverage could be adjusted across space almost instantaneously while catering to 'local' needs.

Space – blockchain technology has the potential to shape different interactions between individuals and places, further blurring the divide between local and global. Blockchains are distributed across computers, which are often spread across places. Blockchain applications allow us to exchange and transfer value and information across space. Blockchain technology and related applications can be global in scope and in scale while at the same time catering to the specific needs of individuals in set locations. This dual relationship with space could support the tailoring of insurance products by expanding the range of products across places and by enabling nearly instantaneous adjustments of insurance coverage and pricing across space (and time). Further, blockchain technology could transform insurance models, shifting from today's predominantly centralised and spatially anchored paradigm to new models of peer-to-peer and mutual insurance platforms where location becomes relatively less material as a selection criteria.

What if … there were no more disputes about the 'last' will and testament? When someone dies and the coroner verifies death and cause of death to their blockchain, then their last will and testament is released publicly, their health records are donated to medical research charities and their life insurance policy pays out automatically.

Time - Blockchain technology 'time stamps' interactions and records 'debt' over long period of times. Blockchain applications might affect our perception of time in two possibly contradictory ways. Blockchains could shorten time perception through the tailoring of insurance products across space (coverage) and time (event-specific insurance). Think of the collaborative economy models of Uber or Airbnb, perhaps specific coverage for the days a person uses their car as a taxi or their home as a hotel would be added to their normal motor or home policy. Simultaneously, blockchain might lengthen perceptions of time by introducing a sense of immutability as no one can walk away from their blockchain data, and transactions records cannot be altered or deleted.

What if … any group of people could create their own pooling system on the spot? These could be instant mini-insurers or mini-mutuals, a collaborative economy approach to insurance. An extensive Indian family might provide mutual health insurance to each other, backing it up with a combination of reciprocal arrangements with uncorrelated UK village health schemes and a standard international reinsurance product that a global reinsurer had developed for such family schemes. What if insurers never needed to fund risks? For example, people could more easily have adjustable payments pooled to reflect rising and falling risk levels. Unemployment insurance could be merged with educational loans and deals struck over a lifetime so that young people could be funded in education, insured against unemployment, yet simultaneously be extending part of their employment income to provide others with risk cover.

Mutuality – People's perception of risk is likely to be influenced by technological innovation and applications such as blockchains. Today's predominant model in the insurance industry is a fully-funded central body contracting with individuals. Blockchain applications could change the way insurers mutualise. If successful at scale, over time this could lead to new players entering the market and disintermediation of traditional insurance through the automation of certain insurance products, probably around well-known and common risks. Blockchain technology could empower people to manage (some of) their risk more directly, with peer-to-peer and mutual insurance platforms based on blockchains, perhaps only partially funded. Going back to the collaborative economies example (e.g. Uber, Airbnb) applied to insurance, in this case, insurers' role could shift over time towards expert advice provision and management of mutual pooling mechanisms, rather than directly absorbing risk. The technology could also support financial inclusion and new models of interactions between individuals and insurance providers, which could lead to additional benefits in terms of customer satisfaction, stability, confidence, transparency, and accountability.

Forecasting the adoption of new technology is fraught with peril, but a forward-looking report has to try. Most insurance companies do not yet seem ready to experiment with blockchain technology. They find it difficult enough to understand Bitcoin or cryptocurrencies. Non-insurers are more likely to be the first to create insurance or insurance-related applications. Blockchain applications in insurance are likely to start with digital identity systems and management of personal data.

Third-party identity provision seems to be maturing. There are several projects underway to provide 'open identity', e.g. OpenID Connect or the Estonian government's identity services for non-nationals or the Gov.uk Verify scheme, that give some indication of how this might evolve. Applications that collect, assess, and manage data as well as access to interconnecting devices at distance across the Internet of Things will create demand for better identity and advanced analytics. Down the line, novel products based on smart contracts seem most likely for new areas of insurance, (e.g. the collaborative economy insurance products) or policies covering new risks arising with the use of blockchain technology (e.g. digital asset protection), rather than displacing existing products. Finally, with more confidence gained from experience, traditional insurance models may be displaced.

At this stage, three areas deserve more attention by mainstream insurers. First, they could experiment by building 'private' blockchains, unconnected to the blockchain used by Bitcoin or others, using these pilots to discuss with clients and regulators how the future might work. Second, they need to explore how private blockchains might be maintained and paid for, experimenting with different protocols and economic structures. Third, they should critically examine not just their existing information technology architecture, but also their existing and future products, in order to see where products or risk management could be improved by using blockchain technology and related applications. Every personal insurer's core computer system is, at heart, a big, centralised transaction ledger. At the very least, blockchains deserve to be evaluated technologically by insurers, as a potential replacement for today's central database model.

Blockchain technology is at an early stage of development, with many possibilities, and innumerable unknowns. Private sector interest in commercial applications is increasing rapidly. Governments seem to favour a 'wait and see' approach, leaving it to the private sector to experiment with the blockchain, though several governments are encouraging experimentation. Blockchain technology may not be complicated for cryptographic experts and computer scientists to use but remains complex to non-expert audiences. Awareness is rising rapidly, but education will be needed. Numerous initiatives that seek to reduce blockchain's technical complexity might help it become widespread. Blockchain technology is not a solution, rather part of the answer to what insurance may look like in future.

This report would be written very differently only months from now…

2 INTRODUCTION

2.1 Background

Blockchain technology was first introduced in 2009 with Bitcoin, a cryptocurrency-based distributed payment protocol. Bitcoin and other cryptocurrencies (also called AltCoins) gained significant momentum in 2013 with Bitcoin's sharp price rise, the historic high being US$1124.76 on 29 November 2013. High prices and high volatility attracted speculation, as well as proliferation of competitive and complementary cryptocurrencies. Arguably, there are over 500 AltCoins based on blockchain technology as of November 2014.

Technologists have drawn attention to the technology underpinning cryptocurrencies, known as blockchain. Blockchain's main innovation is a public transaction record of integrity without central authority. Blockchains are decentralised by nature that is shared by all nodes connected to a set network. Blockchain technology offers everyone the opportunity to participate in secure contracts over time, with a secure record of what was agreed at that time.

Z/Yen and the Long Finance community's interest in cryptocurrencies and blockchain technology began with a thought experiment on a hypothetical electronic currency, 'Pecunium', in 2005. In 2008, Long Finance established the Eternal Coin programme, exploring concepts of value and money (Cooper, 2010). A 2011 research project on emerging architectures for money and commerce noted the potential of cryptocurrencies to transform transactions across time and space (Z/Yen Group, 2011). Since 2011 cryptocurrencies and blockchain technology have become an area of research interest for Long Finance with a series of events and discussions exploring how blockchain technology could be applied in conventional financial services, including insurance.

This report is the output of a 2014 Long Finance research project entitled "People, Risk and Uncertainty over Time: How Blockchain Technology Might Transform Personal Insurance" (more information). The project sought to explore:

- how blockchain technology functions and how it could be applied in finance;
- how blockchain technology and related applications could be relevant to the insurance industry, with a focus on personal insurance;
- what could be the likely implications of applying blockchain technology in personal insurance, particularly in terms of relationships between insurers and insured; transactions through time; perception(s) of risk; and identity and personal history management.

2.2 Approach & methodology

Following desk research, Z/Yen organised a workshop on 11 September in London "People, Risk and Uncertainty over Time: How Might Blockchain Technology Transform Personal Insurance" (more information). This workshop invited insurance and financial services professionals, as well as cryptographic technology experts, to discuss blockchain technology and the implications of applying it to personal insurance. Interestingly, half the audience (about 30 people) claimed to have used Bitcoins.

Between August and November, the Z/Yen team interviewed a cross-section of 30 blockchain technology experts, system developers, insurance industry professionals, regulators, consumer bodies, trade bodies, and research institutes in Europe, North America, Australia and Asia. These semi-structured interviews covered blockchains and related applications, their possible relevance to insurance, and risks, benefits, and obstacles to applying blockchain technology in personal insurance.

In order to encourage international participation and present preliminary findings, a webinar was held on 1 October, "How Might Blockchain Technology Transform Personal Insurance" (more information).

Further, Z/Yen led five presentations and discussions on blockchains at larger events with groups ranging from 30 to 200 people, between September and November, as follows:

- financial services providers, Europe;
- financial service providers, Asia;
- financial service providers, USA;
- central bankers, UK;
- regulators and compliance officers, Europe.

These events were invaluable in assessing current knowledge and thinking.

2.3 Report outline & acknowledgments

This report comprises five chapters. Beside the executive summary (chapter 1) and the introduction (chapter 2), the report provides an overview of the technology and its possible uses in chapter 3; summarises the insurance industry landscape, in particular opportunities and challenges related to innovation and technology in chapter 4; and, outlines possible applications of blockchain technology, related implications for insurance as well as concluding thoughts in chapter 5. *Appendix 1* lists the affiliations of people who have kindly contributed to this project. *Appendix 2* contains a glossary of technical keywords, either used in this report or commonly used in other documents about this technology. *Appendix 3* provides the bibliography, though much of the reference material is online and mutable.

We would like to thank all the participants who either contributed to discussions during events or agreed to semi-structured interviews. We received enthusiastic participation from everyone on this project, and it was a pleasure to meet so many people thinking creatively about the future of insurance. We owe a special thanks to Carrie Tian of Harvard University who kindly assisted in the early stages of the project while doing an internship at Z/Yen. While there were many direct and indirect contributors, the conclusions in this report are the sole responsibility of Z/Yen Group.

3 ABOUT BLOCKCHAIN TECHNOLOGY

This chapter provides an overview of blockchain technology and how it functions (section 3.1). It goes on to examine related distributed applications (section 3.2), including smart contracts and decentralised autonomous organisations. Section 3.3 outlines issues in relation to security, mining centralisation and pseudonymous features, some of which could compromise the viability of the technology over time. Section 3.4 analyses future prospects for the blockchain technology and related applications including technological issues related to scalability; monetary considerations; the regulatory environment; and, the need for awareness raising and education about the technology and its applications.

3.1 Explaining the blockchain

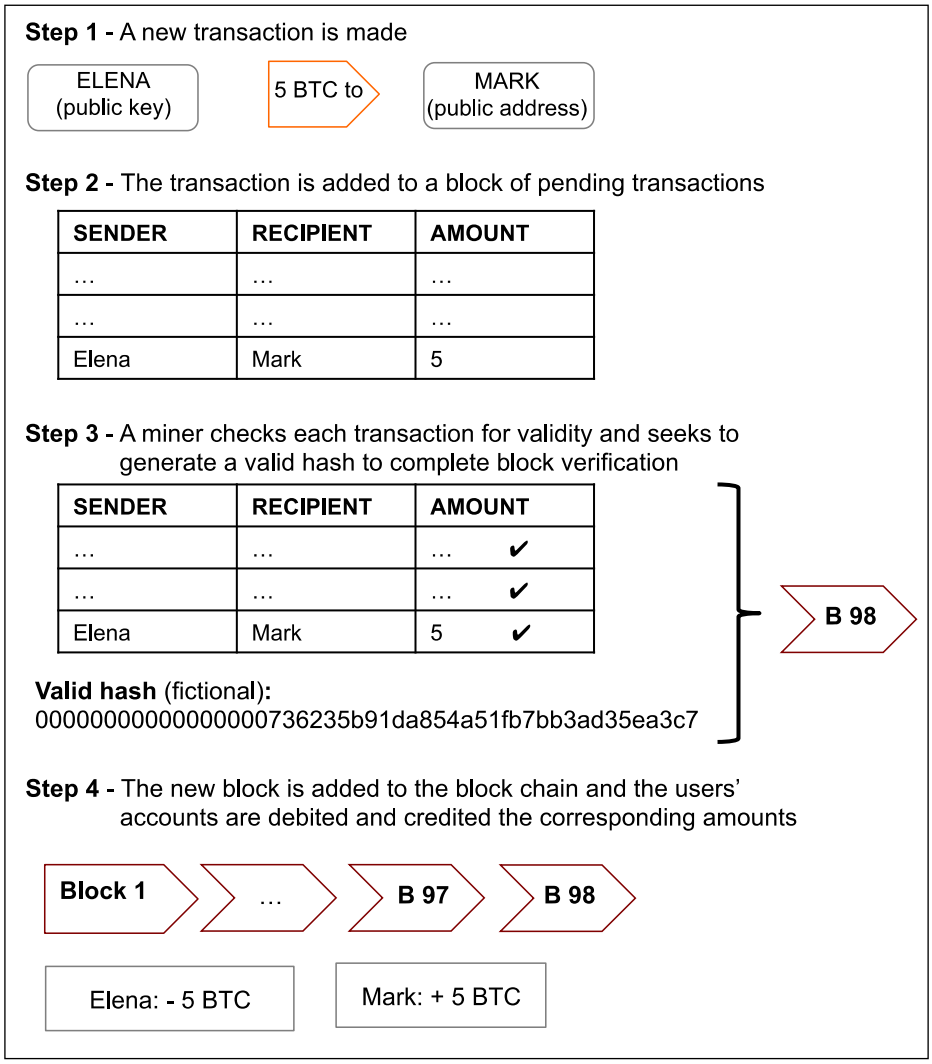
A **blockchain** is a transaction database based on a distributed cryptographic ledger shared amongst all nodes participating in a system. It is public in that it is decentralised and shared by all nodes of a system or network. There is integrity as double-spending is prevented through block validation. The blockchain does not require a central authority or trusted third party to coordinate interactions, validate transactions or oversee behaviour.

People use trusted third parties in many roles in finance, as custodians, as payment providers, as poolers of risk, i.e. insurers. Trusted third parties in finance provide four functions. They validate the existence of something to be traded; they prevent duplicate transactions, i.e. someone selling the same thing twice; they record transactions in the event of dispute; and, they act as agents on behalf of clients, associates or members. If you believe in the integrity of blockchain technology, then it might largely displace two roles of a trusted third party, no double-spending and providing a verifiable public record of all transactions.

Blockchain technology first emerged with Bitcoin, a cryptocurrency-based distributed payment protocol, released anonymously in 2009. As explained by its creator, who uses the pseudonym Satoshi Nakamoto, Bitcoin is meant as “a purely peer-to-peer version of electronic cash [which] would allow online payments to be sent directly from one party to another without going through a financial institution” (Nakamoto, 2009:1). *Box 1* on page 14 provides an overview of Bitcoin.

A full copy of the blockchain contains every transaction ever executed, making information on the value belonging to every active address (account) accessible at any point in history. Every block contains a long reference number or hash of the previous block, thus creating a chain of blocks from the genesis block to the current block. Figure 2 on the next page illustrates how a transaction is recorded on the blockchain, based on the Bitcoin protocol.

Figure 2 – sample transaction (simplified) with Bitcoin



Each new block of transactions to be added to the blockchain contains the following information:

- all transactions pending since the last block was added;
- the hash of the previous block, acting as a 'pointer' or link to previous blocks in the chain;
- a 'nonce', i.e. an arbitrary number used only once in cryptographic protocols.

Validation is required for a new block to be added on to the blockchain. This validation process, also called mining, allows pending transactions to be confirmed; enforces a chronological order on the blockchain; protects the neutrality of the blockchain; and enables different computers (or nodes) to agree on the state of the system at any given time (Bitcoin Project, n.d.).

For Bitcoin, block validation (or consensus) occurs through 'Proof-of-Work' using the SHA256 algorithm, which generates cryptographically secure one-way hashes. Proof-of-Work (PoW) is a function that is hard to compute, but easy to verify, which serves as a probabilistic cryptographic proof of the quantity of computational resources controlled by a given node, and takes on average about 10 minutes with

Bitcoin (Buterin, 2013). Every block requires a PoW with a pre-specified difficulty level in order to be valid, and in the event of multiple competing blockchains the chain with the largest total quantity of PoW is considered to be valid (GitHub, 2014). To validate a block, 'miners' apply a hash function to the information contained in the new block, generating a 64-character string known as 'hash'. For a block to be accepted the hash of its information must start with a large number of zeros at the front. The process of finding a valid hash is computationally intensive, as the number of zeros at the front increases, making it harder to generate a valid hash. The blockchain makes it very difficult if not impossible for previous transactions to be altered (which would imply regenerating all the subsequent blocks's hashes) or for fake transactions to be accepted. This PoW validation process is how Bitcoin is able to guarantee its validity as a public ledger for all transactions in its history and their ordering.

Since Bitcoin was launched, alternative PoW algorithms have emerged such as script Proof-of-Work. Some consensus processes can require multiple PoW algorithms (e.g. Myriad, a protocol using five different PoW algorithms simultaneously) or dual-purpose PoW algorithms, which solve a specific 'useful' problem while producing PoW to secure the network (e.g. Primecoin for which PoW is used with prime number discovery) (Antonopoulos, 2014).

Other validation or consensus processes include 'Proof-of-Stake' (PoS), a system by which existing owners of a currency can 'stake' currency as interest-bearing collateral[1], applied for instance by the BlackCoin protocol (Buterin, 2013; Vasin, 2014; Antonopoulos, 2014); 'consensus protocol', a consensus driven algorithm applied every few seconds by all nodes in order to maintain the correctness and agreement of the network, which is used for instance by Ripple (Schwartz, Youngs & Britto, 2014) ; and, zero-knowledge proof, a cryptographic method by which one party (the *prover*) can prove to another party (the *verifier*) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true, used for example by Zerocash, a new protocol being developed to provide a privacy-enhanced version of Bitcoin (Zerocash, 2014).

The debate remains unresolved as to which validation process can best simultaneously guarantee speed, efficiency and security, though PoW seem to be the most commonly used process.

Miners' reward is equally an important aspect of the validation process and contributes to the the smooth running of a blockchain protocol. As Michael Nielsen, a scientist and programmer, puts it:

> *"For the proof-of-work idea to have any chance of succeeding, network users need an incentive to help validate transactions. Without such an incentive, they have no reason to expend valuable computational power, merely to help validate other people's transactions. And if network users are not willing to expend that power, then the whole system won't work. The solution to this problem is to reward people who help validate transactions. In particular, suppose we reward whoever successfully validates a block of transactions by crediting them with some infocoins [AltCoins]. Provided the infocoin [AltCoin]*

[1] Users can reserve a portion of their currency holdings, while earning an investment return in the form of new currency (issued as interest payments) and transaction fees.

reward is large enough that will give them an incentive to participate in validation." (Nielsen, 2013)

So far, blockchain miners are primarily rewarded through newly minted AltCoins (e.g. Bitcoin, Ethereum), which are automatically generated once a new block is validated. Alternative rewards include: transaction fees, thus shifting the cost on to users of the system (e.g. Bitcoin uses voluntary fees to get faster validation); or offering a reward other than currency like for example Twister, a peer-to-peer microblogging platform, which rewards miners by giving them the ability to send promoted messages ('spams') to users.

Of the blockchain protocols that have emerged since Bitcoin was launched in 2009 or are being developed, most are based on AltCoins. For some, the currency is only a secondary feature used as a token to allocate something else (e.g. resource, contract). At the time of writing and to the research team's knowledge, two are not based on AltCoins.

AltCoins are decentralised currencies based on distinct blockchain protocols, usually developed from a copy (also known as fork) of the Bitcoin source code, though some have been developed from scratch. Most AltCoins tend to be fairly similar to Bitcoin. When they do differ from Bitcoin, it is usually on one or more of the following aspects: the monetary policy (e.g. currency supply, issuance rate or speed, coin reward); the consensus mechanism used to validate transactions; and/or other specific features such as anonymity (Antonopoulos, 2010). AltCoins (including Bitcoin) can be obtained either by mining blocks of transactions (as AltCoins are generated mathematically at a pre-determined rate every time a block of transaction is validated); by accepting them as payment from another user; or by purchasing them from a user or intermediary in exchange for some other accepted mean of payment (cash or credit card). (Bollen, 2013)

Figure 3 below provides a sample list of existing and emerging blockchain protocols.

Figure 3 – Examples of blockchain protocols

Name	Description	Based on currency?	Validation process	Year launched
Bitcoin	Cryptocurrency and payment protocol	Yes – bitcoins (BTC)	PoW	2009
BlackCoin	Cryptocurrency and payment protocol	Yes – blackcoins	PoS	2014
Ripple	Payment protocol and currency exchange	Yes – ripples (XRP)	Consensus ledger	2011
NameCoin	Distributed domain name management, developed from the first fork of the Bitcoin protocol	Yes - namecoins	PoW	2011
Bitmessage	Distributed communication protocol used to send encrypted messages	No	PoW	2012

Name	Description	Based on currency?	Validation process	Year launched
Ethereum	Blockchain operating system (i.e. a decentralised platform and programming language) to support and host distributed applications	Yes – ether	PoW	2015 (tbc)
Hyperledger	Open source platform for creating private currencies or recording assets, and allowing their transfer	No (could support different AltCoins)	Consensus pool	2014 (tbc)
Zerocash	Privacy-preserving version of Bitcoin, where payment transactions do not contain any public information about the payment's origin, destination, or amount; their correctness is demonstrated via a zero-knowledge proof	Yes – zerocoins (anonymous) and basecoins (non-anonymous)	Zero-knowledge proof	2014-15 (tbc)

At the time of writing, distributed platforms continue to be developed, some of which are not based on blockchain and thus not included in the table above. To give one example much talked about recently, MaidSafe, a fully decentralised platform on which application developers can build decentralised applications, is based on a network involving vaults acting as transaction managers, one of their many roles. Transactions on the network are unchained meaning that only the previous owners/participants are known.

Box 1 – About Bitcoin

Bitcoin is a distributed online payment system introduced as open-source software in 2009. Payments are recorded in a public ledger using its own unit of account, also called bitcoin.

Bitcoin supply is capped by design at 21 million bitcoins. Bitcoins are issued as a reward for processing transaction blocks, currently at a rate of 25 bitcoins per block validated until 2016 when the rate will be halved (to 12.5 bitcoins). It is estimated that the supply limit will be reached between 2110 and 2140.

As well as rewarding mining, bitcoins can also be obtained by accepting them as a payment or by buying them on exchanges in exchange for real world currencies such as USD. There are no fixed exchanges rates between bitcoins and fiat currencies. As of 19 November, one bitcoin is worth USD 377.50, a price which has been fairly volatile over the last two years. Bitcoin reached a historic high of US$1124.76 on 29 November 2013 (blockchain.info, n.d.).

Bitcoin users own keys (a private key and a public key) that allow them to prove ownership of transactions in the Bitcoin network, unlocking the value to spend bitcoins and transfer them to a new recipient. Those keys are often stored in a digital wallet on each user's computer. Possession of the key that unlocks a transaction is the only prerequisite to spending bitcoins, putting the control entirely in the hands of each user. Users can transfer bitcoins over the network to do just about anything that can be done with conventional currencies, such as buy and sell goods, send money to people or organisations, or extend credit. The main difference is that bitcoins are entirely virtual. There are no physical coins. (Antonopoulos, 2014)

The decentralised nature of Bitcoin and therefore its independence from central banks and monetary authorities is what made it popular initially (Bollen, 2013).

Bitcoin seems to have the most potential as a medium of exchange, given lower transaction costs and fees compared to other payment systems, but price volatility and security issues could hinder its acceptance. Bitcoin's potential as a currency has been disputed on the grounds that it has been a fairly poor unit of account and store of value so far. This is partly due to its elevated price volatility and security issues but also to allegations of affiliation with black market and other illegal trade activities.

3.2 Distributed applications

Distributed applications are being developed on top of blockchain protocols. Such applications are interesting as they add benefits of automation and efficiency gains, using decentralisation and cloud computing. Distributed applications can include smart contracts and decentralised autonomous organisations.

Smart contracts (SCs) are self-administered contracts or scripts built on top of a blockchain protocol and enforced when certain pre-defined conditions are met. Automated contracting systems already exist in finance, for example with online applications for credit cards or for personal loans based on pre-set requirements or automated algorithmic processes to buy or sell stocks under pre-defined rules on exchanges. Nick Szabo, one of the first to explore cryptographic scripts and to coin the term 'smart contract' defined it as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises" (Szabo, 1996). When hosted on a blockchain, smart contracts are run in a decentralised manner and thus do not require centralised control or monitoring to function.

Smart contracts can help to make decisions and automate relationships. Beyond increased speed and efficiency, SCs are said to avoid the textual ambiguity of (some) real world contracts though factual ambiguity persists (De Filippi, 2014). SCs are deterministic, implying that all the possible outcomes of the contract (including penalties for breach of contract) must be explicitly stipulated in advance. There are however questions about their validity and enforceability in the real world. Efforts such as the Common Accord - an initiative focusing on the codification and automation of legal documents, are underway to strengthen integration between smart contracts and contracts in the real world. For example, a SC can reference a

real world contract (RWC) with a hash and a RWC can reference a SC as a schedule, leading to court-enforceable contracts with the benefits of automation and efficiency.

Decentralised autonomous organisations (DAO) are "algorithmically-governed programmes that, in using trustless decentralised computing, can serve as a way to formalise multilateral relationships or transactions outside of traditional legal architectures" (McKinnon, Kulman et Byrne, 2014: 1). Essentially DAOs are more sophisticated types of smart contracts usually involving the following elements:

- shareholders or members;
- a governance system facilitating collective decision-making, for example on how the organisation should allocate its funds;
- a way for the DAO to fund itself either through the sale of services or through endowments.

In this case, the blockchain is used to enforce decisions once pre-defined conditions based on collective decisions are met (Buterin, n.d.).

Bitcoin appears to be the first DAO (e.g. Aron, 2014; McKinnon, Kulman et Byrne, 2014), albeit a simple executor of one-way transactions. People who own Bitcoins are shareholders in the 'company' which offers financial services; earns revenue through transaction fees; and, pays a salary to its employees (miners) without anyone being specifically in charge. Decisions (i.e. to alter the protocol) are taken collectively (at a 51% majority of users). DAOs have been shown to be possible using blockchain technology, but do not exist other than as cryptocurrencies. Initiatives, like Project Douglas, are working on long-term decentralised applications in an open source setting. In June 2014, Project Douglas released the ERIS platform, a first take at how to create a DAO based on consensus-driven applications relying on decentralised architecture, using blockchain technology and web 3.0 features (McKinnon, Kulman et Byrne, 2014). Significant progress has already been made on decentralised decision-making through consensus governance. Work is ongoing to design decentralised task management and asset management frameworks.

Conceptually, DAOs raise legal issues in terms of liability and accountability, especially so as our legal systems are designed to assign responsibilities and liabilities to actual human beings. Theoretically, DAOs are autonomous entities subsisting independently from any legal, moral or physical entity. In the absence of ownership or control by any given identity, who is accountable, in charge and responsible for operations? Even when the creation of a DAO can be tied to a person and that person can be assigned responsibility in case of wrongful behaviour, no mechanism can prevent the DAO from continuing to run autonomously (De Filippi, 2014). At the moment, coupling a DAO with a real-world legal entity (like for smart contracts above) would be one way to benefit from the efficiencies related to blockchain and cryptographic technologies while complying with legal formalities in the jurisdictions where they operate (McKinnon, Kulman et Byrne, 2014).

Automation is not always the best option. As Vitalik Buterin, the co-founder of Ethereum, said "automation is simply a paradigm that is likely to have large benefits in certain particular places and may not be practical in others" (Buterin, n.d.: 23).

Technology experts interviewed for this research project largely echoed this statement.

Current and emerging distributed applications can be categorised as financial, such as financial derivatives, hedging contracts; semi-financial applications such as notaries; and, non-financial applications such as online voting and decentralised governance arrangements (Buterin, s.d.). Figure 4 below provides some examples of existing and emerging distributed applications.

Figure 4 – Examples of distributed applications

Name	Description	Type	Category	Year
Agora Voting	Voting platform	SC	Non-financial	2012
Bitnation	Platform based on decentralised governance built on blockchain and its own AltCoin. Aims to empower people to create their own local governance tools and to provide similar services as governments	DAO-related	Possibly all-encompassing	2014
Bitshares	Community of DAOs, allowing to invest in DAOs	DAO-related	Financial	2014
Colored coins	Open standard protocol allowing to 'colour' AltCoins according to a corresponding type of assets (e.g. property, object, bonds, shares) and operating on top of the Bitcoin protocol	SC-related	Financial	2012
Counterparty	P2P financing e.g. crowdfunding, based on Bitcoin protocol	SC	Financial	2013
ERIS	Platform to create, test and run decentralised governance-driven applications including DAOs, hosted on Ethereum blockchain protocol	DAO-related	Possibly all-encompassing	2014
Monegraph	Registry for digital art, based on NameCoin protocol	SC	Semi-financial	2014
Proof of Existence	Notary system, based on Bitcoin protocol	SC	Semi-financial	2012
Twister	P2P microblogging platform based on Bitcoin and BitTorrent protocols	SC	Non-financial	2013

Distributed applications expand the range of items that can be encoded on the blockchain well beyond mere financial transactions. Figure 5 on the next page provides a categorisation of items that could in theory be recorded or stored on the blockchain using distributed applications models.

Figure 5 – Taxonomy of 'blockchainable' items

Category	Items
Financial instruments, records, models	Currency, private and public equities, bonds, derivatives, voting rights associated with financial instruments, commodities, derivatives, transaction records (e.g. trading), mortgage or loan records, crowd-funding, P2P lending, microfinance, (micro)charity donations etc.
Public records	Land and property titles, vehicle registries, business license, business ownership/ incorporation/ dissolution records, regulatory records, criminal records, passport and ID, birth or death certificates, voting ID, registration and rights, health and safety inspections, tax returns, building and other types of permits, court records, government/ listed companies / civil society - accounts and annual reports etc.
Private records	Contracts, ID, signature, will, trust, escrow, any other type of classifiable personal data (e.g. physical details, date of birth, taste) etc.
Semi-private/semi-public records	High school/university degrees and professional qualifications, grades, certifications, human resources records, medical records, accounting records, business transaction records, locational data, delivery records, genome and DNA, arbitration, genealogy trees etc.
Physical asset keys (in relation to Internet of Things)	Key to home, office, car, locker, safety deposit box, mail box, hotel rooms etc.
Intellectual property	Copyrights, licenses, patents, proof of authenticity or authorship etc.
Other records	Cultural, historical events, documentary (e.g. video, photos, audio), (big)data (weather, temperatures, traffic), sim cards etc.

[Source – adapted from Ledra Capital, 2014]

Distributed applications can be tied to real world information, objects or events by incorporating mechanisms such as oracles, arbitrators or escrow systems (most of which are already used in real life). Oracles are trusted third parties (sensor, person, software) providing real time, real world information. A crop insurance example was frequently encountered. A crop insurer could conclude a smart contract with a farmer where payment is triggered by a trusted third party data feed. In this example, perhaps 20 days without precipitation should trigger payment. The smart contract would be fed weather data from a national weather service, and when there were 20 dry days the farmer would find that funds were available for him or her to collect.

If the transaction involves delivering an object, the smart contract can include an escrow system, whereby the recipient confirms receipt of the object prior to activating payment. Finally smart contracts can incorporate the use of arbitrators (single or multiple) to assess the quality of a service or authenticity of an object.

A smart contract can integrate multiple oracles or arbitrators and then design an algorithm to communicate relevant information to the blockchain.

Respondents working in this field suggested that distributed applications are likely to evolve significantly over the next five years. More sophisticated arrangements interfacing the virtual and the physical worlds are likely to emerge, including in relation to the 'Internet of Things', that is solutions to interconnect uniquely identifiable embedded computing devices within the existing Internet infrastructure. An example here might be that 'wearable' health monitors find that someone who obtained lower insurance rates based on agreeing to take exercise had failed to undertake sufficient exercise to justify the discount.

3.3 Further blockchain issues

Other specific issues that emerged during our research deserve further consideration, including security, decentralisation and anonymity.

Security

Blockchain protocols are often described as utterly secure, but the architecture relies on public-key cryptography. For two decades there has been discussion about whether or not larger quantum computers could break public-key cryptographic systems, if and when they arrive with sufficient 'qbits'. The whole encryption field is fascinating, but it is also true to say that if public-key cryptography is cracked, then credit cards, the SWIFT bank transfer system, and most areas of e-commerce would be rendered vulnerable, along with many other applications that require security.

Blockchain system robustness stems from a decentralised architecture and the absence of a single point of failure or control, analogous to the resilience of the internet's multi-nodal structure. The paper that introduced Bitcoin to the world (Nakamoto, 2009) explained how the system had been designed to make it 'impractical' for someone to take over the blockchain, though technically not impossible. Dan Kaminsky, a security expert who tried hard to break Bitcoin without success, concluded that it was "preternaturally sound" (Kaminsky 2013). Because all of the identifying data on a blockchain protocol is hashed, it would take an impractically long time to discover by brute force enough information to fake a transaction.

Some respondents noted that a decentralised system raises the question as to who is responsible to fix or to address any shortfalls in the event that it becomes compromised. Others point out that the system has shown it can evolve when problems arise. Some questioned block validation timings (e.g. there is on average a 10 minute delay between when you process a transaction on Bitcoin and when it is validated) and the extent to which low latency advantages (being geographically closer to the core of the calculations) could arise. Timings are being actively discussed with proposals to get validation perhaps beneath ten seconds – perhaps a problem with payments, but not necessarily with many of the personal insurance applications discussed in this paper.

Though existing blockchains have so far proven secure, security issues tend to arise when the virtual world interfaces poorly with the physical world. The biggest cause seems to be the lack of understanding and poor security measures taken by

blockchain protocols' users and exchanges (De Filippi & Mauro, 2014). When typical users interact with a blockchain, they are not just using a protocol. They are often also using software that stores their wallet or account information for them or they are interacting with intermediaries such as cryptocurrency exchanges. These are the places where users are most vulnerable to hacking and other security incidents. For instance, Mt Gox – an online exchange where users could buy Bitcoins – was shut down in February 2014 after enduring daily cyber-attacks and having 750,000 Bitcoins stolen (The Telegraph, 2014).

Mining (De)centralisation

A major concern that has emerged with Bitcoin over the past year is mining centralisation. Mining centralisation can potentially harm a blockchain system in terms of bias against certain transactions or certain public keys, by blocking or delaying block validation or even by modifying the ledger in the past. Even more worrying, a mining pool attaining 51% of the computing resources involved with a blockchain protocol, would be more vulnerable to a user or entity gaining control over that pool and wrongfully using that hashing power.

While the Bitcoin protocol was conceived as decentralised, the reality has shown that mining is no longer a highly decentralised and egalitarian pursuit mainly for two reasons. First, specific equipment is not necessarily readily available to every user, such as application-specific integrated circuits (ASICs) required to mine. Second, blockchain validation is not performed locally as most miners (whether independent or specialised companies) tend to rely on centralised mining pools to provide block headers. A few mining pools now dominate the processing power in the Bitcoin network (Buterin, n.d.). In April 2013, a mining pool called BTC Guild implemented a mining centralisation mitigation plan involving measures to limit the creation of new accounts, raise fees and remove getwork-based pool servers should the pool speed reach over 40 to 45% of the Bitcoin network (BTC Guild, 2013). In June 2014, a mining pool called GHash.IO did attain 51% of the Bitcoin network's computing resources (GHash.IO, 2014). While the group promised not to abuse this power, the incident highlighted a worrisome security flaw.

No easy fixes exist to address this issue, except perhaps faith in the free market. In response to fears and arguments stating that mining centralisation could endanger the viability of Bitcoin over time, some argue that the Bitcoin market can fix itself and that a decentralised Bitcoin market is in the 'self-interest' of its community (including miners), pointing to the 'self-interest' of miners who switch pools when one overgrows in computing capacity. (Faggart, 2014)

On the technical side, developers of subsequent blockchain protocols (including Ethereum) are working on ways to avoid mining centralisation for example by removing the benefit of specialised hardware, by randomising nonces more regularly or by encouraging miners to switch pools (see for example Ethereum white paper (Vitalik, n.d)).

Pseudonymity

Bitcoin and other blockchain protocols are often described as anonymous because it is possible to participate in transactions without giving any personally identifying information. To be precise, most protocols like Bitcoin are pseudonymous, meaning

that transactions are made under a pseudonym (the public key or address). Public keys or addresses can be traced back in the ledger in terms of transaction history. These do not however provide information about the owner of the address, unless that user acknowledges ownership of that address or inadvertently discloses that information, which in turn implies that all transactions made with that public address can be tied to that person.

Semi-anonymous features can present many drawbacks especially when used in payment systems, including theft and lack of accountability. As with Bitcoin one user can have multiple public keys, therefore an adequate regime to protect identity is needed to address the relationship between the identity of an individual and the identity on a marketplace. Finding the balance between an appropriate level of privacy combined with the possibility of accessing user information in certain circumstances (pre-determined by the user community or prescribed by law) would indeed be more socially desirable than anonymity.

Authentication and know-your-customer (KYC) processes are already in place in part of the blockchain universe. For example, most AltCoins exchanges are required by governments to collect data on their user base. That information is however not disclosed to third parties.

Over time, authentication processes and pre-determined access frameworks are likely to address some of the shortcomings or risks associated with pseudonymity. Authentication processes could take different forms including the use of trusted third parties or distributed notaries. Reputation ratings and white or black listings could also strengthen disclosure and lessen risk. Some respondents went further and suggested that while a unified ID system seems a long way off, if it were to exist it would probably use blockchain technology.

3.4 Future prospects

Public attention has so far focused on Bitcoin and similar protocols as digital currencies and innovative payment systems (sometimes called Bitcoin 1.0). Attention is now shifting to the blockchain as a distributed platform for financial and interactive innovation, which could support the development of, and host, distributed applications (Bitcoin or blockchain 2.0). Blockchain 2.0 discussions touch upon assets records and transfers, reputation and identity management, intellectual property ownership, and data storage. Some already envisage blockchain (or Bitcoin) 3.0 either as blockchain technology applications beyond currency and contracts into new areas such as health, science and culture (Swan (a), 2014) or, going even further, as distributed information management all around (Swan (b), 2014).

The core of blockchain is “a method to create decentralised peer-validated time-stamped ledgers” of transactions (or interactions) (Scott, 2014: 1). Right now, blockchain technology and related applications are still in early stages. Experimentation is ongoing and desirable to further test the solidity of the system and the range of its potential uses and applications. The blockchain ‘community’ remains fairly small though scattered around the globe and well connected.

Technology: issues and recent developments

At the time of writing, the main technological issues is the scalability of a blockchain, due to the lengthy initial download of the blockchain over time (Bitcoin blockchain size amounts to over 24 GB as of 11 November 2014 (Blockchain Info, n.d.)) and the limited block size (i.e. 1MB for Bitcoin) which in turn limits the number of transactions per second (7 tps for Bitcoin) (Bitcoin Wiki, n.d.). Further, existing blockchain protocol designs (e.g. Bitcoin, Ethereum) require every transaction in a protocol to be processed by every node of the network (Buterin, n.d). Propositions to address these issues include BitTorrent downloads to speed the initial transaction data download; blockchain compression; pruned version of blockchains; and, splitting the blockchain into different data structures (for example, a finite blockchain which keeps N blocks into the past, an account tree which keeps account balance for every address with a non-zero balance, and a 'proof chain' which is an (ever growing) slimmed down version of the blockchain (Bruce,2014)). (Andersen, 2014)

The blockchain technology and related applications are constantly evolving with new models being discussed, developed and tested. IBM for example is looking into using the blockchain technology for an Internet of Things platform, called Adept, and backed by other P2P technologies – BitTorrent for file sharing and Telehash for encrypted messaging (Hajdarbegovic, 2014).

Interoperability across blockchain protocols does no longer seem inaccessible. Recent technological developments being discussed include the creation of 'pegged sidechains', "a sidechain[2] whose assets can be imported from and returned to other chains" (Back, et al., 2014: 8), which would enable interoperability and two way asset movements between chains, thus alleviating market and development fragmentation across protocols (Back, et al., 2014).

AltCoin – a necessary component of a blockchain protocol?

Most blockchain protocols and especially those hosting platforms for distributed applications are currently AltCoin-driven. AltCoins can be viewed as tokens facilitating behaviour. Tokens are primarily needed to reward the validation process or mining. While other rewards such as transaction fees or alternative compensations exist, AltCoin-based protocols seem so far to be the most efficient.

Discussions on forums[3] and social media[4] have been questioning the viability of a blockchain protocol without AltCoin, pointing to the Bitcoin blockchain and arguing that economic incentives (in this case monetary reward in the form of newly minted Bitcoins) are critical to Bitcoin's security. This would suggest that even when the purpose of the token is non-monetary, economic incentives would still be needed to ensure block mining and ultimately the smooth running of the blockchain. Somebody has to be paid to 'forge' (sic) new links in the blockchain.

For a non-monetary blockchain protocol, the user community as a whole would need to have a sufficiently strong shared interest in the maintenance of the protocol or have sufficient incentives to mine blocks for the rest of the community (e.g. Twister and promoted messages). These types of arrangements can lead to free riding or

[2] blockchain whose assets can be imported from and returned to other chains (Back et al., 2014)
[3] e.g. Hacker News - https://news.ycombinator.com/item?id=8446998
[4] e.g. Rodolfo Novak's tweet - https://twitter.com/nvk/status/522115773918359552

tragedy of the commons problems. Some respondents suggested that the energy content embedded in a blockchain could be an indicator of validity. The historic energy consumed to build a blockchain over time might indicate the level of comparative community support.

Blockchain: public, semi-public, private?

Current blockchain protocols are public so that, in principle, everyone can participate and check whether a transfer comes from the rightful public address. Openness and transparency is what informs decentralised consensus and ultimately keeps the system secure.

Some respondents have taken further the idea that companies (or other institutions) could issue asset-backed tokens, thus suggesting that these companies or entities could set up their own blockchain protocol. While this would be interesting to explore further, one has to remember that as soon as there is a single point of control or behaviour coordination, the system can no longer be fully decentralised. This is an area that deserves more attention. Research should consider ways of maintaining transparency and integrity while 'privatising' the maintenance and possibly the scope of a blockchain.

Regulation

Regulation of AltCoins and blockchain-related applications is still in early stages. "Governments have been struggling with whether to class AltCoins as a meaningless token, a trade token, a weightless commodity, or a currency. Classification is important for matters as diverse as corporate and personal taxation, value added taxation, financial regulation, formulation of monetary policy, and statistic" (Mainelli and McDowall, 2014). Recent regulatory attempts have focused primarily on defining AltCoins, their acceptance, classification and corresponding tax treatment. Regulatory attention is now shifting to intermediaries operating in this ecosystem, as illustrated by the New York State Department proposal for BitLicense Regulatory Framework unveiled in July 2014 (see box 2 below).

Some countries have banned or declared illegal the use of Bitcoin and other cryptocurrencies (for example, China and Vietnam have banned the use of Bitcoins by financial institutions), other make it very difficult to use or buy Bitcoins (for example, in Iceland, it is illegal to buy Bitcoins with kronas). Most other countries seem to have relatively benign views on Bitcoin so far (e.g. Europe, UK, Australia). The USA seems to be particularly active both in accepting Bitcoin, but also in struggling to regulate it. The USA's complex and numerous regulators could take some time to provide a coherent approach to Bitcoin supervision. For more information, two sources – BitLegal and the US Library of Congress' Bitcoin Survey, provide comprehensive and up to date information on the legal status of cryptocurrencies such as Bitcoin.

In a comparative analysis of the legal status of cryptocurrencies in Australia, the European Union, the United Kingdom, and the USA based on existing financial services, banking and currency regulation, Rhys Bollen highlights how most regulatory regimes are not well-designed to cater for this type of payment system and suggests that future regulation should aim to "be broad [in scope], outcomes focused, technology neutral and future proof to the extent of the possible" (Bollen,

2013: 292). Four areas to be considered by regulators are (1) information - ensuring that sufficient information for consumers to assess risk is publicly available; (2) transactions and options for legal redress if anything goes wrong; (3) asset protection – solutions or requirements to protect AltCoin-based assets from loss or theft; and, assuming that a digital currency protocol reaches a critical size, (4) competition – measures to avoid the concentration of operators.

Box 2 – BitLicense Regulatory Framework proposal

In July 2014 New York State Department Financial Services (NY DFS) unveiled a BitLicense Regulatory Framework covering consumer protection, anti-money laundering and, cyber security rules tailored for virtual currency firms (NY DFS, 2014). Among the first detailed attempts to regulate actors within the digital currency space, once finalised, NY DFS' regulatory framework is likely to be regarded as a basis for other state and national policies. While a licensing framework could open new commercial opportunities by reducing the perceived risk and the existing regulatory uncertainty surrounding start ups and companies operating in the space, the Bitlicense proposal has stirred much debate with respect to its scope and breadth of application. The proposal was open for comments until 21 October. Opposing arguments include that the proposal is (wrongfully) targeting software companies and open source projects instead of solely financial intermediaries; could hinder innovation and lead to higher barriers of entry in the market; and would threaten some of the privacy features inherent to blockchain protocols and related applications (see for example Allaire, 2014; Reitman, 2014 or Coinbase, 2014).

When asked about future regulation, most respondents stated that they would welcome regulatory clarity on the grounds that recent uncertainty has been hampering AltCoin acceptance, use and related commercial development prospects. For example, the UK Digital Currency Association has been pushing hard for regulation. Some argue for self-regulation or better standard-based regulation (e.g. ISO standards) involving the industry as a way of improving practices and coordinating behaviour in the sector while maintaining a certain degree of flexibility and allowing for existing regulatory frameworks to adapt. Others noted how existing fears and criticisms such as 'Bitcoin could disrupt the hegemony of the state' are similar in nature to early reactions when the Internet was created. Ultimately (as with the Internet) the technology is likely to be co-opted by normal citizens. At the moment, governments seem to be letting the private sector experiment with the technology before building regulation around it.

Awareness and education

Blockchain technology can be difficult to comprehend. Taking Bitcoin as an example, we can talk of Bitcoin as a currency, a decentralised public ledger, a payment system or even as a 'platform' to host distributed applications. It is confusing. One group of qualified financial professionals on a training course spent two hours acquiring a basic understanding of just Bitcoin. With such high knowledge barriers, acceptance will be slow. Complexity also slows technological application. On the other hand, technologists have shown an ability in many areas to provide simplicity, e.g. phone 'apps'. The difficulty for Bitcoin and blockchains though is that high levels of trust are also required for serious use. Money is non-frivolous to most

people. Complexity impedes trust, and therefore impedes take-up doubly. However, innovation is helping to simplify things.

The difficulty in comprehending blockchain technology could be more significant for people who were not born into the digital world (also referred to as 'digital immigrants') even though they have since then adapted to part or most of it, than for 'digital natives' (Prensky, 2001). Over time, blockchain technology and related applications could contribute to a generational language barrier, particularly so as new generations grow up learning to code and digital technology and coding initiatives proliferate (see for example the UK Hour to Code or Code for Progress in the US).

First, blockchain technology, starting with the Bitcoin protocol, was released as an open source technology (and codes) allowing copies to be made and thus code altered and further developed with new protocols. Subsequent developments have followed similar open-source trajectories, as illustrated by GitHub, a code host and collaborative review platform on which most blockchain-related codes have been released. A community, albeit initially of experts such as computer scientists and software developers, is growing stronger and more diverse, working on technology improvements and brainstorming about, and developing further, possible applications in this field.

Second, the same community is devoting time and resources to promote and disseminate information on Bitcoin, other AltCoins and blockchain technology, and to make it simpler to understand. For example, Bitcoin has a very comprehensive and well-referenced section on Wikipedia[5], which includes information on the functioning of the underlying technology; the economics of the digital currency Bitcoin; and, about related risks and opportunities. The blockchain community has also developed a number of resources including its own wiki (e.g. Bitcoin wiki, 907 pages as of 13 November 2014), statistics (e.g. bitcoin charts or Blockchain Info), video tutorials (e.g. Bitcoin Properly or the video series on Bitcoin by Khan Academy) and more. Community members are gathering around the world to discuss the technology, its functioning and possible applications with, at the time of writing, nearly 580 Bitcoin Meetup groups across 73 different countries accounting for a total of 67,000 members (Meetup, 2014) and a number of others Meetup groups with 'blockchain' in their title. Of the many other community projects, the following are worth noting: online courses such as Bitcoin Education Project and Udemy's tutorials; dedicated news outlets such as Bitcoin Magazine and CoinDesk; and, the Bitcoin Foundation, which aim is to standardise, protect and promote Bitcoin.

Many describe blockchain technology as a 'global innovation that is likely to last one way or another'. Respondents suggested that education and information are important to raise awareness on the technology and related applications and ultimately to support consumer-friendliness.

[5] http://en.wikipedia.org/wiki/Bitcoin

4 ABOUT PERSONAL INSURANCE

This chapter provides an overview of insurance issues which are deemed relevant when considering potential applications for blockchain technology in this sector, particularly attitudes towards risk (section 4.2); trends shaping the future of the industry (section 4.3); and, the role of technology and innovation (section 4.4).

4.1 Protection

Insurance is a risk management mechanism designed to protect the financial well-being of individuals, companies and other entities by transferring the costs of a potential significant loss to other entities, i.e. insurance companies, in exchange for monetary compensation, i.e. premiums. Based on the 'law of large numbers', insurance companies pool different types of risk and use statistical analysis to project what their actual losses will be within a given class.
Premiums are generally invested to generate income, which allows paying for actual losses while generating a profit. In most instances, the absolute level of risk exposure of an insurance company will outweigh the capital held on its balance sheet. Thus, insurance companies often seek to transfer risk to third parties through reinsurance policies, which help to stabilise expected results, strengthen their financial situation and protect against catastrophic losses. (BSI and Long Finance, 2014: 6)

Personal insurance focuses on protecting people and their families against adverse effects on lives and living. Different types of insurance exist, some of which are mandatory (e.g. car insurance), some others are required in certain instances (e.g. property insurance can be a requirement for a mortgage contract) and others are free from obligation to contract though often deemed sensible (e.g. life insurance). Personal insurance products include life, car, health, home, temporary and permanent disability, income protection, injury, pet, travel, and recreational vehicle.

As Mary McAleese, president of Ireland, expressed it in her remarks to the European Insurance Forum in Dublin on 30 March 2010:

> *"The certainty and confidence that insurance provision brings to all our daily lives, whether business or personal, enables us to breathe more easily, to find the confidence to let innovation flourish and to engage with the present and the future, chastened by the past but not allowing the fear of the possible to paralyse us in the present."* (McAleese, 2010)

4.2 Typology of risk attitudes and corresponding behaviours

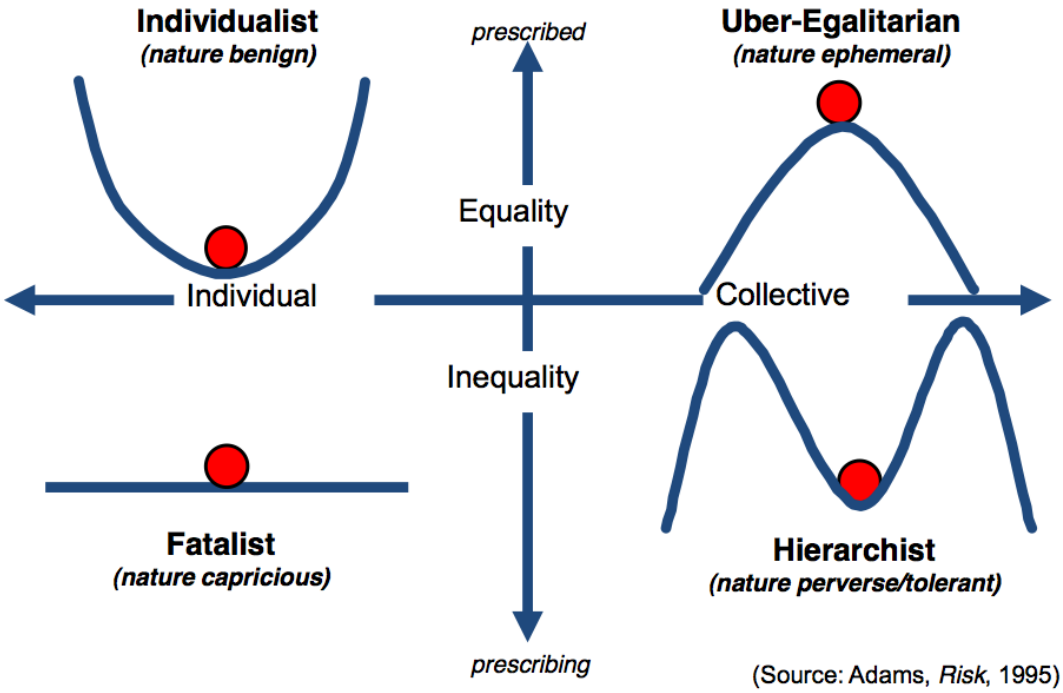
Upon identifying a risk, there are three generic responses, (1) accept the risk; (2) mitigate through preventive measures that reduce the likelihood or impact of the risk; or, (3) transfer all or part of the risk to a third party (e.g. by contracting with an insurance company).

Different people exhibit different risk profiles at different times and in different situations. Three types of behaviours are commonly distinguished: *risk adverse* – people who tend to shy away from risks and prefer to have as much security and certainty as is reasonably affordable in order to lower their discomfort level; *risk seeker* – people likely to pay to enter into risky endeavours as long as a positive

return is possible; and, *risk neutral* – individuals who will not pay extra to have the risk transferred to someone else, nor will they pay to engage in a risky endeavour (Baranoff, Brockett and Kahane, 2014). People's attitude towards risk is likely to influence their relationship with insurance. The more risk averse a person is in a given situation, the more likely he or she will want to transfer that specific risk onto someone else.

Adams (1995), Hollings and others, working on culture, divide people's views on specific risks into four risk profiles, as illustrated in Figure 6. The first division is into those who look at collective risk versus those who look to themselves (the horizontal axis on the graph below). They also categorise people into those who see the world as one at the top where authority sets the rules, equally applied even if unfair, and the bottom where people make the rules themselves (the vertical axis on the graph below).

Figure 6 – Risk-Reward People Typology



It is important to stress that individuals exhibit all of these profiles at different times. For example, someone may be an *individualist* happily taking risks setting up their own company, but a *fatalist* about paying parking fines, an *über-egalitarian* about climate change, and a *hierarchist* about drug use. Each profile has a 'ball' on a slope that, if destabilised, might roll out of their world. Taking each quadrant in turn:

- ***Fatalist - Unsettled Times***: the *fatalist* sees nature as capricious. Nothing they do changes the way the ball moves. At best, it will all come back and bite them. At first glance, the *fatalist* is uninteresting, but over time it seems to be the quadrant of the majority (for example when not contesting an invalid parking ticket).
- ***Individualist - Free for All***: it would take a complete catastrophe to disturb the *individualist*'s little ball. Nature is benign – it will not hurt him or her.

- ***Über-egalitarian – Control Freaks***: the *über-egalitarian* is almost a parody of a 60's or 70's socially-conscious individual. The ball is barely being held stable. Nature is ephemeral, about to be overwhelmed at any minute, thirty years ago it was the coming Ice Age, today it is global warming.
- ***Hierarchist - Power Brokers***: the *hierarchist* sees nature as something to be overcome, but manageable. The little ball is stable within 'normal conditions', but extremes are to be avoided. The *hierarchist* is a natural bureaucrat and loves decisions based on sound thinking, however irrational the result. (Mainelli, 2004)

Of the four profiles, when people are in the *über-egalitarian* and the *hierarchist* profile they are most likely to transfer risk onto a third party (an insurance company), though the former will do it out of pure risk aversion, while the latter will probably apply cost-benefit analysis. To some extent *individualists*' willingness to contract insurance is likely to be based on personal experience of certain risks, while *fatalists* will rarely buy insurance.

A third way to look at risk and people is from the viewpoint of insurance companies. On the one hand, people are assessed and categorised according to the risk they represent in a given category in terms of behaviour, based on relevant data points (e.g. age, gender, location, risk history) and predictive analytics. On the other hand, customers also represent risks to insurance companies: risk of fraud for example by faking or exaggerating losses; or, moral hazard, by changing behaviour after getting insurance, thereby increasing their risks (Simon 2000).

People's attitude to risk not only influences their choices on sharing risk with third parties but also their attitudes to change and novelty, including technological innovation. Sections 4.3 and 4.4 below explore how technology and innovation could transform relationships between insured and insurers over time. The above risk-reward people typology is used in section 5.3 to discuss respondents' diverse views on the relevance of blockchain technology and possible applications in insurance.

4.3 Insurance: current and future prospects

This section highlights a few trends relevant to this report where technology could transform relationships between insurance companies and the insured over time. Perhaps the biggest points are that we live in an increasingly global, connected, and crowded world of cities.

The global average age is rising rapidly. Among more developed countries (total population 1.2 billion in 2005), overall median age rose from 29.0 in 1950 to 37.3 in 2000, and is forecast to rise to 45.5 by 2050 (UN Data). Cities are increasingly central to economic growth. In 1900, 14% of the world lived in cities; by 1950, 30%. The 50% mark was crossed in 2008 and demographers estimate 70% by 2050. Over 400 cities host more than a million people with 600 cities expected to generate 65% of global growth by 2020, of which 440 are in emerging markets. This suggests insurance growth potential in emerging markets given increasing urban infrastructure investments and rising consuming classes. Innovation and simplification along the insurance value chain is perhaps more likely in emerging economies. Closer market

segmentation to the city level could also bring benefits especially for large and diverse cities in emerging market economies (Acord and Equinix, Part 1, 2014).

Of the challenges ahead, public trust is one of the biggest challenges faced by the insurance industry (Spencer, 2013: 1). According to PwC's recent study on the lack of trust facing financial services in the UK, only 27% people trust their insurance company (PwC (a), 2014: 3). People tend not to trust what they do not understand. This relates partly to the perceived complexity and lack of clarity associated with insurance policies, with customers failing to understand the key aspects of a policy and how it could add value and meet their needs. Similarly, the insurance industry as a whole suffers from a negative image related to claims processing and settling, often viewed as complex, not always fair and rather lengthy, even though the industry has taken steps over the years to improve their processes. Related to trust, improving customer experience is increasingly becoming a determinant of competitiveness. Putting customers first, knowing them, responding to their long-term needs by taking into account changing attitudes and expectations and by ensuring an adequate quality of service and degree of protection can contribute to positively improving customer experience of insurance (Spencer, 2013; PwC (b), 2014).

Insurance companies have a role to play in educating customers, the public and policy makers about current and future risks. A 2012 industry study highlighted how public perception of risks is not well-informed, suggesting that risk professionals have a role to play in educating and promoting greater awareness of the various risks, present and future, their possible impact and their likelihood, to both the public and policymakers (Franklin (a), 2012). The importance of financial education has repeatedly been highlighted, especially longer-term life-planning aspects such as retirement savings and insurance as a way to help customers make better choices for themselves and their future (see OECD, 2006 for example). Better education on insurance is likely to translate into demand for tailored insurance products and services, thus stimulating new product development. Customers will also be able to better assess the risk-return ratio of products (El Moyanery, 2013).

Risk avoidance and more particularly loss prevention measures are becoming increasingly important and could support a shift in the way industry operates from reactive and remedy-based to a more proactive and preventive insurance model (Acord & Equinix (Part 2), 2014). One way insurers can manage risk is indeed by making customers more prepared through advisory services and economic incentives which could in turn result in avoided claims (Live Work Studio, n.d). Deemed to be in the joint interest of customers and insurers, preventive measures usually translate into reduced premiums for customers as such measures (e.g. driver training programmes) reduce the possibility that a loss will occur or reduce the severity of the possible loss (e.g. a car accident).

Global, connected, and crowded cities are good breeding grounds for innovative risk-sharing applications. This report has already noted a collaborative economy of people trading directly with each other globally on housing and taxis. If consumers trust these economic structures, then it is only a matter of time before applications disintermediate insurers' risk transfer and risk management functions.

4.4 The role of technology and innovation

Technology represents an opportunity to improve insurance industry practices, but also to develop adequate protection and preventive measures in case of failure, especially at scale (Franklin (b), 2012). So far the industry has been perceived to be fairly reactive to technology, to have issues with IT prioritisation and implementation, and ultimately to be relatively slow to innovate and change. "Typically, insurance companies spend 50 to 70% of their IT budget on simply running the business" (Acord & Equinix (b), 2014: 13). Technology has a role to play in improving insurance's position and competitiveness, first through benefits in terms of insurance product distribution channels and interaction with customers, and over time with opportunities for innovation in terms of organisational structure and management, business models and product development, as well as knowing customers better (Spencer, 2013; Acord & Equinix (b), 2014).

Technological modernisation can lead to reduced market costs and access to more business globally. Advanced techniques for data analysis, interpretation and application coupled with greater data flows can support know-your-customer processes as well as insurance product tailoring and development (PwC (b), 2014). Mobile technologies and social media have the potential to transform interactions between insurance companies and customers and to simplify value chain processes and operations. Internet of Things solutions could translate into more accurate data on risks and exposure, and could potentially inform feedback control processes which in turn could result in substantial loss prevention (Light, 2014). Better and more data could lead to far more accurate risk modelling, pricing and thus tailoring of products and services. Over time this could translate into individualised insurance solutions based on individual actions rather than the statistical average of a large group (Gittleson, BBC news, 2013). (Acord & Equinix (b), 2014)

Many technologies are reaching maturity including mobile ICT and social media. It's not the technology *per se* that matters rather how technology is used to change an organisation, its offering and its interactions with customers. Echoing industry respondents on the topic, as data becomes increasingly available, identifying the right data, how it is valuable and how to analyse, interpret and apply it are the deciding factors. As a result, technology and related innovations could greatly transform the nature of insurance and risk pooling. New technologies create (or demand) new business models, including new approaches to engaging with customers, managing risk, claims and even management processes. (Acord & Equinix (b), 2014)

Box 3 – Big Data

Mobile technology, social media and emerging Internet of Things devices and sensors all contribute to increased connectedness and to changing the way we perceive data and its uses. While we are just at the beginning and currently 99% of the objects in the world are still unconnected, this is predicted to change rapidly and to have a huge impact on real-time information.

Big Data is about data. How we produce, consume and engage with data is changing fast along with technology. Information, whether structured, semi-structured or raw data, has the potential to transform business models and processes, and bring benefits to many, including insurers. Data driven solutions can bring benefits and add value in terms of information usage rate; improved accuracy and collection of performance related-data; sophisticated analytics to support decision-making; and, ultimately customer selection and services, as well as product and services (McKinsey 2011).

Three big data trends can be distinguished. First, big data leverages untapped data sources, including newly emerging telematics sensors. Second, big data requires automation technologies to support real-time information collection and analysis. Third, big data is changing the nature of organisational structures and systems towards more adaptable and less vulnerable systems (World Economic Forum, 2014).

Data is already a central asset upon which insurers base their decisions, whether in relation to underwriting, risk management, pricing or claims management. While the industry has made progress in capturing and analysing much of the structured information associated with their products and policyholders, there is value in unstructured and semi-structured information that remains untapped (IBM, 2013; Palmer, 2014). Big Data sources are likely to evolve from internal data (e.g. transactions, log data, events) to encompass external data sources such as social media, telematics devices, external feeds, geospatial, free form text, images and videos (IBM, 2013). As more data becomes available to insurers, including real time data, the use of predictive analytics in insurance will spread and could lead to risk management becoming more efficient and cheaper. This in turn could impact on insurance companies' competitive advantage particularly regarding prospects for business growth, risk management, loss control and customer engagement (IBM, 2013). (Acord & Equinix (b), 2014)

Big Data is not without challenges for companies wishing to embrace such solutions, including in terms of data query or visualisation, or how to manage ever-increasing amounts of data. Big Data solutions also raise issues in terms of data privacy, security and ethics, thus calling for appropriate standards and governance models to oversee data use and applications. (World Economic Forum, 2014)

While technology may bring opportunities for the insurance industry to improve its own practices, it also creates new areas of risk such as data security, privacy and 'new' systemic points of failure. The industry has a role to play by identifying key risks associated with new technologies and by providing economic incentives for users to limit their exposure to the downside risks associated with these. The ability of the insurance industry to provide adequate levels of protection is an important condition for innovation and the dissemination of technology (Franklin (b), 2012).

5 BLOCKCHAINS AND INSURANCE

This chapter explores how blockchain technology could interact with insurance; possible implications in terms of relationship between individuals, insurance and insurers; and current perspectives on the relevance and potential of blockchain technology, based on interview responses and insights gained through event discussions. Section 5.1 provides an overview of emerging and existing blockchain applications which could be relevant to insurance. Section 5.2 analyses the possible implications of applying blockchain technology for insurance along four key dimensions – identity, space, time and mutuality – and ultimately explores how this could affect relationships between individuals and insurance companies over time. Section 5.3 analyses respondents' view on the potential for blockchain technology in insurance (according to the risk reward people typology explored in section 4.2) and provides further considerations for future prospects. Finally, section 5.4 shares concluding thoughts on blockchain technology, its possible applications and suggests areas where further research and experimentation are needed.

5.1 Emerging and conceptual applications

Blockchain technology is said to have potential for financial services application, including insurance, through distributed applications hosted on decentralised platforms, such as: Bitcoin, the first blockchain protocol released in 2009; Ethereum, an open platform which could host distributed applications; or, BitNation, a more recent project which aims to provide financial services applications including insurance (though not much information is yet available).

Distributed applications appear particularly promising in the short term. First, applications could support the automation of insurance products based on betting-like insurance products and financial derivative contracts. Crop insurance is often quoted as an example of hedging mechanism against adverse consequences of bad weather on a farmer's harvest, which could be automated through a smart contract hosted on a blockchain protocol and using an oracle, in this case a trusted weather data feed (Buterin, n.d: 25).

Second, blockchain technology and distributed applications open up the range of assets and information that can be managed and stored on and from the blockchain, some of which can be relevant to insurance. Interesting models include applications to create universal digital IDs (e.g. World Citizenship Passport (McMillan 2014)) or to store genetic and medical record data using for example Genecoin, which allows individuals to securely back up their own DNA by recording it on the blockchain or, DNA.Bits which aims to provide access to large samples of anonymised medical records and genetic data through the blockchain.

Third, new insurance solutions could emerge to handle risks arising from blockchain technology usage (e.g. account hacking on exchange where individuals can buy AltCoins to participate on a blockchain), digital asset protection or even in relation to the security of Internet of Things solutions, depending on demand (i.e. the extent to which individuals want to outsource emerging risks to third party providers) and feasibility.

5.2 Possible implications – identity, space, time, and mutuality

Blockchain technology and related applications could have implications for insurers in four ways – identity, space, time, and mutuality.

Identity

Blockchain technology and related applications could transform the way we manage digital identity (ID), personal information and history. An ID scheme relying on a decentralised blockchain combining a public ledger of records with an adequate level of privacy could rival state-backed identity (which is generally checked against other databases, uses biometric data and is backed by law) in terms of security through decentralisation and cryptography.

Such an identity scheme could help to fill existing gaps in terms of digital identity verification and authentication. Much effort has been invested into systems than can recognise and verify digital IDs. Social media networks are trying to make their accounts a form of ID though these generally fail to meet basic trust requirements as most are issued without verification. A number of digital ID schemes are emerging, including OpenID Connect, a protocol combining an identity layer and an authorisation server, which allows clients of all types (e.g. developers) to request and receive information about authenticated session and end-users across websites and apps without having to own or manage password files. Governments too are trying to set up digital ID systems and authentication processes. The UK for example unveiled in September 2014 Gov.UK Verify, a public services identity assurance programme which uses a network of trusted and vetted third party providers instead of relying on a centralised database, though testing is on-going (Glick 2014). Estonia has been operating a national digital ID scheme for a decade and is now planning to extend application to foreign non-residents, which would in effect separate state-backed ID from location, provided that other countries (e.g. within the EU) recognise it (The Economist, 2014).

The problem lies in providing a digital ID that is trusted and can be used widely. In practice, a blockchain-based identity scheme could take the form of a distributed application hosted on a blockchain protocol which could use arbitrators (i.e. pre-determined experts authenticating documents or information submitted) or oracles allowed to cross-reference information securely with other data sources (including governmental ones). The application could enable additional functions including personal data storage, authorised access frameworks for external providers or even reputation ratings. Functionalities intended to realise the value of private data are already being developed (for example Meeco, a private data management solution on an ad-free platform). Combining authentication and personal data management functionalities with decentralised and secure blockchains could lead to new frameworks for identity management. If successful, such an identity scheme could remove government monopolies on managing their citizens' identities and data. Further, it could empower individuals to store and manage their data, including access to their personal history records.

Recent events in the blockchain ecosystem have led to the Windhover Principles for Digital Identity and Trust, an open digital framework introduced in October 2014 by

the Institute for Data Driven Design (ID3[6]) and over twenty digital currency firms. Rooted in the belief that individuals should have control of their digital personal identities and personal data, the Principles aim "to ensure secure personal identity, trust and access to shared open data on the Internet" and to encourage self-governance solutions such as DAOs (ID3, 2014). In relation to the Principles, the Open Mustard Seed (OMS[7]) platform, a self-deploying and self-administrating infrastructure layer for the Internet, will allow to iteratively test, implement and deploy granular technical solutions to trust, privacy and governance. The Principles are thought as a first step towards enabling individuals not only to control their identities and data but also to comply with regulatory requirements such as anti-money laundering and know-your-customer requirements in the case of AltCoins and other blockchain-based applications, in an effort to address concerns and criticisms over privacy, security and transparency with existing schemes.

Personal identity verification, authentication and data management could bring significant benefits for many sectors. In insurance, the streamlining of digital authentication and better management of personal data and history disclosure could translate into more direct and efficient relationships between insurance companies and individuals. Over time, this could bring additional benefits by reducing identity and claim frauds.

At a time where access and control over one's own data is becoming increasingly sensitive, empowering individuals to store, update and manage access to their data seems rather appealing, particularly in relation to healthcare. In a recent article, Melanie Swan explored four ways in which blockchain technology could be used for health-related applications, three of which relate to information management. First, blockchain could facilitate the storage and administration of personal health records, and help individuals to manage permissions for third parties such as doctors to access. Second, the blockchain could support the emergence of health research commons, whereby personal health records stored on the blockchain are aggregated and users contribute on a voluntary basis, taking advantage of the pseudonymous nature of the blockchain. Third, the blockchain could perform health-related notary functions by confirming the existence of health-related information such as proof of insurance, test results, prescriptions, referrals, conditions and more (Swan (a), 2014). This type of data-driven distributed solution could also be beneficial to insurance companies, products and processes.

Space

Blockchains are distributed across networks of computers, themselves distributed across space. Blockchain technology has the potential to shape different interactions between individuals and places, further blurring the divide between local and global. Blockchain technology and related applications can be global in scope and in scale as to some extent the only requirement from a user perspective is to have a computer, an Internet connection and eventually a credit card to buy AltCoins. At the same time, blockchain applications can cater to the specific needs of individuals in set locations.

[6] A non-profit founded out of MIT Media Lab - https://idcubed.org/
[7] https://idcubed.org/open-platform/platform/ and https://docs.openmustardseed.org/

This dual relationship with space could support the tailoring of insurance products in two ways: by expanding the range of insurance products across space and by adjusting insurance coverage and pricing depending on location and time. The former could contribute positively to financial inclusion with some products becoming available where they were previously not, for example in places where there is not sufficiently strong market demand or enough quality data (e.g. creditworthiness). The latter suggests that the integration of blockchain applications as part of 'Big Data' solutions, including managing interconnected devices at distance (Internet of Things), could lead to nearly instantaneous adjustments of insurance coverage and pricing through more comprehensive datasets and advanced analytics across space (and time – see below). This could in turn lead to additional efficiency gains.

Insurance business models are fairly centralised and anchored spatially (e.g. by insurance provider, by country, by market, by region). Blockchain technology could 'de-localise' towards models of peer-to-peer and mutual insurance where location is both more and less material. Less material in that people can contract with each other round the globe using robust technology. More material in that people can handily set up local insurance vehicles easily. The mid-ground might be many local vehicles sharing global reserving or reinsuring facilities.

Time

Blockchain technology 'time stamps' transaction records and records 'values' (debts) over long periods of time on the blockchain. Two interactions between blockchain and time appear worth distinguishing here. First, blockchain technology is likely to exacerbate the range of time and increase the number of possibilities, for example by fragmenting contractual time to the second and by allowing multiple product combinations. As outlined before, distributed applications and the prospect they offer in terms of self-administration could translate into real-time adjustments to insurance coverage and policies. Further, blockchain technology opens the way to insurance products with varying time horizons such as short-term or time-specific insurance contracts. As a result blockchain technology could shorten time cycles and have implications in terms of insurance products tailoring across time.

Second, and to some extent in contradiction with the former, blockchain technology lengthens time by introducing a sense of immutability, as transactions records persist as long as the blockchain persists. Records cannot be altered over time, though their content (i.e. what is recorded in the transaction) can move around. For example, the information pertaining to an asset being recorded on the blockchain cannot be altered and remains indefinitely, though that asset might be transferred to another user or function. The probable persistence and accuracy of those records might alter people's views of longer-term contracts.

Respondents suggested that self-administration of risk protocols through distributed applications could have implications in terms of insurance coverage adjustments across time and space. Respondents highlighted however that the primary challenge lies in finding the right 'insurance' model based on the blockchain and that experimentation in this context is more likely to start with more common and well-known risks (e.g. car accident) and related insurance products (e.g. car insurance),

or extensions to such risks, e.g. the collaborative economy bringing private automotives and houses into the commercial sector[8].

Mutuality

Blockchain technology could favour the emergence of alternative risk management models shifting away from risk pooling, the predominant model in insurance. Such blockchain-based risk management models could include self-managed or administered risk protocols, peer-to-peer insurance platforms and even fully funded solutions.

Blockchain-based solutions could help to automate and achieve efficiency gains by using smart contracts, which in turn could lead to self-administration of certain insurance products, such as betting-like insurance products or hedging mechanisms (e.g. crop insurance). As mentioned before, changes in input data could therefore automatically be reflected in premium and coverage across space and time. Some respondents suggested that over time disintermediation could take place as a result of automation, particularly for well known and perhaps more common risks.

Blockchain technology could support the rise of peer-to-peer insurance platforms and thus contribute to enabling self- and mutual- risk management frameworks. Distributed mutualisation combined with the 'wisdom of crowds' could support efficient claim management and fraud reduction. Further, such insurance mini-mutuals might increase the need and spread but perhaps reduce the size of typical reinsurance. Some respondents mentioned how blockchain technology could enable modern versions of 'Protection & Indemnity Clubs' (see box 4 on the next page) where the blockchain provides a platform for participants to take on pre-determined risk and manage it, possibly in conjunction with expert advice. As a result, in such instances, insurance companies' role is likely to evolve from that of risk handlers to one of risk management advisors.

Blockchain-based insurance solutions could in theory blossom into fully funded blockchains. A set of rules would be written and set up as a DAO. Premiums would be paid and recorded on the blockchain, and claims payments and surplus distributions would equally be paid through the blockchain. Prescribed rules and scripts under certain conditions would lock and unlock funds. This is not a likely scenario in the near-term, but one could imagine a DAO contained in a completely automated blockchain. Customers would no longer rely on intermediaries, rather wholly on the technology and its persistence. As an example, insurers handle asset and investment management in order to assume risk. The insurer is an 'institutional agent' for the shares of policy-holders and under pressure by activists to vote shares. DAO tools such as 'coloured coins' could let policyholders exercise voting rights in listed equity investments or to shape investment strategies for the institutional agent.

[8] A UK review of the collaborative economy, "Unlocking the Sharing Economy" by Debbie Wosskow published by the UK Department for Business, Innovation & Skills in November 2014 revealed that insurance product development needs to encompass collaborative economy services so that more consumers not only have peace of mind but are more likely to use collaborative services (Wosskow, 2014)

Box 4 – Protection & Indemnity insurance

Protection & Indemnity (P&I) insurance is a form of international maritime insurance providing cover for its ship-owner and chartered members against third party liabilities relating to the use and operation of ships through a P&I club, an independent non-profit making mutual insurance. P&I clubs emerged in the mid-1800s as an attempt to fill the gap of conventional insurance to cover third party claims.

P&I clubs cover a wide range of liabilities including personal injury to crew, passengers and others on board, cargo loss and damage, oil pollution, wreck removal and dock damage. Clubs also provide a wide range of services to their members on claims, legal issues and loss prevention, and often play a leading role in the management of casualties. In the event of a claim and before it can be compensated, the claim is inspected carefully, has to be lawful and not covered by other types of insurances, all other conditions being met.

P&I clubs are typically formed of ship-owners and ship operators, who undertake rigorous process to join. Each year, all members must pay a certain amount in. If the claims exceed the pooled money, the members of the club must add supplementary money. If there is surplus money, it gets returned to the members or applied toward a future year. Unlike most insurance, there are no outside stakeholders to answer to and P&I clubs are not for profit.

P&I clubs are still very much in use today, particularly in the United Kingdom, Japan, United States, and Scandinavia. There are 13 major clubs that account for 90% of the world's sailing tonnage. While there is no global regulation requiring all ships to be covered by P&I club insurance, the European Union adopted EU Directive 2009/20/EC on the insurance of ship-owners for maritime claims which requires all ships travelling in EU waters to have some form of P&I insurance as of January 2012 (European Union, 2009).

[Main source: International Group of P&I Clubs]

Blockchain technology may not revolutionise the way insurance operates. Nonetheless, it is likely to support wider trends of financial inclusion and new models of interactions between individuals and service providers including insurers. As a result, the technology and its applications could eventually contribute to changing the role and function of insurers in society. Blockchain technology and distributed applications could for example support access to affordable and quality insurance products through distributed micro-insurance solutions combined with mobile technologies; or, by extending insurance product coverage to previously excluded populations, provided that adequate identity and information management functionalities (e.g. notary or personal data management function) are in place.

Taking the concept of decentralised blockchain operated platforms further could lead to the emergence of decentralised marketplaces where insurance companies compete to meet the needs and requirements of clients or groups of clients whether in terms of insurance products or risk management expertise and advice. Such blockchain-based marketplaces could also emerge for other types of services

including healthcare i.e. with doctors and health facilities competing to meet the needs of clients-patients in terms of treatment. Distributed identity and reputation systems (e.g. distributed ratings) could add useful functionalities to this type of platforms for example by improving transparency both ways, in terms of accurate disclosure from individuals to insurance companies and the other way around by enabling greater accountability of insurance companies to customers and regulators.

As people become more educated about risk (e.g. through Internet-based resources), technology, such as blockchains, can contribute to empowering them to manage certain risks directly. Should this materialise at scale, the shift in insurers' role from risk handler to expert advice and knowledge provider in relation to direct risk management (including preventive measures) is likely to be reinforced.

5.3 Opportunities for transformation

We can apply the risk reward people typology explored in section 4.2 to the diversity of views on blockchain and insurance encountered during this research project. The *fatalist* does not anticipate any particular change arising from the use of blockchain technology and even questions the relevance of the technology and asks what it would improve that does not already exist. Automated processes and self-administered payments for example already exist in certain areas of financial services and do not necessarily require blockchain technology to function. The *hierarchist* is generally more open to blockchain technology and sees how it could deliver efficiency gains to the industry and customers through automation, increased competition and eventually new products in relation to digital assets and Internet of Things solutions. Accordingly, blockchain technology applications could lead to incremental changes, though suitable regulation is required. Finally, the *individualist* and the *über-egalitarian* think of the blockchain technology and related applications as something that could radically change the nature and scope of the insurance industry, through disintermediation of the industry, the emergence of new actors including distributed peer-to-peer insurance platforms, trends encouraging and empowering self-management of risk and thus contributing to changing the role of insurers to advisors on how to manage risk. For the *individualist* the blockchain is an exciting and positive development. For the *über-egalitarian* it is a dangerous technology which will incur unintended consequences.

To be fair, most respondents shared the *hierarchist* view. In the short to the medium term, and based on interview responses, blockchain technology and related applications seem to offer interesting prospects in relation to identity and data management; insurance product development and tailoring; and, big data and data integrity solutions. In the event that blockchain technology takes off and insurance-related applications emerge, this could well open the market to new third party providers other than insurers and support the emergence of peer-to-peer insurance platforms but some degree of centralisation is likely to stay and disintermediation does not seem very realistic.

Bitcoin, the first blockchain, only dates back to 2009 and is probably the result of years of research. While blockchain technology offers interesting prospects, existing uncertainties and unknowns regarding the technology itself, surrounding regulation and the feasibility of related applications being discussed and explored, cast doubt

over the potential for blockchain technology to significantly transform the way the insurance industry operates in the near term.

Blockchain technology adoption and the development of related applications in insurance is likely to depend on insurance readiness and appetite. So what about insurers' views of blockchain technology? Respondents from this sector suggested that blockchain technology seemed to be most promising as a decentralised payment system at this stage. Insurance players and their digital innovation units in particular seemed interested and willing to learn more about the technology, though not yet ready to embrace it. When asked about the potential for applying blockchain technology to insurance beyond payment system applications, respondents felt that most other applications presently being explored (including distributed applications for identity and personal data management) were not imminent.

Blockchain technology in insurance is likely to start with the use of smart contracts; the use of blockchain as custodian depositories; and the development of digital integrity applications in relation to identity, data and history over time. Down the line, blockchain applications could support insurance product development and tailoring as well as the collection, assessment and management data, in relation to advanced analytics and Internet of Things solutions. Ultimately, how blockchain and related applications evolve will depend on people's risk/reward appetites. Insurance companies do not seem ready to experiment. Outsiders may be the first to create initial insurance applications but eventually if the rewards arrive, insurance companies are likely to integrate such start-ups and begin changing themselves.

5.4 Concluding thoughts

> "*Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate*." (Marc Andreesen (co-author of Mosaic, co-founder of Netscape, and Bitcoin investor), 2014)

Blockchain technology offers prospects for multiple applications whether financial, semi-financial or non-financial. There is a broad range of 'blockchainable' items, beginning with currency and leading to just about any registry, many trusted third party roles, wider databases, and many forms of information services.

Blockchain technology is new and further experimentation is inevitable. Blockchain technology developments continue in an open-source setting within a connected and dynamic community. There is scope for further exploration and research regarding the technology itself. For example, we would welcome exploration of alternative rewards for block validation and constructing private blockchain protocols.

Wider issues to be considered include:

- the economics of the technology, particularly mining decentralisation and scalability;
- regulation, with calls for self-regulation or standard-based regulation but also for regulatory certainty; and,

- education and awareness, making it easier for non-expert audiences to understand the benefits and risks, as well as use the technology appropriately and safely.

Any financial services professional should be excited at a technology that simultaneously improves integrity and security while also reducing costs. When a technology reduces production costs rapidly, e.g. the printing press and book publishing, production flourishes. We expect to see a proliferation of blockchain applications in financial services, including insurance. We hold some hope that these applications have the potential to make insurance work better for consumers and society.

Appendix 1 – Acknowledgements

We received enthusiastic cooperation from everyone involved in this project. Some help was given at several open presentations followed by discussion. Some help was given confidentially. We would like to thank the people involved in events and those who agreed to semi-structured interviews. Without assigning any responsibility for our conclusions, nor any endorsement of our work, people working at the following organisations were particularly helpful to us and we thank them:

AMNT
Australian Centre for Financial Research
BitcoinByte
BNY Mellon
British Computer Society
Berkman Centre for Internet & Society
Bitcoin Education Project
Bloomberg
Boston College
Capital Eight
CERSA CNRS Université II Paris
Chartered Institute for Securities & Investment
CompliCoin
Consult Hyperion
Citi
City of London Police
City University
CryptoComposite
Dietrich-Bonhoeffer-Berufskolleg
Direct Line Group
DVFA
Ebix UK
Efficienarta
Elliptic
Endava
Ensanda
ERIS / Project Douglas
EY
Estates Investment Exchange
Ethereum
Global Advisors (Jersey)
Hiscox
HSBC
Hyperledger
IBM UK
Identifi
iGTB
Interxion
Isle of Man
Lily Innovation Advisors
Lloyd's of London
London School of Economics
MaidSafe
Microexchanges
Misys Financial Software
MIT Media Lab
New Economics Foundation
NewFinance
Nordic Enterprise Trust
Northern Trust
NSW Fair Trading
Oliver Rothschild Corporate Advisors
OSTC
Pembroke Partnership
Preferred Global Health
PwC UK
RFIB
RGA UK Services Limited
States of Alderney
Suncorp Group
Swiss Finance Institute
SwissRe
The Resourceful Company
The City UK
UCL ISRS
Ultimate Risk Solutions
United Kingdom Digital Currency Association
William Garrity Associates Ltd
Willis

Appendix 2 – Glossary

[Sources – Oleg Andreev's glossary on GitHub and Andreas M. Antonopolous' "Mastering Bitcoin"]

AltCoin: Decentralised (crypto)currency based on a distinct blockchain protocol, usually developed from a copy (or fork) of the Bitcoin source code, though some are developed from scratch. The first AltCoin – IXCoin – was launched in August 2011.

Blockchain: A public ledger of all confirmed transactions in a form of a tree of all valid blocks (including orphans). Most of the time, 'blockchain' means the main chain, a single most difficult chain of blocks. The blockchain is updated by mining blocks with new transactions. Unconfirmed transactions are not part of the blockchain.

Cryptocurrencies: digital technologies for debt exchange that rely on cryptography and decentralised peer-to-peer networking (Mainelli and McDowall, 2014).

Decentralised autonomous organisations: algorithmically-governed programme that, in using trustless decentralised computing, can serve as a way to formalise multilateral relationships or transactions outside of traditional legal architectures (McKinnon, Kulman et Byrne, 2014: 1). Essentially, DAOs are more sophisticated types of smart contracts involving shareholders or members; a governance system allowing collective decisions on how the organisation should allocate its funds; and a way for the DAO to fund itself either through the sale of services or through endowments.

Double spend: A fraudulent attempt to spend the same transaction output twice. There are two major ways to perform a double spend: reverting an unconfirmed transaction by making another one which has a higher chance of being included in a block (only works with merchants accepting zero-confirmation transactions) or by mining a parallel blockchain with a second transaction to overtake the chain where the first transaction was included.

Fork: Refers either to a copy of a source code (to create an AltCoin-driven protocol based on an existing protocol code) or, more often, to a split of the blockchain when two different parts of the network see different main chains. In a sense, fork occurs every time two blocks of the same height are created at the same time. Both blocks always have the different hashes (and therefore different difficulty), so when a node sees both of them, it will always choose the most difficult one. However, before both blocks arrive to a majority of nodes, two parts of the network will see different blocks as tips of the main chain.

Full node: A node which implements all of a blockchain protocol (e.g. Bitcoin) and does not require trusting any external service to validate transactions. It is able to download and validate the entire blockchain. All full nodes implement the same peer-to-peer messaging protocol to exchange transactions and blocks, but that is not a requirement. A full node may receive and validate data using any protocol and

from any source. However, the highest security is achieved by being able to communicate as fast as possible with as many nodes as possible.

Genesis block: A very first block in a blockchain with hard-coded contents and an all-zero reference to a previous block. For Bitcoin, the genesis block was released in January 2009.

Halving: Refers to reducing the monetary reward for blockchain protocols like Bitcoin which rewards miners with newly minted AltCoins. For Bitcoin, halving occurs every 210,000 blocks (approximately every four year). Since the Bitcoin genesis block to a block 209999 in December 2012 the reward was 50 BTC. Until 2016 it will be 25 BTC, then 12.5 BTC and so on until 1 satoshi around 2140 after which point no more bitcoins will ever be created. Due to reward halving, the total supply of bitcoins is limited: only about 2100 trillion satoshis will ever be created.

Hash function: Takes a group of characters (called a key) and maps it to a value of a certain length (called a hash value or hash). The hash value is representative of the original string of characters, but is normally smaller than the original. Hashing is done for indexing and locating items in databases because it is easier to find the shorter hash value than the longer string. Hashing is also used in cryptographic encryption.

Lightweight client (or node): Compared to a full node, lightweight node does not store the whole blockchain and thus cannot fully verify any transaction. There are two kinds of lightweight nodes: those fully trusting an external service to determine wallet balance and validity of transactions (e.g. blockchain.info) and the apps implementing Simplified Payment Verification (SPV). SPV clients do not need to trust any particular service, but are more vulnerable to a 51% attack than full nodes.

Meta-chain: software layers implemented on top of Bitcoin implementing a platform/protocol overlay inside the bitcoin system.

MetaCoin: software layers implemented on top of Bitcoin implementing a currency-inside-a-currency.

Mining: Process of adding transaction records to a blockchain. Mining confirms to the rest of the network that unique transactions have taken place. (Swan (b), 2014)

Mining pool: service that allows separate owners of mining hardware to split the reward proportionally to submitted work. Since probability of finding a valid block hash is proportional to miner's hash rate, small individual miners may work for months before finding a big per-block reward. Mining pools allow steadier stream of smaller income. Pool owner determines the block contents and distributes ranges of nonce values between its workers. Normally, mining pools are centralised. P2Pool is a fully decentralised pool.

Nonce: Stands for ‘number used once’. A 32-bit number in a block header, which is iterated during a search for proof-of-work. Each time the nonce is changed, the hash of the block header is recalculated. If the nonce overflows before valid proof-of-work is found, an extra nonce is incremented and placed in the coinbase script. Alternatively, one may change a merkle tree of transactions or a timestamp.

Private key: A 256-bit number used in ECDSA algorithm to create transaction signatures in order to prove ownership of certain amounts of bitcoins or other AltCoins. Private keys are stored within wallet applications and are usually encrypted with a pass phrase. Private keys may be completely random or generated from a single secret number ("seed").

Public key: Usually it is represented by a pair of 256-bit numbers ("uncompressed public key"), but can also be compressed to just one 256-bit number (at the slight expense of CPU time to decode an uncompressed number). A special hash of a public key is called address. Typical Bitcoin or AltCoin transactions contain public keys or addresses in the output scripts and signatures (or Private Keys) in the input scripts.

Proof of Work: a number that is provably hard to compute. That is, it takes measurable amount of time and/or computational power (energy) to produce. In Bitcoin it is a hash of a block header. A block is considered valid only if its hash is lower than the current target (roughly, starts with a certain amount of zero bits). Each block refers to a previous block thus accumulating previous proof-of-work and forming a blockchain.

Proof of Stake: system by which existing owners of a currency can 'stake' currency as interest-bearing collateral. Somewhat like a Certificate of Deposit (CD), participants can reserve a portion of their currency holdings, while earning an investment return in the form of new currency (issued as interest payments) and transaction fees.

Smart contract: Self-administered contracts or scripts built on top of a blockchain protocol and enforced in a distributed way when certain pre-defined conditions are met.

SHA 256: SHA stands for Secure Hashing Algorithm and describes algorithms that generate cryptographically secure one-way hash (also referred to as a message digest). SHA algorithms can produce message digests or hashes of different size. The number next to the acronym indicates the number of bits, in this case 256 bits.

Wallet: An application or a service that helps keeping private keys for signing transactions. Wallet does not keep bitcoins or AltCoins themselves as they are recorded in the blockchain. "Storing bitcoins" usually means storing the keys.

Web wallet: A web service providing wallet functionalities including the ability to store, send and receive AltCoins. User has to trust counter-party to keep their AltCoins securely and ready to redeem at any time. It is very easy to build your own web wallet, so most of them were prone to hacks or outright fraud. The most secure and respected web wallet is *Blockchain.info*. Online exchanges also provide wallet functionality, so they can also be considered web wallets. It is not recommended to store large amounts of bitcoins in a web wallet.

Appendix 3 – Bibliography

Acord & Equinix. *Challenge to Change Part 1: Embracing the Economy, Poeple and the Future of Insurance.* Industry report, Equinix, 2014, 1-17.

Acord & Equinix. *Challenge to Change Part 2 - The Impact of Technology.* Industry report, Equinix, 2014, 1-18.

Acord & Equinix. *Challenge to Change Part 3 - The Future of Insurance.* Industry report, Equinix, 2014, 1-19.

Adams, John. *Risk.* Psychology Press, 1995.

Allaire, Jeremy. "Thoughts on the New York BitLicense Proposal." *Circle.* 13 August 2014. (accessed Novemebr 14, 2014).

Andersen, Gavin. "A Scalability Roadmap." *Bitcoin Foundation (Blog).* 6 October 2014. (last accessed November 20, 2014).

Andreesen, Marc. "Why Bitcoin Matters". *DealBook. The New York Times*. 21 January 2014. (last accessed November 20, 2014)

Antonopoulos, Andreas M. *Mastering Bitcoin.* O'Reilly Media Inc., 2014.

Aron, Jacob. "Bitcoin: How Its Core Technology Will Change The World." *New Scientist*, February 2014.

Back, Adam, et al. "Enabling Blockchain Innovations with Pegged Sidechains." White paper, Blockstream, 2014, 1-25.

Baranoff, Etti, Patrick L. Brockett, and Yehuda Kahane. "1.3 Attitudes towards Risk." In *Risk Management for Entreprises and Individuals v 1.0*, by Etti Baranoff, Patrick L. Brockett and Yehuda Kahane. Flat World Education, 2014.

Bazdarevic, Nejra. "Notre Sphère Privée Est Morte: Entretien avec Alexis Roussel." *InvestNews*, September 2014: 20-22.

Benedict, Kevin, and Peter Abatan. "Insurance Disrupted - Crowdsourced Policies and Social Marketing." Cloud Computing Journal, 19 May 2014.

Birch, David G.W. "What Does Cryptocurrency Mean For The New Economy." In *Handbook Of Digital Currency*. To be published.

Bitcoin Project. "How Does Bitcoin Work?" *Bitcoin Project.* (last accessed November 20, 2014).

Bitcoin Wiki. "Scalability." *Bitcoin Wiki.* (last accessed November 20, 2014).

Blockchain Info. "Size of the Bitcoin blockchain." *Blockchain Info.* (last accessed November 20, 2014).

Cooper, Malcolm. "In Search of the Eternal Coin: A Long Finance View of History". Long Finance. March 2010. 1-30.

Bollen, Rhys. "The Legal Status of Online Currencies: Are Bitcoins the Future?" *Journal of Banking and Finance Law and Practice* (Thomson Reuters) 24, no. 4 (December 2013): 272-293.

Brown, Richard G. "Cryptocurrency Products and Services will Determine Adoption of the Currency - Not the other Way Around." *Richard Gendal Brown - Thoughts on the Future of Finance.* Blog. 5 October 2014.

—. "The Latest In Cryptocurrencies." Presentation. Financial Services Club. 6 October 2014.

Bruce, J.D. "The Mini-Blockchain Scheme." 2014, 1-13.

BTC Guild. "BTC's Guild's Mitigation Plan." *Bitcoin Forum.* 5 April 2013. (last accessed November 20, 2014).

Buterin, Vitalik. *Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform* . White Paper, Ethereum, Ethereum.

—. "What Proof of Stake Is And Why It Matters." *Bitcoin Magazine.* 26 August 2013.

Coinbase. "Comments on Proposed Rulemaking regarding Regulation of the Conduct of Virtual Currency Businesses - DFS-29-14-00015-P." San Francisco: Coinbase, 28 August 2014.

De Filippi, Primavera. "Legal Framework For Crypto-Ledger Transactions." 2014.

—. "Tomorrow's App Will Come From Brilliant (And Risky) Bitcoin Code." *Wired*, March 2014.

De Filippi, Primavera, and Raffaele Mauro. "Ethereum: the Decentralised Platform that Might Displace Today's Institutions." *Internet Policy Review* (Alexandre von Humbolt Institute for Internet and Society), August 2014.

El Monayery, Rania. "Insurance Awareness." *The Macrotheme Review* 2, no. 7 (Winter 2013): 147-155.

European Union (Parliament and Council). "DIRECTIVE 2009/20/EC on the insurance of shipowners for maritime claims." 23 April 2009.

Faggart, Evan. "Bitcoin Mining Centralization: the Market is Fixing Itself." *Coin Brief.* 18 June 2014. (last accessed November 20, 2014).

Fargo, Scott. "Falling Bitcoin Price is the Perfect Storm for Centralization of Bitcoin Mining." *CCN.* 23 September 2014. (last accessed November 20, 2014).

Franklin, Ben (a). *Future Risk: How technology could make or break our world.* Industry report, The Chartered Insurance Institute, 2012, 1-40.

Franklin, Ben (b). *Future Risk: Insuring for a stronger world.* Industry report, The Chartered Insurance Institute, 2012, 1-32.

GHash.IO. "Bitcoin mining pool GHash.IO is preventing accumulation of 51% of all hashing power." *GHash.IO.* 2014. (last accessed November 20, 2014).

GitHub. "Blockchain Based Proof Of Work." *GitHub.* March 2014. (last accessed November 20, 2014).

Gittleson, Kim. "How Big Data is changing the cost of insurance." *BBC news.* BBC news, 15 November 2013.

Glick, Bryan. "GDS unveils 'Gov.UK Verify' public services identity assurance scheme." *ComputerWeekly.* 16 September 2014. (last accessed November 20, 2014).

Goldman, Sachs & Co. "All About Bitcoin." *Top of Mind*, 11 March 2014: 1-25.

Grigorik, Ilya. "Minimum Viable Block Chain." *Igvita.* 5 May 2014. (last accessed November 20, 2014).

Hajdarbegovic, Nermin. "IBM Sees Role for Block Chain in Internet of Things." *CoinDesk.* 10 September 2014. (last accessed November 20, 2014).

Houses of Parliament, Parliamentary Office of Science & Technology. "Alternative Currencies." *PostNote*, August 2014.

IBM. *Analytics: The real-world use of big data in insurance.* Industry report, IBM, 2013.

ID3. "21 Top Bitcoin and Digital Currency Companies Endorse New Digital Framework for Digital Identity, Trust and Open Data". Press release. 20 October 2014.

Kaminska, Izabella. "The Problem With Bitcoin." *FT Alphaville*, 3 March 2013.

Kaminsky, Dan. "Let's Cut Through the Bitcoin Hype: A Hacker-Entrepreneur's Take." *Wired*, 3 May 2013.

Knight, Christopher, and Alan Butler. *Civilization One: The World Is Not As You Thought It Was.* Watkins Publishing, 2004.

Ledra Capital. "Bitcoin Series 24: The Mega-Master Blockchain List." *Ledra Capital.* Antonis Polemitis. 11 March 2014. (last accessed November 20, 2014).

Light, Donald. *The Internet of Things and Property/Casualty Insurance.* Industry report, Celent, 2014, 1-18.

Live Work Studio. "Insurance: Nobody Wants a Claim." *Live Work Studio.* (last accessed November 20, 2014).

Mainelli, Michael. "Personalities of Risk/Rewards: Human Factors of Risk/Reward and Culture." *Journal of Financial Regulation and Compliance* (Henry Stewart Publications) 12, no. 4 (November 2004): 340-350.

Mainelli, Michael, and Bob McDowall. "Building Bit - What's A Poor Government To Do About AltCoins." *Banking Technology* (Informa plc), April 2014: 30-33.

McAleese, Mary, President of Ireland, Remarks to the European Insurance Forum, RDS Concert Hall, Dublin, 30 March 2010

McKinnon, Dennis, Casey Kulman, and Preston Byrne. "Eris - The Dawn of Distributed Autonomous Organizations and the Future of Governance." *Humanity + Magazine*, 17 June 2014.

McKinsey. *Big data: The next frontier for innovation, competition and productivity.* Industry report, McKinsey Global Institute, 2011, 1-156.

McMillan, Robert. "Hacker Dreams Up Crypto Passport Using the Tech Behind Bitcoin." *Wired*, 30 October 2014.

Meetup. *Bitcoin Meetup Groups.* November 2014. (last accessed November 20, 2014).

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." White paper, 2009, 1-9.

New York State Department of Financial Services. "NY DFS releases proposed BitLicense Regulatory Framework for Virtual Currency Forms." *NY DFS.* 17 July 2014. (last accessed November 20, 2014).

Nielsen, Michael. "How the Bitcoin protocol actually works." *Data-driven intelligence.* 6 December 2013. (last accessed November 20, 2014).

OECD. *The Importance of Financial Education.* Policy Brief, OECD, 2006, 1-6.

Palmer, Danny. "Insurance industry 'behind' on harnessing big data." *Computing News.* Computing News, 18 August 2014.

Prensky, Marc. "Digital Natives, Digital Immigrants". *On the Horizon*. MCB University Press. Volume 9, No 5. October 2001

PwC. *Stand Out For The Right Reasons: How Financial Services Lost Its Mojo and How It Can Get It Back.* Industry report, PwC, 2014, 1-16.

PwC. *Top Issues: The Insurance Industry in 2014.* Industry report, PricewaterhouseCoopers LLP, 2014, 1-44.

Reitman, Rainey. "Beware the BitLicense: New York's Virtual Currency Regulations Invade Privacy and Hamper Innovation." *Electronic Frontier Foundation.* 15 October 2014. (last accessed November 20, 2014).

Rosenfeld, Meni. "Overview of Colored Coins". 4 December 2012. (last accessed November 20, 12014)

Schwartz, David, Noah Youngs, and Arthur Britto. *The Ripple Protocol Consensus Algorithm.* White paper, Ripple Labs Inc 2014, Ripple Labs Inc., 2014, 1-8.

Scott, Brett. "Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain." *E-International Relations.* 1 June 2014.

Simon, Gary. "Insurance: Risk Sharing - Presentation at the Stern School." New York: New York University , 5 March 2000.

Skinner, Chris. "There Is No Next Big Thing... Get Over It." *Financial Services Club Blog.* 25 September 2014.

Spencer, Robin. "General Insurance in the Twenty-First Century: Meeting the Challenges." *CII Thinkpiece*, May 2013: 1-4.

Swan, Melanie (a). "Blockchain Health - Remunerative Health Data Commons & HealthCoin RFPs." Institute for Ethics and Emerging Technologies. Blog. 29 September 2014.

— (b). "Blockchain: The Information Technology of the Future." Compiled by Bitcoin Meetup. 1 October 2014.

— (c). "Decentralised Money: Bitcoin 1.0, 2.0, and 3.0." *Institute for Ethics & Emerging Technologies.* 11 November 2014. (last accessed November 20, 2014).

Szabo, Nick. "Smart Contracts: Building Blocks for Digital Markets." *Extropy* , no. 16 (1996).

The Economist. "Estonia Takes the Plunge: A National Identity Scheme Goes Global." *The Economist.* 28 June 2014.

The Telegraph. "Bitcoin exchange MtGox 'faced 150,000 hack attacks every second'." *The Telegraph.* 09 March 2014.

Vasin, Pavel. *BlackCoin's Proof-of-Stake Protocol v2.* White paper, White paper, 2014.

Warren, Jonathan. *Bitmessage: A Peer-to-Peer Message Authentication and Delivery System.* White paper, Bitmessage, 2012, 1-5.

Woo, David, Ian Gordon, and Vadin Iaralov. *Bitcoin: A First Assessment.* Bank of America Merrill Lynch, Bank of America Merrill Lynch, 2014, 1-10.

World Economic Forum. *The Global Information Technology Report 2014: Chapter 1.5 Managing the Risks and Rewards of Big Data.* Industry report, World Economic Forum, 2014, 61-66.

Wosskow, Debbie. *Unlocking The Sharing Economy: An Independent Review*. UK Department for Business, Innovation and Skills. November 2014.

Z/Yen Group. *Capacity, Trade and Credit: Emerging Architectures for Money and Commerce*. Industry report. Z/Yen Group, London, UK: City of London Corporation, ESRC and Recipco. 2011. 1-196.

Zerocash. "How Zerocash works." *Zerocash.* 2014. (last accessed November 20, 2014).

Websites

2014. Agora Voting (last accessed November 20, 2014).

2014. Bitcoin (last accessed November 20, 2014).

2014. Bitcoin Foundation (last accessed November 20, 2014).

2014. Bitcoin Magazine (last accessed November 20, 2014).

2014. Bitcoin Properly (last accessed November 20, 2014).

2014. Bitcoin wiki (last accessed November 20, 2014).

2014. BitLegal (last accessed November 20, 2014).

2014. Bitmessage (last accessed November 20, 2014).

2014. Bitnation (last accessed November 20, 2014).

2014. Bitshares (last accessed November 20, 2014).

2014. BlackCoin (last accessed November 20, 2014).

2014. Blockchain Info (last accessed November 20, 2014).

2014. CoinDesk (last accessed November 20, 2014).

2014. Code for Progress (last accessed December 17, 2014).

2014. Colored coins (last accessed November 20, 2014).

2014. Common Accord (last accessed November 20, 2014).

2014. Counterparty (last accessed November 20, 2014).

2014. DNA.Bits (last accessed November 20, 2014).

2014. ERIS (last accessed November 20, 2014).

2014. Ethereum (last accessed November 20, 2014).

2014. Genecoin (last accessed November 20, 2014).

2014. GitHub (last accessed November 20, 2014).

2014. Institute for Data Driven Design (last accessed December 10, 2014).

2014. International Group of P&I Clubs (last accessed November 20, 2014).

2014. Long Finance (last accessed December 17, 2014).

2014. Monegraph (last accessed November 20, 2014).

2014. OpenID Connect (last accessed November 20, 2014).

2014. Project Douglas (last accessed November 20, 2014).

2014. Proof of Existence (last accessed November 20, 2014).

2014. Hyperledger (last accessed November 20, 2014).

2014. Twister (last accessed November 20, 2014).

2014. UK Hour to Code (last accessed December 17, 2014)

2014. UN Data. (last accessed November 20, 2014).

2014. Zerocash (last accessed November 20, 2014).

2014. Z/Yen Group (last accessed November 20, 2014).

