Building a risk market for the digital age **17th August 2015**

Michael Folkson
michaelfolkson@gmail.com

Abstract

The Internet was originally developed as a network for information exchange. Now a multitude of entrepreneurs and software developers are building the Internet for value exchange. The next logical progression is to build the Internet for risk exchange. Just as units of currency can be transferred to a third party, insurance contracts transfer risk exposures to a third party. Blockchain technology has the potential to radically transform how the insurance industry operates and how risk exposures are shared and distributed. Just as Bitcoin offers a protocol for peer-to-peer value transmission bypassing the traditional banking system, an insurance industry leveraging a public blockchain presents an opportunity for individuals and entities to transparently retain, share or transfer risk exposures without the requirement for risk exposures to sit on an insurance company's balance sheet. The insurance industry is already presented with a multitude of opportunities to broaden its coverage of risks whilst concurrently making coverage more affordable to policyholders. However, risk aversion, lack of innovation and an uninspiring public perception may prevent it from taking advantage of these opportunities. As the data available to consumers, companies and governments proliferates, it is vital that all participants become more risk aware and risk literate so that they are able to separate the signal from the noise when making decisions based on this data. The insurance industry has in previous eras been an entrepreneurial, pioneering sector and new technologies such as the blockchain can be leveraged to reboot the sector and reengage with its clients on the subject of risk.

Imagining the future of insurance

Science fiction frequently offers inspiration for what an industry could look like in future. The short speculative fiction entitled 'Know When to Hold'Em' by K.G. Jewell is a somewhat dystopian vision of futuristic insurance but it does explain how the user interface of a peer-to-peer insurance market could operate. In the story, the lead character Jonas acts as an insurer on the platform MicroRisk. Among the microrisks he chooses to provide insurance coverage for are vacation sickness, exam results, fashion (two individuals wearing the same outfit at an event) and being stood up on a first date. He is required to post collateral into his MicroRisk account before insuring a risk and is able to audit claims before paying out on them. The policyholder's premium and the insurer's collateral are frozen in escrow until the contract closed. Some of these risks may be difficult to price due to limited data and increased moral hazard. However, the story does stir the imagination when envisaging what personal risks

could be insured if the requirement to go through a conventional insurance company was lifted.

A brief history of the insurance industry

The transfer and distribution of risk dates back to at least to the second millennia B.C. In approximately 1750 B.C. Mediterranean sailing merchants paid their lender an additional sum to agree to terminate their liability conditional on the shipment being stolen or lost at sea. Lloyd's of London originated from a coffee shop in the City of London in approximately 1688. It is a corporate body rather than a company and acts as a partially mutualized marketplace where investors ("members") group together in syndicates to insure particular risks. As at December 2014, there were 96 Lloyd's syndicates. The capital structure is organized such that there are three levels of assets backing the liabilities; syndicate level assets, member's funds held in trust at Lloyd's and central assets. Central assets are held by the Corporation of Lloyd's for the rare instances where the first two levels of assets are unable to meet all liabilities. The Corporation determines the level of capital members must invest to support their proposed underwriting.

There are a number of participants in the Lloyd's market. Brokers act as intermediaries to connect insurance buyers and sellers. Underwriters determine the premiums that should be charged in conjunction with the actuaries who also estimate the reserves required to meet future claims on an ongoing basis. Claims adjusters verify the legitimacy of insurance claims and assess the size of the payout. It is a market that emphasizes the importance of tradition and face-to-face interaction. It is generally slow to exploit new technologies as demonstrated by the slow transition from paper to digital records. However, its unique history and capital structure with syndicates competing under the Lloyd's umbrella has helped build a successful and enduring global brand. As with Lending Club (see later), a sign of its maturity is that many syndicates now closely resemble traditional insurance companies and indeed many of their members are the world's major insurance groups.

The peer-to-peer lending model

There are many parallels between the banking and insurance industries with both sectors rewarded for accepting risk exposures. Rather than lending out funds and (hopefully) receiving them back at a future point in time, insurance companies receive funds in advance and return them contingent on future events. Leading investors like Warren Buffett prefer this business model as insurers benefit from the "float" which allows them to generate returns on the premiums collected before they are returned to policyholders. The peer-to-peer lending model has thrived in recent years with companies like Lending Club, Prosper and Zopa facilitating over a billion dollars of loans between individuals. Lending Club originally launched in 2007 as a Facebook application hoping to leverage the trust

between members on the social platform. Its success is at least partly explained by reestablishing a direct link between investors and specific credit risk exposures at a time of economic uncertainty, sovereign debt crises and complex too big to fail banking institutions. These direct credit risk exposures allow an investor to diversify her overall portfolio and there are minimal infrastructure costs in comparison to traditional retail banks. In 2012 Lending Club allocated 20% of the loans on their platform for institutional investors echoing the maturing in Lloyd's of London's evolution.

The peer-to-peer insurance model

Similarly, a peer-to-peer insurance platform reestablishes a direct link between investors and specific insurance risk exposures. Today's insurance companies and Lloyd's syndicates are so large, complex and heavily regulated that the direct link between an investor and specific insurance risks has eroded. If an investor wants exposure to insurance risk to diversify her portfolio, she has little option but to invest in the shares of an insurance group and be exposed to multiple insurance risks in addition to asset risks such as sovereign bonds. It is extremely difficult to match an investor's risk appetite with specific insurance risks such as personal or commercial, home, car, health or travel. Moreover, it is impossible for an investor to opt out of specific risk exposures. The only insurance risks investors can get direct exposure to are credit and catastrophe risk through the issue of catastrophe bonds. The peer-to-peer insurance model offers investors an opportunity to generate higher investment returns, transparency with regards to risk exposures and the satisfaction of directly insuring individuals or businesses rather than investing in a faceless insurance company. It offers policyholders access to cheaper premiums, faster claim payments and insurance coverage that might not be available through traditional channels.

Lloyd's of London has transitioned from agreeing peer-to-peer contracts in a 18th century coffee shop to a highly regulated, centralized institution for collecting risk exposures from all around the world. It was a logical evolution for an institution originally built to serve a small trusted community but now matching capital providers with international policyholders. There are now prohibitive barriers to entry for startups in the insurance industry, which has resulted in an industry that is slow to innovate and struggles to compete for top talent. A recent Accenture report[1] found that just two percent of recent college graduates wanted to work in the US insurance industry. However, total global premiums for property and casualty insurance continue to grow, reaching $4.9 trillion in 2013[3]. Crucially the opportunities for growth in this industry are vast as technology disrupts many of the key industries it provides coverage to.

Bitcoin, the sharing economy, Internet of Things, self-driving cars, 3D printing and artificial intelligence are effectively incubating a perfect storm for slow moving incumbents in various industries. The insurance

industry is no different. There are vast amounts of data that are being generated by telematics and smart devices such as connected meters and detection devices that could be leveraged for risk mitigation, insurance pricing, real-time coverage adjustments and claims validation. Lack of technological expertise, legacy IT systems, operational complexity and internal conflicts over potential cannibalization prevent insurance companies from fully exploiting these innovations. This presents an extremely attractive opportunity for new entrants to build a new industry from the ground-up exploiting technological innovations and the various models for sharing and distributing risk such as peer-to-peer insurance, mutuals and captives. Rakuten, the Japanese online marketplace, has recently moved into the insurance space by acquiring an insurance underwriter which grants them access to data which could potentially be used to drive sales.

Perhaps the innovation with the greatest power to restructure the insurance industry is the blockchain that underlies Bitcoin. Satoshi Nakamoto's white paper 'Bitcoin: A Peer-to-Peer Electronic Cash System' describes a protocol for enabling peer-to-peer monetary transfer without requiring a financial institution. Bitcoin depends on the sharing and replication of a universal accounting ledger or database of every transaction made by every participant. It provides a mechanism for all of the participants to arrive at a consensus that is cryptographically verifiable. Richard Brown proposes that the blockchain provides an environment for two separate revolutions; a censorship-resistant platform for open, permissionless innovation and a blueprint for building more efficient industry-level systems. Satoshi Nakamoto's primary achievement of preventing users spending the same bitcoin on multiple occasions ('double spending') without a reliance on a trusted third party is an historic feat. However, it is worth emphasizing the obvious that this protocol does not wholly eradicate reliance on trusted third parties for all financial contracts. For example, escrow mechanisms that are easily built using the Bitcoin protocol may still require dispute resolution if there is a disagreement over whether the goods or services delivered are of sufficient quality.

Nevertheless an escrow transaction built on a Bitcoin-like blockchain could be a template for how future insurance contracts are constructed. The insurance buyer and the insurance seller could transfer the premium and the collateral respectively into a multi-signature (2-of-3) Bitcoin wallet. The third signatory to the wallet would be the arbiter. Funds would be released from the wallet conditional on 2 parties signing the transaction preventing the buyer, seller or arbiter from fraudulently seizing the funds. This can technically be done by recording the 3 public keys in the following locking script:

2 <Public Key A> <Public Key B> <Public Key C> 3 OP_CHECKMULTISIG

At least 2 of those public keys must provide signatures to release the encumbrance such as in the following unlocking script:

OP_0 <Signature A> <Signature C>

Alternatively, because multi-signature scripts can be cumbersome to use and take up significantly more memory than a basic Bitcoin transaction, an alternative would be to use a pay-to-script-hash. This replaces the locking script with a cryptographic hash such that the 'redeem script' matching that hash is presented at redemption.

Smart contracts on Ethereum

Building the first decentralized peer-to-peer digital currency was such a step into unchartered territory that Bitcoin was purposefully limited for security and efficiency reasons. Its scripting language is deliberately not Turing complete (able to simulate other computer languages) with restricted functionality such as an inability to construct loops. Ethereum is able to leverage the achievements of Bitcoin and relax some of its restrictions by building an independent blockchain and programming language with greater functionality. If it succeeds, Ethereum will be a more natural platform for the construction of smart contracts such as insurance contracts as it is state aware and blockchain aware. (The success of Ethereum is not dependent on it replacing Bitcoin. Many observers believe there will be a number of independent blockchains co-existing in future with linkages between them.) Nick Szabo defines a smart contract as "a computerized transaction protocol that executes the terms of a contract". Alternatively Tim Swanson describes it as a "simple rules engine; cryptographically assured business logic that has the ability to execute and move value". Similarly to Bitcoin, smart contracts hold the potential to simultaneously minimize fraud, minimize the reliance on trusted intermediaries and minimize the costs of enforcing the contract.

Ethereum has been described as a "world computer" and a "platform for platforms" which makes it easy to build applications for providing decentralized services on the Internet. Applications such as marketplaces, social networks, payment systems, elections and asset registers can be deployed on the blockchain without needing to set up or maintain servers. The cryptocurrency or digital token associated with the Ethereum blockchain is called Ether and this is used to pay transaction fees and 'fuel' the execution of smart contracts. Sending a transaction to a contract causes its code to execute and the more computation it requires the more ether it consumes. Unlike Bitcoin that is primarily a currency and a payment system, Ethereum provides access to a vast virtual machine able to read and write executable code and data to a blockchain. It will enable the building of decentralized autonomous organizations (DAOs) that encode the assets and bylaws of an organization into self-enforcing smart contracts offering the potential for a 'minimum viable bureaucracy'[34].

The role of the claims adjuster

Just as the execution of a standard escrow contract will rely on an arbiter to resolve disputes between the buyer and the seller, the execution of an insurance contract relies on claims adjusters to verify that incoming claims are valid and if necessary estimate the monetary value of the claim. This service will vary from reviewing evidence submitted by the claimant to physically inspecting the scene of the insured event depending on the magnitude of the claim. It is currently difficult to automate this function and artificial intelligence is not yet advanced enough to rebuff all human attempts of fraudulent submissions. In the fictional example used previously ('Know When to Hold'Em'), the insurer (Jonas) has the option to pay for an audit for each claim he receives. It is not clear whether this audit is carried out by employees hired by the Microrisk platform or external auditors. A real life peer-to-peer insurance platform also has these options but there are additional options if it aspires to be a truly decentralized platform minimizing reliance on a trusted third party.

The role of reputation systems in decentralized applications

Decentralized platforms heavily rely on the efficacy and dependability of reputation systems. The upside of bypassing centralized services such as eBay, Kickstarter or Uber is that no third party can charge excessive fees, impose restrictive policies, prohibit Bitcoin payments or present a single point of failure in the storing of users' personal data. However, the downside is that no organization is responsible for maintaining the integrity of the system. Instead a mixture of user feedback, reputation scoring and financial incentives must be combined to construct robust reputation systems. The alternative is to build quasi-decentralized systems that may be an improvement on centralized systems but don't accrue all the benefits of purely decentralized systems. For example, the various activities of an insurance company could be unbundled so that some activities are automated whilst others are outsourced to external providers. It may be the case that quasi-decentralized systems will need to be built as an intermediate step or that optimal systems will never be purely decentralized. However, it makes sense to fully explore all the options and capabilities of this revolutionary technology before falling back on how current systems already operate.

The role of reputation systems in online commerce

OpenBazaar is a decentralized network for peer-to-peer online commerce that has no fees and cannot be censored. It is effectively an amalgamation of eBay and BitTorrent connecting buyers and sellers directly. Many of the components of OpenBazaar contracts will be required for insurance contracts. Cryptographic keys establish identity, digital signatures prove an identity agreed to the contract and a cryptographic hash of the contract acts as a tamper-proof record of the contract. Products are paid for using

multi-signature escrow contracts (explained earlier) with arbiters digitally signing transfer of funds to the seller or back to the buyer in case of disagreement over the quality or specifications of the goods delivered. Open Bazaar's reputation system relies on users rating and providing feedback on other buyers, sellers and arbiters. The ratings of arbiters and documentation relating to their prior decisions are accessible to buyers and sellers so that they can agree on an arbiter prior to the building of the transaction. For example, documentation may include feedback from winning and losing parties and evidence of adherence to dispute resolution standards to allow users to assess the quality of past decisions.

The role of oracles in prediction markets

Augur is a decentralized platform for prediction markets built on the Ethereum blockchain. The Augur white paper describes a prediction market as "a place where individuals can wager on the outcome of future events". It is common in financial trading to think about matching speculators (investors seeking greater exposure to risk) with hedgers (investors seeking to reduce their risk exposures). Although there may be societal value by tapping into the "wisdom of the crowd", Augur essentially provides a platform for individuals to speculate on the probability of future events. Buying insurance is generally considered a hedging activity associated with a desire to transfer risk exposures to another party. The majority of prediction markets won't intersect the risks covered by insurance contracts though it is plausible that there will be overlap with prediction markets related to weather or earthquakes for example.

Augur has a similar need for the equivalent of claims adjustors in that it requires accurate reporting on the outcome of events, after the events occur. For example, a prediction market on the next U.S. President requires a process for determining who won the presidency and therefore which wagers were successful. Augur solves this by pre-selling 'Reputation tokens' which will give their holders the ability to receive a proportion of the trading fees in return for reporting on the outcome of events. These tokens can be automatically lost and redistributed if specific holders fail to report correctly on events. Rather than a single arbiter being assigned such as with OpenBazaar, each event is reported upon by multiple individuals and these reports are compared to establish the correct outcome.

Reputation systems across platforms

Bitrated is building a trust platform across the cryptocurrency economy and this will arguably be the most sophisticated online reputation system built to date. Its reputation engine determines a Bitrating score using historical ratings from previous trades, metrics from online accounts such as Twitter followers or Reddit karma and what it defines as a 'web of trust'. This leverages the trusted relationships between each 'trust agent' so that they are able to vouch for one another to increase their Bitrating score. However, if a user you have vouched for receives a negative rating, this will

also reduce your own Bitrating score. This incentivizes users to be careful whom they vouch for. Given that Bitrated collects data across various platforms, it is possible that decentralized platforms such as OpenBazaar and Augur could utilize Bitrated's reputation system in future and conversely that Bitrated could adjust users' Bitrating scores in response to users' behaviors on those platforms. Trust agents on Bitrated have the ability to monetize their high Bitrating scores by acting as arbiters in the facilitating of transactions and the resolving of disputes. Bitrated is considering charging fees to make it more costly to manipulate its reputation system and it is also conceivable that receiving online tips from customers using micropayment services like ChangeTip could increase your Bitrating score.

Honing in on the startup business model

In 'Zero To One' Peter Thiel provides two particularly valuable pieces of advice to startups seeking to leverage network effects. He advises startups to "dominate a specific niche and then scale to adjacent markets". Just as Amazon originally focused on selling books and Facebook targeted students at Harvard University, Ebay "started by dominating small niche markets catering to small-time hobbyists". In addition, Thiel recommends that rather than aiming to disrupt a market, startups should seek to expand the market overall and avoid competing with incumbents head on. Heeding this advice guides an insurance startup to look at products or services that traditional insurance companies are unwilling or unable to develop at the current time. Insurance companies are typically slow to capitalize on recent technological developments or newly accessible data in the design, underwriting or pricing of insurance contracts. One potentially fruitful avenue for a startup to explore is the role of insurance in the nascent industry of the Internet of Things. Not only is there an Internet of Things prototype built on a blockchain but this prototype also provides an opportunity to automate the troublesome role of the claims adjuster.

Insurance and the Internet of Things

In January 2015, IBM and Samsung released a proof of concept for ADEPT (Autonomous Decentralized Peer-To-Peer Telemetry), a platform for Internet of Things devices that is autonomous, decentralized, peer-to-peer and able to withstand individual points of failure. Building a decentralized platform for potentially billions of devices was motivated by the limitations of centralized approaches which are described as expensive, lacking privacy and difficult to secure with limited scalability. In addition, IBM believes that every device could become "a point of transaction and economic value creation" for owners and users and "able to autonomously react to changes in markets". The blockchain can be used as the system of record for contracts between devices, the owners of the devices and the manufacturers of the devices. Among the benefits of using a blockchain for this purpose are guaranteed data availability, data sharing, uptime and

code execution. It is a transparent system that assigns users pseudonymous identities.

One of the prototypes IBM presented utilizing the ADEPT architecture was an autonomous washing machine which was able to detect a failing part, check whether the failing part was under warranty and place a request with the nearest service vendor without human intervention. Although this is a valuable service in the consumer market, perhaps the greater opportunity lies in private and public sector supply chains where it is extremely difficult to receive instant updates on failing parts and automatically call on outstanding warranties. Everledger is an example of a startup that is using the blockchain to create a decentralized ownership ledger for high value assets. Solutions such as this will allow owners and insurers to monitor the location and status of fixed assets simultaneously to avoid the procurement of unnecessary replacements and fraudulent insurance claims.

The ADEPT architecture uses the Telehash protocol for secure, encrypted, trustless peer-to-peer messaging for commands such as starting a washing cycle. The BitTorrent protocol is used for distributed file sharing for larger files such as diagnostic data detailing the performance of the washing machine. The Ethereum blockchain is used for device registration, contract lookup and transactions between devices. When the washing machine detects an air filter failure it checks its warranty status on the blockchain. If it is in warranty, it finds an authorized service provider who is registered on the blockchain and places a replacement order. The service provider is able to independently look up the device ID and the smart contract reference to verify that the warranty claim cited by the washing machine is indeed valid. The service call details are then reported to the owner.

A warranty is essentially a form of insurance contract. Although a manufacturer may offer a free product warranty for a specific term, the purchaser may choose to buy an extended warranty from the manufacturer or a third party. This extended warranty contract can be recorded on the blockchain and integrated into the ADEPT prototype such that the washing machine checks the extended warranty status in the case of an expired warranty. If the extended warranty contract includes a deductible in the event of a claim, this digital payment may be made automatically over the blockchain to the insurer at the point the contract is triggered. IBM will be sharing the code developed as part of the ADEPT proof of concept at a later date and is developing an API suite for the ADEPT core stack. As more applications are built and more assets are registered to the blockchain, the opportunities to attach insurance contacts will multiply.

Why should we pursue decentralization?

There are two main arguments to pursue decentralization and they revolve around risk and innovation. These are generally perceived as competing forces with innovation introducing new and in some cases unforeseeable

risks to a company or an industry. However, decentralization can open up opportunities for permissionless innovation at the edge whilst also decreasing the fragility and risk of collapse of the system. A highly centralized system only allows innovation when permission is granted by the central participant, requiring an almost clairvoyant prescience in the future of innovation. In such a system, human bias and self-interest at the center can prevent valuable research and development from being advanced and excessive fees can be charged to even participate in the system. Similarly, a centralized financial system requires executives and regulators to have a clairvoyant prescience in spotting future bubbles, predicting which employees will engage in fraudulent activities and which latent risks are hidden in hideously complex derivative portfolios. Unsurprisingly they have not been up to the task and the financial system has lurched from one crisis to another. A decentralized system does not eliminate human bias or self-interest but it prevents downside risks from being concealed and concentrating at the center that can cause entire systems to collapse. Participants can unilaterally exit and the system carries on regardless. In addition storing customer data with trusted third parties presents a single point of failure that has been exploited by hackers on countless occasions (Target, Sony, etc).

Insurance and Big Data

The volume, velocity and variety of data generated by digital devices presents various opportunities for insurance companies such as adjusting policyholders' premiums and coverage in real time depending on the policyholders' latest behaviors and risk levels. For example, telematics enable the monitoring of a policyholder's driving to continuously reassess the probability that they will be involved in a car accident. In addition, companies such as Counsyl rely on its customer base becoming more risk aware and more risk literate. Counsyl offer individuals and families access to granular data about their bodies, their health and their genetics. This access to new sources of data will impact life choices and future insurance needs. It is critical that the end user understands the implications of these results if this is going to lead to more informed, risk literate decisions. Unless this litmus test is met, the new sources of data will have little value.

The public perception of the insurance industry

Buying lottery tickets and gambling at resorts like Las Vegas and Macau are immensely popular despite games such as lotteries, roulette and pontoon being simple games with fixed odds. Their popularity relies on distraction, delusion, glamour and expert marketing. Sports betting at least has variable odds but how many gamblers spend the time to consider the odds, stakes and payoffs of their own life decisions with the same vigor that they consider sports outcomes? Financial trading relies on judgment and technical analysis in the long term but in the short term it is essentially speculating on the direction and speed of the herd of humans, algorithms and bots. In comparison insurance generally has a public perception of

being dull and mandatory. However, not only does it require the evaluation of uncertain variable odds for a diverse assortment of risks, it is also a public good providing a mechanism for transferring risks from those unable or unwilling to be exposed to them. It encourages us to discard myths and superstitions and mentally prepare for a wider range of outcomes. It emboldens us to live richer, more adventurous lives and address vivid downside risks rather than worrying obsessively about them. A valid criticism of insurance is that it is bureaucratic and subject to complex, onerous regulation and this leads to insurance premiums being more expensive than they need to be.

Conclusion

Although private blockchains (or 'permissioned distributed ledger systems') are useful for keeping databases in sync in a more trusted environment, they are an incremental innovation when compared to the potential of public blockchains. Just as Bitcoin opens the floodgates for peer-to-peer transactions and permissionless innovation, peer-to-peer insurance leveraging a smart contracts protocol such as Ethereum could provide a platform for matching insurance buyers and insurance sellers for any risk they agree to exchange. This marketplace would be a radical paradigm shift from today's centralized and spatially anchored insurance industry. The blockchain provides the opportunity to build a more innovative, expansive and transparent industry that evolves to the needs and requirements of its users. Z/Yen believes that the role of the insurer could shift from accepting risk exposures onto its balance sheet to providing expert advice and management of various mechanisms for its customers to retain, share and pool risk exposures. This project aims to build a risk market for the digital age and this white paper is the beginning. Please contact me if you would like to participate.

Glossary

Bitcoin – A digital currency and peer-to-peer payment system that enables instant, global payments. Users can transact directly without requiring an intermediary such as a banking institution. Transactions are verified by network of computers (miners) and recorded in the blockchain. There is no central authority and any changes to the software must be the supported by the majority of the network's participants. The open source software was released in 2009.

Blockchain – A ledger or database of every transaction made by participants. Transactions are verified using cryptography and collected into blocks of transactions that are confirmed using decentralized consensus across the network. This eliminates the reliance on a trusted third party to validate transactions. Also see Permissioned distributed ledger.

Claims adjuster – Also loss adjuster. Assumes the responsibility of scrutinizing insurance claims to determine the extent of the insuring company's liability. This includes verifying that the claimant has not violated the terms of the contract.

Cryptography – The enciphering and deciphering of messages in secret code. Bitcoin uses public key cryptography that allows transactions to be signed with a private key without exposing the private key. The network can validate that the transaction was signed by the correct private key but cannot decipher what alphanumeric characters make up that private key. Miners compete for the rewards of newly minted bitcoin by solving cryptographic puzzles that collect groups of transactions into blocks.

DAO – Decentralized Autonomous Organization. The assets and bylaws of an organization are programmed into software code that is self-enforcing. It has the ability to execute and move value without any central control. Also see smart contract.

Deductible – The amount that must be paid by out of the pocket of the policyholder in the event of any future claim. The insurer will compensate the claimant for value above this deductible amount.

Digital signature – The secure digital equivalent of signing a check. The Elliptic Curve Digital Signature Algorithm (ECDSA) ensures funds are only transferred by the owner of the private key. The private key is used to generate the signature and the public key can be used to verify that this signature is valid. Also see Cryptography.

Ethereum – A world computer or platform for platforms that makes it easy to build applications for providing decentralized services on the Internet. Unlike Bitcoin that is primarily a currency and a payment system,

Ethereum provides access to a vast virtual machine able to read and write executable code and data to a blockchain.

Escrow – A contractual arrangement in which funds are traditionally placed in the control of an independent third party to protect both buyer and seller. The funds are released on the completion or termination of the transaction. Note that with multi-signature Bitcoin escrow contracts, the third party is unable to steal the funds without the complicity of either the buyer or seller.

Internet of Things – A network of physical objects (e.g. light bulbs, heaters) with embedded software and sensors that are connected to the Internet. This enables them to send and receive data whilst being controlled remotely.

Multi-signature – An address that is associated with more than one private key. Transactions must be signed or authorized by multiple private keys. An m-of-n address is associated with n private keys and requires signatures from at least m of these private keys to transfer funds.

Permissioned distributed ledger – A private blockchain that limits access and/or right to modify to specific users. In contrast anyone can read, send a transaction or participate in the consensus process on a public blockchain.

Reputation system – A mechanism for collecting, aggregating and distributing feedback about users' past behavior

Smart contract –A computerized transaction protocol that executes the terms of a contract. The software code is capable of holding, transferring, receiving or spending digital assets.

Sybil attack – An attack to undermine a reputation system by counterfeiting multiple identities and using them to disproportionately influence the network.

Turing-complete – A programming language able to simulate any other language with conditions, loops and read/write memory.

Wallet – A file that stores the private key(s) that a user needs to transfer funds. There are web, desktop, mobile, hardware and paper wallets that offer varying tradeoffs between security and usability.

Bibliography

1. Accenture. *Missing an Opportunity - Talent Supply Chain.* North America: Accenture.
2. Antonopoulos, A. M. (2015). *Mastering Bitcoin.* O'Reilly.
3. Aon Benfield. (2014). *Insurance Risk Study.* Aon Benfield.
4. Bernstein, P. (1998). *Against the Gods - The Remarkable Story of Risk.* John Wiley & Sons.
5. Bitrated. (2015). *About Bitrated*. Retrieved from Bitrated: https://www.bitrated.com/about
6. Brody, P., & Pureswaran, V. (2014). *Device democracy: Saving the future of the Internet of Things.* IBM Institute for Business Value.
7. Brody, P., Pureswaran, V., Panikkar, S., & Nair, S. (2015). *Empowering the edge - Practical Insights on a decentralized Internet of Things.* IBM Institute for Business Value.
8. Brown, R. G. (2015). *Bitcoin and Blockchain: Two revolutions for the price of one*. Retrieved from Thoughts on the future of finance: http://gendal.me/2015/07/23/bitcoin-and-blockchain-two-revolutions-for-the-price-of-one/
9. Buterin, V. (2013). *A Next-Generation Smart Contract and Decentralized Application Platform.* Ethereum.
10. Coinkite. (2015). *Bitcoin Escrow Payments With Coinkite Multi-Signature*. Retrieved from Coinkite: http://blog.coinkite.com/post/124840306576/bitcoin-escrow-payments-with-coinkite
11. Coinslists. (2015). *Bitcoin Buyer Protection*. Retrieved from Coinslists: https://coinslists.info/index.php/2015/06/09/bitcoin-buyer-protection/
12. Davis, J. (2015). *Peer to peer insurance on an Ethereum blockchain.*
13. DeFigueiredo, D., & Barr, E. (2014). *TrustDavis: A Non-Exploitable Online Reputation System.* University of California at Davis, Computer Science. UC Davis.
14. Duguid, A. (2014). *On the Brink: How a Crisis Transformed Lloyd's of London.* Palgrave Macmillan.
15. Ethereum. (2015). *Frontier Guide.* Ethereum.
16. Folkson, M. (2009). History repeating itself? *The Actuary* .
17. Jewell, K. (2013). Know When to Hold 'Em. *Nautilus* .
18. Lloyd's of London. (n.d.). *Lloyd's capital structure*. Retrieved from Lloyd's: https://www.lloyds.com/lloyds/investor-relations/lloyds-capital-structure
19. Lloyd's of London. (n.d.). *The Lloyd's Market*. Retrieved from Lloyd's: https://www.lloyds.com/lloyds/about-us/what-is-lloyds/the-lloyds-market
20. Morgan Stanley, BCG. (2014). *Insurance and Technology - Evolution and Revolution in a Digital World.* Morgan Stanley, BCG.
21. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* www.bitcoin.org.

22. OpenBazaar. (2015). *What is OpenBazaar?* Retrieved from OpenBazaar: https://blog.openbazaar.org/what-is-openbazaar/
23. Peel, C. (2015). Ethereum - Introduction and Solidity examples.
24. Peterson, J., & Krug, J. (2014). *Augur: a Decentralized, Open-Source Platform for Prediction Markets.* www.augur.net.
25. Pureswaran, V., Panikkar, S., & Nair, S. (2015). *Empowering the edge - Use case abstract for the ADEPT proof-of-concept.* IBM Institute for Business Value.
26. Renton, P. (2012). *The Lending Club Story.* Amazon Media.
27. Sanchez, W. (2015). *OpenBazaar - Ratings, reviews and reputation.* Retrieved from Slideshare: http://www.slideshare.net/drwasho/openbazaar-ratings-reviews-and-reputation?related=1
28. Swan, M. (2015). *Blockchain: Blueprint for a New Economy.* O'Reilly.
29. Swanson, T. (2015). *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems.* www.ofnumbers.com.
30. Swanson, T. (2014). *Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management.* Amazon Media.
31. Szabo, N. (1994). *Smart Contracts*. Retrieved from Nick Szabo's Essays, Papers and Concise Tutorials: http://szabo.best.vwh.net/smart.contracts.html
32. Sztorc, P. (2014). *Truthcoin: Peer-to-Peer Oracle System and Prediction Marketplace.* Truthcoin.
33. Thiel, P. (2015). *Zero to One.* Virgin Books.
34. Thomson, L. (2014). Minimum Viable Bureaucracy.
35. Wikipedia. (n.d.). *History of insurance*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/History_of_insurance
36. Wikipedia. (n.d.). *Lloyd's of London*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Lloyd%27s_of_London
37. Wood, G. (2015). *Ethereum: A Secure Decentralised Generalised Transaction Ledger Final Draft.* Ethereum.
38. Z/Yen Group. (2014). *Chain of a Lifetime: How Blockchain Technology Might Transform Personal Insurance.* Long Finance.
39. Zindros, D. (2015). *A pseudonymous trust system for a decentralized anonymous marketplace.* National Technical University of Athens.