Ottocoin White Paper

Team Ottocoin

Revision 1 - Ottocoin v. 1.0.0 - April 2017

Abstract

As the world moves toward digitization, players in every industry are racing to stay on top of the competition. And blockchain technology is paving the way to support the significant digital transformation especially in data sharing. The core concept that drives its adoption is an open distributed ledger that holds a complete historical record of every transaction that promises integrity in its verification process within a peer-to-peer network. Ottocoin is leveraging on this technology to offer an alternative insurance policy against internet liabilities for both corporates and individual users. We believe that our unique method of delivering policies through disbursement of tradable currency will reward people who seek to insure themselves against potential economic losses.

Table of Contents

Introduction

The current transaction system is a centralised system, often controlled and managed by a third party organization. Digital payments and currency transfer requires financial institutions or credit card providers as middleman in order to complete the transaction: thus, all data and personal information fall under the purview of these organisations, instead of staying between the two principal entities directly involved with the transaction [2]. Mechanisms for completing transactions include managing costs that arise in the form of processing fees, transfer taxes and the maintenance of collateral, as well as the risk of either parties not fulfilling their terms [1].

In an age where personal data and information can be used against individuals, cyber security has become a top priority. Financial institutions and credit card providers have gone through great lengths to ensure that sensitive information that can potentially be stolen by cyber criminals are kept under lock and key but it has become harder, and more expensive, to prevent attacks from much more savvy cyber criminals [2].

Cryptocurrency was a term first described in 1998 by Wei Dai [3] on the cypherpunks mailing list, suggesting the idea of a new form of money that is created, controlled and managed by cryptography, instead of a central authority. In 2009, Satoshi Nakamoto published a white paper on a cash transaction system based on a peer-to-peer network. He created the first block of the block chain; called “Genesis Block” that contains a single transaction, which generates 50 cryptocurrency called Bitcoin, to the benefit of the creator of the block [4]. The goal of blockchain technology is to create a decentralized environment where transactions occur without third party interference.

Blockchain is a distributed database that is shared - and continually reconciled - in the network. The data is recorded in a public ledger and every node - computer connected to the blockchain network - are privy to the information of every transaction ever completed [4]. In order for a transaction to be completed, it has to be validated and relayed back by nodes, which are anonymous. This attribute ensures that the system

remains transparent and remains decentralized. The blockchain ledger is not stored in any single location and virtually incorruptible by hackers as it will require a large amount of computing power to alter any unit of information on the blockchain.

Security concerns

However, it is important to note that even though blockchain technology appears to be a suitable solution for conducting transactions in a virtually secure and transparent environment, security incidents and their impacts on economic losses have also increased with its use. Throughout the years after the inception of Bitcoin, many scams and distributed denial-of-service (DDoS) attacks on exchanges and mining pools have been reported, and in a study by Vasek et. al. [5] that studied a variety of scams involving Bitcoin, the authors noted that $11 million worth of Bitcoin has been contributed to scams, between 2011 and 2014.

In addition to Bitcoin scams, the ecosystem is not entirely secure from more serious criminal activity, including fraud and money laundering. In March 2012, over 43,000 Bitcoins were stolen from Bitcoinica trading platform [6]; in September 2012, $250, 000 worth of Bitcoins were appropriated from the Bitfloor currency exchange [7] and most notably the Mt. Gox disaster has amounted to a loss of $460 million worth of Bitcoins to hackers [8]. It is interesting to note that while blockchain technology is an ecosystem that espouses decentralization, it has also birthed third party intermediaries to support Bitcoin transactions. Ironically, these intermediaries that act as de facto centralized authorities pose more risks to Bitcoin holders than any other type of security breaches [9].

The goal of this paper is to introduce the application of a new cryptocurrency in providing insurance against potential economic loss due to cyber crimes. In the first part of this paper, we will expund on the proposal of a new cryptocurrency which aims to address the issues underlying internet liabilities mentioned above. Specifically, we propose a new token, Ottocoin, which will distributed in return for Bitcoins that will be

utilised to create the financial backbone for parties vulnerable against cyber attacks. In the second part, we will illustrate our roadmap that will extend the application of Ottocoin in other services to raise its value in the market for a higher return in investment.

Ottocoin

As the hype surrounding Bitcoin begins to settle down, blockchain technology has taken the spotlight due to its potential to change the way we deal with transactions, not only in the financial sector but also in a wide range of industries. Just recently, IBM has announced the launching of a blockchain platform for US oil trade. This platform will enable trade documents, shipment updates, payment status and delivery to be recorded and shared on a single ledger that will be shared with the parties involved [10]. Other examples of the utilisation of blockchain technology include the fight against food fraud [11], equity crowd-funding platform [12] and digital certification [13].

We believe that Blockchain technology can be extended to other sectors that have not been explored yet, at least, not commercially or in depth. We believe that with our own uniquely designed cryptocurrency, Ottocoin, we will offer a wide range of services by utilising Ottocoin as a trading currency on our platform. Similar to Bitcoin, Ottocoin is based on blockchain technology: all transactions are recorded on an open ledger, in a decentralised peer-to-peer network.

Ottocoin Development Process

Due to the problems ASIC chips brought on the digital currency platform, a new currency, Litecoin was created. Litecoin attempted to utilize the Scrypt hashing algorithm, which is more memory intensive than SHA256, to deter ASIC use. As of January 2014, there are now Scrypt ASIC chips being deployed by the Chinese for mining. So far, around 1000 Mhash of Gridseed ASIC chips have been brought online and used on the litecoin and middlecoin.com network. The Chinese chips have not been

released on the greater market at large, but eventually they will, and the same problems that SHA256 currency faces will come to the Litecoin and other Scrypt currency networks next.

Where does Ottocoin fit into this? Scrypt was utilized by Litecoin to try and deter ASIC use because large memory requirements are the best way to try and make ASIC financially unfeasible. Litecoin held out for a while, but the original memory requirements in the barebone litecoin distribution were just not high enough to lock out ASIC completely. Ottocoin has now been released as the logical evolution of Litecoin and introduces what's known as "Adaptive N-Factor". The N-factor component of Scrypt determines how much memory is required to compute the hashing functions. Ottocoin N–factor increases with time to stay one step ahead of any possible ASIC development. For the long, foreseeable future, GPU computing will be the fastest method of computation for Vertcoin, but CPU computation will eventually make gains as Nfactor increases.

Our Mission

For most people, taking up insurance is a complicated process that involves parsing through complex and difficult legal language in the documents involved. The expectation that an insurance against potential liabilities is worth the difficulties involved is almost always discouraging in the face of even more complex and drawn-out claiming process. In addition, there's a growing number of fraud involved from both sides of the parties that cost the industry millions of dollars every year [14].

The idea of insurance is practical, if not a noble one. The practice insurance can be traced back to the times of European commercialisation era, particularly Northern Italy, Portugal and Spain [15]. Although there were no insurance contract written and signed then, it was understood that there was a contractual arrangement where one or more persons assumes the risks of losses to which others are exposed to. In those days, merchants found that by dividing their cargoes among a number of ships, they can

reduce the potential economic loss from ships being destroyed or cargoes stolen during shipment. If one ship is destroyed, instead on one merchant losing everything, each of the participating merchant only lose a small portion.

In modern day practice, premium paid in exchange for a policy is “pooled”, and in the event of unfortunate losses stipulated in the policy, claims submitted will be paid out using the money that has been collected. It seems so simple, yet so many people are still wary with taking up insurance despite the economic benefits it ensures. Here we have listed down several issues people experience in the insurance industry and what we offer as solutions:

Problem: Money collected from premiums paid are merely redistributed by an intermediary (insurance company) rather than in return for a legitimate product or service. In order for one party to claim for their loss, several other parties need to pay thousands in premiums in order to cover the loss while receiving no money in return throughout their policy. Essentially, people are paying for a piece of paper that will only be needed when a loss occur, if ever.

Our solution: Bitcoin will replace money to pay for premium and in exchange for the policy, a sum of Ottocoin will be disbursed to the insurance taker. Unlike conventional policy that is merely a piece of paper that is legally binding, Ottocoin can be traded on the market. Thus, creating value as demand increase and rewarding insurance takers.

Problem: The insurance industry is not exempted from fraud activity. In fact, in a study conducted by the Coalition Against Fraud, insurance fraud costs the industry around $80 billion a year across all lines of insurance caused by fraudulent claims [16]. There is also an increasing concern that insurance companies are taking advantage of their customers by imposing very stringent process in claiming to pay out as little money as possible.

Our Solution: Blockchain technology is noted for its immutable open ledger concept and we are leveraging blockchain to manage claims in a transparent, responsive and irrefutable manner. For instance, multiple claims will be rejected as the network would have already verify and relay a claim that has been made. On top of that, the decentralized platform ensures that multiple copies of the complete historical records are kept within a large network and that the integrity is maintained as it leaves very little room for data manipulation.

Problem: The main source of headache for insurance takers, and to an extent, insurance companies is the claiming process. In theory, the process is very much straightforward. A claim is submitted, verified for its validity and coverage, the liability assessed and reported, the case file examined and processed and finally, settlement offered. In reality, claim handling involves a lot of parties involved in assessing the claim which results in slow turnaround time when insurance takers expect to be paid without delay once they put in their claim.

Our Solution: Our service is based entirely on blockchain technology and the system itself will ensure that the sharing of data is more streamlined and that all parties involved can easily and instantly access and update relevant information on the distributed ledger. An automatic insurance policy that is written into a smart contract will ensure that a settlement is made for an insurable event without manual administration once a complete claim is verified by the network.

Model

We are seeking to redefine the way insurance is practiced. In addition to the obvious advantages blockchain technology offers in terms of a more transparent, accurate and efficient system, our approach in offering our insurance policies ensures that insurance takers would be rewarded for it.

The first stage of our project will help build the financial backbone for community and websites that are experiencing disruption in their system that can cause significant economic loss. Our insurance policies will also be extended to individual users with potential risks for loss from hackers activity. Ottocoin will act as a substitute for payments in other cryptocurrency and will enable people to be rewarded for their work.

Similarly with current practices, insurance takers pay a premium for a policy that contains the terms and conditions under which we agree to compensate the loss after an unforeseen event. That is where the similarities end. In addition to the policy, or proof-of-insurance, we will disburse a sum of Ottocoin that can be traded and exchanged in the market (initially, it can only be traded with Bitcoin but an infrastructure for exchanging to fiat currency is in our long-term outlook).

An example of how our model works is shown below:

Company A wants to insure against $1 million worth of asset. In order to take up our insurance, the net value will be converted to Bitcoin. Company A will pay a premium of up to 10% of the total value of asset in BTC (rate is subject to change) in exchange for a sum of Ottocoin based on an assigned exchange rate of 0.05Ottocoin/XBT.

$1 = 0.0008XBT
$1 million = 829.2946XBT
1XBT = 0.05Ottocoin
829.946XBT = 16,585.892Ottocoin

10% of total value of asset ($100,000) = 82.9946XBT/1659.892Ottocoin

In return, a proof-of-insurance and Ottocoin amounting to the premium paid will be given to the company which can be traded in the exchanger.

Acquiring our insurance is made simple and easy through our online platform. Our main objective is to make our insurance policy accessible and transparent through adopting blockchain technology. The steps are explained below:

1. Register an account on our online platform.
2. Enter the market value of asset to be covered.
3. System will determine how many Ottocoin you need to buy.
4. Users will need to enter their wallet address which will be linked to the insurance policy. This policy will be “locked” based on their wallet address.
5. Users can get the amount of Ottocoin required from the web or exchanger.
6. Users must put the amount into the locked wallet. At the same time, a proof-of-insurance will be deposited into the wallet.
7. Then the policy will be activated.
8. Once policy is activated, users can use Ottocoin for trading or any other purposes.

By leveraging blockchain technology in our platform, we will ensure that the claiming process meets the expectation of insurance takers. Our claiming process requires that insurance takers meet with the basic conditions to complete it. Insurance takers must have:

1. Proof-of-insurance
2. The original 10% amount of premium paid in the linked wallet.
3. Relevant documents (i.e. evidence, police reports, third party reports)

Once the claim made have been verified by the network, the case will be investigated and once the conditions stipulated in the policy have been met, a settlement will be offered and paid out automatically through our platform. We will be disbursing all claims with fiat currency based on the current market value of Ottocoin at that point in time.

Roadmap

We are offering a new cryptocurrency in the market with an ambitious and wide-ranging blockchain project. The roadmap for the launch of Ottocoin is as below:

Date	**Target**
2016 March 2017	Idea Testnet Launched
May 2017	Mainet Launched Commence Phase 1:ICO
	Product launch: Internet liability insurance Desktop & Web Wallet Launched
June 2017	Commence Phase 2: ICO Operation of Ottocoin-BTC Exchange
2018	Launch online payment gateway Global Expansion
2020	Open Ottocoin for mining Operation of Ottocoin-fiat currency exchange

The first phase of our project is to offer 6 million pre-mined Ottocoin during our ICO and in the second phase we will be offering 1.2 million Ottocoin. To buy Ottocoin, we will only accept payment in Bitcoin and we are offering an initial rate of 0.04XBT for every Ottocoin which will be increased in Phase 2.

Appendix

[1] Merton R.C, and Bodie Z. A Conceptual Framework for Analyzing the Financial System. In: Crane, D.B. eds. The Global Financial System: A Functional Perspective. Boston: Harvard Business School Press, 1995. Available from: https://www.researchgate.net/profile/Zvi_Bodie/publication/228224831_A_Conceptual_Framework_for_Analyzing_the_Financial_Environment/links/0deec51a38bb1ce588000000.pdf

[2] Asokan, N., Janson, P.A., Steiner, M. and Waidner, M., 1997. The state of the art in electronic payment systems. *Computer*, *30*(9), pp.28-35. Available from: http://dx.doi.org.secure.sci-hub.bz/10.1109/2.612244.

[3] Wei Dai. b-money. Available from: http://www.weidai.com/bmoney.txt.

[4] Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K., 2016. Where Is Current Research on Blockchain Technology?—A Systematic Review. *PloS one*, *11*(10), p.e0163477. Available from: http://dx.doi.org/10.1371/journal.pone.0163477

[5] Vasek, M. and Moore, T., 2015, January. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. In *International Conference on Financial Cryptography and Data Security* (pp. 44-61). Springer Berlin Heidelberg. Available from: http://dx.doi.org.sci-hub.bz/10.1007/978-3-662-47854-7_4.

[6] Leyden, J. Linode hackers escape with $70k in daring Bitcoin heist. The Register (March 2012). Available from: http://www.theregister.co.uk/2012/03/02/linode_bitcoin_heist/

[7] Lee, T. Hacker steals $250k in bitcoins from online exchange bitfloor. Ars Technica (September 2012). Available from: http://arstechnica.com/tech-policy/2012/ 09/hacker-steals-250k-in-bitcoins-from-online-exchangebitfloor/

[8] McMillan, R. The Inside Story of Mt. Got, Bitcoin's $460 million Disaster (March 2014). Available from: https://www.wired.com/2014/03/bitcoin-exchange/.

[9] Moore, T. and Christin, N., 2013, April. Beware the middleman: Empirical analysis of Bitcoin-exchange risk. In: *International Conference on Financial Cryptography and Data Security* (pp. 25-33). Springer Berlin Heidelberg. Available from: http://dx.doi.org.sci-hub.bz/10.1007/978-3-642-39884-1_3.

[10] Samburaj, D. IBM Launches Blockchain Platform for US Oil Trade (April 2017). Available from: https://www.cryptocoinsnews.com/ibm-launches-blockchain-platform-us-oil-trade/

[11] Palmer, D. Alibaba turns to Blockchain to fight against food fraud (March 2017). Available from: http://www.coindesk.com/alibaba-pwc-partner-to-fight-food-fraud-with-blockchain/

[12] Neuroware. Crowdfunding Innovation in Decentralization with the World's first licensed bitcoin-based ECF campaign (October 2016). Available from: http://neuroware.io/blog/crowdfunding-innovation-in-decentralization/

[13] Prisco, G. MIT Media Lab Releases Code for Digital Certificates on the Blockchain (June 2016). Available from: https://bitcoinmagazine.com/articles/mit-media-lab-releases-code-for-digital-certificates-on-the-blockchain-1465404945/

[14] Deloitte. Blockchain applications in Insurance. Avalaible from: https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-deloitte-blockchain-app-in-insurance.pdf

[15] Vance, W.R., 1908. The early history of insurance law. *Columbia Law Review*, *8*(1), pp.1-17. Available from: http://dx.doi.org/10.2307/1109564

[16] Coalition Against Insurance Fraud. By the Numbers: Fraud Statistics. Available from: http://www.insurancefraud.org/statistics.htm#1