CONFERENCE PROCEEDINGS

2nd Blockchain International Scientific Conference 11 March 2020, Edinburgh

1. Cryptocurrencies And Cyberlaundering: The Need For Regulation

Gian Marco Bovenzi
Syracuse University College of Law, USA
Category: Oral Presentation

Abstract

Data show that cyber organized crime was beyond 39% of global cyber breaches in 2018, with peaks of 70% in 2011 and 80% in 2015. In addition, 46% of Bitcoin transactions involve illegal activities (for an estimated value of $76 billion) and cryptomining is the motive of 30% of security breaches. Given this alarming scenario, the objective of this paper is to stress the urgent need for governments to enhance regulations specifically addressing the issue of cryptocurrencies exploitation for cyberlaundering purposes. Criminal organizations historically breathe through money laundering, and according to scholars and media reporting they currently might find in cryptoassets fertile grounds for their aims of financial gain. The anonymity underlying blockchain causes indeed serious biases to investigations, as encryption represents a challenge for law enforcement officers in linking transactions to physical identities. Adopting a comparative legal analysis methodology, the paper will assess the current global legal framework underlining its positive outcomes, its deficiencies, and what is yet to be done. This paper concludes pointing out two possible solutions: first, the implementation of international instruments of cooperation is crucial, given the transnational and cross-border nature of organized crime. Considering sovereign States' hesitancy in adopting globally accepted protocols or treaties, bi- or multi-lateral agreements might represent a temporary solution. Second, governments should tailor their national legal and policy frameworks focusing on cyberlaundering prevention, such as cash control or limitation of fund transfers for single users, or ensuring methods of identification such as mandatory registration of users.

Keywords: *Cryptocurrencies, cyberlaundering, organized crime, money laundering, blockchain*

Themes: *Cyberlaundering, organized crime, cryptocurrencies*

2. Jurisdiction on the Blockchain

Bedrettin Gürcan
University of Szeged Faculty of Law and Political Science, Hungary
Category: Oral Presentation

Abstract

Blockchain technology brings several services to our daily and business life. Its impact on the business culture, moral of the law and the data security has been discussing since the blockchain technology has been emerged. In this paper, we will discuss the jurisdiction of the blockchain technology. Blockchain was developed through the combination of several technologies including peer-to peer networks, asymmetric (public key) cryptography, time stamping, and the proof of work consensus mechanism. Blockchain provides an infrastructure for smart contracts to be executed in decentralized, without 3rd party presence.

Business transactions on the blockchain is completely independent from the location where parties of the legal entities located. Some challenges are decentralized storage of large computer networks, anonymity of the parties, and unspecified values exchanged where it is not sure it these ‵‵goods" are included United Nations Convention on Contracts for the International Sale of Goods. (CISG). With the developments of smart contracts, parties can devise mechanism whereby disputes on the agreement can be resolved by private adjudicators through self-enforcing decisions, the enactment of which does not depend on state controlled recognition and enforcement procedures.

3. 5 W's of Workers Compensation insurance, compliance and fraud

Srinivas Ratnam
Andhra University College of Engineering, Vizag, India
Category: Oral Presentation

Abstract

Workers compensation is type of insurance that grants benefits to injured worker who are injured on the lines of the duty. Quantum of benefits such as payment of bills/providing medical care vary depending upon the premium purchased. Employers participate in this program by law or to protect themselves from lawsuit in case of worker going legally against them. Workers Compensation Insurance benefits both employer (to protect their business against lawsuit) and employee/worker (to get benefits related to injury at worksite). In order for all the involved parties to be protected under the Workers compensation Insurance benefits or from liability benefits, they have to be in compliance with the state law. But due to the existing and disconnected parading of people/process/processors/information asymmetry, many frauds are taking place by involved stakeholders such as Insurance leakage/underwriter leakage due to people/process, submitting false claims due to people/processors and many more. The impact of being non-compliant and committing fraud leads to heavy cost of premium, higher medical care cost and so on. This paper attempts to address 5 W's (WHO, WHAT, WHEN, WHERE, WHY) of workers compensation insurance, compliance and various source of frauds and how state-of-the-art technology such as Blockchain, Artificial Intelligent, IoT, Virtual Agents can address such problems by focusing on Aviation industry and Independent contractors and the rush in adopting Blockchain/AI. This report provides statistics on insurance fraud, fraud indicators and so on. This paper also addresses various ways to protect environment by reducing massive consumption of papers. Keywords: Blockchain, Artificial Intelligent, IoT, Virtual Agents, Workers compensation insurance intermediation, monitoring the monitor Themes: blockchain, information asymmetry

4. The Need for Cyber Resilient Enterprise Distributed Ledger Risk Management Framework

Robert E. Campbell, Sr.
Capitol Technology University, USA
Category: Oral Presentation

Abstract

Critical infrastructure sectors are increasingly adopting enterprise distributed ledgers (DLs) to host long-term assets,systems, and information that is considered vital to an organization's ability to operate without clear or public plans and strategies to migrate safely and timely to post-quantum cryptography (PQC). A quantum computer (QC) compromised DL would allow eavesdropping, unauthorized client authentication, signed malware, cloak-in encrypted session, a man-in-themiddle attack (MITM), forged documents, and emails. These attacks can lead to disruption of service, damage of reputation and trust, injury to human life, and the loss of intellectual property, assets, regulated data, and global economic security. In 2018, Gartner revealed that a QC is a digital disruption that organizations may not be ready and prepared for, and CIOs may not see it coming.1 On September 18, 2019, IBM announced that the largest universal QC for commercial use would be available in October 2019.2 On October 23, 2019, Google officially announced "Quantum Supremacy," "by performing a calculation in 200 seconds that would take a classical supercomputer approximately 10,000 years."3 DL cyber resilience requires "reasonable" measures, policies, procedures, strategies, and risk management before large-scale deployment. Cyber resilience implementations must be a critical component during the design and building phase, or during the initialization phase. The most significant existing attack vector for enterprise DLs is the public key infrastructure (PKI), which is fundamental in securing the Internet and enterprise DLs and is a core component of authentication, data confidentiality, and data and system integrity [1] [2]. Effectively implementing and managing a quantum-resistant PKI solution requires adherence to PKI standards, industry requirements, potential government mandates, certificate management policies, training personnel, and data recovery policies that currently do not exist. This research discusses security risks in enterprise DL PKI, areas that can be compromised, and provides an idea of what should be in a PKI DL Risk Management Framework plan.

Keywords: *cyber resilience, PKI, quantum computing, distributed ledger, cyberattack, risk management framework, hyperledger fabric*

5. Blockchain Governance: What we can learn from the Economics of Corporate Governance

Darcy W.E. Allen and Chris Berg
RMIT University Blockchain Innovation Hub, Australia
Category: Oral Presentation

Abstract

Understanding blockchain governance is urgent. This paper uses the transaction cost economics of governance to identify and clarify the tradeoffs that projects make when they are designing blockchain governance systems. Blockchain governance is the processes by which stakeholders – all those are affected by and can affect the network – exercise bargaining power over the network itself. But blockchains interact with, and are shaped by, external institutional frameworks (such as firms who act as institutional investors for tokens, firms that provide exchange services, and governments who regulate on-ramps to the network). Bargaining power in blockchain governance is shaped by 1) the distribution of bargaining power endogenous to the consensus mechanism, 2) exogenous governance structures built on top of an instrumental consensus mechanism, and 3) the needs of bootstrapping. Each impose contradictory pressures towards and against decentralisation. The paper argues that blockchain governance is a specific instance of the general category of the governance of decentralised economic organisation, from protocol decision-making processes, to the organisation of blockchain foundations, to the structures of decentralised autonomous organisations built as applications on top of the blockchain protocol, to the coordination of business consortia that data on a blockchain network. Approaches to governance design in blockchain systems are infused with normative beliefs about the institutional systems outside the blockchain space. We map this against a subjective institutional possibility frontier, offering a framework whereby the tradeoffs for different approaches to blockchain governance can be examined.

Keywords: *governance, blockchain, transaction cost economics, stakeholders, protocol*

6. Are Blockchain based systems the future of Project Management? A preliminary exploration

Robin Renwick
Cork University Business School, University College Cork, Ireland
Category: Oral Presentation

Abstract

Modern institutions are increasingly organized around the fulfilment of discrete goal-specific projects.Correspondingly, the scale, complexity, and diversity of actors involved in projects has also increased. Fortunately, a range of tools and technologies exist to support contemporary project management. The quality and fit of these tools is key to making sure projects remain successful. It is not yet clear whether incremental change and development of these tools is capable of keeping up with growing demands and evolving organisations; tasks involving disparate departments, members, and stakeholders with varying interests and priorities. Many issues with existing tools revolve around scale, trust, and valuation - leading to stratification as preferences appear for any number or combination of proprietary systems. Blockchain technologies may provide support for a new wave of project management systems, allowing managers a new range of capability and feature sets to aid their praxis. This paper presents an explorative case-study, in which open ended interviews are conducted with practicing project managers. Interviews are analysed to understand issues that exist with the currently deployed tools and technologies. Five constructs emerge: transparency, control, dynamic status updating, incentives, and trust. Feedback suggests blockchain-based alternatives could offer significantly better performance on each of these constructs.

Keywords: *blockchain, project management, trust, distributed ledgers, qualitative research*

7. Browser-based crypto mining and EU data protection and privacy law: a critical assessment and possible opportunities for the monetisation for web services

C.F. Mondschein
Maastricht University Faculty of Law, European Centre on Privacy and Cybersecurity (ECPC), The Netherlands

Abstract

Recently, browser-based crypto mining (or browser mining) received attention in academic literature, mainly from work in the field of computer science. Browser-based crypto mining describes the act of websites or other actors mining cryptocurrencies for their own gain on client-side user hardware, which mainly takes place by mining Monero through Coinhive or similar code-bases. Although the practice gained infamy through the various ways in which it was illicitly deployed, browser mining has the potential to act as an alternative means for the monetisation of web services and digital content. A number of studies explored browser mining for monetisation purposes and highlighted its short-comings compared to traditional advertisement-based monetisation strategies. This paper discusses the practice in light of EU data protection and privacy law, notably the General Data Protection Regulation (GDPR) and the ePrivacy Directive, which is currently being overhauled and aligned with the GDPR. It adds to the discussion surrounding the feasibility of browser mining as a potential alternative for monetisation by (i) exploring the legality of browser mining in relation to EU data protection and privacy law (ii) and by identifying possible benefits regarding the protection of individuals' personal data and privacy by deploying browser mining. It is argued that employing browser mining in a transparent and legitimate manner may be an additional option to financing websites and online services due to the growing legal pressure on advertisement models such as programmatic advertisement that rely on the exploitation of large amounts of personal data and ad networks.
Keywords: *Cryptocurrency; Mining; Blockchain; GDPR; Privacy and Data Protection; EU Fundamental Rights*

8. Algebraic methods in the analysis of persistency of attacks in decentralized systems

Oleksandr Letychevskyi
Glushkov Institute of Cybernetics, Ukraine
Category: Oral Presentation

Abstract

The paper considers the use of formal algebraic methods in blockchain system safety and security and in the evaluation of the persistency of an intruder's attacks. A model of blockchain algorithm is presented as the specification of a behaviour algebra. The research problem is the reachability of vulnerabilities and violations of safety properties that are presented in the database as behaviour algebra models. The model uses different methods realised in behaviour algebra theory: algebraic matching, symbolic modelling, static detection of invariants and other methods. It allows significant decrease of false positives and more accurate detection of issues, including deep hidden ones. The algebraic modelling of detected issues also allows for an evaluation of the persistency of attacks on the system. The advantages of this technology are that it can be successfully applied in multiagent environments of distributed systems. Examples of the technology demonstrate the detection of re-entrancy attack in smart contracts, double-spending attack in consensus algorithms and violation of equilibrium in a token economy. The algebraic methods are developed as SDK for decentralised system development and web platforms for access to an algebraic server.

Keywords: *algebraic modelling, symbolic execution, smart contracts, token economy, consensus algorithms, distributed systems*

9. Blockchain to Negate Malware

S.P.M Bergstrom
Quantum1Net, Spain
Category: Oral Presentation

Abstract

Just as Proof of Work was created by Cynthia Dwork and Moni Naor to manage DoS attacks and block spam emails, blockchain can be used to verify data consistency and negate malware and virus attacks. A firewall works by stopping all data that have not been requested from the inside of the firewall, as any data has not been requested is then considered malicious. So, to be able to introduce malware, phishing and social engineering is used to get to the inside of the firewall and infect the machine or device. By using a network overlay and register the network data movements on a blockchain, malicious software can be detected and negated via a consensus function of the network, where the work in the PoW would consist of the data transport not CPU cycles. The reason to use a blockchain is that without an immutable storage a malicious actor could first take over the data moment register and then inject the malware without being detected.

Keywords: *Malware, Blockchain, decentralized consensus, Cybersecurity*

10. Distributed Ledger Technologies And Internet Of Things, A Devices Attestation System For Smart Cities

E Pioli Moro and Alistair Duke
British Telecommunications plc, UK
Category: Oral Presentation

Abstract

Traditional IT security mechanisms are generally not well-suited for IoT devices, where processing and network connectivity should be kept at minimal. Consequently, IoT devices have been recently identified as an easy target for cyber-attacks, like for example on the Mirai botnet Distributed Denial of Service attacks in 2016, where various devices were hacked into and taken over. Different solutions have been developed aiming at guaranteeing the security at both the devices application layer and the network layers. Few succeeded to deliver the flexibility necessary for IoT devices. Even fewer have implemented an effective threats detection system, and just a handful have realised all the previous in a fully decentralised fashion, including this one. This Distributed Ledger Technology (DLT) attestation system is maintained and supported by most, or all, IoT devices because it is based on a light-weight DLT protocol. It comprises of a system for authorisation and authentication for the individual devices as well as includes an anomalies detection system based on smart contracts. A demonstration was built to support a Smart City use case. The objective is to guarantee, in a decentralised manner, the security of low computational power devices executing the sensing function and their connectivity, and therefore the correct functioning of the system. On the demonstrator, the system was ran using DLT supported by the sensors connectivity bridge (built using Raspberry Pi's). The system proved to be rapid to develop, flexible with regards to systems changes and resilient to attacks to both individual IoT devices and to the DLT.

Keywords: *Internet of Things, Distributed Ledger Technologies, Blockchain, attestation, smart cities*

11. Privacy Laws, Non-fungible-tokens and Genomics (DNA)

Daniel Uribe, Genobank.io, USA
Gisele A Waters, Symbiotica LLC, USA
Category: Oral Presentation

Abstract

This article analyses some of the main legal requirements in the new California Consumer Protection Act (CCPA) & General Data Protection Regulation (GDPR) with regard to the intersection between regional privacy law, smart contracts (such as Fungible & Non-Fungible-Tokens) and genomic data. The CCPA & GDPR law imposes several restrictions on the storing, accessing, processing and transferring of personal data. This has generated some challenges for lawyers, data brokers and business enterprise engaged in blockchain offerings, especially as they pertain to high risk data sets such as genomic data. The architecture and technical features of Non-Fungible-Tokens, Distributed Storage & Wallets to trace, store and govern DNA (Genomics) datasets will allow donors (data subjects) to establish digital ownership, control in alignment with privacy laws using customizable code or "Programmable Privacy Smart Contracts". Therefore, in order for stakeholders to be legally compliant, the design of blockchain value propositions should include additional privacy-by-design capabilities in the smart contract coding language itself. This article describes the three domains and begins to explore how data engineers can begin to explore the challenges of coding privacy law, the legal requirements into the earlier stages of the architectural design of the computer code. This automated process focuses on Smart Contracts (NFT's) and genomic data requirements which include selection of a genetic data information schema and a privacy-code that follows programming logic to process sensitive information based on that schema. Programmable privacy is a unique way to write and design computer code, which can automatically check the legal compliance of the smart contractual framework in a trustless and decentralized way. The schema contains a set of legal questions that have been specifically designed to require Cloud providers to disclose relevant information and comply with the legal requirements established by the CCPA and/or GDPR.

Keywords: *blockchain, NFT, smart contracts, California Consumer Protection Act, privacy, private cloud, distributed Storage, IPFS, genomics, DNA, data broker, privacy law, GDPR, CCPA*

12. Transformation or Adaptation of Blockchain at Crossroad of Institutional to Distributed Trust Journey? A Public Sector Perspective

Ali Shahaab[1], Ross Maude[2], Chaminda Hewage[1], Imtiaz Khan[1]
[1]*Cardiff School of Technologies, Cardiff Metropolitan University, United Kingdom*
[2]*Companies House, Cardiff, United Kingdom*
Category: Oral Presentation

Abstract

Blockchain technology has been commended as a solution that can help with disintermediation and filling the consistently increasing trust challenges faced by corporate and public sector. Public services are seeking solutions that can help establish trust and increase transparency with its citizens and businesses are undertaking extensive business analysis to determine the need and effectiveness of blockchain like platforms as the basis for transforming their existing platforms. Due to the decisive nature, most of the analysis results thus indicate that if a trusted third party is an option, then blockchain should not be used. Here we argue that all information technology systems rely on a suite of technologies and therefore blockchain should also be added to the technology stack rather than taking an "all or nothing" approach. We also argue that analysing the effectiveness of futuristic technology like blockchain with industrial age methodology and mind set may limit the realisation of its impact on society and economy. Therefore, we propose to take a heuristic approach where different properties of blockchain technology needs to be mapped against different aspects of current business process with a futuristic view in mind. Taking Companies House – a government organisation that holds over four million UK based companies records as an example, we demonstrate how certain business processes in Companies House can benefit from adapting a blockchain based solution.

Keywords: *trust, blockchain, public services, distributed ledger technology, business process*

13. Modern portfolio theory: a blockchain theoretical model

Alfio Puglisi
Kings College London, UK
Category: Oral Presentation

Abstract

Crypto assets, such as Bitcoin and Ethereum have attracted the interest of investors across the globe. The model presented in this paper is based on the idea of a DLT-based market for securities, where investors have the option of switching between traditional financial securities to crypto-assets. The model based on two game framework (government vs investors) demonstrates that investors are utility maximisers and in the event of unstable exchange rate policy and inflationary pressure, the investors switch between the two assets classes under consideration. In the event of a public DLT based market for crypto assets, the model also shows that there are AML risks and regulatory challenges both for regulators, central bankers in order to track online financial activities of retail consumers.

14. Cost Benefit Analysis of permissioned and permissioneless blockchain solutions

Carlos Castro-Iragorri [1], Federico Lopez [2], Olga Giraldo [3]
[1] *Universidad del Rosario, Colombia*
[2,3] *Linking Data, Colombia*
Category: Oral Presentation

Abstract

This paper is a case study that analyses the adoption of blockchain technology in the management of learning records and the issuance of academic certificates. In this use case we identify service providers that have adopted a permissionless approach and on the other hand consortiums of academic institutions that are in the process of building permissioned networks. We explore the challenges faced by both approaches and obtain information from competing projects to provide an approach for cost benefit analysis in blockchain projects.

Keywords: *permissioned, permissionless, digital credentials, cost benefit analysis, blockchain, economics*

15. Emerging Regulatory Approaches To Blockchain Based Token Economy

Agata Ferreira
Warsaw University of Technology, Poland
Category: Oral Presentation

Abstract

Blockchain enabled digital scarcity, which has opened up the whole new dimension of possibilities for token economy, particularly with relation to rights and assets that have not been traded electronically before. Blockchain based tokenization of rights and assets brought also new set of legal and regulatory challenges. Regulators and legislators are yet to address many of the issues raised by blockchain based tokenization, from decentralization, token characterization to cross border harmonization and regulatory compliance with traditional market infrastructure. Lack of regulatory alignment can undermine many of the benefits of token economy. Lack of legal certainty may not only stifle innovation and slow down mainstream adoption of blockchain based tokenization, but it can also raise the risks for the investors and harm the reputation of the industry. The emerging regulations vary in approach. Liechtenstein became the first country to have a comprehensive technology neutral regulation of the token economy. Malta and Singapore also represent progressive jurisdictions for blockchain regulations. However, most jurisdictions, including the US and the EU, have not yet formed clear policy for blockchain regulation and many legal questions remain open. The paper examines whether there is an emerging dominating regulatory approach or prevailing regulatory direction for the future of token economy. It also highlights the existing regulatory void and divergent approaches to blockchain based tokenization. Finally, the paper concludes that there is an urgent need to provide clear legal and regulatory framework if the potential of the token economy is to be realised.

Keywords: *blockchain, tokens, token economy, blockchain regulation*

16. Using Blockchain for Evidence purpose in Civil Cases in Poland

Rafael T. Prabucki
The University of Opole, Law and Administration Faculty, Poland
Category: Oral Presentation

Abstract

For some period of time Blockchain technology has been used for many purposes all over the world. There are many various types of reports that indicate that Blockchain technology is used to maintain a national database of records, for example for processing electronic records containing information about lands. Additionally, many private or public entities are interested in such a solution. The question arises - how to prove the facts in the dispute, when data is stored or protected by applying the solution based on the Blockchain technology? The answer to this question is narrowed down to civil issues. Currently, the Smart City trend will shows that blockchain issues will be intensively used in heavy contract area (energy, transport). Furthermore, the Polish law has introduced a new tool, in the form of a contract of evidence (similar to the Parol Evidence Rule), which may increase the popularity of so-called smart contracts. The research methodology is based on the analysis of existing regulations, which may be relevant to the Polish Court's perception of evidence based on blockchain technology. Moreover, legal scientific studies that indicate the risks associated with proving certain facts in such a way will be analysed. All efforts have been taken in order to obtain conclusions regarding the future of this type of solution in Poland.

Keywords: *evidence, blockchain, registers, civil cases, smart contract, polish law*

17. Solidity + : A language for Robust programming of Smart Contracts

RK Shyamasundar, Snehal Borse, Prateek Patidar
Department of Computer Science and Engineering
Indian Institute of Technology Bombay, India
Category: Oral Presentation

Abstract

Smart Contracts handle and transfer assets of considerable value. Thus, it is crucial that their implementation be secure against attacks which aim at stealing or tampering the assets. In the recent past, there have been several attacks that have exploited existing vulnerabilities in smart contracts. The functioning and deployment of smart contracts is somewhat different from the classical programming environments. Once a smart contract is up and running, changing it, is very complicated and nearly infeasible. One of the reasons is that when a contract is created, it is immutable; once deployed on the Blockchain it stays there forever. If we find a defect in a deployed smart contract, a new version of the contract has to be created and deployed. When we deploy a new version of an existing contract, data stored in the previous contract does not get transferred automatically to the newly refined contract. We have to manually initialize the new contract with the past data which makes it very cumbersome. Similarly, neither updating a contract nor rolling back an update is possible; this greatly increases the complexity of implementation and places a huge responsibility while being deployed initially on the Blockchain. Smart contract languages today are derived from extensions of general purpose languages like Javascript. While the similarity make smart contract languages look familiar to software developers it is inadequate to accommodate the domain-specific requirements of digital contracts. Smart contracts have not only shed light on the benefits of digital contracts but also on their potential risks. Some of the prominent smart contract languages are Solidity, GO etc. Like all software, smart contracts can contain bugs and its' vulnerabilities can be exploited that can have direct financial consequences. Thus, it is very important to have a sound methodology, that is practical enough for use by a large community of smart contract programmers to check the contracts for crucial properties. Solidity is one of the widely used languages for programming smart contracts. It has been designed for Ethereum architecture. Several security vulnerabilities in Ethereum smart contracts have been discovered both by hands-on development experience, and by static analysis of contracts on the Ethereum Blockchain. These vulnerabilities have been exploited by several attacks on Ethereum, causing huge loss of money. One of the most successful of these attacks managed to steal $60M from the DAO contract, but its' effects were cancelled after an harshly debated revision of the Ethereum Blockchain. There has been a significant amount of work done in analyzing correctness of smart contracts. Some of the major deficiencies of these explorations are (1) analysis is based on the bytecode generated for Ethereum rather than smart contracts in Solidity, (ii) analysis is approximate and have severe limitations in usage due to over-/ or under-approximation. In this talk, we want to address the following question: Using a stark resemblance of Solidity programs with distributed programs, can we arrive at a concurrent programming language approach of arriving at simple specifications of Solidity programs similar to classical declarations used in concurrent programming languages that leads to robust programming of smart contracts. We describe the design and use of language Solidity!, for programming smart contracts; Solidity + is essentially the same as Solidity except for declarations. We show how a vast variety of vulnerabilities encountered in programming smart contracts in Solidity no longer exist in Solidity! , due to declarations. We further show that Solidity! can be automatically transformed to Solidity – thus, enabling effective debugging at source level. Another important outcome of using of Solidity +, is thatbrings out an outline of a proof carrying code for the smart contract for free – needless to emphasize that it is a very welcome feature for smart contracts on Blockchains.

18. A Peer-To-Peer Publication Model On Blockchain

Imtiaz Khan and Ali Shahaab
Cardiff Metropolitan University, UK
Category: Oral Presentation

Abstract

For centuries journals remain the primary platform for scientific communication and act as the trusted third party to ensure the quality and integrity of the peer reviewed published works. However, past few decades witnessed a sharp rise of research irreproducibility and retraction to a point that now is deemed as crisis. Addressing this crisis here we present a peer-to-peer (P2P) publication model that utilise blockchain and smart contract technologies. Focussing primarily on researchers and reviewers, the conceptual P2P publication model addresses the sociocultural and incentivisation issues related to irreproducibility crisis where publication will be incremental and authorship will be accumulative and shared with reviewers. The concept of P2P publication model was inspired by the transformational journey music publishing industry has undertaken as it traverse through vinyl age (complete album) to Spotify age (song-by-song) along with growing inclination towards building an incremental album with feedback from fans and establishing a decentralised and automated revenue collection and sharing system using blockchain and smart contract technologies. Incremental publishing of scientific work through P2P publication model will relieve researchers from the burden of publishing complete and "good results", also at the same time reviewers will be recognised and incentivised in a competitive manner to undertake rigorous review work. P2P publication model aims to transform the century old publication model and incentive structure in alignment with the context and aspiration of 21st century scientific endeavours.

Keywords: *research reproducibility, blockchain, sociocultural issues, publication*