CONFERENCE PROCEEDINGS

1st Blockchain International Scientific Conference 12 March 2019, London

1. Blockchain investigations – Beyond Money

Simon Dyson
Edinburgh Napier University, UK
Category: Oral Presentation

Abstract
Cryptocurrency investigations have centred almost entirely around the transfer of value "money" or a cryptocurrency asset. The use of cryptocurrency for illicit purposes, especially Bitcoin, is well documented both in academic writing, media reporting and even film documentaries. The infamous Silk Road market place in addition to the millions of dollars spent within dark markets on drugs, guns and assassinations have grabbed the headlines. This paper looks at how blockchain is creating new areas of investigation that are yet to be explored in detail. This scenario based paper examines the hosting of stolen data (P.I.I) personal identifiable information on a distributed blockchain host where the data is also stored. The platform used is based on Ethereum infrastructure but demonstrates just one available platform that poses the paradigm. The paper examines the considerations through the lens of an incident responder / cyber investigator, forensics examiner and data controller. The scenario highlights distinct differences in considerations from a traditional response compared to dealing with the immutable and unstoppable distributed technology. The paper concludes that more is needed to be done to understand digital forensics in the blockchain era and the need to develop beyond track and trace in the cryptocurrency investigative tool box. The discussion also brings forth how data retention and GDPR requires consideration when applying it blockchain systems.
Keywords: *Blockchain, Distributed-hosting, Distributed-storage, Ethereum, Swarm, Forensics*

2. Cryptocurrencies & Initial Coin Offerings: Are they Scams? An Empirical Study

Daniel Liebau[1], Patrick Schueffel[2]
[1]*IE Business School*
[2]*HEG Fribourg School of Management*
Category: Oral Presentation

Abstract
The volume of Initial Coin Offerings (ICOs) had risen steeply with an all-time high market capitalisation of close to 1 Trillion USD in December 2017. Since then, the digital asset market has slumped, retreating to approximately 200 Billion USD by mid-2018. Stakeholders of the crypto industry have pondered the reasons for this retrenchment and are increasingly focusing on the notion that many ICOs could be scams. A recent industry study even went as far to claim that 80% of all ICOs are indeed scams. In this paper, we investigate the question whether these scams are as common as claimed. We do so by first defining what a scam is and secondly, by drawing on empirical data to assess the number of cases fitting such a definition. Building on Principal Agent Theory and based on the statistical analysis of our empirical data set we attempt to establish the current state of affairs with regards to scams in the cryptocurrency world. The results of our study divert from salient beliefs.
Keywords: *blockchain, scam, ICO, digital assets, ethics, crypto-currency, token*
JEL Classifications: *D01, D21, D26, D53, D84, K24*

3. The Application of Behavioural Heuristics to ICO Valuation and Investment

Maxwell Stanley
University of Essex, UK
Category: Oral Presentation

Abstract

Blockchain projects have seen a rush of investment in the form of Initial Coin Offerings (ICOs) over the past eighteen months, yet little is understood about how to valuate these projects. This research looked at the application of behavioural heuristics to ICO valuation and investing. Identified were six variables that may play a role due to key behavioural biases. These variables, coin value, market capitalisation, ease of understanding, market sentiment, maximum ICO bonus level, and pre ICO social media levels were analysed using Pearson's correlates for their correlation with return on investment. The data was collected from numerous ICO websites along with Twitter data. Fundamental analysis was taken from Coincheckup due to this being a major source of information for many retail investors and uses a well-defined methodology. Sentiment data was collected from Twitter and assessed using crimson hexagons Sentiment tool. Ease of understanding was evaluated using AWS Blockchain business canvas. All information was compiled into a single dataset and the top 47 projects in terms of ROI were utilised. Ease of understanding was found to be significantly correlated ROI. Ease of understanding was then combined with fundamental analysis to develop a hybrid model of evaluation for Cryptocurrency projects. This model substantially outperformed fundamental analysis alone with a 33.6% improvement on ROI. In conclusion, current methods of fundamental analysis for Blockchain projects are inadequate to capture their potential future value. Investors, devoid of appropriate tools, limited knowledge and experience due to the relative novelty, are being influenced by behavioural factors such as ease of understanding. It is therefore impertinent that investors and entrepreneurs alike take such factors into consideration.

Keywords: *blockchain, behavioural economics, behavioural heuristics, ICO, cryptoeconomics, tokenomics*
JEL Classifications: *D02, D71, H11, P16, P48, P50*

4. Assigning Residual Rights to Smart Contracts

Lucas Leger
Conservatoire des Arts et métiers
Category: Oral Presentation

Abstract

One of the promises of smart contracts is to remove third parties to structure trading relationships in the digital world, from market platforms to organizations themselves. The conditions under which trade will take place is enforced through self-executing programs that run on blockchains. In this theoretical paper, we investigate how can we assign optimal residual rights within smart contracts? Indeed, in traditional organizations like firms, ownership rights are well established. As shown by Grossman and Hart (1986) in their seminal work an optimal distribution of residual rights, i.e. control over the use of assets, protect stakeholders and owners "from future holdups by other trading partners." In blockchain-based networks this setup does not exist, because i) assets are especially human capital, ii) funds are stored on the blockchain where residual rights lay in the hand of a third party: miners and the so-called whales who basically control the consensus protocol. Using The DAO hack as a use case, we demonstrate that most smart contracts lack governance mechanisms to protect and incentivize both owners and investors, especially when things do not go according to plan. Then, we apply the formal framework of incomplete contract theory to design a smart contract that would automatically assign optimal residual rights.

Keywords: *Smart contracts, Incomplete contracts, residual rights, governance, DAO*

5. Parameters for building sustainable blockchain application initiatives

Lewis Laidin, Kassandra A. Papadopoulou
The University of Manchester, UK
Category: Oral Presentation

Abstract
Despite the demand and interest for the technology, there are still major challenges for blockchain application initiatives (projects and ventures) to be sustainable and reliable. While starting a non-blockchain initiative already comes with its own sets of challenges and has around 50% failure rate, starting a blockchain initiative rises the rate to 90% due to additional variables and confusions on top. Such a situation deters innovators and eventually dampens innovation, requiring priority for actions. This paper attempts to contribute by compiling and outlining the various key variables required to be considered, creating a set of parameters for blockchain initiators. Through secondary data collection: literature reviews, report studies and primary data collection: interventional and observational case study, interviews with blockchain researchers, businesses and entrepreneurs, this paper categorises variables into blockchain-related and venture-related categories, outlining consideration points for each variables. To summarise the variables and by consulting theories of innovation and adoption, it is then concluded in the paper that concept validation entailing both initiative feasibility and user-demand, is of key importance, both for blockchain innovation, for trust between ecosystem stakeholders and for the venture sustainability.
Keywords: *blockchain, business, initiatives, challenges, barriers, parameters, feasibility, concept*
JEL Classifications: *D04, D07, D08, I07, O03, Y04*

6. Blockchains and Financial Intermediation – An alternative approach to monitor the Monitors

Klara Sok
Conservatoire National des Arts et Métiers
Category: Oral Presentation

Abstract
The emergence of Bitcoin, blockchains and distributed ledger technologies led some commentators call for the end of banks, or at least for a profound change in financial intermediation (Antonopoulos, 2016): what if, indeed, there were an alternative solution to producing and distributing financial services to society, to the one we know today? What if organizing markets in a different way, with the use of information technology, could mechanically decrease uncertainty, just by design? Could the panopticon architecture of distributed autonomous organizations (DAOs) be a substitute to current financial intermediation? This research work proposes a theoretical framework aiming at supporting socio-economic analyses of blockchain-based innovations applied to financial intermediation, through the lens of institutional information transformation. Financial intermediation is considered as a solution to information asymmetries resulting in market inefficiencies (such as adverse selection and moral hazard) between demand for financing and financing offering. Financial institutions operate as informational "monitors" on behalf of funders (Diamond, 1984) and are themselves monitored ("monitoring the monitor") through financial regulation and institutional surveillance. This research aims at theoretically demonstrating how distributed ledgers and distributed consensus, applied to financial transactions, could impact the structure and efficiency of our financial system, depending on their organizational design and institutional embeddedness.
Keywords: *blockchain, Bitcoin, financial intermediation, cryptofinance, monitoring the monitor, fintech*
Themes: *blockchain, financial intermediation, monitoring the monitor, oracles, information asymmetry, adverse selection, moral hazard, fintech, regtech*

7. Capital mobility in light of emerging technologies: the case of crypto-asset investment

Alfio Puglisi
Kings College London, UK
Category: Oral Presentation

Abstract

The benefits of Blockchain technologies in finance are widely acknowledged but there are concerns on the risks associated with it. In this space, crypto-assets are new financial innovation and have only recently begun to attract the attention of financial regulators. What remains to be seen is how different jurisdictions approach regulations regarding Blockchain applications, not only in concept but also in actual practices.

This paper takes a cross-country comparative approach of the diverse types of governance strategies taken to date to address the risks posed by Blockchain technologies and their fit to current orthodoxies of regulatory governance. It examines the (in) adequacy of traditional approaches to regulating and governing Blockchain technologies and of the actions of government with new approaches.

For instance, in December 2017 the International organisation for securities (IOSCO) published on its website a non-binding statement on crypto-assets and initial coin offerings (ICOs), emphasizing crypto-assets as a form of security. Regulatory preferences at national and international level differ. Offshore jurisdictions respond to markets via a responsive regulatory framework, allowing players with more flexibility. On the other hand, most developed economies acknowledge the issues but yet have implemented any specific strategies. Thus, this regulatory uncertainty fuels self-regulatory frameworks administered by private enterprises. Self-regulatory frameworks can be explained in terms of a coordination game between actors in the crypto space. To do so, this paper employs a comparative politics approach to examine policy preferences.

Results shows that regulatory institutions allow jurisdictions to protect sector's competitiveness and lead the way to the race of the global FinTech hub. Self-regulation allows players to shape public debate in the area of crypto-finance

8. Blockchain and Distributed Ledger Cryptography Evaluation in Post-Quantum World

Rob Campbell
Capitol Technology University
Category: Oral Presentation

Abstract

This paper evaluates the current cybersecurity vulnerability of the prolific use of Elliptical Curve Digital Signature Algorithm (ECDSA) cryptography in use by the Bitcoin Core, Ethereum, Bitcoin Cash, and enterprise blockchains such as Multi-Chain and Hyperledger projects such as Fabric, and Sawtooth Lake. These blockchains are being used in Media, Health, Finance, Transportation and Government with little understanding, acknowledgment of the risk and no known plans for mitigation and migration to safer public-key cryptography. The second aim is to evaluate ECDSA against the threat of Quantum Computing and propose the most practical National Institute of Standards and Technology (NIST) Post-Quantum Cryptography candidate algorithm lattice-based cryptography countermeasure that can be implemented near-term and provide a basis for a coordinated industry-wide lattice-based public-key implementation. Commerical quantum computing research and development is rapid and unpredictable, and it is difficult to predict the arrival of fault-tolerant quantum computing. The current state of covert and classified quantum computing research and development progress is unknown and therefore, it would be a significant risk to blockchain and Internet technologies to delay or wait for the publication of draft standards. Since there are many hurdles Post-Quantum Cryptography (PQC) must overcome for standardization, it is the author's view that coordinated large-scale testing and evaluation must be now.

Keywords: *ECDSA, blockchain, post-quantum, lattice-based cryptography, cybersecurity*

9. Leveraging Blockchain Technology for the Social Determinants of Health

Marquesa Finch
Patientory Association
Category: Oral Presentation

Abstract

Although not a new technology, blockchain has increased in popularity since 2017 as a technology that may prove to have many benefits for the healthcare industry. With secure technology and encryption mechanisms, blockchain can give rise to a new era digital healthcare technologies with improved access to patient data.

For blockchain, 2018 has no doubt been a milestone year. At the time this paper was written, over $21 Billion had been raised in 2018 alone on tokens sales over 905 ICOs. And while cryptocurrency may be experiencing an adjustment, one thing is clear--blockchain's utility across industries is poised to disrupt many of our current systems for exchanging data, information, as well as money. Within healthcare, blockchain's immutable distributed ledger offers solutions for many pain points within our healthcare system including privacy, trusted record keeping, and data coordination/access. While the identified use cases in healthcare are numerous, one stands out in particular-- the coordination and access to trusted data in addressing the social determinants of health.

The barriers to data sharing among clinical entities are breaking down as technology solutions become evident and accepted. Blockchain technology provides the means to create a trust protocol verifying identity and transactions. The ability to trust the process, trust the security, trust the identity and intersect with clinical and public health imperatives will enhance data management, care coordination and improve the process and outcome of individual and community health.

10. Distributed Stateless Society: Liberty, Manorialism and State

Aleksei Gudkov
UCL Centre for Blockchain Technologies, UK
Category: Oral Presentation

Abstract

Decentralization, creativity and freedom are the key notions describing all major trends on blockchain. Common cultural identity allows forming a stateless society in virtual world. Stateless society exists without any sort of state attribute. Distributed stateless society is formed on the on-line network and blockchain technology. The Distributed stateless society has no territory, sovereignty and central authority with coercive power. The core values of stateless society are liberty and cooperation based on anonymity and voting. Speaking in favor of human right we should accept the right to be anonymous. Anonymity guaranties personal freedom through negative liberty on distributed network. The right to be anonymous is important not only for participants of distributed stateless societies but also for fighting with censorship and personal information collection. Economic development of the Distributed stateless society is based on smart contracts and cryptocurrency, which make available exclusion of intermediaries. Though, the adaptation to off-line word has some problems. The major problem of adaptation of blockchain technology is competition between math law, code and legal rules. The blockchain technology under traditional legal regulation has a good chance for implementation in a close system for data management but not for a creation of legal facts yet. I propose to support autonomy of blockchain technology and prohibit it from traditional operational model with human verification and old fashion regulation. We have all chances to create cooperative distributed society to achieve the balance between private and public needs. The Cooperative distributed society should be based on concept of private ordering, where all interested parties rely on self-regulation by creation of self-governance system recognized and legitimized by state authority. The critical element

of the self-governance structure is self-regulatory body. It is reasonable to build a community-driven self-regulatory body to find a compromise between stateless society and traditional regulation. We should speak for independent self regulatory layer for blockchain network. I call for discussion on freedom on blockchain network and invite you to take part in creation of a distributed cooperative society.
The present article aims analysis of stateless societies; reviews historical development of the concept; discuss the features of Distributed stateless society, variants of adaptation blockchain technology, threats of distributed manorialism; and helps to uncover conflicts and opportunities.

11. Data Transparency in Interbank Lending

Andrew Seski[1], John B. Zirnkilton[2]
[1] *University of Delaware, USA*
[2] *Broad Reach Management LLC*
Category: Oral Presentation

Abstract
Considerations and Limitations of Tracking Quality of Collateral with DLTs:
1. Goal: Call to attention the overlap in focus by multiple central banks and boards of financial stability: opacity in bilateral repo markets, defining high quality liquid assets, and oversaturation of short-term funding for long-term projects. DLTs: a distributed ledger across interbank lending networks for access to uniform market data, origination of collateral, and the number of market participants relying on that asset for liquidity would serve as a single portal into capturing hard-to-track market data that countries rely upon for systemic risk modeling.
Exploring limitations of ethereum-based smart contracts:
A. While incredibly fast to read from, blockchains are also incredible slow to read to.
B. Upper limits of chosen fields encoded into smart contracts are reached quickly when the associated logic is complex.

DLT Proposal and Call to Action

1. Market Issues:
A. No window into the complex repo markets, relying on ETF data to model liquidity provisions.
B. Slow and inefficient settlements, centralized trust, and asymmetric information.
C. No way to adequately regulate what is unknown.

2. Proposed Solutions:
A. A single distributed ledger to track the full lifecycle of both sides of transactions in interbanking networks including derivative exposures and further measuring the shadow banking network.
B. Encoded smart contracts that only settle with matching regulatory requirements.
C. Aim to negate a need to rely on Self-Regulatory Organizations, Central Clearing Houses, and Rating Agencies for uniform information.

3. Call to Action:
A. Review requirements of defining high quality liquid assets across borders and provide increased transparency in collateral management.
B. Continue to explore methods to merge and update multiple technological infrastructures into a single portal of access to uniform information.