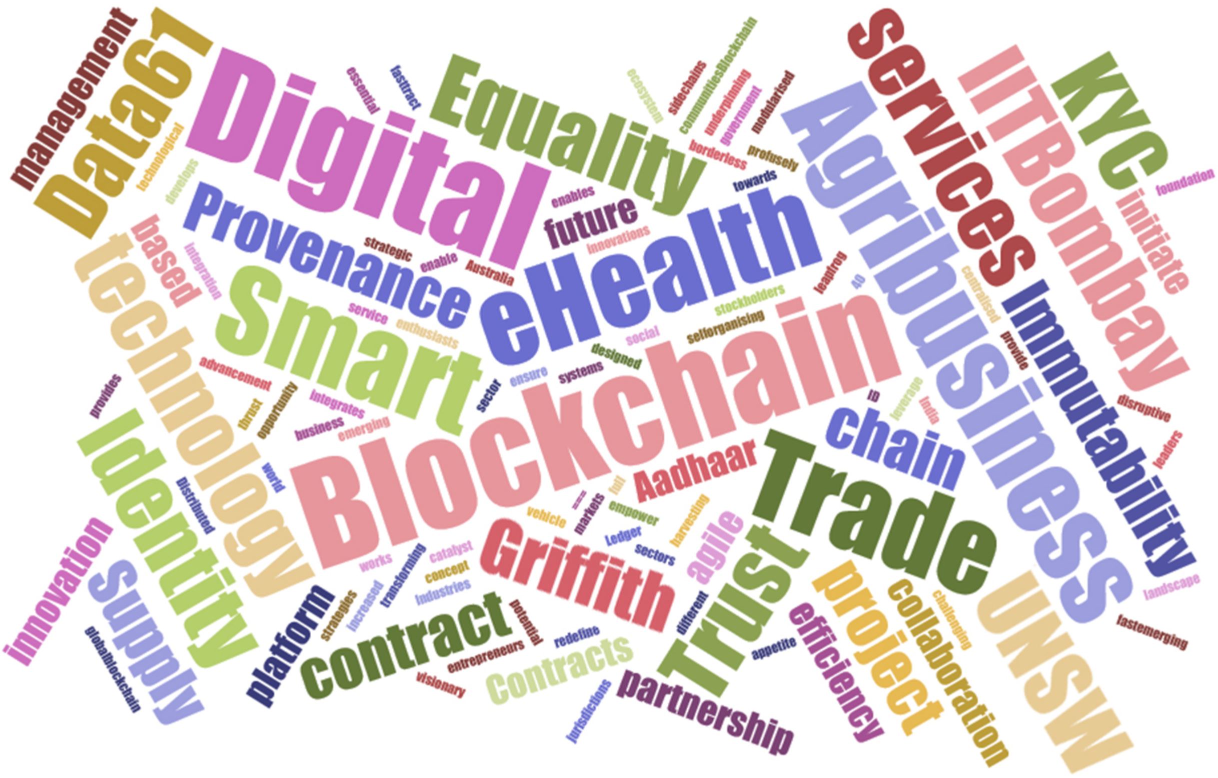
Griffith
UNIVERSITY

The 4th Symposium on Distributed Ledger Technology



10 December 2019

Griffith University

Welcome!

Dear Colleagues,

On behalf of the Organising Committee, we would like to welcome you to The 4th Symposium on Distributed Ledger Technology that will be held at Brisbane, Australia on 10 December 2019. Building on the success of the previous symposia, this event will cover technical, legal, regulatory, business and societal aspects of the innovative technology and its applications.

The SDLT 2019 program features two keynote addresses, technical sessions, lightning talk session, and a panel discussion. We have a great line-up of speakers and registered participants, who are some of the world leading researchers and practitioners in this area from academia and industry.

The CFP received excellent response from around the world, with high quality accepted papers. We thank all the authors of the submitted papers and the reviewers for their insightful review comments.

This forum provides an excellent opportunity for sharing the latest development on the promise of enabling ‘new deals on data’ from different angles, and for collaborating on future projects.

We thank all the sponsors, who generously supported to ensure this event is a success.

4th Symposium on Distributed Ledger Technology

Tuesday, 10 December 2019 (8.00am – 5.30pm)

N79_1.05, Nathan Campus, Griffith University

Program Schedule

8.00am: Registration and Coffee on Arrival

8.30am: Welcome Address

Prof Carolyn Evans, Vice Chancellor and President, Griffith University

8.35am: Opening Remarks

Prof Andrew Smith, Pro-Vice Chancellor, Griffith Sciences

8.40am: Keynote Speech - 1

Chair: Prof Paulo de Souza, Head of School, ICT, Griffith University

Economic Identity in a Digital Economy

Prof Jason Potts, Director, RMIT Blockchain Innovation Hub, RMIT University

9.20am: Technical Session - 1

Chair: Prof Raja Jurdak (Queensland University of Technology)

Multi-Factor Authentication using an Enterprise Ethereum Blockchain

David Hyland-Wood (University of Queensland, ConsenSys/ PegaSys)

EnergyPie: A Hyperedge-based Blockchain Market Model

Karumba Samuel (UNSW), Salil S. Kanhere (UNSW) and Raja Jurdark (QUT)

10.00am: Morning tea

10.30am: Technical Session - 2

Chair: Davin Holmes (Anonyome Labs)

Application Level Authentication for Ethereum Private Blockchain Atomic Crosschain Transactions

Peter Robinson (University of Queensland/ ConsenSys/ PegaSys)

Towards Declarative Smart Contracts

Kevin Purnell (Macquarie University) and Rolf Schwitter (Macquarie University)

Towards Model-Driven Expressions of the Blockchain Ethical Design Framework

Zoran Milosevic (Deontik)

11.45am: Lightning Talk Session

Chair: Don Sands (Synengco Pty Ltd)

Open End-to-End Encrypted Messaging

Steven McCown (Anonyome Labs), Paul Ashley (Anonyome Labs) and Jon St. John (Anonyome Labs)

Cellular Automata-based Puzzles for ASIC-resistant Proof of Work

Rade Vuckovac (Griffith University)

A Nonparametric Method for Measuring Cybersecurity Risk

Patrick O'Callaghan (University of Queensland)

12.20pm: Photo Session

12.30pm: Lunch

1.45pm: Keynote Speech - 2

Chair: Dr Kamanashis Biswas (Australian Catholic University)

How to Build a Government Ecosystem using Blockchain Technology

Katrina Donaghy, CEO and Co-Founder, Civic Ledger

2.20pm: Technical Session - 3

Chair: Lawrence Lim (PCCW Global)

Unlocking Additional Value Through Smart Market Trading in Water Quality and Treated Wastewater using Blockchain Technology

Anik Bhaduri (Griffith University), Vallipuram Muthukkumarasamy (Griffith University), James C.R. Smart (Griffith University), Joe McMohan (Griffith University), Kamanashis Biswas (ACU), Aditya Kaushik (IISc) and Rob Braunack (Civic Ledger)

Blockchain for the Red Meat industry: Where and How?

David Barnes (Griffith University), Yong Wu (Griffith University), Peter Tatham (Griffith University) and Vallipuram Muthukkumarasamy (Griffith University)

3.00pm: Afternoon tea

3.30pm: Technical Session - 4

Chair: Zhe Hou (Griffith University)

Digital Twins and Distributed Ledger Technology: What Can They Learn From Each Other?

Valeri Natanelov (Queensland University of Technology), Gerd Wagner (Brandenburg University of Technology) and Marcus Foth (Queensland University of Technology)

Behavioural Analysis of Cryptocurrencies Investors

Hai Yen Tran, Tracey West and Victor Wong

4.10pm: Panel Discussion

Chair: Dr Raghavendra Ramesh (Consensys/ PegaSys)

Challenges and Opportunities for DLT Application and Future Directions

Guangdong Bai (University of Queensland), Katrina Donaghy (Civic Ledger), Ali Dorri (Queensland University of Technology), Richard McKeown (Integrated Capital), Jason Potts (RMIT)

5.00 – 5.30pm: Close of Symposium & Networking

Keynote Speech 1

Economic Identity in a Digital Economy

Prof Jason Potts, Director, RMIT Blockchain Innovation Hub, RMIT University

Abstract:

The quality of identity affects the ability of firms to product-quality discriminate through the coproduction of identity and data. Government supply of identity (and regulatory constraints on the private supply of identity) induces a low-quality identity equilibrium, harming consumer welfare and distorting industry competition (specifically, inducing horizontal mergers). We argue that blockchain technology using zero knowledge proofs can disrupt this bad equilibrium by facilitating privacy without secrecy.

Bio: Jason Potts is Professor of Economics in the School of Economics, Finance and Marketing at RMIT University, and Director of the Blockchain Innovation Hub, the first social science research institute on Blockchain in the world. Dr Potts is a Fellow of the Academy of Social Sciences of Australia and one of Australia's leading economists on economic growth, innovation and institutions, and on the economics of cities, culture and creative industries. He is editor of the Journal of Institutional Economics. His latest books are Innovation Commons (OUP) and Understanding the Blockchain Economy (Elgar).

How to Build a Government Ecosystem using Blockchain Technology

Katrina Donaghy, CEO and Co-Founder, Civic Ledger

Abstract:

In this practical discussion, Katrina will step through five important considerations when working with government to solve problems where blockchain technology has advantages over legacy systems. These five points for discussion are based on her three-plus years experience co-creating project and products with all levels of government in Australia.

Bio: Katrina Donaghy is the Chief Executive Officer and Co-Founder of Civic Ledger, a multi-award winning Australian GovTech start-up helping governments to be more efficient, effective, accessible and transparent in an ever-increasing digital society. Prior to founding Civic Ledger, Katrina was a career bureaucrat spanning 20+ years in both state and local government in Australia working in the areas of strategy, program delivery and revenue optimisation to improve the customer experience with government.

Multi-Factor Authentication using an Enterprise Ethereum Blockchain

David Hyland-Wood
PegaSys, ConsenSys and
School of ITEE, The University of Queensland
Brisbane, Australia
david.wood@consensys.net

***Abstract*—A method is presented to use an Enterprise Ethereum blockchain with particular configuration and the addition of smart contracts as a multi-factor authentication or multi-party authorisation device to protect command channels from cybersecurity exploitation. The general approach has been previously discussed in the context of spacecraft control. We believe this work to be generally applicable to many enterprise scenarios, such as whenever a command execution would be difficult to roll back (e.g. permanent erasure of data, control of critical infrastructure, large monetary transfers, or weapons release).**

***Index Terms*—blockchain, Ethereum, cybersecurity, authentication, authorisation**

I. Introduction

Existing enterprise information systems are widely acknowledged to be vulnerable to many forms of cybersecurity attacks [1], [2]. Such vulnerabilities are particularly dangerous when compromised networks and user accounts are used to issue commands that would be difficult or impossible to roll back. Obvious examples include permanent erasure of data, control of critical infrastructure, large monetary transfers, or weapons release.

The author's research team has recently proposed a means of securing spacecraft command pathways using a blockchain [3]. Specifically, that work determined that a consensus algorithm with immediate finality should be used (IBFT 2.0 [4] was chosen), and suggested a read-only relationship between a remote device and a verifying blockchain. However, the approach can be generalised to any information technology system, regardless of the specific command pathway or type of asset being commanded.

Encryption of command pathways to remote devices is surprisingly uncommon. One recent industry survey found just 45% of surveyed enterprises "have an encryption strategy applied consistently across their enterprise." [5] The same survey found an even smaller percentage (28%) encrypt IoT devices. This rather unfortunate state of affairs suggests the need for additional means of securing communication to edge devices.

II. Method

Two possible ways to secure command communication may be borrowed from experiences with securing cloud computing and weapons systems: multi-factor authentication and multi-party authorisation. Either may be used to secure edge devices by using call-backs to acquire external information for verification of a command prior to its execution.

Multi-factor authentication is used to ensure that a user is who they say they are. For example, one may provide credentials to log onto a bank's IT systems, and then subsequently be asked to confirm this login request via an email, message to a registered mobile phone, or use of a separate hardware token. The second, hopefully independent, confirmation of the user's identity significantly increases the challenges facing a remote attacker attempting to gain unauthorised access.

Similarly, multi-party authorisation requires a separate party to validate an operation one wishes to perform before being allowed to proceed. In the case of a banking system, a bank may wish to confirm an attempt to close a joint account with any other account holders before taking action.

Fig. 1 illustrates the communication paths for simple command passing (Fig. 1a). For either the multi-factor authentication or multi-party authorisation scenarios, a separate step may be inserted as an additional check (a confirmation of an authentication, authorisation or both) prior to command execution (Fig. 1b).

The use of an Enterprise Ethereum [6] blockchain as a confirming system allows for some interesting and useful concepts to be employed. A blockchain is a naturally distributed system that must come to consensus on new information in order to operate. The addition of arbitrary smart contract execution allows users of an Ethereum blockchain to encode whatever business logic is appropriate for a given use case. A smart contract may be written to require actions taken by blockchain users, off-blockchain processes (e.g. via [7]), other smart contracts, or any combination thereof. There is no theoretical limit to the business logic that may be so encoded (although implementations clearly have many practical limitations, e.g. inability of hardware or operating system to execute business logic with high algorithmic complexity).

For example, a smart contract may be written so a command destined for an edge device will not be validated by the contract until an authenticated user confirms their identity via a separate communications path (multi-factor authentication) or multiple authenticated users confirm the command's validity (multi-party authorisation). Commands may also be checked for correctness of form (syntax), usefulness in an operational context, or any other automated checks that may be encoded in a smart contract.

Adjusting edge device software to read from a remote system prior to command execution should require minimal changes for those systems that allow for remote software updates. The bulk of the work to implement multi-factor authentication and/or multi-party authorisation would fall to

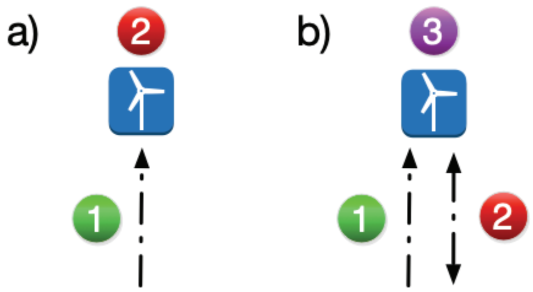


Fig. 1. Options for command execution

a blockchain, where it can be more easily reached, extended, maintained and managed.

Implementation of additional computation, communication, implementation, etc, for the purpose of improving cybersecurity is often and rightly viewed as an economic cost. It is therefore important to note that a spectrum of options exist to improve the security of edge device call-backs so that the level of protection is proportional to the perceived risk, i.e. the probability of the attack and the expected consequences or impact of such an attack. Reading a command verification from a blockchain may be itself sufficient to protect against a single account disclosure, but only if the communication channel is secure and the blockchain node returning the information is not in itself compromised. Security could be improved by (e.g.) having an edge device query more than one node on the blockchain, using a so-called trusted oracle to cryptographically sign a command verification at the smart contract, using some verifiable computing scheme to produce a proof that the command verification has actually been included in the blockchain and cannot be removed (except, perhaps, with negligible probability). It would also be possible in cases where sufficient computing power exists on an edge device to run a "light" blockchain client. A light client would allow an edge device to directly verify the Merkle path to a command verification.

Fig. 2 illustrates a complete multi-factor authentication and multi-party authorisation example. The steps are followed in alphabetical order:

a) An operator proposes a command to be sent to an edge device;
b) Some number of automated processes (zero or more) confirm command syntax and perhaps applicability in the operational context;
c) Some number of humans (zero or more) confirm the command should proceed;
d) The smart contract sets the entry of the command approval table associated with the hash of the command to the Boolean value True;
e) The operator sends the command to the edge device;
f) The edge device hashes the command and verifies that the entry of the approval table associated with the hash is set to True using one of the techniques listed above; and
g) Finally, the edge device executes the command if and only if the command verification was successful.

It is worth noting the blockchain nodes come to consensus after each write to the smart contract.

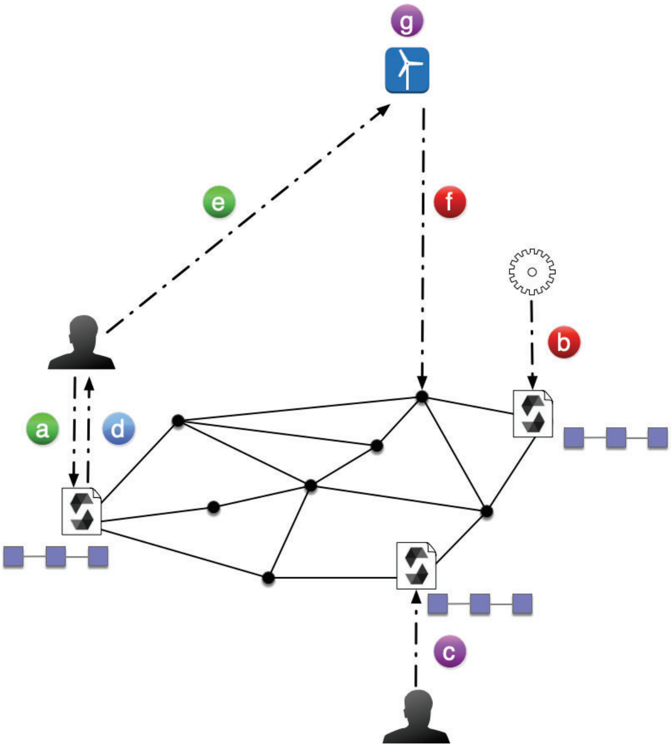


Fig. 2. MFA and MPA backed by a blockchain

III. Conclusions and Further Work

A high-level and general method was presented to perform multi-factor authentication and/or multi-party authorisation using an Enterprise Ethereum blockchain. Following the more complete work in [3], an IBFT 2.0 consensus algorithm was suggested, along with smart contracts to implement the desired functionality.

The key benefit of this approach is to provide a much higher level of authentication and/or authorisation security. An attacker would need to gain control over an arbitrary number of user accounts and be able to use those accounts to perform actions on the blockchain in order to confirm an inappropriate command. This approach can reduce the likelihood of command exploitation, but not denial of service attacks, against remote systems with limited, or adjustable, overhead proportional to the perceived or actual risk of command execution..

Our next step is to implement this approach in the Solidity smart contract language on a private Enterprise Ethereum blockchain and analyse its behaviour to determine any practical scaling or security issues. We will need to determine all mitigated and remaining attack vectors.

IV. Acknowledgements

The author gratefully acknowledges ConsenSys AG for financially supporting this research, especially its PegaSys division. Peter Robinson, Roberto Saltini, Sandra Johnson and Christopher Hare, all of PegaSys, participated in the research in [3] that led to this short paper. Thanks also to Peter Robinson, Sandra Johnson, Horacio Mijail Anton Quiles and Raghavendra Ramesh of PegaSys for reviewing this paper.

References

[1] P. Kotzias, L. Bilge, P.-A. Vervier, and J. Caballero, “Mind your own business: A longitudinal study of threats and vulnerabilities in enterprises.” in *NDSS*, 2019.

[2] R. Gafni and T. Pavel, “The invisible hole of information on smb’s cybersecurity,” *Online Journal of Applied Knowledge Management*, vol. 7, no. 1, 2019.

[3] D. Hyland-Wood, P. Robinson, R. Saltini, S. Johnson, and C. Hare, “Methods for securing spacecraft tasking and control via an enterprise ethereum blockchain,” in *37th International Communications Satellite Systems Conference (ICSSC)*. Ka and Broadband Communications, Navigation and Earth Observation Conference, October 2019.

[4] R. Saltini and D. Hyland-Wood, “Ibft 2.0: A safe and live variation of the ibft blockchain consensus protocol for eventually synchronous networks,” *arXiv preprint arXiv:1909.10194*, 2019.

[5] Ncipher, “Global encryption trends study.” [Online]. Available: https://go.ncipher.com/rs/104-QOX-775/images/2019-Ponemon-France-Encryption-Trends-Study-fr-ar.pdf

[6] E. E. Alliance, “Enterprise ethereum client specification v2,” 2019.

[7] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, “Town crier: An authenticated data feed for smart contracts,” in *Proceedings of the 2016 aCM sIGSAC conference on computer and communications security*. ACM, 2016, pp. 270–282.

EnergyPie: A Hyperedge-based Blockchain Market Model

Samuel Karumba
Computer Science and Engineering
University of New South Wales
Sydney, Australia
s.karumba@student.unsw.edu.au

Salil S. Kanhere
Computer Science and Engineering
University of New South Wales
Sydney, Australia
salil.kanhere@unsw.edu.au

Raja Jurdak
Science and Engineering
Queensland University of Technology (QUT)
Brisbane, Australia
r.jurdak@qut.edu.au

***Abstract*—Energy efficiency and the adoption of renewable energy sources (RES)are some of the proven approaches employed to reduce carbon emissions. Application of blockchain in distributed energy trading (DET) systems has brought potential solutions in tracking adoption of RES and energy efficiency efforts from generation, distribution, to consumption processes. However, theses blockchain-based DETs faces processing overheads, security and privacy issues. This paper proposes EnergyPie: a unified market model based on blockchain and hypergraph. EnergyPie market model aims to preserve data security and privacy, and distribute trust while ensuring platform efficiency.**

***Index Terms*—blockchain, hypergraph, distributed energy trading, decarbonisation**

I. Introduction

Human activities related to greenhouse gas emissions are estimated to have raised the average global surface temperature by 1.0°C. The International Panel on Climate Change estimate it to reach 1.5°C between 2030 and 2052 if current daily emission rate of 408 parts per million continues. On the flip side, the European Union (EU), predicts reaching zero-emission by 2040 [1] if we build new carbon-neutral infrastructure, curtail the use of fossil fuel, model decarbonization pathways through policies and government subsidies, and promote adoption of renewable energy sources (RES).

In the last decade, the emergence of RES prosumers (producers-and-consumers) has transformed energy generation and trading patterns from centralized to distributed. Additionally, the government has introduced policies aimed at increasing the adoption of RES with predominant ones being solar feed-in tariffs popular in Australia and net-metering popular in EU countries [2]. However, renewable 2019 global status report [3] indicates that those countries with set emission reduction targets failed to meet them for the year 2019. In addition to adoption of RES we need policies and systems that promote energy efficiency in buildings, transport, and power sectors.

To improve efficiency in these sectors, blockchain [4] technology has recently been adopted in the development of distributed energy trading (DET) systems designed to spearhead decarbonization due to its salient features of decentralized trust, immutability, and transparency in tracking emissions. However, these systems suffer from lack of interoperability, poor scalability, and high processing overheads owing to issues such as limited bandwidth, sharing restriction, and privacy restrictions. Consequently, there are two key challenges that need to be addressed: (i) Double counting - where a renewable energy certificate (REC) issued for a kilowatt hour of renewable energy is traded more than once in separate tracking systems; (ii) Data privacy - since data in blockchain-based trading networks is replicated to all node for provenance this significant reduces confidentiality.

In this work, we investigate the use of blockchain and hypergraphs [5] to design an inter-operable clustered energy trading blockchain with separate data vectors for tracking emissions in the energy sector to avoid double counting and ensure data privacy. The primary objective of this clustered network structure is to deliver distributed trust through multiple validation points, privacy and scalability by reducing the number of nodes storing each transaction and transparency by ensuring interoperability between clusters to eliminate double counting. To achieve this goal, we propose a relational market structure detailing the clustering process, secure exchanges between clusters and data privacy techniques used.

II. Tools and Methods

A. Blockchain

A blockchain is a distributed ledger technology (DLT) comprised of a suite of technologies. These DLTs are increasingly been used to coordinate decentralized trust in P2P networks, offering security and transparency by taking advantage of their salient properties of distribution, provenance, immutability and transparency [6]. These properties are embedded in its constituent components: the distributed ledger, cryptographic protocols, and consensus protocol.

B. Hypergraphs

The most common conception of a graph connects two objects with an edge between them modeled as a pairwise relationship, such networks are known as peer-to-peer networks. In discrete mathematics, a hypergraph is the most general concept of a system with finite set and form, which groups multiple nodes into sets hyperedges. Here one edge connects more than two nodes to model relationships among multiple entities or participants in a network [5]. Usually denoted as

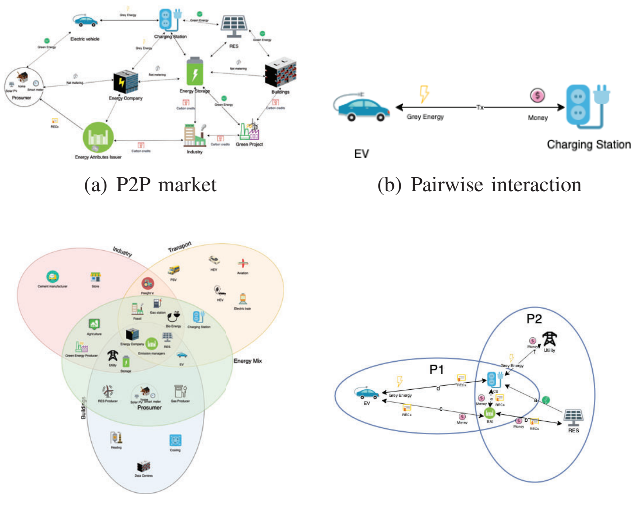
$H = (V, E)$, where V is a finite set of vertices or nodes and E is a hyperedge set − subsets of vertices.

Hypergraph based solutions have been proposed in several use cases such as partitioning in modeled social networks to ease scaling problem [7], in neural networks framework for data representation through high-order correlation learning [8], and drawing complex relationships beyond pairs in linear connectivity problems [9] such as DNA matching.

III. EnergyPie

Combining the two technologies in Section II, we design and implement EnergyPie − a unified market model for distributed energy trading based on the proposed relational market structure concepts. Our aim is to realize the following three main design goals.

First, distributed trust. Currently, energy trading in P2P networks shown in Fig. 1(a) is characterized by multi-bilateral transaction exchanges of heterogeneous energy commodities or assets among participants. Each trade relationship is pairwise as illustrated in Fig. 1(b) and thus for a replay attack, the same commodity could be transferred to more than one party in different tracking systems. In the unified networks Fig. 1(c), we use hyperedges to represent different blockchain networks referred to as sub-chains interacting together to track cross-asset transfers in the EnergyPie system. To facilitate cross-chains transfers we use nodes at the intersection of sub-chains referred to as adjacent nodes to validate cross-chains transactions since they are considered to be participate in both sub-chains forming a unified system.



(a) P2P market

(b) Pairwise interaction

(c) Unified market

(d) Relational interaction

Fig. 1. Energy markets

Secondly, we ensure platform performance and scalability. In blockchain-based P2P market models, each trade transaction is validated and recorded by all network participants where the consensus mechanism requires 51% of the participants to agree on it. However, the untrustworthy threshold of a transaction in private blockchains is much lower [10] as we require only up to 10% failed invalidation responses to consider a transaction nontrustworthy. We adopt association rules using support and confidence constraints [11] to determine transaction endorsement, validation, and storage thresholds. This significantly reduces processing costs and communication overheads.

Lastly, we ensure data security and privacy. Data in blockchain-based DET systems is replicated on each participant's nodes. Although data on private blockchains is encrypted, brute force attacks could compromise data confidentiality in such systems. We use hyperedges, association rules thresholds and secure multiparty computation techniques to validate and store encrypted transaction data on a subset of nodes. These techniques allow cross sub-chains computations on encrypted transaction data without compromising its integrity.

IV. Future work

We are currently in the process of implementing and testing the EnergyPie market model to simulate relational trades among participants in buildings, transport, power and industry sectors. In our future work we extend the market model to include an energy efficiency tariff that will capture the end-users' effort in energy efficiency to curtail use of fossil fuels. The tariff will aim to reward green energy consumption and carbon abatement efforts using a reputation metric.

References

[1] VEIL, *Pathways 2040*, 2017.

[2] M. E. Peck and D. Wagman, "Energy trading for fun and profit buy your neighbor's rooftop solar power or sell your own-it'll all be on a blockchain," *IEEE Spectrum*, vol. 54, no. 10, pp. 56–61, 2017.

[3] REN21, "Renewables 2019," no. October, p. 335, 2019.

[4] S. Nakamoto and S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf." [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.221.9986

[5] A. Bretto, *Hypergraph Theory*, 2013.

[6] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, "A Taxonomy of Blockchain-Based Systems for Architecture Design," *Proceedings - 2017 IEEE International Conference on Software Architecture, ICSA 2017*, pp. 243–252, 2017.

[7] Z. K. Zhang and C. Liu, "A hypergraph model of social tagging networks," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2010, no. 10, 2010.

[8] Y. Feng, H. You, Z. Zhang, R. Ji, and Y. Gao, "Hypergraph Neural Networks," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 33, pp. 3558–3565, 2019.

[9] M. Thakur and R. Tripathi, "Linear connectivity problems in directed hypergraphs," *Theoretical Computer Science*, vol. 410, no. 27-29, pp. 2592–2618, 2009. [Online]. Available: http://dx.doi.org/10.1016/j.tcs.2009.02.038

[10] C. Qu, M. Tao, and R. Yuan, "A hypergraph-based blockchain model and application in internet of things-enabled smart homes," *Sensors (Switzerland)*, vol. 18, no. 9, 2018.

[11] J. Lee, G. L. Park, and E. H. Kim, "Development of wind speed prediction model in Jeju City," *Communications in Computer and Information Science*, vol. 341 CCIS, pp. 20–26, 2012. [Online]. Available: https://dx.doi.org/10.1007/978-3-642-35248-5$_4$

Application Level Authentication for Ethereum Private Blockchain Atomic Crosschain Transactions

Peter Robinson PegaSys, ConsenSys and University of Queensland
peter.robinson@consensys.net peter.robinson@uqconnect.edu.au

***Abstract*—Atomic Crosschain Transaction technology allows composable programming across private Ethereum blockchains. It allows for inter-contract and inter-blockchain function calls that are both synchronous and atomic: if one part fails, the whole call graph of function calls is rolled back. Traditional Ethereum contract functions can limit which accounts can call them by specialised application program logic. This is important as it allows application developers to specify which callers can execute functions that update contract state. In this paper we introduce the strategy required to restrict which contracts on one blockchain can call a function in a contract that is deployed on another blockchain. We show that validating the Originating Blockchain Id (the blockchain the crosschain function call started on), From Blockchain Id, and From Account provides contracts with certainty that a function call came from a specific contract on a specific blockchain.**

I. Introduction

Atomic Crosschain Transactions [1] for Ethereum Private Sidechains [2] and private Ethereum blockchains allow for inter-contract and inter-blockchain function calls that are both synchronous and atomic. Atomic Crosschain Transactions are special nested Ethereum transactions that include additional fields to facilitate the atomic behaviour securely. This new type of Ethereum transaction has great promise, but introduces a new set of challenges.

Traditional Ethereum transactions [3] execute within a single blockchain. For example, in Fig. 1 an Externally Owned Account (EOA) submits a transaction that calls the function `sender` in `Contract A` that in turn calls the function `receiver` in `Contract B`. `Contract B` could be a simple contract that holds data and has little or no business logic. `Contract A` may be a complex contract that holds the majority or all of the business logic of the application. The business logic may need to change over time. Additionally, like any complex software, a complex contract may have defects which need to be resolved. The typical approach to this scenario in a blockchain setting is to deploy a new version of `Contract A` and have `Contract B`'s `receiver` function only allow calls from the newly deployed `Contract A` [4]. The Solidity code that would allow this to occur is shown in Listing 1.

On line 2 of the listing `msg.sender`, the address of the contract or EOA that called this function, is compared against a variable `authorisedAddress`. This value is the address of the deployed instance of `Contract A` that is authorised to call the `receiver` function. The transaction executing the function call is aborted if the two values do not match. This line of code ensures `Contract B`'s `receiver` function can only be called by functions in an authorised deployed instance of `Contract A`.

Listing 1: Application Authentication

```
1 function receiver() external {
2   require(msg.sender == authorisedAddress);
3   ...
4 }
```

The scenario for a crosschain transaction is more complex. In Fig. 2 `Contract A` has been deployed to `Private Blockchain A` and `Contract B` has been deployed to `Private Blockchain B`. An EOA submits a transaction that calls the function `sender` in `Contract A` on `Private Blockchain A` that in turn calls the function `receiver` in `Contract B` on `Private Blockchain B`. This paper describes the application logic required to limit function calls to the function `receiver` in `Contract B` to only those coming from `Contract A` on `Private Blockchain A`.

II. Atomic Crosschain Transactions

A. Nested Transactions

Atomic Crosschain Transactions are nested Ethereum transactions and views. Transactions are function calls that update state. Views are function calls that return a value but do not update state. Fig. 3 shows a EOA calling a function `funcA1` in contract `conA1` on blockchain `Private Blockchain A`. This function in turn calls function `funcB`, that in turn calls functions `funcC` and `funcA2`, each on separate blockchains.

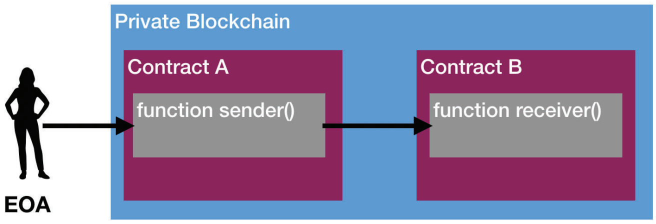


Fig. 1: Traditional Transaction Function Call within One Blockchain

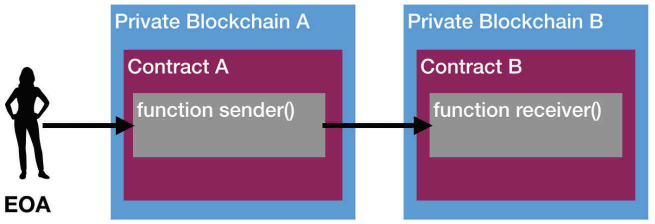


Fig. 2: Crosschain Transaction Function Call across Two Blockchains

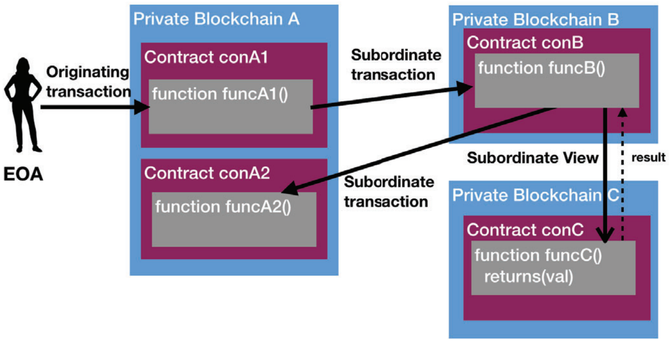


Fig. 3: Originating Transaction containing Two Nested Subordinate Transactions and a Subordinate View

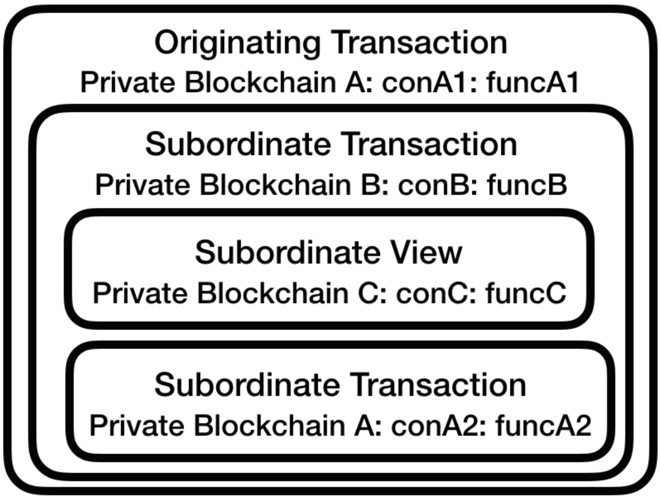

Originating Transaction
Private Blockchain A: conA1: funcA1
Subordinate Transaction
Private Blockchain B: conB: funcB
Subordinate View
Private Blockchain C: conC: funcC
Subordinate Transaction
Private Blockchain A: conA2: funcA2

Fig. 4: Nested Transactions and Views

The transaction submitted by the EOA is called the *Originating Transaction*. The transactions that the Originating Transaction causes to be submitted are called Subordinate Transactions. Subordinate Views may also be triggered. In Fig. 3, a Subordinate View is used to call `funcC`. This function returns a value to `funcB`.

Fig. 4 shows the nested structure of the Atomic Crosschain Transaction. The EOA user first creates the signed Subordinate View for `Private Blockchain C`, contract `conC`, function `funcC` and the signed Subordinate Transaction for `Private Blockchain A`, contract `conA2`, function `funcA2`. They then create the signed Subordinate Transaction for `Private Blockchain B`, contract `conB`, function `funcB`, and include the signed Subordinate Transaction and View. Finally, they sign the Originating Transaction for `Private Blockchain A`, contract `conA1`, function `funcA1`, including the signed Subordinate Transactions and View.

When the EOA submits the Originating Transaction to a node, the node processes the transaction using the algorithm shown in Listing 2. If the transaction includes any Subordinate Views, they are dispatched and their results are cached (Lines 1 to 3). The function is then executed (Lines 4 to 17). If a Subordinate Transaction function call is encountered, the node checks that the parameter values passed to the Subordinate Transaction function call match the parameter values in the signed Subordinate Transaction (Lines 6 to 8). If a Subordinate View function call is encountered, the node checks that the parameters passed to the Subordinate View function call match the parameter values in the signed Subordinate View (Lines 9 and 10). The cached values of the results of the Subordinate View function calls are then returned to the executing code (Line 11). If the execution has completed without error, then each of the signed Subordinate Transactions is submitted to a node on the appropriate blockchain (Nodes 18 to 20).

Listing 2: Originating or Subordinate Transaction Processing

```
1  For All Subordinate Views {
2    Dispatch Subordinate Views & cache results
3  }
4  Trial Execution of Function Call {
5    While Executing Code {
6      If Subordinate Transaction function called {
7        check expected & actual parameters match.
8      }
9      Else If Subordinate View function is called {
10       check expected & actual parameters match
11       return cached results to code
12     }
13     Else {
14       Execute Code As Usual
15     }
16   }
17 }
18 For All Subordinate Transactions {
19   Submit Subordinate Transactions
20 }
```

B. Blockchain Signing and Threshold Signatures

BLS Threshold Signatures [5], [6] combines the ideas of threshold cryptography [7] with Boneh-Lynn-Shacham(BLS) signatures [8], and uses a Pedersen commitment scheme [9] to ensure verifiable secret sharing. The scheme allows any `M` validator nodes of the total `N` validator nodes on a blockchain to sign messages in a distributed way such that the private key shares do not need to be assembled to create a signature. Each validator node creates a signature share by signing the message using their private key share. Any `M` of the total `N` signature shares can be combined to create a valid signature. Importantly, the signature contains no information about which nodes signed, or what the threshold number of signatures (`M`) needed to create the signature is.

The Atomic Crosschain Transaction system uses BLS Threshold Signatures to prove that information came from a specific blockchain. For example, in Fig. 3, nodes on `Private Blockchain B` can be certain of results returned by a node on `Private Blockchain C` for the function call to `funcC`, as the results are threshold signed by the validator nodes on `Private Blockchain C`. Similarly, validator nodes on `Private Blockchain A` can be certain that validator nodes on `Private Blockchain B` have mined the Subordinate Transaction, locked contract `conB` and are holding the updated state as a provisional update because validator nodes sign a *Subordinate Transaction Ready* message indicating that the Subordinate Transaction is ready to be committed.

C. Crosschain Coordination

Crosschain Coordination Contracts exist on *Coordination Blockchains*. They allow validator nodes to determine whether the provisional state updates related to the Originating Transaction and Subordinate Transactions should be committed or discarded. The contract is also used to determine a common time-out for all blockchains, and as a repository of Blockchain Public Keys.

When a user creates a Crosschain Transaction, they specify the Coordination Blockchain and Crosschain Coordination Contract to be used for the transaction, and the time-out for the transaction in terms of a block number on the Coordination Blockchain. The validator node that they submit the Originating Transaction to (the *Originating Node*) works with other validator nodes on the blockchain to sign a *Crosschain Transaction Start* message. This message is submitted to the Crosschain Coordination Contract to indicate to all nodes on all blockchains that the Crosschain Transaction has commenced.

When the Originating Node has received Subordinate Transaction Ready messages for all Subordinate Transactions, it works with other validator nodes to create a *Crosschain Transaction Commit* message. This message is submitted to the Crosschain Coordination Contract to indicate to all nodes on all blockchains that the Crosschain Transaction has completed and all provisional updates should be committed. If an error is detected, then a *Crosschain Transaction Ignore* message is created and submitted to the Crosschain Coordination Contract to indicate to all nodes on all blockchains that the Crosschain Transaction has failed and all provisional updates should be discarded. Similarly, if the transaction times-out, all provisional updates will be discarded.

D. Crosschain Transaction Fields

Originating Transactions, Subordinate Transactions, and Subordinate Views contain the fields shown in Table I. Some of the information in the standard Ethereum transaction fields are exposed to blockchain application contract code, such as the `value` field via the Solidity code `msg.value`. The new extended crosschain transaction fields are made available to blockchain application contract code via a precompile contract.

All nodes that process the transaction check that the `Coordination Blockchain Id`, `Crosschain Coordination Contract`, `Crosschain Transaction Time-out`, `Crosschain Transaction Id`, and `Originating Blockchain Id` are consistent across the transaction or view they are processing, and the nested Subordinate Transactions and Views. The nodes also check that the `To` address and `From Address`, and the blockchain identifier obtained from the `V` field and the `From Blockchain Id` match across transactions and views.

The `To` address is the address of the contract containing the function called on a blockchain. For example, the function (f1) in contract (c1) could call a function (f2) in another contract (c2) on the same blockchain (b1). The second contract (c2) could call a function (f3) in a contract (c3) on another blockchain (b2) via a Subordinate Transaction. The `From Address` of the Subordinate Transaction will match the `To` address of the transaction on the first blockchain (b1). This will be the address first contract (c1). It will however, not match the address of the second contract (c2), which is the function that caused the Subordinate Transaction to be triggered.

III. Application Authentication

As with traditional Ethereum transactions, the type of application level authentication required for a Crosschain Transaction will be application dependent.

Field	Description
Standard Ethereum Transaction Fields	
Nonce	Per-account, per-blockchain transaction number.
GasPrice	Amount offered to pay for gas for the transaction.
GasLimit	Maximum gas which can be used by the transaction.
To	Address of the account to send the value to, or the address of a contract to call.
Value	Amount of Ether to transfer.
Data	Encoded function signature and parameter values.
V	Part of the transaction digital signature & blockchain identifier this transaction must execute on.
R	Part of the transaction digital signature.
S	Part of the transaction digital signature.
Additional Crosschain Transaction Fields	
Type	Type of crosschain transaction (e.g. Originating Transaction)
Coordination Blockchain Id	Blockchain identifier of Coordination Blockchain to use for this transaction.
Crosschain Coordination Contract	Address of the Crosschain Coordination Contract to use for this transaction.
Crosschain Transaction Time-out	Coordination Blockchain block number when this transaction will time out.
Crosschain Transaction Id	Identifies this crosschain transaction.
Originating Blockchain Id	Blockchain identifier of the blockchain the Originating Node is on.
From Blockchain Id	Blockchain identifier of the blockchain that the function call executed on that resulted in this Subordinate Transaction or View being submitted.
From Address	*To* address from the transaction or view that resulted in this Subordinate Transaction or View.
Subordinates	List of Subordinate Transactions and Subordinate Views that are called directly from this transaction or view.

TABLE I: Crosschain Transaction Fields

A. No Authentication

Many functions will need no authentication at all. That is, functions can be designed such that it is safe to execute a transaction or return results of a view to any caller who is able to access the function.

B. Using `msg.sender` or `tx.origin`

From the perspective of each Originating Transaction, Subordinate Transaction or View, `msg.sender` and `tx.origin` operate in the same way as a standard Ethereum transaction. That is, if an EOA submitted a transaction that called a function in contract A that then called a function in contract B on the same blockchain, `msg.sender` for contract B is contract A, and is the EOA for contract A. In both cases `tx.origin` would be the EOA. In the context of a node processing an Originating Transaction, Subordinate Transaction or View, for the purposes of `msg.sender` and `tx.origin`, the transaction or view appears as a separately signed transaction. Given the similarities with standard Ethereum, `msg.sender` and `tx.origin` could be used in the same way as standard Ethereum to authenticate which EOA or contract on the same blockchain called a function call using code similar to that shown in Listing 1.

A key difference between standard Ethereum views and Subordinate Views is that Subordinate Views are signed. As such, the variables `msg.sender` and `tx.origin` can be used within Subordinate Views, whereas they are not set in

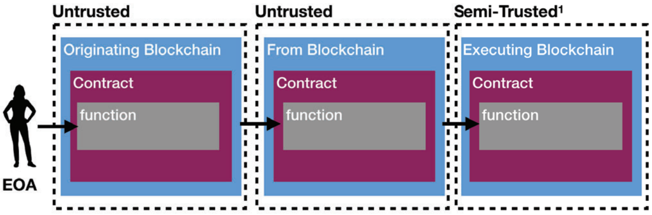


Fig. 5: Scenario 1: From and Originating Blockchain Untrusted

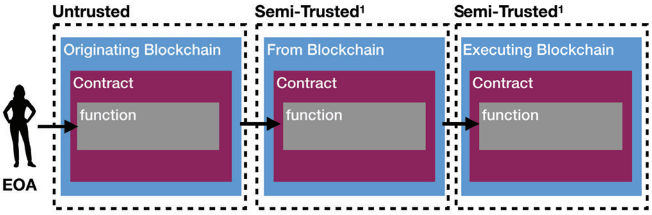


Fig. 6: Scenario 2: Originating Blockchain Untrusted

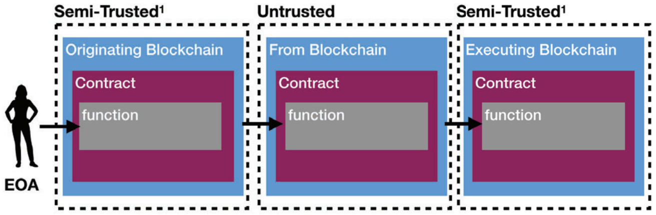


Fig. 7: Scenario 3: From Blockchain Untrusted

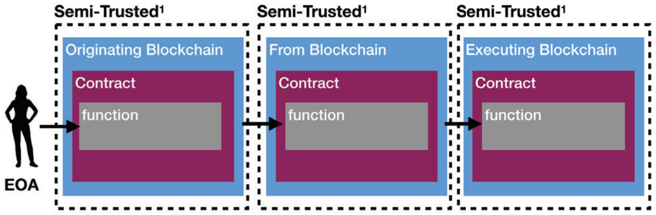


Fig. 8: Scenario 4: From and Originating Blockchain Semi-Trusted[1]

the context of normal Ethereum views (except for the case of `msg.sender` when one contract calls another contract).

C. From Blockchain Id, From Address, and Originating Blockchain Id

If a contract needs to only respond to calls from a certain contract on a certain blockchain, then the code in Listing 3 should be used. The code checks that the `From Blockchain Id` and `From Address` match the authorised blockchain and address, and checks that the blockchains represented by `From Blockchain Id` and `Originating Blockchain Id` are semi-trusted. By semi-trusted it is meant that fewer than `M` validators operating the blockchain are Byzantine. Note that this scenario implies the contract should allow for any `msg.sender` and `tx.origin`.

Listing 3: Crosschain Application Authentication

```
function receiver() external {
  address fromAddr = infoPrecompile(FROM_ADDR);
  uint256 fromBcId = infoPrecompile(FROM_BCID);
  uint256 origBcId = infoPrecompile(ORIG_BCID);
  require(fromAddr == authorisedFromAddress);
  require(fromBcId == authorisedFromBcId);
  require(origBcId == authorisedOrigBcId);
  ...
}
```

IV. Analysis

This section analyses the appropriateness of using the `Originating Blockchain Id`, `From Blockchain Id`, and `From Address` fields as a method of authentication, and requiring the blockchains identified by `Originating Blockchain Id` and `From Blockchain Id` be semi-trusted. Figures 5 to 8 show four possible scenarios. The participant could not trust the blockchains represented by `Originating Blockchain Id`, `From Blockchain Id` (scenario 1, Figure 5), just semi-trust the `From Blockchain Id` or `Originating Blockchain Id` (scenario 2, Figure 6 and scenario 3, Figure 7), or semi-trust both blockchains (scenario 4, Figure 8). In the figures, the *Originating Blockchain* is the blockchain identified by the `Originating Blockchain Id`, the *From Blockchain* is the blockchain identified by the `From Blockchain Id`, and the *Executing Blockchain* is the blockchain executing the transaction that contains the application level authentication logic.

A. Scenario 1

If neither the Originating Blockchain or the From Blockchain are trusted, then a nefarious actor operating the validator nodes on the blockchains could maliciously construct a Subordinate Transaction and submit it to the Executing Blockchain. The nefarious actor could create valid Crosschain Transaction Start and Commit messages and submit them to the Coordinating Blockchain, thus making it appear that all nodes on all blockchains should commit all parts of the Crosschain Transaction.

The nodes on the Executing Blockchain have no basis to trust information in the Subordinate Transaction submitted to them or the Crosschain Transaction status indicated by the Crosschain Coordination Contract. As such, there is no method of application level authentication to restrict which contract on which blockchain can call a function in a contract if neither the Originating Blockchain nor the From Blockchain are semi-trusted.

B. Scenario 2

If the From Blockchain is semi-trusted, but the Originating Blockchain is not trusted, then a nefarious actor could create a malicious Crosschain Transaction. Rather than submitting a Subordinate Transaction to the From Blockchain, they could bypass the blockchain, constructing a malicious Subordinate Transaction with forged From Blockchain Id and From Address, and submit it to the Executing Blockchain. The nefarious actor could create valid Crosschain Transaction Start and Commit messages and submit them to the Coordinating Blockchain, thus making it appear that all nodes on

[1] Semi-trusted is defined as having fewer than `M` Byzantine validator node on a blockchain.

all blockchains should commit all parts of the Crosschain Transaction.

In this scenario, the nodes on the Executing Blockchain have no way to be certain that the Subordinate Transaction submitted to them originated from the From Blockchain. As such, there is no method of application level authentication to restrict which contract on which blockchain can call a function in a contract if the Originating Blockchain is not semi-trusted.

C. Scenario 3

If the Originating Blockchain is semi-trusted, but the From Blockchain is not trusted, then a nefarious actor could claim a Subordinate Transaction being executed by the From Blockchain was ready to be committed when it was not. The nefarious actor would not be able to forge the From Address or the From Blockchain Id of the subordinate transaction as validators on the Originating Blockchain would detect the mis-matched To and From Address addresses or blockchains identifiers, and reject the invalid Crosschain Transaction. In this case, they would refuse to mine the Originating Transaction and refuse to create the Crosschain Transaction Start message.

In this scenario, the nodes on the Executing Blockchain are certain that the Subordinate Transaction submitted to them has authentic From Address and From Blockchain Id information. However, there is no certainty that the Subordinate Transaction submitted to the From Blockchain will be committed to that blockchain.

D. Scenario 4

If both the Originating Blockchain and the From Blockchain are semi-trusted, then a nefarious actor is unable to subvert the protocol. Similarly to section IV-C, invalid transactions they submit will be rejected by validators nodes on the Originating Blockchain. Validator nodes on the Execution Blockchain can be sure that if the Crosschain Coordination Contract indicates that the transaction should be committed, then all nodes, including the From Blockchain, are ready to commit their provisional updates.

V. Implementation

Examples of the Atomic Crosschain Transaction application authentication code is available on github.com [10].

VI. Discussion

The system assumes that blockchains involved in a crosschain transaction are semi-trusted, where semi-trusted is defined as having fewer than M Byzantine validators nodes operating a blockchain. This assumption of having a threshold number of Byzantine validator nodes is the same type of assumption that Byzantine Fault Tolerant (BFT) consensus protocols make [11], [12]. As blockchains that support Atomic Crosschain Transaction technology are likely to use a BFT consensus protocol, if more than a threshold number of validator nodes were Byzantine, then the blockchain's consensus protocol, as well as the crosschain transaction protocol, would fail.

VII. Conclusion

Application programmers need to restrict which callers can call functions in their contracts to update state. Traditional Ethereum security practices are not sufficient for a crosschain transaction context. This paper presents the fundamental building blocks of a crosschain authentication framework on which application-level authentication can be built. In particular, when using Atomic Crosschain Transactions, the Originating Blockchain Id, From Blockchain Id, and the From Account crosschain transaction fields can be used to ensure a function in a contract on a blockchain is only callable from certain contracts on certain blockchains, assuming that the participant that configured the contract trusts that fewer than a threshold number of validators on the blockchains indicated by the Originating Blockchain Id, From Blockchain Id are Byzantine.

Acknowledgment

This research has been undertaken whilst I have been employed full-time at ConsenSys. I acknowledge the support of University of Queensland where I am completing my PhD, and in particular the support of my PhD supervisor Dr Marius Portmann.

I acknowledge the co-authors of the original Atomic Crosschain Transaction paper [1] Dr David Hyland-Wood, Roberto Saltini, Dr Sandra Johnson, and John Brainard for their help creating the technology upon which this paper is based. I acknowledge Dr Raghavendra Ramesh for his ideas on improvements to the *From Address* field. I thank Dr Catherine Jones, Dr David Hyland-Wood, Dr Raghavendra Ramesh, Dr Sandra Johnson, John Brainard and Horacio Mijail Anton Quiles for reviewing this paper and providing astute feedback.

References

[1] P. Robinson, D. Hyland-Wood, R. Saltini, S. Johnson, and J. Brainard, "Atomic Crosschain Transactions for Ethereum Private Sidechains," 2019. [Online]. Available: https://arxiv.org/abs/1904.12079

[2] P. Robinson, "Requirements for Ethereum Private Sidechains," 2018. [Online]. Available: http://adsabs.harvard.edu/abs/2018arXiv180609834R

[3] G. Wood, "Ethereum: a secure decentralized generalised transaction ledger," Github, p. Github site to create pdf, 2016. [Online]. Available: https://github.com/ethereum/yellowpaper

[4] P. Robinson, "Ethereum Engineering Group: Advanced Solidity and Design Patterns - YouTube." [Online]. Available: https://www.youtube.com/watch?v=VhzafmGGmzo&t=534s

[5] A. Boldyreva, "Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme." [Online]. Available: http://www-cse.ucsd.edu/users/aboldyre

[6] P. Robinson, "Ethereum Engineering Group: BLS Threshold Signatures - YouTube." [Online]. Available: https://www.youtube.com/watch?v=XZTvBYG9pn4

[7] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979. [Online]. Available: https://cs.jhu.edu/ sdoshi/crypto/papers/shamirturing.pdf

[8] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004. [Online]. Available: https://doi.org/10.1007/s00145-004-0314-9

[9] T. P. Pedersen and D. W. Davies, "A Threshold Cryptosystem without a Trusted Party," in *Advances in Cryptology EUROCRYPT '91*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991, pp. 522–526. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-46416-6_47

[10] PegaSys, "Atomic Crosschain Transaction Sample Code Github Repository." [Online]. Available: https://github.com/PegaSysEng/sidechains-samples

[11] Y.-T. Lin, "EIP 650: Istanbul Byzantine Fault Tolerance," 2017. [Online]. Available: https://github.com/ethereum/EIPs/issues/650

[12] R. Saltini, "IBFT 2.0 Gray Paper version 0.2," 2019. [Online]. Available: https://github.com/PegaSysEng/ibft2.x/raw/master/gray_paper/ibft2_gray_paper.pdf

Towards Declarative Smart Contracts

Kevin Purnell and Rolf Schwitter
Department of Computing
Macquarie University, NSW 2109, Australia
kevin.purnell@hdr.mq.edu.au|rolf.schwitter@mq.edu.au

***Abstract*—Blockchain technologies promise improvements to legal documents, yet their use requires programmers and risks hacking, so widespread adoption depends on removing programmers and improving verification. We tackle these problems via a sophisticated user interface that auto-generates declarative smart contract code in the form of answer set programs. We demonstrate improved usability and testing effectiveness by implementing a legal document as a smart contract on our purpose built simulator and find that our solution supports adoption because it starts with a legal document, allows human-in-the-loop interaction, and is tolerant of varying levels of automation.**

***Keywords*– smart contract, declarative**

I. Introduction

With the exception of contracts in some well-funded industries [7], legal contracts and documents are often clumsy, expensive to use and prone to ambiguities. Emerging blockchain technologies hold the promise of changing this, however, the tools for coding these 'smart contracts' require programmers, are vulnerable to programming errors and have been shown to contain exploitable features. For example, the Ethereum ecosystem we benchmark against currently provides a ECMAScript compliant procedural programming language (Solidity) for programming smart contracts which compiles to bytecode executable on the Ethereum Virtual Machine (EVM) [16]. This language is evolving rapidly to address its weaknesses as the primary smart contract language [15], the most famous exposé being the 'The DAO' hack which lost approximately USD50M [4]. We attempt a balanced understanding of Solidity's weaknesses by using preliminary evaluation criteria that have the perspective of the ultimate end-user (lawyers, business-people and the general public). These are, 1) ease of use (it is desirable that smart contracts can be created by untrained users); 2) understandability (builds confidence that the contract does what is intended); 3) ease of testing (helps identify and remove bugs); 4) free of security exploits and errors at deployment (self-evident); 5) scalability (the method can handle complex contracts); 6) cost (costs should not be prohibitive). When assessed with this evaluation framework it is clear that Solidity is a poor fit.

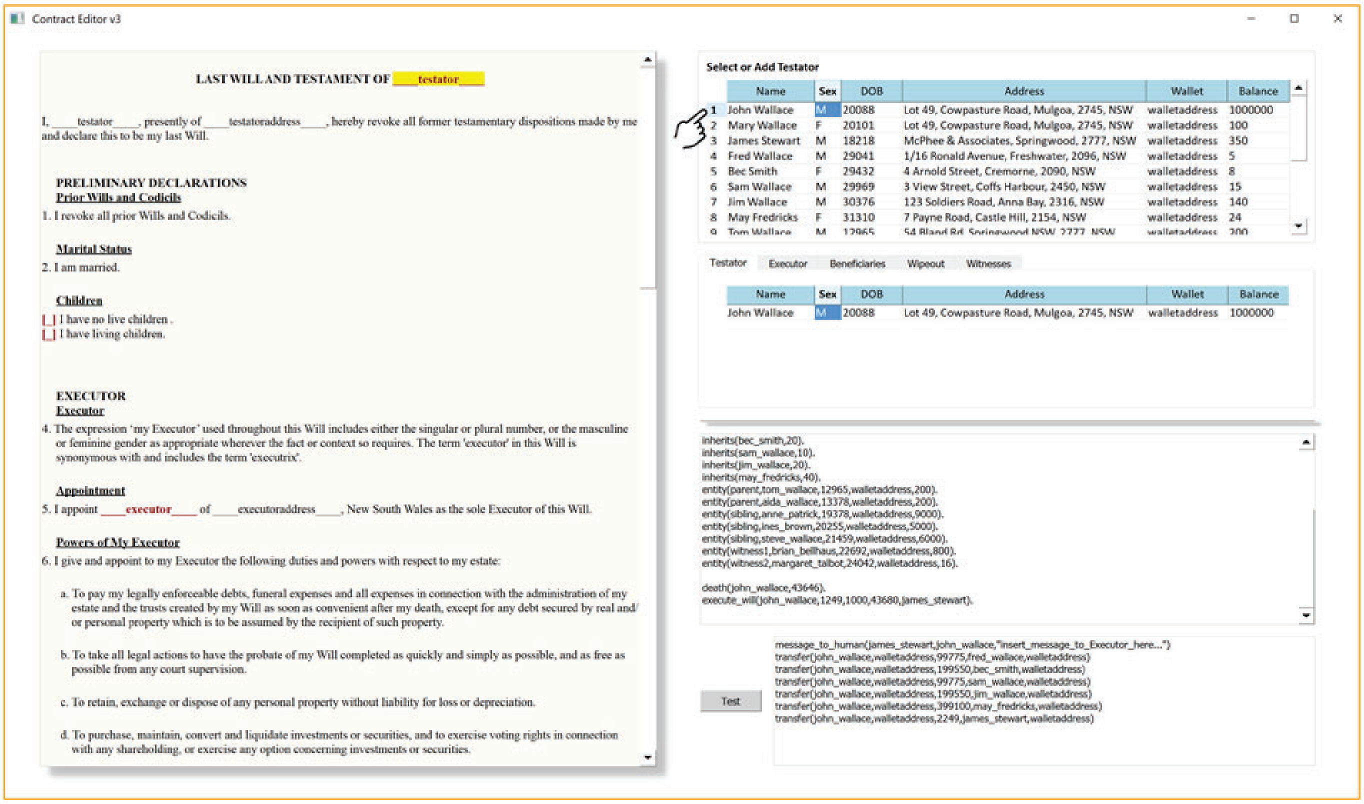
II. Declarative Smart Contracts

We re-frame the problem as one of translating an existing legal contract or document to an executable smart contract with help from an interactive user interface.

Firstly, we replace Solidity with a successful declarative programming language (Answer Set Programming, hereafter ASP) [2] which simplifies coding and makes auto-generation of code easier. ASP is a recent declarative knowledge representation language with a close connection to non-monotonic logics that provides ASP with the power to model default negation, deal with incomplete information, and encode domain knowledge, defaults, and preferences in an intuitive and natural way [3]. ASP is elaboration-tolerant [12], meaning that the language accepts changes in a problem specification without the need to rewrite the entire program [10], implements weak and strong negation in order to deal with a local form of the closed world assumption, and is order-independent. These features provide the flexibility needed to implement our approach, allowing us to model legal logic in an intuitive way and split code into **facts**, **logic program** and **events**, a structure mirrored in legal documents. For legal documents of a given type, the **logic program** is the same with only the assertional knowledge **(facts)** differing. This allows translation of legal documents to be split into two stages. Our first stage is equivalent to the creation and publishing of a standard form contract template (SFCT) [9] with the addition of a matching logic program. This simplifies our second stage where the SFCT is completed with specific information and the logic program instantiated, giving an overall approach with favourable economics. Note that the idea of pairing text and code together has been in use in the financial markets for decades in the form of Ricardian Contracts [6], which have achieved legal status.

Secondly, we devise an intuitive user interface that auto-generates code by building on the use of the SFCT. One option for a user interface is to support instantiation of such a form. Compared to other alternatives [11], SFCTs have the advantage of being familiar to users, and generally are already in electronic format, often marked-up with HTML. This is the approach used by the OpenLaw [14] initiative which we see as confirming that some lawyers are comfortable retaining the traditional sequential text format of legal documents. A further significant but possibly overlooked advantage is that traditional paper format handles contracts of arbitrary complexity. Using sequential text to express complex ideas appears culturally embedded, is hard to duplicate with other approaches, and not featured in most other smart contract research.

To investigate the above ideas we developed a blockchain simulator that includes a Smart Contract Editor (SCE), and used this tool to implement a legal document ('Will and Testament') as a smart contract, with some assumptions.


Contract Editor v3

LAST WILL AND TESTAMENT OF ____testator____

I, ____testator____, presently of ____testatoraddress____, hereby revoke all former testamentary dispositions made by me and declare this to be my last Will.

PRELIMINARY DECLARATIONS
Prior Wills and Codicils
1. I revoke all prior Wills and Codicils.

Marital Status
2. I am married.

Children
[_] I have no live children .
[_] I have living children.

EXECUTOR
Executor
4. The expression 'my Executor' used throughout this Will includes either the singular or plural number, or the masculine or feminine gender as appropriate wherever the fact or context so requires. The term 'executor' in this Will is synonymous with and includes the term 'executrix'.

Appointment
5. I appoint ____executor____ of ____executoraddress____, New South Wales as the sole Executor of this Will.

Powers of My Executor
6. I give and appoint to my Executor the following duties and powers with respect to my estate:

a. To pay my legally enforceable debts, funeral expenses and all expenses in connection with the administration of my estate and the trusts created by my Will as soon as convenient after my death, except for any debt secured by real and/ or personal property which is to be assumed by the recipient of such property.

b. To take all legal actions to have the probate of my Will completed as quickly and simply as possible, and as free as possible from any court supervision.

c. To retain, exchange or dispose of any personal property without liability for loss or depreciation.

d. To purchase, maintain, convert and liquidate investments or securities, and to exercise voting rights in connection with any shareholding, or exercise any option concerning investments or securities.

Select or Add Testator

	Name	Sex	DOB	Address	Wallet	Balance
1	John Wallace	M	20088	Lot 49, Cowpasture Road, Mulgoa, 2745, NSW	walletaddress	1000000
2	Mary Wallace	F	20101	Lot 49, Cowpasture Road, Mulgoa, 2745, NSW	walletaddress	100
3	James Stewart	M	18218	McPhee & Associates, Springwood, 2777, NSW	walletaddress	350
4	Fred Wallace	M	29041	1/16 Ronald Avenue, Freshwater, 2096, NSW	walletaddress	5
5	Bec Smith	F	29432	4 Arnold Street, Cremorne, 2090, NSW	walletaddress	8
6	Sam Wallace	M	29969	3 View Street, Coffs Harbour, 2450, NSW	walletaddress	15
7	Jim Wallace	M	30376	123 Soldiers Road, Anna Bay, 2316, NSW	walletaddress	140
8	May Fredricks	F	31310	7 Payne Road, Castle Hill, 2154, NSW	walletaddress	24
9	Tom Wallace	M	12965	54 Bland Rd, Springwood NSW, 2777, NSW	walletaddress	200

Name	Sex	DOB	Address	Wallet	Balance
John Wallace	M	20088	Lot 49, Cowpasture Road, Mulgoa, 2745, NSW	walletaddress	1000000

```
inherits(bec_smith,20).
inherits(sam_wallace,10).
inherits(jim_wallace,20).
inherits(may_fredricks,40).
entity(parent,tom_wallace,12965,walletaddress,200).
entity(parent,aida_wallace,13378,walletaddress,200).
entity(sibling,anne_patrick,19378,walletaddress,9000).
entity(sibling,ines_brown,20255,walletaddress,5000).
entity(sibling,steve_wallace,21459,walletaddress,6000).
entity(witness1,brian_bellhaus,22692,walletaddress,800).
entity(witness2,margaret_talbot,24042,walletaddress,16).

death(john_wallace,43646).
execute_will(john_wallace,1249,1000,43680,james_stewart).
```

```
message_to_human(james_stewart,john_wallace,"insert_message_to_Executor_here...")
transfer(john_wallace,walletaddress,99775,fred_wallace,walletaddress)
transfer(john_wallace,walletaddress,199550,bec_smith,walletaddress)
transfer(john_wallace,walletaddress,99775,sam_wallace,walletaddress)
transfer(john_wallace,walletaddress,199550,jim_wallace,walletaddress)
transfer(john_wallace,walletaddress,399100,may_fredricks,walletaddress)
transfer(john_wallace,walletaddress,2249,james_stewart,walletaddress)
```

Fig. 1. Smart Contract Editor showing "Will and Testament" on left and Smart Instantiation Editor at top right

III. Implementation Details

We take an existing legal document and create an electronic version by adding markup at instantiation points, called instantiation place holders (IPHs). Each IPH has embedded with it a variable identifier, variable type, action, cardinality and scrolling information. Our smart contract editor downloads this electronic version and the matching logic program as templates from a distributed ledger dedicated for this purpose.

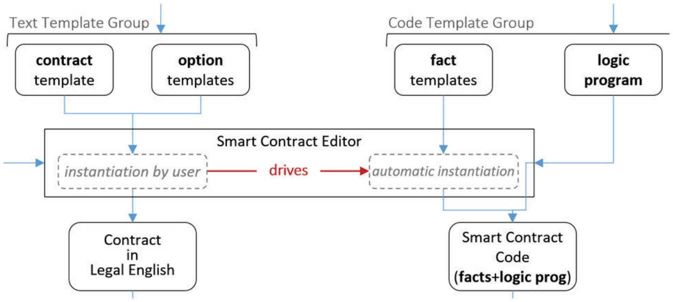
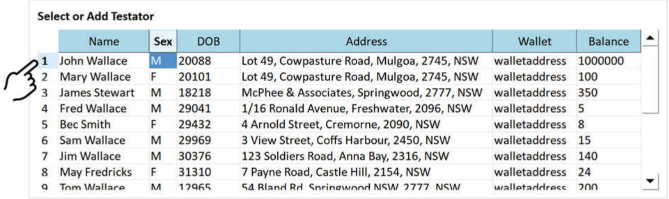


Fig. 2. Templates downloaded by our Smart Contract Editor

Our work shows that filling out the legal document (Fig. 1 left side) can automatically instantiate the logic program by auto-generating ASP **facts** (Fig. 2). Once the smart contract is written and tested, deployment to the blockchain simply involves aggregating the auto-generated ASP **facts** and the invariant ASP **logic program** as a smart contract transaction.

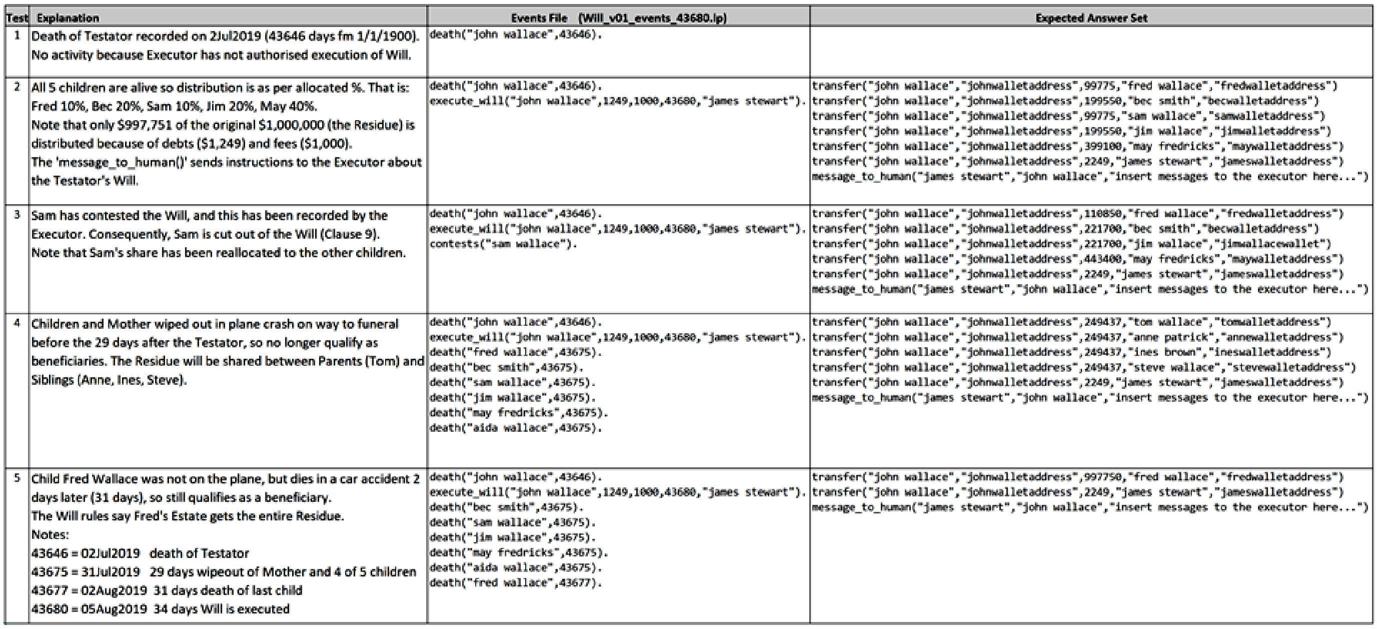
This means we replace bytecode with ASP, requiring the embedding of an ASP grounder/solver tool within the EVM.

The specification embedded with each active IPH allows our smart contract editor to know what type of information is required, where to find it, and how to process and display it. In the emerging blockchain environment, this information is often available from distributed ledgers, but in the case of information about people (entities), we propose an enhancement to wallets beyond the storage of cryptocurrencies. Personal information such as name, date of birth and address, is commonly called Personally Identifiable Information (PII) [13] and is a key concern of cybersecurity and privacy researchers. We propose that PII is stored offline in hardware wallets with owners having control over how it is accessed (similar to [8]). Our SCE guides the user during smart contract creation with mini-editors specific to the variable type, called Smart Instantiation Editors (SIEs).


Select or Add Testator

	Name	Sex	DOB	Address	Wallet	Balance
1	John Wallace	M	20088	Lot 49, Cowpasture Road, Mulgoa, 2745, NSW	walletaddress	1000000
2	Mary Wallace	F	20101	Lot 49, Cowpasture Road, Mulgoa, 2745, NSW	walletaddress	100
3	James Stewart	M	18218	McPhee & Associates, Springwood, 2777, NSW	walletaddress	350
4	Fred Wallace	M	29041	1/16 Ronald Avenue, Freshwater, 2096, NSW	walletaddress	5
5	Bec Smith	F	29432	4 Arnold Street, Cremorne, 2090, NSW	walletaddress	8
6	Sam Wallace	M	29969	3 View Street, Coffs Harbour, 2450, NSW	walletaddress	15
7	Jim Wallace	M	30376	123 Soldiers Road, Anna Bay, 2316, NSW	walletaddress	140
8	May Fredricks	F	31310	7 Payne Road, Castle Hill, 2154, NSW	walletaddress	24
9	Tom Wallace	M	12965	54 Bland Rd, Springwood NSW, 2777, NSW	walletaddress	200

Fig. 3. Smart Instantiation Editor (SIE) for 'entities'



Test	Explanation	Events File (Will_v01_events_43680.lp)	Expected Answer Set
1	Death of Testator recorded on 2Jul2019 (43646 days fm 1/1/1900). No activity because Executor has not authorised execution of Will.	death("john wallace",43646).	

2	All 5 children are alive so distribution is as per allocated %. That is:
	Fred 10%, Bec 20%, Sam 10%, Jim 20%, May 40%.
	Note that only $997,751 of the original $1,000,000 (the Residue) is distributed because of debts ($1,249) and fees ($1,000).
	The 'message_to_human()' sends instructions to the Executor about the Testator's Will.
		death("john wallace",43646).
		execute_will("john wallace",1249,1000,43680,"james stewart").
			transfer("john wallace","johnwalletaddress",99775,"fred wallace","fredwalletaddress")
			transfer("john wallace","johnwalletaddress",199550,"bec smith","becwalletaddress")
			transfer("john wallace","johnwalletaddress",99775,"sam wallace","samwalletaddress")
			transfer("john wallace","johnwalletaddress",199550,"jim wallace","jimwalletaddress")
			transfer("john wallace","johnwalletaddress",399100,"may fredricks","maywalletaddress")
			transfer("john wallace","johnwalletaddress",2249,"james stewart","jameswalletaddress")
			message_to_human("james stewart","john wallace","insert messages to the executor here...")

3	Sam has contested the Will, and this has been recorded by the Executor. Consequently, Sam is cut out of the Will (Clause 9).
	Note that Sam's share has been reallocated to the other children.
		death("john wallace",43646).
		execute_will("john wallace",1249,1000,43680,"james stewart").
		contests("sam wallace").
			transfer("john wallace","johnwalletaddress",110850,"fred wallace","fredwalletaddress")
			transfer("john wallace","johnwalletaddress",221700,"bec smith","becwalletaddress")
			transfer("john wallace","johnwalletaddress",221700,"jim wallace","jimwallacewallet")
			transfer("john wallace","johnwalletaddress",443400,"may fredricks","maywalletaddress")
			transfer("john wallace","johnwalletaddress",2249,"james stewart","jameswalletaddress")
			message_to_human("james stewart","john wallace","insert messages to the executor here...")

4	Children and Mother wiped out in plane crash on way to funeral before the 29 days after the Testator, so no longer qualify as beneficiaries. The Residue will be shared between Parents (Tom) and Siblings (Anne, Ines, Steve).	death("john wallace",43646).
		execute_will("john wallace",1249,1000,43680,"james stewart").
		death("fred wallace",43675).
		death("bec smith",43675).
		death("sam wallace",43675).
		death("jim wallace",43675).
		death("may fredricks",43675).
		death("aida wallace",43675).
			transfer("john wallace","johnwalletaddress",249437,"tom wallace","tomwalletaddress")
			transfer("john wallace","johnwalletaddress",249437,"anne patrick","annewalletaddress")
			transfer("john wallace","johnwalletaddress",249437,"ines brown","ineswalletaddress")
			transfer("john wallace","johnwalletaddress",249437,"steve wallace","stevewalletaddress")
			transfer("john wallace","johnwalletaddress",2249,"james stewart","jameswalletaddress")
			message_to_human("james stewart","john wallace","insert messages to the executor here...")

5	Child Fred Wallace was not on the plane, but dies in a car accident 2 days later (31 days), so still qualifies as a beneficiary.
	The Will rules say Fred's Estate gets the entire Residue.
	Notes:
	43646 = 02Jul2019 death of Testator
	43675 = 31Jul2019 29 days wipeout of Mother and 4 of 5 children
	43677 = 02Aug2019 31 days death of last child
	43680 = 05Aug2019 34 days Will is executed
		death("john wallace",43646).
		execute_will("john wallace",1249,1000,43680,"james stewart").
		death("bec smith",43675).
		death("sam wallace",43675).
		death("jim wallace",43675).
		death("may fredricks",43675).
		death("aida wallace",43675).
		death("fred wallace",43677).
			transfer("john wallace","johnwalletaddress",997750,"fred wallace","fredwalletaddress")
			transfer("john wallace","johnwalletaddress",2249,"james stewart","jameswalletaddress")
			message_to_human("james stewart","john wallace","insert messages to the executor here...")

Fig. 4. Example test cases for 'Will and Testament'

SIEs act on the specification embedded in each active IPH by retrieving and presenting information if it is available, so that input is reduced to mouse clicks or a screen touches. The SIE in Fig. 3 lists entities (legal usage) that are candidates for 'testator'. This list is generated from wallets invited to the smart contract creation session where the owner has authorised access to PII. The overall result is that users fill out the form by tabbing between IPHs, selecting data with mouse clicks or screen touches, not aware that they are generating an executable ASP program.

We envision that a commercial implementation of the smart contract editor would be a collaborative distributed web app having many of the features present in Discord, like VoIP voice, text chat and video in addition to a shared real-time view of the current smart contract session [5].

Note that this example also illustrates our type hierarchy; for example, type 'testator' is of meta-type 'entity'. This is an important feature that simplifies both auto-coding and testing.

Our system controls state via **events**, essentially **facts** that occur at a certain point in time and are deployed to the blockchain in sequential transactions. Our system requires that all code (that is **facts**, **logic program**, and **events** in subsequent associated transactions) be aggregated before being executed by a miner, allowing **events** to control the state of the system. For example, we signal a death to the smart contract by deploying a transaction with the following ASP code (an **event**) to the blockchain (the integer is date of death):

```
death("John Doe",43002).
```

In an actual implementation, this transaction is likely to be automatically generated when new transactions are added to another distributed ledger (i.e. a distributed ledger managed by the Registry of Births, Deaths and Marriages).

As can be seen from the table of test cases (Fig. 4) the 'Will and Testament' we implement is non-trivial, yet we achieve a significant reduction in complexity, highlighted by the small number of atoms covering all **facts** allowed, being `entity/5`, `inherits/2`, and `creation/2`. Similarly, **events** allowed are `death/2`, `contests/2`, and `execute_will/5`, so the testing space involves combinations of only 6 atoms, simple enough in this instance for an exhaustive testing approach.

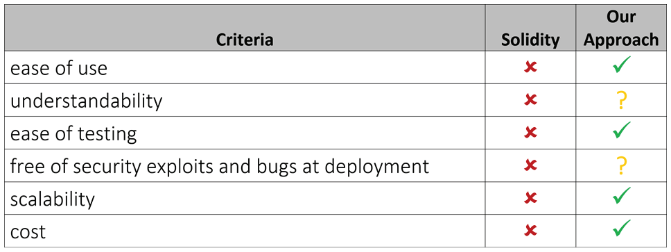
ASP generates results as 'answer sets', shown in the right column of Fig. 4; primarily money transfers coded by atom `transfer/5`. We also allow e-mails/text messages to be generated with atom `message_to_human/3`. We envisage Ethereum executing these commands via an interface that translates these answer sets.

Other features and simplifying mechanisms that our approach uses, include: 1) options (a variable type that allows selection of different blocks of legal text and ASP code); 2) the exploitation of object attributes allowing automatic instantiation of all attributes associated with a variable; 3) active and non-active IPHs (supports 2 above); 4) the use of meta-variables to implement a type hierarchy for variables.

Features planned in future work include: 1) visualisation of testing; 2) formal verification of ASP code; and 3) the use of clearing houses to guarantee contract performance or provide compensation.

IV. Results

Our implementation of the 'Will and Testament' demonstrates that the combination of an intuitive user interface with a declarative approach to smart contract generation has two important benefits: 1) improved ease of use, and 2) improved testing effectiveness. The advantages over Solidity



Criteria	Solidity	Our Approach
ease of use	✗	✓
understandability	✗	?
ease of testing	✗	✓
free of security exploits and bugs at deployment	✗	?
scalability	✗	✓
cost	✗	✓

Fig. 5. Comparing our approach with Solidity

are illustrated by assessing against our preliminary evaluation criteria.

In addition to the above benefits, we note the potential for significant blockchain space savings because at a minimum, only ASP **facts**, ASP **events**, and the contract key/contract version need be stored on the blockchain. All other components are invariant and stored on our envisaged template distributed ledger keyed by contract type and version. This means that the text smart contract can be reconstructed from templates, with variables discovered from ASP **facts** and ASP **events**. Such a scheme would require a small adjustment to the mining procedure, which at present only aggregates blockchain transactions.

Our investigation of the broader benefits from conversion of legal documents to smart contracts reveals that for a ’Will and Testament’ the key benefit is the ability to specify up front all the terms and conditions and then have these carried out over time as desired automatically. When applied to a typical Real Estate Sale contract, the benefit is different, focused more around automation of the often complex sale process.

We also investigated a third more complex contract (CEO employment contract). This type of contract relies on a different type of legal reasoning (not deductive logic) and ’performance’ [1] that cannot easily be defined; for example, ”faithfully and diligently serve the interests of the employer”.

Our limited investigation has identified 1) type of legal reasoning, and 2) type of ’performance’, as some of the factors determining the automatability of a legal contract. A useful aid for this task would be exhaustive taxonomies of types of legal document, types of legal reasoning, and types of ’performance’.

V. Conclusion

We have identified a cost effective and scalable approach to the creation and deployment of smart contracts that improves usability and testing, and is supportive of adoption because conversion starts with current legal documents. Further, our approach is tolerant of varying levels of automation and allows human-in-the-loop interaction. Smart contracts are seen as game changing, and should issues with usability, security and cost be solved, the economic impact is likely to be large.

References

[1] Australian Contract Law. 2010. “Performance and termination.” Australian Contract Law. Accessed Sep 11, 2019. https://www.australiancontractlaw.com/law/termination.html.

[2] Calimeri, Wolfgang Faber, Martin Gebser, Giovambattista Ianni, Roland Kaminski, Thomas Krennwallner, Nicola Leone, Francesco Ricca, Torsten Schaub. 2015. ASP-Core-2 Input Language Format. Technical Report, ASP Standardization Working Group.

[3] Brewka. 2011. “Answer Set Programming at a Glance.” Communications of the ACM 54 (12): 93-103.

[4] Chohan, Usman. 2017. “The Decentralized Autonomous Organization and Governance Issues.” Social Science Research Network. 4 Dec. Accessed Sep 11, 2019. https://ssrn.com/abstract=3082055.

[5] Discord Inc. 2019. Discord App. 11 Sep. Accessed Sep 11, 2019. https://discordapp.com/.

[6] Grigg, Ian. 2004. “The Ricardian Contract.” Proceedings of the First IEEE International Workshop on Electronic Contracting. Washington, DC, USA: IEEE Computer Society Washington, DC, USA. 25-31.

[7] Investopedia. 2019. Business-to-Consumer (B2C). 20 May. Accessed Sep 11, 2019. https://www.investopedia.com/terms/b/btoc.asp.

[8] Jäger, Oliver. 2013. “Technologien für das Privacy Wallet.” paper, Trier.

[9] JCT. 2019. About JCT. 11 Sep. Accessed Sep 11, 2019. https://corporate.jctltd.co.uk/about-us/.

[10] Lierler, Yuliya. 2017. “What is answer set programming to propositional satisfiability.” Constraints 307-337.

[11] Marks, Eric. 2018. “The Case for Graphical Smart Contract Editors.” Medium. 30 Apr. Accessed Sep 11, 2019. https://medium.com/pennblockchain/the-case-for-graphical-smart-contract-editors-8e721cdcde93.

[12] McCarthy, John. 1988. “Mathematical logic in artificial intelligence.” Daedalus (Common Sense) 297-311.

[13] NIST. 2019. National Institute of Standards and Technology - Information Technology Laboratory - Computer Security Resource Center. 11 Sep. Accessed Sep 11, 2019. https://csrc.nist.gov/glossary/term/personally-identifiable-information.

[14] OpenLaw. 2019. “About.” OpenLaw Docs. 11 Sep. Accessed Sep 11, 2019. https://app.openlaw.io/about.

[15] Prestwich, James. 2018. Declarative Smart Contracts. 2 Sep. Accessed Sep 11, 2019. https://prestwi.ch/declarative-smart-contracts-2/.

[16] Wood, Gavin. 2017. “Ethereum: A secure decentralised generalised transaction ledger EIP-150 REVISION.” Yellow Paper.

Towards model-driven expressions of the blockchain ethical design framework

Zoran Milosevic [1,2]
[1]Deontik, Australia
[2]Institute for Integrated and Intelligent Systems, Griffith University, Australia

Abstract — **This paper investigates model-driven extensions of the blockchain ethical design framework developed by Laponte and Fishbane [1]. The extensions are motivated by our recent proposal to provide a model-driven approach to expressing ethics principles and ethics concepts in digital health, including new privacy and AI challenges [2]. Our model-driven approach is based on the precise modelling concepts from the ISO ODP Enterprise Language standard [3]. The combination of the intentional design approach from the blockchain ethical design framework and the precise modelling concepts for expressing the enterprise aspects of distributed systems, including governance, accountability and privacy, provides a sound foundation for a tool-based design and deployment of responsible distributed ledger solutions.**

Keywords – ethics; distributed ledgers; blockchain; privacy; consent; deontic logic; ODP enterprise language; AI.

I. EXTENDED ABSTRACT

Laponte and Fishbone recently proposed a blockchain ethical design framework, which adopts the intentional design approach in order to address the specific challenges of blockchain, while carefully supporting different needs and characteristics of various users. For example, the change in the deployed blockchain solution is significantly more complicated to support than in a traditional digital solution because any information already in a blockchain is immutable and distributed. The intentional design allows to identify what attributes need to be prioritized at the expense of others in the design process [1].

The overarching goals of the framework are to (1) give decision makers an outcome-focused and user-centric tool to assess the context-specific consequences and ethical implications of their blockchain design choices; and (2) to enable them to use this understanding to make the appropriate values-based design choices to achieve better social outcomes [1].

Three phases are identified in the framework.The first phase is defining the approach to creating social impact, and it involves the initial work of understanding the desired outcome and explicitly defining an approach with which to achieve this outcome. The second phase is the design and implementation of the blockchain through a design spiral that reveals the impacts of design choices on the desired outcome and on the people affected by the design. The third phase is the maintenance, in which the steps from the first two phases are periodically revisited throughout the life cycle of a blockchain project to ensure that the technology is still achieving its desired impact [1].

The design and implementation stage involve addressing several key ethical consideration areas. These are: *governance*, *identity*, *access*, *verification and authentication*, *ownership of data*, and *security*. The framework provides an analysis of how particular design choices in each area will affect the desired outcome and the participants. This analysis is presented in terms of well-developed guidelines for decision makers and these form a structured approach to designing and implementing a specific distributed ledger solution.

We believe that these design guidelines can be further extended in terms of model-driven expressions for relevant concepts in the framework, in particular for each of the ethical considerations identified. This is motivated by our recent proposal to provide a model-driven approach to expressing ethics principles and ethics concepts in digital health, including new privacy and AI challenges [2]. Our model-driven approach is generic and based on the use of precise modelling concepts from the ISO ODP Enterprise Language (ODL-EL) standard. Three groups of modelling concepts are that of relevance for this blockchain ethical design framework are introduced next.

A. Community concepts

The main structuring concept in the ODP-EL, called *community*, is used to describe a grouping of interested parties involved in a particular social context and their behaviour, including the use of digital technology, in support of their objective. That behaviour is specified in terms of *community roles*, which can be filled by specific enterprise objects, either humans or digital systems. An *enterprise object* is any object in an enterprise specification, with special types of *party*, modelling a legal entity, and *active enterprise object*, modelling an entity which can participate in some behaviour.

Community can be used to model governance related concepts in the framework, namely [1]:

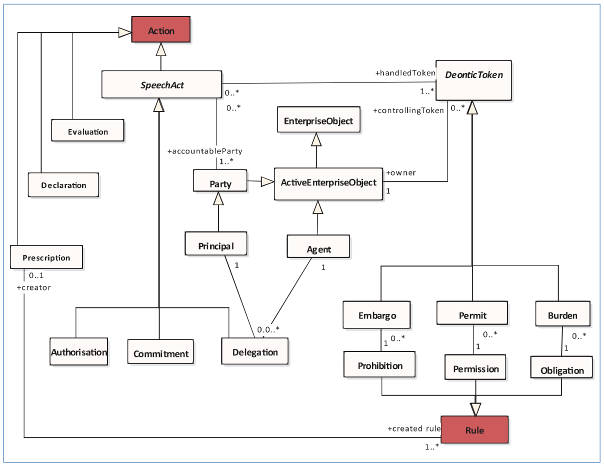
- the stakeholders, their roles, and how their roles are established
- the processes, rules, and regulations (both technical and otherwise) that apply to the roles
- defining how these rules and roles change over time
- describing a plan for closing out or continuing the system if key stakeholders leave

Governance also covers the rules and regulations of digital identity, data ownership, and security, as well as data access and verification and authentication.

Community defines policies that apply to the roles and enterprise objects filling the roles. This includes the business, social and legal rules, processes and relationships between roles in the community. They can be described by applying the deontic and accountability concepts, introduced next.

B. Deontic concepts

The ODP-EL supports modelling of obligations, prohibitions and permissions as constraints on behaviour. In addition, the standard provides concepts for modelling the dynamics of deontic constraints i.e. when they become applicable to the actions of parties and how they are passed among parties (and/or active enterprise objects). These are relevant for the governance, compliance and management of interactions between autonomous decision-making components and humans in a system. This is achieved by introducing a special type of enterprise object, called *deontic token*, which captures deontic assertions. The deontic tokens are held by the parties involved and holding one controls their behaviour. There are three types of deontic tokens: *burden*, representing an obligation, *permit* representing permission and *embargo*, representing prohibition. In the case of a burden, an active enterprise object holding the burden must attempt to discharge it either directly by performing the specified behaviour, or indirectly by engaging some other object to take possession of the burden and perform the specified behaviour. In the case of permit, an object holding the permit is able to perform some specified piece of behaviour. In the case of embargo, the object holding the embargo is inhibited from performing the behaviour.



Another concept for modelling the dynamics of deontic constraints is *speech act* [3]. This is a special kind of action used to modify the set of tokens held by an active enterprise object. The name was chosen by analogy to the linguistic concept of speech act, which refers to something expressed by an individual that not only presents information but performs an action. Thus, a speech act intrinsically changes the state of the world in terms of the association of deontic tokens with active enterprise objects. This modelling feature allows the specification of speech acts that can be performed by people and AI systems, yet distinguish them when necessary to establish links with ethics, legal and social norms. These modelling concepts are shown in the figure (action and rule are the ODP foundational concepts [4]).

C. *Accountability concepts*

The deontic modelling framework presented provides a rich model to define many types of deontic constraints across AI systems and human actors. This framework is further extended to support traceability of obligations of parties, according to their broader responsibilities derived from ethical, social or legal norms. These extensions cover a set of accountability concepts introduced next [3]:

Principal is a party that has delegated something (e.g. authorisation or provision of service) to another. *Agent* is an active enterprise object that has been delegated something (e.g. authorisation, responsibility of provision of service) by, and acts for, a party.

Delegation is an action that assigns something (e.g. authorisation, responsibility of provision of service) to another object, e.g. agent.

Commitment, is an action resulting in an obligation by one or more participants in the act to comply with a rule or perform a contract, and this will be assigned a burden.

Declaration, is as an action by which an object makes facts known in its environment and establishes a new state of affairs in it. This can for example be performed by an AI system (or a party managing it) informing the interested parties about the result of some analysis.

Evaluation, is an action that assesses the value of something. Value can be considered in terms of various variables e.g. importance, preference and usefulness.

Prescription, is an action that establishes a rule. Prescriptions provide a flexible and powerful mechanism for changing the system's business rules at runtime, enabling its dynamic adaptation to respond to business changes. This is important to support the applicability of new policies reflecting new legislations, recommendations from AI applications or new governance rules.

Authorisation, is an action indicating that a particular behaviour shall not be prevented. Unlike a permission, an authorisation is an empowerment. So, the enterprise object that has performed authorisation will issue a required permit and will itself undertake a burden to facilitate the behaviour.

D. *Implementation and Tooling Options*

The community, deontic and accountability concepts can be used to model social, ethics and legal rules related to the stakeholders affected by blockchain as well as decision makers involved in creating responsible blockchain systems. These concepts can be applied through various design stages for a blockchain-based solution but can be also used to monitor actions of agents in the system and enforce them via smart contracts.

These modelling concepts are also mapped to UML in the UML profile for ODP standard [4] and can be implemented in any UML tooling supporting model-driven engineering. Some vendors, most notably NoMagic [5], provide free RM-ODP plugins.

We believe that the combination of the intentional design approach from the blockchain ethical design framework and the precise modelling concepts for expressing the enterprise aspects of distributed systems, including governance, accountability and privacy, provides a sound foundation for a tool-based design and deployment of responsible distributed ledger solutions.

REFERENCES

[1] Laponte, C, Fishbane, R., *The Blockchain Ethical Design Framework*, Beeck Center, Georgetown University, June 2018.

[2] Milosevic, Z., *Ethics in Digital Health: a deontic accountability framework*, Proc. IEEE EDOC 2019 conference, Oct. 2019.

[3] ISO/IEC 15414, *Information technology: Open distributed processing, Reference model – Enterprise Language*, 3rd ed, 2015.

[4] P.F. Linington, Z. Milosevic, A. Tanaka and A. Vallecillo, *Building Enterprise Systems with ODP, An Introduction to Open Distributed Processing*, Chapman & Hall/CRC Press, 2011.

[5] NoMagic Inc, www.nomagic.com

BLOCKCHAIN FOR THE MEAT INDUSTRY: WHERE AND HOW?

David Barnes
Department of Business Strategy and Innovation
Griffith University
Brisbane, Australia
david.barnes@griffith.edu.au

Yong Wu
Department of Business Strategy and Innovation
Griffith University
Gold Coast, Australia
yong.wu@griffith.edu.au

Peter Tatham
Department of Business Strategy and Innovation
Griffith University
Gold Coast, Australia
p.tatham@griffith.edu.au

Vallipuram Muthukkumarasamy
School of Information and Communication Technology
Griffith University
Gold Coast, Australia
v.muthu@griffith.edu.au

Abstract

Substitution and counterfeiting in global supply chains pose a significant challenge for businesses due to the negative impact these fraudulent products can have on brand reputations and sales margins. Unsurprisingly, therefore, there are instances where red meat products have been falsely marked with a popular country of origin, such as Australia, in order to take advantage of the perception of premium quality associated with the meat products from these countries. In collaboration with the Australian Meat Processor Corporation (AMPC) a research team from Griffith University undertook a project to investigate the potential use of blockchain technology to establish product traceability for the Australian red meat industry. Specifically, the project examined (1) what types of information, (2) at what places along the meat supply chain, and (3) how the information should be collected in order to facilitate the use of blockchain technology.

Project Methodology

The research team adopted a multi-methodological approach to investigate the use of blockchain to traceability for the red meat industry. Such approaches combine multiple methodologies to explore research problems [1, 2], and are particularly useful for formulation, approximation, analysis and solution of complex logistics and supply chain problems [3]. The approaches selected were

1. Supply Chain Operations Reference Process Mapping

The project utilised the Supply Chain Operations Reference (SCOR) framework as the basis for processing mapping "as-is" and "to-be" scenarios, which was then strengthened by further process decomposition beyond the SCOR model. Process mapping is "a valuable communication device to understand how processes operate and where responsibility lies" [4].

A web-based application was developed to facilitate the collection of detailed information, such as processes time and resources required for collecting traceability information, for each step

2. Scenario Building

Using the SCOR framework the research team established scenarios to investigate the integration of blockchain technology into meat processing facilities and assess the associated costs and benefits for each scenario. A base scenario ("as-is" scenario) was constructed which reflected the existing meat processing operations. The base scenario served two purposes: 1) to acquire a thorough understanding of the current operations; and 2) to serve as the basis for the development of different scenarios where traceability is established.

Based on the desired level of traceability, two further scenarios (the "to-be" scenarios) were constructed. The first focussed on traceability at the batch level, i.e., providing meat traceability based on the current batch processing information used by meat processors noting that this does not support one-to-one traceability. In order to offer one-to-one traceability, the current meat processing flow will need to be adjusted slightly and the second scenario was designed to provide this based on a proposed boning room redesign.

Once the scenarios had been constructed, comparisons between the "as-is" and the "to-be" scenarios highlighted the changes needed in order that these could become the focus of further and more detailed investigation.

3. Data Collection

The focus for data collection was to determine the nature and attributes of the information that would need to be collected to enable the use of blockchain, and how this corresponded with the physical flows. Given that meat products are packaged in processor facilities, the meat processing stage is the key to establishing traceability throughout a supply chain. Thus, the project team focused on this stage through a case study based on the processes undertaken at Australian Country Choice (ACC) – which was recommended by AMPC as an industry exemplar. The project team undertook a walkthrough of the ACC processing facility from the entry of a live animal through all the processing stages to the end retail/bulk pack, and this underpinned the development of the "as-is" scenario.

4. ROI Analyses

The data collected were then fed into an ROI calculator which, together with fixed investments, produced the results for ROI analyses to assess the feasibility of each scenario. The research team also estimated the size of the expected benefits in order to allow the team to develop a better understanding of the potential cost recovery options. Total expected price increases (per kilogram) and total expected labour cost savings were the two sources of benefits used to help users decide the potential ROIs

Project Outcome

During this project, a base scenario ("as-is" scenario) was constructed to reflect the existing meat processing operations. Two "to-be" scenarios were then proposed based on the desired level of traceability: the first focused on traceability at the batch level tracking all the products leaving the boning room of meat processing facilities; and the second on one-to-one traceability (i.e., paddock to plate). The project outcomes included:

1. Process maps for both the "as-is" and the "to-be" scenarios.

2. Recommendations on data collection to establish traceability for meat processors using considerations of what data was needed, where it should be collected, how this would be achieved and who would be responsible for collecting it.

3. The proposed boning room redesign to enable one-to-one traceability, given the current boning room operations usually lead to mixing of primal cuts.

4. The development of the web-based application to conduct process mapping and ROI analysis.

ROI Analysis

The ROI analysis results for meat processors on the scenario where one-to-one traceability is desired indicated that a redesign to the boning room, and thus operational changes to the current meat processing practices (and hence additional investment), were required. Two ROI analyses were therefore conducted to assess the feasibility of this approach. The first ROI analysis focused on understanding the fixed cost implications of developing one-to-one traceability; and the second ROI analysis considered a number of benefits resulting from the use of one-to-one traceability.

Benefits for Industry

1. Market advantage in a future market

   i. Food provenance is becoming an increasingly important consideration for consumers, particularly within export markets where there have been cases of fraudulent products entering the retail stream. Blockchain can secure the supply chain in a digital manner and work with existing physical measures to further protect a brand's perception within the retail market.

   ii. Early adopters of blockchain technology might gain advantages such as product competitiveness or customer loyalty. Furthermore, brands implementing the technology are likely to give consumers confidence in their products authenticity and quality and this may secure or capture more market share in the future.

   iii. Consumers are likely to be interested in more than just the product provenance information. Meat product brands can seek to differentiate themselves by providing the 'story' behind their products such as the farming region and the approaches used by farmers to produce high quality meat.

2. Labour cost savings/automation

   i. Developments in automated red meat processing have the potential to integrate well with traceability systems.

   ii. Automation will also help address the issues of rising labour cost and labour supply in the long run.

3. Regulatory compliance and risk reduction

   i. Adoption of increased traceability systems may also help address the regulatory requirements. Companies operating a traceability system are likely to be ahead of the game and in a strong position to guide and inform policy development in a more advantageous way.

   ii. A blockchain enabled one-to-one traceability system would enable a meat cut's full history to be determined with certainty in a very short amount of time. This in turn would enable a quicker response to an emerging health-related situation, and more importantly limit the extent of damage arising from the incident to farmers, processors and retailers who are not affected or involved.

Conclusion

While providing the desired traceability is unquestionably challenging, the potential benefits inherent in securing Australia's global reputation as a quality red meat producer and the potential for improved market outcomes may be considerable. Furthermore, current market indications are that there will be a growing demand for provenance information in both the domestic and international markets. Thus, early implementation of a blockchain-supported system would clearly place Australian producers, processers and retailers in a competitive position.

Recommendations to develop this initial research project further include undertaking a market survey, targeting both domestic and international end consumers, in order to collect the market perceptions of the benefits of one-to-one traceability. A pilot implementation of the proposed one-to-one traceability within a typical meat processing facility is also needed in order to confirm our initial understanding of the main technical requirements and implementation challenges. This pilot could also then inform business decisions around, but are not limited to, (1) understanding the optimum product mix that should be produced, (2) which types of meat are trending on the market, and (3) consumer preferences in relation to the production locational differences for meat products.

References

[1] Singhal, K., Singhal, J., 2012. Imperatives of the science of operations and supply-chain management. Journal of Operations Management, 30(3), 237-244.

[2] Singhal, K., Singhal, J., 2012. Opportunities for developing the science of operations and supply-chain management. Journal of Operations Management, 30(3), 245-252.

[3] Srivastava, S., 2007. Green supply chain management: A state-of-the-art literature review. International Journal of Management Reviews, 9(1), 53-80.

[4] Collier, D., Evans, J., 2007. Operations Management: Goods, Services and Value Chains. Thomson South-Western.

Open End-to-End Encrypted Messaging

Steven H. McCown
Anonyome Labs
Mapleton, Utah, USA
smccown@anonyome.com

Paul Ashley
Anonyome Labs
Toowong, Australia
pashley@anonyome.com

Jon St John
Anonyome Labs
Salt Lake City, UT, USA
jstjohn@anonyome.com

***Abstract*—Text messaging has largely supplanted email for short person-to-person communications, as well as, critical business notifications. SMS, the original cellular-based text messaging, provided a valuable delivery service, but omitted encryption, leaving messages unprotected. While current end-to-end encrypted (E2EE) messaging services provide encryption, it is at the expense of interoperability, which limits secure messaging to within a single provider's network (known as a "walled garden"). This paper abstract examines the migration from SMS to E2EE and presents a method of exchanging E2EE messages between separate providers using self-sovereign identity (SSI) methodologies.**

Keywords—messaging, encryption, blockchain, ledger, self-sovereign identity, identity

I. Email vs. Messaging

Email drew everyday users to the internet, because it was simple and fast ... *ask a question and get a quick answer*. While email remains popular (281 billion emails sent in 2018 growing by 5% per year [1]), messaging is winning for the same reason. Domo reported [2] that mobile users send 15,220,700 text messages every minute, which is nearly 8 trillion messages annually. Why are users switching? Email often feels too formal (e.g., *to, from, subject, body,* etc.), while messages are short to send and quick to read. This trend has attracted businesses who connect with customers through messages to send appointment reminders, fill prescriptions, send fraud alerts, etc. This shift in preferred communication methods provides an opportunity to redesign key technology elements to better protect user privacy and to enable new business capabilities.

II. SMS Messaging and Modern Security Needs

When SMS messaging (*text messaging*) was created, it largely leveraged pre-existing infrastructure costs by sending the new personal messages over the existing GSM signaling channels when they were not in use. By leveraging existing signaling channels, SMS messages had to match the general format of the signaling messages. This was a great advancement, because it kept costs lower while providing a new billable service. However, SMS did not include any user-level encryption and this left SMS messages unencrypted as they passed within the cellular carrier's infrastructure.

Thanks to data breaches becoming a common occurrence [3], today's users are painfully aware of the need to protect their private data and are increasingly moving away from SMS and are choosing end-to-end encryption (E2EE) messaging apps to ensure that only the intended recipient can read their messages. Increasing security by combining E2EE with enhanced key management and detailed message authentication processes is vital to protecting against many attack vectors, such as forgery (e.g., WhatsApp [4]) and Media File Jacking (e.g., WhatsApp and Telegram [5]), etc.). Making E2EE work (and simple for users to use) requires strong encryption plus some behind the scenes encryption key management that is simplified by emerging Self-Sovereign Identity technologies.

III. Trust on First Use

Secure protocols and strong encryption are vital in establishing private communications channels. However, the first important question is whether a sender has connected with their actual intended recipient or whether they have connected to an incorrect recipient or even a hostile *man-in-the-middle*. In order to connect to the correct party, a sender has three main methods by which to identify the correct recipient.

The first method is used when the two parties are both present in the same physical location where they can use physical verification methods to ensure that they exchange the correct identity information (i.e., public key). One method for physical presence verification is for one user to display a QR code representing their unique ID or public key and then for the other party to scan it with their cell phone or laptop camera. This process conveys information out-of-band from an accompanying messaging system.

The second method for correctly identifying a communication partner works when the two parties are both using the same messaging service. In this instance, both parties have an existing trust relationship with the hosting provider and can query the hosting provider for the other party's public key. This method is as simple as looking up the other party's key using a *phone book* type of service. Hosting providers commonly use this method, today.

A more complicated connection scenario occurs when two parties seeking to communicate are in different physical locations and using different messaging services. In this situation, one or both parties may not trust the other's messaging provider to return the correct public key upon request, so it is important to decouple the public key resolution from the message hosting provider. A blockchain or decentralized ledger will serve as a neutral source of truth for public key resolution. In this scenario, one user can send their blockchain-based identifier (e.g., DID; see below) to the recipient who can use that to retrieve additional information (e.g., public key) from the blockchain. The benefits of this method are that public key retrieval is separate from a remote messaging provider, the most recent public key employed by the DID is returned, and the key returned is verifiable by validating the associated digital signatures.

IV. Self-Sovereign Identity and Key Exchanges

Enabling E2EE, while keeping it simple for users, requires both strong encryption and a simple *hands-off* approach to encryption key management. These processes are simplified through the use of self-sovereign identity (SSI) technologies. A central theme of SSI is that each individual, and not a specific service provider, controls their identity information, which includes any required encryption keys. As a result, an SSI user's encryption keys are held by the SSI user and not by any site or service to which they connect.

SSI users can use their identity information to establish unique encrypted communication channels with each remote site or service where they establish a connection relationship. This is accomplished by negotiating a unique encryption keypair to be used only with the specific site with which it was negotiated during the connection process. A critical benefit of creating unique keypairs for each communication relationship is that this ensures that the compromise of one encrypted relationship does not affect the security of other communication relationships. The process of creating secure connections (e.g., exchanging encryption keys) can be made as simple as scanning a QR code or verifying an SSI identifier via its hosting blockchain. Both methods greatly simplify key exchanges between communication partners. The Sovrin Foundation's whitepaper [6] provides an excellent overview of many additional SSI elements.

From its inception, SMS Messaging has enabled subscribers of one SMS Provider (e.g., telco) to communicate with subscribers of another SMS Provider and this cross-service communication has been a boon for SMS messaging overall. The downside with the SMS protocol is the lack of message encryption. As new over-the-top application providers (e.g., iMessage, WhatsApp, Telegram, Signal, MySudo, etc.) emerged, they provided much needed message encryption. However, due to the complexity of encryption key management at that time, they ended up creating *walled gardens* that could control the encryption key management processes from a centralized location. This also required that message senders and recipients both use the same messaging app and provider, which left them unable to exchange E2EE messages with users of other messaging services. While this provider-centric communication method did succeed in simplifying encryption key management, it also limited message exchange to operate with recipients that belong to the same messaging service. Users have discovered that this limitation requires them to either adopt the messaging app used by their friends or to convince others to adopt their messaging app, which is often a difficult proposition.

V. Enabling Cross-Provider Addressing Using DIDs

On the web, the main identifier is a URL, which is used to navigate to webpages. In SSI, the main identifier is called a Decentralized Identifier or DID [7]. DIDs are conceptually similar to URLs in that as URLs point to webpages, DIDs point to cryptographically verifiable identifiers anchored on a decentralized ledger or blockchain. Figure 1 depicts the similarity between DIDs and URLs:

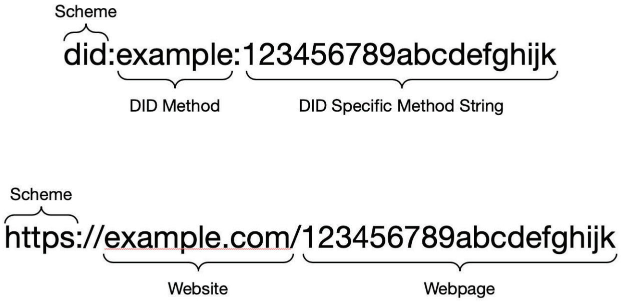

Scheme
did:example:123456789abcdefghijk
DID Method
DID Specific Method String
Scheme
https://example.com/123456789abcdefghijk
Website
Webpage

Figure 1 – DIDs and URLs

When DID Methods (i.e., the sites or services that host the DIDs) provide primitives for cryptographical verification, it makes the DIDs they create also self-certifying. This allows the DID's authenticity to be cryptographically verified by another user or service. This provides a notable benefit over standard URLs in that a DID's ownership and authenticity (along with the data they reference) can be verified before a user chooses to connect to it. When resolving a DID on a blockchain, it returns some additional information, which is known as a *DID Document* (i.e., DID Doc). DID Docs may contain additional information, such as: encryption keys, digital signatures, pointers to additional information, service endpoints, etc. Anchoring DIDs in a decentralized ledger or similar service (i.e., Public DIDs) decouples their authentication mechanisms from the host messaging service and helps avoid potential Man-In-The-Middle (MiTM) situations.

After two users verify each other's identity, they normally create a Pairwise DID, which is used to create a private encrypted communication pathway. In this model, a separate Pairwise DID is created for each communication relationship. Using separate encryption keys for each relationship ensures that if one set of encryption keys is ever compromised, then the rest of a user's encryption keys (i.e., those corresponding to other relationships) remain secure. This is a tangible benefit over traditional public key encryption whereby a single public keypair is used with an unlimited set of partners and a compromise of that keypair would also compromise all of a user's communication partners.

VI. Encrypted Messaging: Putting It All Together

When users install an SSI-enabled messaging client, the initialization process creates a secure SSI storage wallet (to store DIDs and other SSI information) on the local device, creates an initial Public DID, and registers that DID on the blockchain. Using a blockchain as a source of trust enables connecting parties to verify their respective DID's authenticity. When two SSI-based identities decide to connect, they negotiate a unique Pairwise DID (e.g., public keypair) that will be used to encrypt their communications. At a high level, the two parties to a Pairwise DID connection each create a new unique DID that will be used for their specific communication only and nothing else. The Pairwise DID Negotiation Process steps (described below) will show how each party's new DID are effectively connected (in their respective wallets) and used exclusively for private communication between those two parties. An overview of the Pairwise DID negotiation (message exchange) process is described in Figure 2:

1) Party A transmits an Invitation Message to Party B

2) Party B replies with a Connection Request

3) Party A replies with a Connection Response

4) Party B replies with an acknowledgement message

Figure 2 – Pairwise DID Negotiation Process Steps

When Party A (inviter) initiates a DID Exchange process (for creating a pairwise DID) with Party B (invitee), it creates an Invitation Message (e.g., in JSON format) that contains specific information describing the inviter's public DID identity and the transaction they wish to perform. Such information could also include a name label and either a publicly resolvable DID or a service decorator (e.g., service endpoint, recipient keys, and optionally routing keys). An invitee will use the information in the Pairwise DID Invitation Message to validate the inviter's identity (via the blockchain) and then create a new Pairwise DID and compose a reply to the Invitation Message.

In Figure 3 (below), a sample Pairwise DID Invitation Message is shown and contains a reference to the type of message being sent. By following the URL from the type field and loading its contents, Party B can obtain the message schema that describes the message format, required and optional fields, their respective types, etc. In this example, Party A also sends the ID of the message exchange, a human-readable label, their service endpoint, and requisite keys for public key encryption:

```
{
    "@type": "https://didcomm.org/didexchange/1.0/invitation",
    "@id": "12345678900987654321",
    "label": "Alice",
    "did": "did:sov:QmWbsNYhMrjHiqZDTUTEJs"
}
```

Figure 3 – Pairwise DID Invitation Message

Once Party B receives and processes the Invitation Message, it creates a new unique DID that constitutes their part of the to-be-created Pairwise DID, which will be used exclusively for communicating with Party A. After creating this new DID, Party B responds with an Exchange Request message wherein they send this new DID information to Party A. The Exchange Request message also contains logistical information, such as the message ID, the message type, and a human-readable label (as metadata). A sample Pairwise DID Exchange Request Message is shown in Figure 4:

```
{
    "@id": "5678876542345",
    "@type": "https://didcomm.org/didexchange/1.0/request",
    "~thread": { "pthid": "<id of invitation>" },
    "label": "Bob",
    "connection": {
        "did": "B.did@B:A",
        "did_doc": {
            "@context": "https://w3id.org/did/v1"
            // DID Doc contents here.
        }
    }
}
```

Figure 4 – Pairwise DID Exchange Request Message

Upon receiving the Exchange Request message, Party A decodes it and will have Party B's new DID information, which will be used in creating the new Pairwise DID. At this point, Party A creates a new unique DID that will constitute its half of the new Pairwise DID with Party B. To easily create Pairwise DIDs, Hyperledger Indy contains a convenience method called Pairwise.createPairwise(). To use this method, Party A passes a reference to its SSI wallet, its new DID, the new DID received from Party B, as well as, any user-defined meta data that they wish to store with the new Pairwise DID. After this method is called, a Pairwise DID will have been created and stored in their wallet as a Pairwise DID specifically for communicating with Party B. The process thus far has enabled Party A to independently generate a Pairwise DID for communicating with Party B and has done so without having to transmit any private key data.

Next, Party A prepares a Pairwise DID Exchange Response Message as shown below in Figure 5. This message is used to confirm that the Pairwise DID has been created in Party A's wallet and also to send Party A's new DID to Party B. The format of the Pairwise DID Exchange Response Message is shown below in Figure 5:

```
{
    "@type": "https://didcomm.org/didexchange/1.0/response",
    "@id": "12345678900987654321",
    "~thread": {
        "thid": "<The Thread ID is the Message ID (@id)
                of the first message in the thread>"
    },
    "connection": {
        "did": "A.did@B:A",
        "did_doc": {
            "@context": "https://w3id.org/did/v1"
            // DID Doc contents here.
        }
    }
}
```

Figure 5 – Pairwise DID Exchange Response Message

When Party B receives the Pairwise DID Exchange Response Message, it extracts Party A’s new DID information. With this new DID information from Party A, Party B can also call the Hyperledger Indy function, Pairwise.createPairwise(), which results in the new Pairwise DID being created within Party B’s wallet.

At this point, Party A and Party B have respectively each created a new DID (containing a public key), shared those new DIDs with each other, and finally created a new Pairwise DID in their respective wallets that will be used to secure future communications. The overall message flow is highlighted in Figure 6:

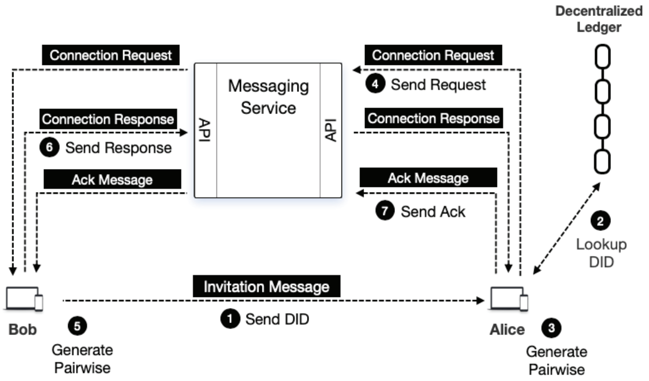


Figure 6 – Pairwise DID Message Flow

At the completion of the Pairwise DID exchange process, both parties can optionally exchange one or more acknowledgement messages to verify that the process has completed properly. To accomplish this, they load the public key corresponding to the recipient, encrypt the message, and transmit it to the recipient according to the routing data included in the DID Doc. To decrypt the message, the receiver selects their negotiated Pairwise DID from their wallet, loads their own corresponding private key, and decrypts the message. While the message hosting provider controls the message transmission, it does not have access to the decrypted message nor the key used to encrypt it. This process is shown in Figure 7:

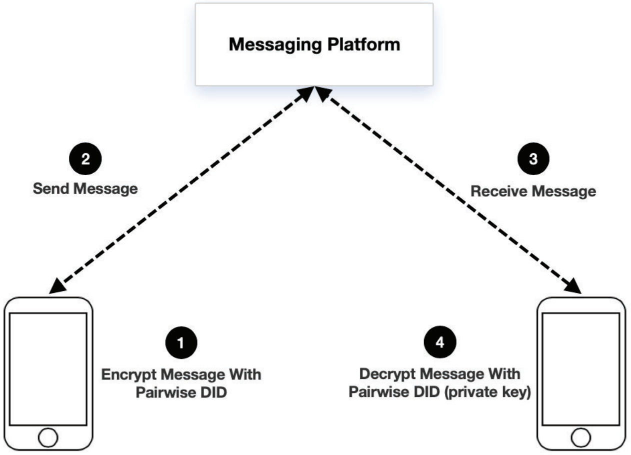

Messaging Platform
2
Send Message
3
Receive Message
1
Encrypt Message With Pairwise DID
4
Decrypt Message With Pairwise DID (private key)

Figure 7 – In-Network Secure Messaging

VII. Encrypted Messaging Between Walled Gardens

The current generation of encrypted messaging apps is operated by many separate messaging providers operating within standalone application ecosystems or *walled gardens*. Such systems include: Apple’s iMessage, Facebook’s WhatsApp, Whisper Systems’ Signal, and Anonyome Labs’ MySudo. These systems only enable E2EE messaging with users operating within the same E2EE ecosystem.

While contemporary E2EE systems provide a higher level of privacy than SMS messages, SSI-based messaging architectures can enable E2EE message exchange between users of *separate* messaging providers. The SSI-based message exchange components are based on the Hyperledger Aries messaging protocols. Messaging providers implementing Hyperledger’s open standards will enable their users to exchange DIDs [8], encrypt messages [9], and exchange messages [10] in a standardized format regardless of whether the senders and recipients are hosted within the same walled garden. A high-level view of this new process of exchanging messages between message hosting providers is shown in Figure 7:

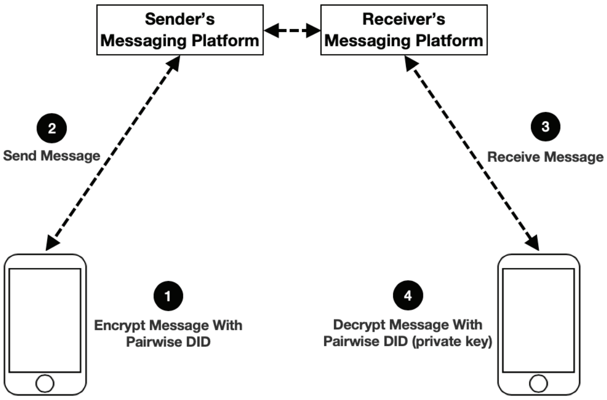

Sender's Messaging Platform
Receiver's Messaging Platform
2
Send Message
3
Receive Message
1
Encrypt Message With Pairwise DID
4
Decrypt Message With Pairwise DID (private key)

Figure 7 – Out-of-Network Secure Messaging

The process of exchanging messages between separate messaging providers is inherent in email and SMS messaging, however, it is notably absent in the current generation of over-the-top E2EE messaging providers. This is due, in part, to the lack of methods for discovering and communicating with remote messaging servers, but also in large measure due to the logistical complexity involved in distributed key management. The Hyperledger Aries protocols, Sovrin ledger, and W3C DID specifications enable the development of an open E2E encrypted messaging service and collectively facilitate the interoperability between compatible messaging providers.

Specific routing protocols are used to exchange messages between different messaging providers and is specified in the Hyperledger Aries protocols as described above. However, the key identifiers that make this possible are contained within the DID Document, itself. Figure 8 shows the key DID Document elements that enable a sender to identify a receiver's messaging endpoint:

```
{
    "@context": "https://www.w3.org/2019/did/v1",
    "id": "did:example:123456789abcdefghi",
    "authentication": [{
            // used to authenticate as did:...fghi
            "id": "did:example:123456789abcdefghi#keys-1",
            "type": "RsaVerificationKey2018",
            "controller": "did:example:123456789abcdefghi",
            "publicKeyPem": "-----BEGIN PUBLIC
                    KEY...END PUBLIC KEY-----\r\n"
    }],
    "service": [{
            // used to retrieve Verifiable Credentials associated
            // with the DID
            "id":"did:example:123456789abcdefghi#vcs",
            "type": "VerifiableCredentialService",
            "serviceEndpoint": "https://example.com/vc/"
    }]
}
```

Figure 8 – Minimal Self-Managed DID Document [11]

In the preceding figure, the DID Document contains an authentication element, which specifies the type of encryption that must be used when communicating with the owner's agent. This enables owners (or their service) to specify the required encryption algorithms and it is up to the sender to match the specified encryption requirements. The service element contains a *Service Endpoint* that specifies the network location where the receiver receives messages and where the sender should send its communications. In the preceding example, the value specified is an https service address. While the Service Endpoint can be described by any valid URI [12], it should be noted that https is the most ubiquitous URI and provides the greatest level of interoperability.

VIII. Compartmentalizing Online User Activity

Online privacy is greatly enhanced by using strong encryption, DID exchange methods, DID Communication protocols, etc. This enables messaging clients to convey messages securely and keep messaging contents limited to the intended recipient(s).

Today's internet users connect to online websites and services while performing a wide variety of activities that include work tasks, family activities, social group interactions, traveling, personal medical research, volunteering, etc. Personal contact points (e.g., email address, phone number, credit card number, etc.) have become the de facto identifiers that websites use to track users and correlate their activity across numerous websites. Ostensibly, this is done to enhance a user's online experience, provide predictive product advertising, etc. However, these correlations are not always limited to advertising and can present numerous privacy risks for unsuspecting users. As an example, if a user uses a single email address (which serves as a tracking identifier for data trackers) during all of their online activities, then data from all of their activities can be collected, correlated, analyzed, and sold for uses other than what the user intended or is aware. This puts user privacy at risk.

To combat this collection, correlation, analysis, and sales process, Anonyome Labs builds upon current privacy solutions (e.g., message encryption) and helps users compartmentalize their online activities. This is done by enabling users to create a new type of situational or activity-based digital identity called a Sudo. Sudo identities contain a unique email address, phone number, and may also generate virtual credit cards. Users may create separate Sudos for each of the online activities they perform. Using Sudos to compartmentalize online activities helps users segment their digital exhaust, which helps block tracking entities from collecting, buying, and selling a user's identity and personal activity data.

The Sudo concept fits naturally with the SSI concepts described in this paper. A user will have a primary verified identity (as a DID on the ledger) that typically will be used with government related SSI use cases e.g. driver's license, university qualifications, health care identifier and so on. The user can also use their Sudos with different SSI use cases that don't mandate use of the verified identity and where compartmentalization provides additional convenience and privacy. Some examples are a user having Shopping, Selling, Dating and Searching Sudos, each with different identifiers (phone numbers, email addresses, virtual credit cards, …) and each with unique SSI identities (as unique DIDs on the ledger).

IX. Interoperable End-to-End Messaging

As evolving threats to user privacy emerge, it is vital that messaging providers deliver new ways of increasing the security for user messages and their host messaging platforms. The platform described will provide secure E2EE messaging capabilities by incorporating self-sovereign identity methods, end-to-end encryption, authenticatable messages, and strong encryption algorithms. Messaging providers incorporating compatible industry standards will enable them to interoperate with many different messaging providers, help make E2EE communications the default online communication method, and break down the communication barriers inherent in contemporary messaging models.

References

[1] Campaign Monitor, "The Shocking Truth about How Many Emails Are Sent", May 2019, https://www.campaignmonitor.com/blog/email-marketing/2019/05/shocking-truth-about-how-many-emails-sent/.

[2] Domo, "Data Never Sleeps 5.0", https://www.domo.com/learn/data-never-sleeps-5, 2017.

[3] Leskin P., "The 21 scariest data breaches of 2018", Business Insider, https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12#2-marriott-starwood-hotels-500-million-20, 30 Dec 2018.

[4] Check Point Research, "FakesApp: A Vulnerability in WhatsApp", https://research.checkpoint.com/fakesapp-a-vulnerability-in-whatsapp/, 7 Aug 2018.

[5] Symantec, "Symantec Mobile Threat: Attackers Can Manipulate Your WhatsApp and Telegram Media Files", https://www.symantec.com/blogs/expert-perspectives/symantec-mobile-threat-defense-attackers-can-manipulate-your-whatsapp-and-telegram-media, 15 Jul 2019.

[6] Tobin et. al, "The Inevitable Rise of Self-Sovereign Identity", Sovrin Foundation, https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf, 28 March 2017.

[7] W3C, "Decentralized Identifiers (DIDs) v0.13", https://w3c-ccg.github.io/did-spec/, 13 Aug 2019.

[8] Hyperledger Foundation, "Aries RFC 0023: DID Exchange Protocol 1.0", https://github.com/hyperledger/aries-rfcs/tree/master/features/0023-did-exchange, 27 May 2019.

[9] Hyperledger Foundation, "Aries RFC 0019: Encryption Envelope", https://github.com/hyperledger/aries-rfcs/tree/master/features/0019-encryption-envelope, 4 May 2019.

[10] Hyperledger Foundation, "Aries RFC 0095: Basic Message Protocol 1.0", https://github.com/hyperledger/aries-rfcs/tree/master/features/0095-basic-message, 6 Aug 2019.

[11] W3C, "Decentralized Identifiers (DIDs) v0.13", https://w3c.github.io/did-core/, 13 Aug 2019.

[12] IETC, "Uniform Resource Identifier (URI): Generic Syntax, https://tools.ietf.org/html/rfc3986, January 2005.

Cellular Automata-based Puzzles for ASIC-resistant Proof of Work

Rade Vuckovac
School of Information and Communication Technology
Griffith University
Southport, QLD Australia
Rade.Vuckovac@griffithuni.edu.au

***Index Terms*—blockchain, proof of work, memory hard functions, reprogrammable functions**

I. Abstract

The terminology for Proof-of-Work (PoW) [1], [2] was introduced to generate a relatively computationally hard question, but the corresponding answer is computationally easy to verify. The first use of PoW was to prevent email spamming [1].

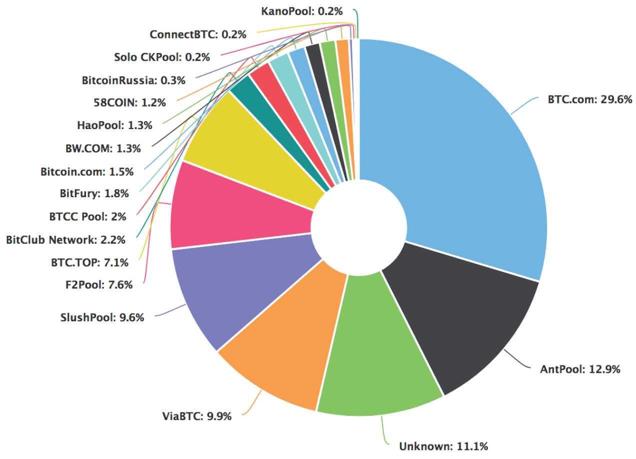


Fig. 1: The biggest Bitcoin Mining Pools [3].

Cryptographic hash functions are the foundation of a mathematical puzzle widely used by PoW consensus in a Blockchain network. For example, Bitcoin (best-known crypto-currency) uses a Hashcash [4] puzzle with the SHA256 as the hash function.

One consequence of using SHA256 is the creation of a non-egalitarian mining environment. With specialised hardware (Application-specific integrated circuit (ASIC)), SHA256 can be evaluated a hundred times faster than with classical CPUs. Thus, big investors can profit from mining. Figure 1 shows the possible segregation of the most prominent Bitcoin miners. A monopoly of the PoW and block creation could be a detrimental factors to the blockchain consensus idea. Hence, the interest for a ASIC-resistant PoW. There are some proposals aiming for this:

- Combined hashing algorithms; For example, X16RT developed by Raven Coin contains 16 different hash function where a decision which one is used for a particular PoW, is a coin flip.
- Memory-hard function; a system where evaluation cost is tied to memory cost. It is assumed that memory hardware cost is approximately the same within a couple of orders across various hardware implementations, including ASIC [5].

It should be noted that the hash functions are not developed with PoW in mind. They have three security properties:

1) **Pre-image resistance**: given a hash, it is difficult to find the message which will result in the given hash.
2) **Second pre-image resistance**: given a particular message, it is difficult to find another message with the same hash.
3) **Collision resistance**: It is challenging to find a pair of messages with the same hash.

While this is enough for designing PoW puzzles, those designs are not flexible enough for adding ASIC resistance.

We suggest that chaos theory might provide features for modelling egalitarian PoW puzzles. The two important properties of systems in chaos theory are:

1) The system's has sensitivity to its initial state or Butterfly Effect (much more popular term). This property indicates that inputs and outputs are not correlated. Even a minuscule change in the initial state will produce a different outcome. That property could be considered equivalent to the avalanche effect required and evident in hash functions [6]. Figure 2 illustrates this point.
2) Computational irreducibility (CI).

   > "*The principle of computational irreducibility says that the only way to determine the answer to a computationally irreducible question is to perform, or simulate, the computation*" [7].

   For example, The N-body problem is a well known mathematical problem. The case $N = 2$ has a closed-form solution meaning there is a set of equations defines bodies in motion, and positions for any desired time point. For $8 > N > 2$, we do not have a closed-form solution, instead there is a set of a complex equation which can only approximate body motions and positions for a given time. Today, only by step by step numerical simulation, $N > 8$ systems can be solved (CI).

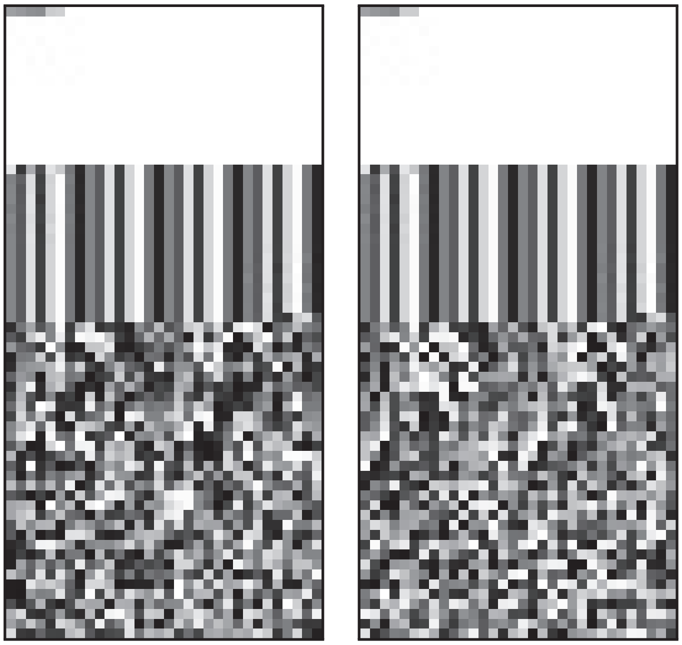


Fig. 2: Two cellular automata evolutions where initial state differs by just one bit.

A. The Proposal

To see chaos properties in action, we can sketch a PoW puzzle as follows. Instead of a hash function, we use a cellular automaton (CA).

Figure 2 shows two CA evolutions from the different initial states. The seeds (strings (a) bits01 and (b) bits02) are the first six top-left pixels (bytes). The sixth pixel on the right image is just one grey shade darker (not visible) than the corresponding pixel on the left. The seed consists of the initial state plus the white region on the top (the top 512 pixels of the image). Even very low entropy produces a complex outcome. It also shows elements of chaos behaviour, where a small initial change produces different outcomes.

With CA we have an initial state which is evolved by rules. The CA from Figure 2 uses the following rules for evolving a single cell:

- 1st step is to create a new state of carry c'.

$$c' = \begin{cases} c \oplus A_{i+1}, & \text{if } A_{i+2} > A_{i+3} \\ c \oplus \overline{A}_{i+1}, & \text{otherwise} \end{cases} \tag{1}$$

  where A is a cell, $\oplus$ is exclusive or and $\overline{A}$ is one complement of A.
- 2nd step is to update a cell A

$$A'_i = A_i \oplus c' \tag{2}$$

- 3rd step is to update current c' value for next cell transformation.

$$c' = c' + d \tag{3}$$

  where $d \neq 0$ is an arbitrarily chosen constant.

The initial state could mimic a Hashcash construct and have a header h (given part) and a part proving that work is performed r (h, and, r). The initial state h, and, r is evolved by applying n cycles (Figure 2 shows initial state and three evolution cycles). If the last row contains predefined pattern p (so many zeros for example), the work is completed. The difficulty to chose r, which will match p are the consequence of the butterfly effect and CI. A small change will modify the outcome drastically and to see what is the last row, an evaluation must repeat through all steps (such is the quickest way). It appears that only an exhaustive search for r will suffice.

B. Advantages

The advantages of the CA approach are:

- Simplicity (the CA's set of rules (Equations (1) (2) (3)) vs. several pages for the SHA256 description [8].
- Memory hardening; the CA can be used as a pseudo-number generator [9]. Then, the memory hardening scenario would be as follows: Initiate a required block of memory with pseudo-random numbers. Use that array a as a source for constant d (Eq 3). For each cell, the update d' is computed by $d' = a_i$ where $i = d \, mod$ size of array (d is the previous constant). Adding a certain memory requirement to the PoW could impact ASIC economy.
- The main advantage of the CA approach is a simple algorithm for modification without impacting the CA's properties:
  - Instead of $A_{i+2} > A_{i+3}$ use $A_{i+2} < A_{i+3}$ (Eq 1).
  - Instead of if $A_{i+2} > A_{i+3}$ use if $A_{i+2} \, mod \, 2 = 0$ (Eq 1).
  - ...

  Implementing the ever-changing algorithm with ASIC is economically prohibitive.

References

[1] Dwork, Cynthia and Naor, Moni, "Pricing via processing or combating junk mail," in Annual International Cryptology Conference, Springer, 1992, pp. 139–147.

[2] Jakobsson, Markus and Juels, Ari, "Proofs of work and bread pudding protocols," in Secure Information Networks, Springer, 1999, pp. 258–272.

[3] Tuwiner, Jordan, "Bitcoin Mining Pools," 2019, https://www.buybitcoinworldwide.com/mining/pools/

[4] Back, Adam and others, "Hashcash-a denial of service counter-measure," 2002.

[5] Percival, Colin, "Stronger key derivation via sequential memory-hard functions," BSDCan, 2009.

[6] H. Feistel, "Cryptography and computer privacy," Scientific American, 228(5), 1973 pp. 15–23.

[7] Israeli, Navot and Goldenfeld, Nigel, "Computational irreducibility and the predictability of complex physical systems," Physical review letters, 92(7):074105, 2004.

[8] "Descriptions of SHA-256, SHA-384, and SHA-512," http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf

[9] Zarezadeh, Zakarya, "Cellular automaton-based pseudorandom number generator," Complex Systems, volume 26, number 4, 2017.

A nonparametric method for measuring cybersecurity risk

Patrick H. O'Callaghan
Australian Institute of Business and Economics
University of Queensland
Brisbane, Australia
http://orcid.org/0000-0003-0606-5465

Abstract—Large-scale cyber attacks unfold dynamically, exploiting unknown (zero-day) vulnerabilities in the interdependencies between diverse entities [1]. The zero-day property of novel attacks means that the associated risks of an attack is inherently difficult to measure. And yet defenders of cyber systems must still evaluate the likelihood of each type attack and then use this information to decide how resources should be deployed and which activities should be curtailed. Moreover, given the dynamic nature of attacks, they need to ensure that their model extends into novel territory without the need for major revisions or knee-jerk reactions that would otherwise be exploited by the attacker. We present a method for evaluating the likelihood of future events that addresses precisely these concerns. It is nonparametric and based on the principle of resampling. It uses only ordinal rankings, making it robust to specification errors. It provides a framework for testing higher-dimensional extensions of the existing model. Finally, via [3] it is furnished with a rigorous axiomatic foundation.

Index Terms—Cybersecurity; risk management; distributed systems; empirical likelihood; coherent risk measures; case-based decision making

I. Introduction

The exponential growth of connections between diverse cyber and physical entities is a testament to the value they add to the 21st century economy. Yet each new interdependency opens a new door through which novel cyber attacks have the potential to be launched. Those who defend against cyber attacks (henceforth defenders) face the problem of evaluating risks that are hard to measure.

Armed with theory and past experiences, defenders need to evaluate the likelihood of different attacks, and on this basis, make decisions regarding which activities or interdependencies to rule out and where to allocate resources. The key obstacle they face is that the next attack will exploit a novel (zero-day) vulnerability. By definition, attacks on novel vulnerabilities, lie beyond the defenders' knowledge and past experiences: for otherwise, they would not be novel. But how can one specify the probability of an event one cannot describe? This suggests that problem is inherently non-Bayesian in the sense that the defender knows her model of the future is incomplete.

In this paper, we describe a general method for estimating the likelihood of attacks on the basis of past observations and ordinal rankings of future events. A central feature of the method is that the resulting beliefs are consistent with the future arrival of attacks that are novel: even though the latter clearly cannot presently be described. This consistency has the benefit of ensuring that, when the time comes, the defender's model can be extended without major revision and without knee-jerk reactions to unfolding events. The importance of this form of dynamic consistency is supported by the fact that attackers plan their actions to exploit the defender's confusion in "the fog of war".

The method we describe is well-suited to machine learning and builds on resampling principles that underlie the common nonparametric bootstrap. It is also supported by an axiomatic foundation that is derived in [3] as an extension of [4].

II. The method

Let $D^\star$ denote the current set of past cases that are accessible to the defender. Each case $c \in D^\star$ is a full description of a past case: the type of the attack (e.g. Distributed Denial of Service, multistage, etc.); the source of the attack; the network vulnerability that was exploited; details of the entities that were compromised; the cost; and so on. Let $\mathcal{D}$ denote the set of (finite) samples that can be generated from $D^\star$. So, for example if $D^\star = \{c_1, \dots, c_n\}$, then $C = \{c_1, \dots, c_{n-1}\}$ belongs to $\mathcal{D}$, but so does $D = \{d_1, \dots, d_{n+1}\}$, where each d_i is a copy of c_1, the latter having been drawn with replacement from $D^\star$ on every single occasion.[1] Two cases are identical if each contributes the same marginal information to any sample to which neither belongs.

Their goal is to accommodate the generation of value whilst preventing some, but certainly not all, risks. Choosing which risks to allow and which to rule out is fraught with difficulty, and for this reason we adopt rules of thumb such as "Don't put all your eggs in one basket." As is often the case with sensible principles, we can formalise them mathematically. And, in this case, via the notion of a coherent risk measure.

This paper is a first attempt at translating the concept of coherent risk measurement, which is well-established

[1] The exact bootstrap [5] proceeds along these lines, but is limited to samples of cardinality n.

in the field of financial risk management, to the setting of cybersecurity. This translation is subtle due to the many differences between risks in finance and risks in cybersecurity. Not only in terms of the nature of the risks themselves, but also in terms of limitations on our ability to observe the interdependencies between the respective network entities.

III. Coherent risk measures

The basic role of a risk measure (or metric) is to provide a ranking of the relevant risks. Conventionally, high risks rank higher than those with a low risk. This (weak) ordering allows decision makers to make informed choices and provides the necessary objectivity that is needed to explain their decisions to and outsiders (such as regulators or managers). In some cases, as in financial markets, decision makers are required, by those in authority, to ensure their actions satisfy constraints that are imposed on a given measure of risk.

In other cases, those in authority can infer from the actions taken by those

IV. Application to cybersecurity

The fact that movements in prices (of financial assets) are publicly available ensures that we can generate reasonably accurate estimates of the likelihood of future events. In contrast, One obstacle to such a translation is that, in finance the fundamental notion is an asset and its interdependency with another is typically measured in terms of a correlation. are

In [2], a coherent risk measure is a rule of

Preserving the security of information held by entities in a network is a central objective for 21st century cybersecurity.

Designers of distributed ledgers choose an optimal point on the locus between efficiency and robustness and build this into their protocol. The protocol that minimises costs associated with validating transactions (by having a single authoriser) fails to be robust to attacks. Permissioned blockchains may be safe, but the collusion involved in excluding potential may carry social costs.

Acknowledgment

The author thanks John Mangan and Raja Jurdak for their encouragement at the early stages of this project.

References

Please number citations consecutively within brackets [1].

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors' names; do not use "et al.". Papers that have not been published, even if they have been submitted for publication, should be cited as "unpublished" [2].

References

[1] A. R. Hota, A. A. Clements, S. Bagchi, S. Sundaram, "A Game-Theoretic Framework for Securing Interdependent Assets in Networks," Game Theory for Security and Risk Management, 157-184, 2018

[2] P. Artzner, F. Delbaen, J.-M. Eber, and D. Heath, "Coherent measures of risk," Mathematical finance, vol. 9.3, pp. 203–228, 1999

[3] P. H. O'Callaghan, "Prudent case-based prediction ," https://arxiv.org/abs/1904.02934

[4] I. Gilboa and D. Schmeidler, "Inductive inference: an axiomatic approach," Econometrica, vol. 71(1), pp. 1–26, January 2003

[5] J. Kisielinska, "The exact bootstrap method shown on the example of the mean variance estimation," Comput Stat, vol. 28, pp. 1061–1077, 2013

Unlocking additional value through smart market trading in water quality and treated wastewater using Blockchain technology

Anik Bhaduri, Vallipuram Muthukkumarasamy, James C.R. Smart, Joe McMohan, Kamanashis Biswas, Aditya Kaushik and Rob Braunack

Introduction: As expanding populations and a changing climate place increasing stress on scarce resources in aquatic and marine environments, new opportunities to unlock additional value from improved management of water quality could be a game-changer (Flörke et al. 2018, Sgori et al. 2018).

It is well recognised that water quality credit markets could increase economic efficiency significantly by allowing pollutant-emitting point-source utilities and developers to buy water quality offsets from land remediation or improved land management practices at non-point source locations further upstream in relevant catchments.

Although some progress has been made, the full range of benefits has been slow to materialise, partly because of uncertainties regarding the security of the environmental improvements that generate the non-point source offsets and the high transaction costs incurred by detailed regulatory approvals.

Moreover, credit supply (e.g., nitrogen credits) can be highly heterogeneous in relevant water quality characteristics (e.g., nitrogen type and environmental impact, timing and location of delivery), thus creating information asymmetry in water quality trading resulting in suboptimal market transactions (i.e. buyers and regulators are unsure of the quality and reliability of the offsets purchased) (Smart 2016). Similar problems of information asymmetry also surround treated wastewater which leads to a widening gap between production and consumption of this increasingly valuable resource.

In this context, the relevant policy issue is how can we overcome information asymmetry, moderate the impact of intrinsic uncertainty, and reap the full benefits of water quality trading?

Blockchain-Based System: Blockchain technology can facilitate transactions in a water market, replace intermediaries, modernise the regulatory processes, and act as an accounting, auditing, interlinking and trading platform that enables emerging water quality markets to function effectively.

The inherent properties of Blockchain such as a distributed shared ledger, a consensus mechanism, smart contracts, tokenisation and asset tracking have the potential to provide a future-proof integrated platform in such markets.

The application of Blockchain is growing in the water sector (Lin et al. 2018) and has been shown to reduce transaction cost and increase market participation (Pee at al. 2018, Poberezhna 2018). Currently, water-related Blockchain implementations are mainly confined to markets such as irrigation water where the quality of the traded product is not a concern. Consequently, Blockchain's potential to address information asymmetry and mitigate the adverse impacts of uncertainty in water-related markets where there is substantial variation in the quality of the traded product remains largely unutilised. Effective and efficient Blockchain-enabled trading markets would help to secure sustainable water supply and water-borne waste management for urban areas into the future.

Using a structure for the smart contract-driven blockchain platform, the paper explores the research and policy opportunity in eliminating the market distortions in water quality trading. It uses two case studies of potential water quality trading markets in South East Queensland (SEQ), Australia (water quality trading) and Bengaluru, India (treated wastewater).

Proposed Model: The diagram below illustrates the proposed smart contract-driven blockchain platform for water quality trading.

In this model, the Market Regulator works as a checkpoint for the whole system and is responsible for policy enforcement, validation and monitoring of all activities in the Blockchain network. The access control and policy enforcement are written in the form of smart contracts which would be triggered when certain conditions are met. The Market Regulator is also connected to the AI

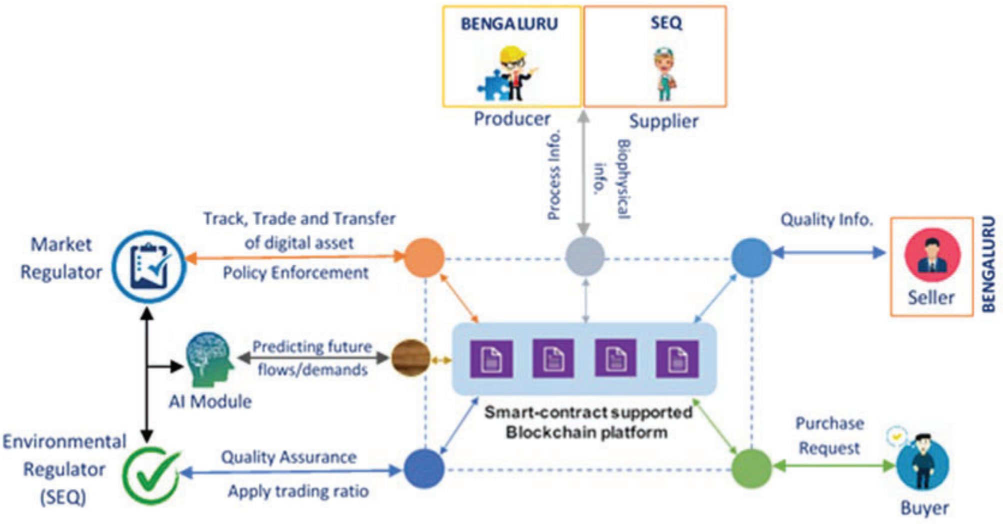


Figure 1: Smart contract-driven blockchain platform for trading in Water Quality and Treated Waste Water

module which implements machine learning algorithms on off-chain data to analyse user behaviours and predict future flows of treated wastewater consumption (for the Bengaluru case) or future demand for nitrogen credits (for the SEQ case). In addition, the AI module will also provide critical information from the system that would better characterise the relationship between demand and supply during peak and off-peak times or seasons.

The treated wastewater producer (for Bengaluru) and the nitrogen offset supplier (SEQ) record the critical steps involved in the wastewater treatment process and the location of on-ground actions that generate the nitrogen credits, respectively, in the chain. For Bengaluru, the seller inputs quality information in the chain obtained through IoT devices. For SEQ, the environmental regulator inputs nitrogen load monitoring data from a water sensor network and compliance data from random verification spot checks of suppliers' on-ground changes to land management practice and land use. For Bengaluru, the smart contract invoked by the market regulator would verify whether the quality of the traded product is up to the mark. For SEQ, the smart contract would carry embedded trading ratios that reflect the offsetting capability of the nitrogen credit for credit buyers at specific locations downstream. These trading ratios would also reflect the intrinsic uncertainty surrounding offsetting ability. Trading ratios would be informed by nitrogen and catchment modelling, data from the water sensor network and prior performance of the specific credit supplier under verification spot-checks. Based on the outcomes, in Bengaluru, the seller will either be rewarded for providing correct information or penalised for providing false information; in SEQ the credit supplier will be rewarded for providing verifiable evidence of practice change and for undertaking the on-ground maintenance required to secure long-term delivery of credits from land-use change.

Three main research questions that follow from the above are, how can a Blockchain-enabled Water Quality Trading Program (WQTP) be used to:

1. Provide an incentive-compatible design mechanism that will reduce information asymmetry.

2. Incorporate a built-in algorithm that will help agents – and where relevant the environmental regulator – to facilitate trading under inherent uncertainties surrounding hydrological and biogeochemical processes in rivers and coastal waters.

3. Integrate an AI/ ML module to enable predictive analysis of the agent's behaviours.

Summary: Block-chain technology can address the heterogeneity in a water quality market, particularly information asymmetry; and ensure robust operation that can reduce current and increasing future cost liabilities arising from deteriorating water quality.

References

Florke, M., C. Schneider, and R.I. McDonald, *Water competition between cities and agriculture driven by climate change and urban growth*. Nature Sustainability, 2018. **1**(1): p. 51-58.

Sgroi, Massimiliano, Federico GA Vagliasindi, and Paolo Roccaro. "Feasibility, sustainability and circular economy concepts in water reuse." *Current Opinion in Environmental Science & Health* 2 (2018): 20-25.

Lin, Y.P., et al., *Blockchain with artificial intelligence to efficiently manage water use under climate change.* Environments, 2018. **5**(3): p. 34.

Poberezhna, A., *Addressing water sustainability with blockchain technology and green finance*, in *Transforming climate finance and green investment with blockchains*, A. Marke, Editor. 2018, Academic Press. p. 189-196.

Smart, J.C.R., et al., *A tradable permit scheme for cost-effective reduction of nitrogen runoff in the sugarcane catchments of the Great Barrier Reef*, in *Report to the National Environmental Science Programme*. 2016, Reef and Rainforest Research Centre Limited: Cairns. p. 75pp.

A Novel Smart Contract Pattern for Blockchain-Based IoT Management

Ralph Deters
Department of Computer Science
University of Saskatchewan
Saskatoon, Canada
deters@cs.usask.ca

***Abstract*—** Facing unprecedented environmental challenges, there is an urgent need for smart solutions that help us reduce our environmental footprint. The rapidly growing Internet of Things (IoT) that enables us to connect the physical and digital world is arguably one of our best technologies to help us achieve this goal. IoT enables devices and services to interact with one another, resulting in short-lived and frequently changing casual interactions. To manage these interactions Capability-Based Access Control (Cap-BAC) that is based on the use of transferable, unforgeable token of authority has emerged as the defacto standard. While Cap-BAC for IoT can be implemented in a variety of ways, the use of Smart Contracts seems to be the most promising due to scalability, security and transparency of the underlying blockchain technology. However, invoking Smart Contracts and transferring tokens leads to serious latency issues within dynamic IoT systems. This paper introduces a novel Smart Contract design pattern for IoT management that is based on the separation of access control and coordination. By establishing a separate coordination layer, that uses a control-driven/process-oriented model it becomes possible to reduce the volume and frequency of interactions between IoT devices/services and Smart Contracts.

Keywords*— *IoT Coordination, blockchain, Smart Contract

I. Coordination and Access Control

Within distributed systems, coordination is concerned with making interactions useful while access control is concerned with making interactions safe. Despite addressing different aspects of interactions, they are related and in many ways complement each other. Both coordination and access control, are defined by policies that can be enforced in a variety of ways. However, within IoT, access control, most notably Cap-BAC [1,2], dominates research and coordination is still an emerging area. Ignoring coordination and relying solely on the use of token-based access control in the form of Smart Contracts leads to very large transaction volumes that tend to overwhelm current blockchain platforms. This, in turn, has given rise to the use of complex IoT proxy patterns e.g. use of edge nodes, sub-chains, side-chains, interconnected blockchains, etc.

This paper argues that coordination and access control are similar but different issues that need to be addressed in different logical layers. Instead of having Smart Contracts handle both issues, there needs to be a specialization of Smart Contracts. By defining a coordination layer that interacts with the access control layer it becomes possible to significantly reduce the need of IoT defines to interact with the Smart contracts and thus reduce latency.

II. Coordination Models

The IoT paradigm [3,4] enables devices and services to interact with one another, resulting in short-lived and frequently changing casual interactions. It is often assumed that devices and services “discover” each other. To manage if and how devices and services interact, access control is used. Given the size and complexity of IoT systems, it is not surprising that IT companies like IBM [5] identified blockchain technology and Smart Contracts as the most suitable platform for distributed management of IoT devices, resources and services. There is no shortage of research publications demonstrating the feasibility and advantages of using Cap-BAC within small-scale IoT feasibility studies. Cap-BAC is based on the use of transferable, unforgeable token of authority and supports capability delegation, capability revocation and custom definition of capabilities. While Cap-BAC for IoT can be implemented in a variety of ways, the use of Smart Contracts seems to be the most promising due to scalability, security and transparency of the underlying blockchain technology. However, as soon as the IoT systems are scaled-up and resource-constrained IoT

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

devices are deployed, serious performance issues emerge. The larger number of IoT devices and services result in a significantly larger number of access validation requests to the Smart Contracts that overwhelm the underlying blockchain platforms.

To minimize the interactions with the blockchain this paper proposes the use of a control-driven/process-oriented coordination layer. Process-oriented coordination models like IWIM [6] differ from the more common data-driven models like Linda [7] in that there is a complete separation of coordination and computation. In a data-driven model, the IoT device/service uses a shared storage e.g. blockchain to coordinate their actions. In a process-oriented model, the IoT devices/services are coordinated most often by the use of coordinator components that configuring the device/service with respect to interactions e.g. where to send the results. The coordinator is informed about state changes of devices/services via events that in turn can result in the reconfiguration of the services/services it manages.

Within the process-oriented model, the coordination of IoT devices/services is primarily a configuration update that is triggered by events from the devices/services or the access control. Please note that, that coordinators can be implemented in a variety of was, for example as Smart Contracts.

III. Coordination Updates

Given the heterogeneity of IoT devices, it is fairly common to use a device/service abstraction layer. Within this layer, the various components of the IoT system (e.g. device/service, coordinator and Smart Contract) are typically exposed as RESTful web services. While this layer enables a fairly straightforward interaction of the IoT components the question of how to coordinate the components remains. Since we use Smart Contracts as coordinators for predefined sets of IoT devices/services, it is up to the IoT device/service to ensure that it has the most recent coordination update. Sending a device/service notification to the abstraction layer ensures that the device/service is aware of a change in the coordination configuration. Upon receiving the notification the device/service contacts its coordinator Smart Contract to request the update. Using this 2-step approach makes it harder for an attacker to re-configure a device/service since she/he needs to control the Smart Contract e.g. obtain the private key associated with the account.

At the moment we consider three cases in which a coordination update is issued:

a) Due to event/events emitted by IoT device/service
b) Due to the access control layer (e.g. changes in access privileges)
c) Due to the owner of the service/device (e.g. need to reconfigure)

The crucial aspect of this Smart Contract pattern is the pushing of coordination updates. Instead of pulling information regarding access to a device/service from a Smart Contract a configuration is sent to the component and used as a cache. This obviously reduces significantly the traffic if we assume that changes to the coordination configuration are infrequent. If however, access control settings and coordination are continuously changed, there is no reduction in traffic. However, in our experience, we haven't encountered a situation in which frequent changes to access and coordination policies were observed.

IV. Evaluation

To evaluate our approach we used our collaboration within the P2IRC project (https://p2irc.usask.ca/index.php). This project focuses on plant phenotype research and involves image capturing, processing and very large data resource repositories. To support distributed management of the resources within the project we deployed a Smart Contract access control solution. Adding the above-described coordination layer allowed us to overcome the serious performance penalties that resulted from the slow transaction processing speeds of the permission-based blockchain.

V. Evaluation

This paper presents a novel Smart Contract design pattern for blockchain-based IoT management. By recognizing the difference of coordination and access control and developing coordination Smart Contracts it becomes possible to significantly improve the performance of the IoT system and to simplify the development of the Smart Contracts.

References

[1] Rotondi, Domenico, and Salvatore Piccione. "Managing access control for things: A capability based approach." In *Proceedings of the 7th International Conference on Body Area Networks*, pp. 263-268. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012.

[2] Levy, Henry M. *Capability-based computer systems*. Digital Press, 2014.

[3] Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future generation computer systems* 29, no. 7 (2013): 1645-1660.

[4] Porkodi, R., and V. Bhuvaneswari. "The Internet of Things (IoT) applications and communication enabling technology standards: An overview." In *2014 International Conference on Intelligent Computing Applications*, pp. 324-329. IEEE, 2014.

[5] IBM Empowering the Edge: Practical insights on a decentralized Internet of Things https://www.ibm.com/downloads/cas/2NZLY7XJ

[6] Arbab, Farhad. "The IWIM model for coordination of concurrent activities." In *International Conference on Coordination Languages and Models*, pp. 34-56. Springer, Berlin, Heidelberg, 1996.

[7] Ahuja, Sudhir, Nicholas Carriero, and David Gelernter. "Linda and friends." *Computer* 8 (1986): 26-34.

Digital Twins and Distributed Ledger Technology: What can they learn from each other?

Valeri Natanelov
QUT Design Lab & Food Agility CRC
Queensland University of Technology
Brisbane, Australia
valeri.natanelov@qut.edu.au

Gerd Wagner
Dept. of Informatics
Brandenburg University of Technology
Cottbus, Germany
wagnerg@b-tu.de

Marcus Foth
QUT Design Lab & Food Agility CRC
Queensland University of Technology
Brisbane, Australia
m.foth@qut.edu.au

Keywords — Digital Twin, Blockchain, Distributed Ledger Technology, Supply Chain Management, Smart Cities

I. Introduction

In recent times, two technology innovations have received significant attention not only from academia but also from industry and government: *Digital Twins* (DT) and *Distributed Ledger Technology* (DLT). However, it appears that the literature is predominantly focusing on either one of these new pieces of technology in depth, and there is hardly any critique or review that creates lateral connections and links between the two. This paper starts to close this gap by asking, what can DT and DLT learn from each other?

In the following, we first set the scene by introducing the context for our analysis: supply chain management (II). We then explain the role that DLT play in supply chain management (III) before we turn our attention to DTs (IV). We conclude by examining challenges with each technology and exploring opportunities for synergies and learnings (V).

II. Supply Chain Management

Supply Chain Management (SCM) is undergoing rapid changes due to increasing digitalisation, including IoT and sensor-based data collection throughout the entire supply chain as a basis for tracking and tracing functions [1]. Consequently, data processing and management is established through cloud technology [2]. The aggregated data or big data can be mined through Artificial Intelligence (AI) and in doing so creating further added value [3]. More recently, blockchain and distributed ledger technology (DLT) introduced further possibilities for value addition in the supply chains through increased in-chain efficiencies [4] complemented by potential consumer surplus value of product traceability [5]–[7]. In addition, DLT for supply chain management extends visibility and transparency, digitalisation and disintermediation, improved data security and smart contracts for integrated business logic [8].

III. Distributed Ledger Technology in SCM

A. Distributed Ledger, Blockchain and Smart Contracts

DLT refers to a decentralised-distributed system of nodes or computing devices [9]. A distributed ledger is a database that is spread over multiple nodes, where each node replicates and maintains an identical copy independently. The main innovation of DLT is the lack of a central authority, i.e. decentralisation. Distributed ledgers provide an auditable history of transaction information visible to all participants of the system. For a more comprehensive overview of the technology, we refer to existing literature [9], [10].

Blockchains can be considered as a subset of DLT. A blockchain is a type of DLT with a specific protocol. In contrast to general distributed ledgers, blockchains package transactions into a block which are linked through cryptographic hashes [9]. In other words, a blockchain is a decentralised ledger that organises data in blocks and updates entries through an append-only structure. The blockchain achieves immutability on top of the prerequisite verifiability and decentralisation characteristics of DLT.

Smart contracts are independent programs that are designed on a blockchain network, such as Ethereum, that contain certain business logic translated into code. Smart contracts are capable of facilitating, automating and enforcing agreements i.e. contracts [11], and are built on blockchain characteristics of verifiability and immutability.

B. IoT

The introduction of IoT into a blockchain enabled supply chain system represents a bridge between the physical and digital world and comes with its own set of challenges [12]. Since the IoT generated data is used as input for smart contracts conditionality, it has to conform to data integrity for maintaining the valuable blockchain characteristics. This requires an additional data verification layer that can be achieved through a private DLT of known participants, verifying data integrity through a consensus mechanism. Figure 1 presents a conceptual overview of a potential data flow in such a system.

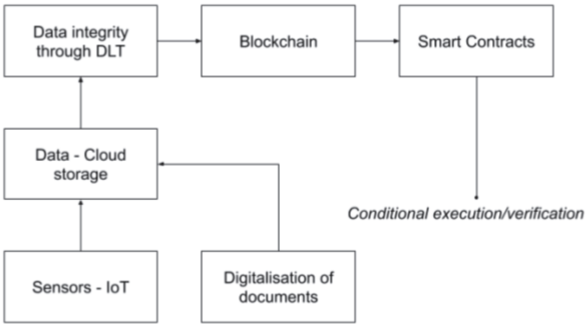

Data integrity through DLT
Blockchain
Smart Contracts
Data - Cloud storage
Conditional execution/verification
Sensors - IoT
Digitalisation of documents

Fig. 1. Data flow conceptualisation

C. Integrated system – the case of BeefLedger

BeefLedger (beefledger.io) is a blockchain smart contract project for providing a secure and immutable record of Australian beef export [13]. The aim of the project is to tackle the problem of food fraud and improve efficiency throughout the supply chain including reduced risk of payments through blockchain enabled Letters of Credit (LOC) and integrated insurance solutions. The project entails multiple layers:

- The physical supply chain with multiple supply chain participants, flow of goods, and flow of capital.

- IoT hardware and software consisting of: cattle weighing devices; smart ear tags; In-Vehicle Monitoring Systems (IVMS); Radio-frequency identification (RFID); Temperature and Relative Humidity (RH) sensors.
- Data processing and management complemented by technology agnostic standards.
- Blockchain and smart contracts for efficient transacting between supply chain participants and credentialed provenance for the end consumer.

BeefLedger presents a holistic example of an advanced digitalised supply chain. The value add is multifaceted, and comprises blockchain certifiability of certain product attributes (e.g. origin / provenance); and efficiency gains in the supply chain, such as smoother capital flows and reduced interest rates; reduced insurance premiums; efficient regulatory compliance; reduced cost of production.

IV. Digital Twins

DT refers to a comprehensive always up-to-date digital representation or replica of an object or system using real-time data for the purpose of visualising current states and simulating future states [14], [15]. Recently, the DT approach has started to receive significant attention in smart city research and practice as more sophisticated 3D modelling, big data analysis, and visualisation and simulation techniques converge [16].

While offering exciting new possibilities for analysis from the helicopter or bird's eye view, DTs and the associated discipline of urban science have been criticised for being overly technocratic and positivist [17], [18] and lacking care and consideration for privacy and surveillance concerns [19], [20].

V. Synergies and Learnings

There are synergies in the way a SCM project such as BeefLedger could benefit from the addition of a DT layer. This could enable: (i) virtual preparation and planning for future economic (and regulatory) scenarios; (ii) learning and adoption by supply chain participants to familiarise with and master the complexity of the system, and; (iii) consumer interaction with DTs for optimal information (re)presentation.

In turn, the current issues and shortcomings of DTs could be ameliorated or resolved with a hybrid approach that combines and integrates the benefits of using DLT, ie. considerations of trust, governance, and *privacy-by-design*. A new and arguably more ethical approach – which could be operationalised in parts through DLT – has been coined *technological sovereignty* [21], [22]. While the premise that data represents potential for value-add and monetisation is widely accepted and acted upon in the SCM space, this issue is still contested in the smart cities space – largely due to a lack of nuanced data governance balancing the needs of citizens at street level with the needs of cities from the bird's eye view. Economic actors across supply chains employ legal, regulatory, and contractual arrangements and frameworks to protect their interests in data ownership and monetisation. This requires a system that affords privacy preservation and confidentiality requirements that can be applied to different actors and data types. Studying the use of DLT and smart contracts in SCM offers new learnings that can be applied to bring about technological sovereignty to the context of data governance in digital twins and smart cities [23].

Acknowledgment

This project was supported by funding from Food Agility CRC Ltd, funded under the Commonwealth Government CRC Program. The CRC Program supports industry-led collaborations between industry, researchers and the community.

References

[1] L. D. Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," *IEEE Trans. Ind. Inform.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[2] L. Jiang, L. D. Xu, H. Cai, Z. Jiang, F. Bu, and B. Xu, "An IoT-Oriented Data Storage Framework in Cloud Computing Platform," *IEEE Trans. Ind. Inform.*, vol. 10, no. 2, pp. 1443–1451, May 2014.

[3] D. E. O'Leary, "Artificial Intelligence and Big Data," *IEEE Intell. Syst.*, vol. 28, no. 2, pp. 96–99, Mar. 2013.

[4] S. Rahmadika, B. J. Kweka, C. N. Z. Latt, and K. Rhee, "A Preliminary Approach of Blockchain Technology in Supply Chain System," in *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, 2018, pp. 156–160.

[5] A. Arora and M. Arora, "Digital-Information Tracking Framework Using Blockchain," *J. Supply Chain Manag. Syst.*, vol. 7, no. 2, pp. 1–7, 2018.

[6] S. E. Chang, Y.-C. Chen, and M.-F. Lu, "Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process," *Technol. Forecast. Soc. Change*, vol. 144, pp. 1–11, Jul. 2019.

[7] J. Chang, M. N. Katehakis, B. Melamed, and J. (Junmin) Shi, "Blockchain Design for Supply Chain Management," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3295440, Dec. 2018.

[8] Y. Wang, J. H. Han, and P. Beynon-Davies, "Understanding blockchain technology for future supply chains: a systematic literature review and research agenda," *Supply Chain Manag.*, vol. 24, no. 1, pp. 62–84, Jan. 2019.

[9] I. Bashir, *Mastering blockchain: Distributed ledger technology, decentralization, and smart contracts explained*. Packt Publishing Ltd, 2018.

[10] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016.

[11] V. Mehta and S. More, "Smart Contracts: Automated Stipulations on Blockchain," in *2018 International Conference on Computer Communication and Informatics, ICCCI 2018*, 2018.

[12] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Bus. Horiz.*, vol. 58, no. 4, pp. 431–440, Jul. 2015.

[13] M. Foth, "The Promise of Blockchain Technology for Interaction Design," in *Proceedings of the 29th Australian Conference on Computer-Human Interaction*, New York, NY, USA, 2017, pp. 513–517.

[14] S. Boschert and R. Rosen, "Digital Twin—The Simulation Aspect," in *Mechatronic Futures: Challenges and Solutions for Mechatronic Systems and their Designers*, P. Hehenberger and D. Bradley, Eds. Cham: Springer International Publishing, 2016, pp. 59–74.

[15] J. A. Marmolejo-Saucedo, M. Hurtado-Hernandez, and R. Suarez-Valdes, "Digital Twins in Supply Chain Management: A Brief Literature Review," Springer, Cham, 2020, pp. 653–661.

[16] M. Batty, "Digital twins," *Environ. Plan. B Urban Anal. City Sci.*, vol. 45, no. 5, pp. 817–820, Sep. 2018.

[17] R. Kitchin, T. P. Lauriault, and G. McArdle, "Knowing and governing cities through urban indicators, city benchmarking and real-time dashboards," *Reg. Stud. Reg. Sci.*, vol. 2, no. 1, pp. 6–28, Jan. 2015.

[18] M. Foth, N. Odendaal, and G. N. Hearn, "The View from Everywhere: Towards an Epistemology for Urbanites," presented at the 4th International Conference on Intellectual Capital, Knowledge Management and Organisational Learning (ICICKM), Cape Town, South Africa, 2007, pp. 127–133.

[19] L. van Zoonen, "Privacy concerns in smart cities," *Gov. Inf. Q.*, vol. 33, no. 3, pp. 472–480, Jul. 2016.

[20] S. Elwood and A. Leszczynski, "Privacy, reconsidered: New representations, data practices, and the geoweb," *Geoforum*, vol. 42, no. 1, pp. 6–15, Jan. 2011.

[21] C. R. Lynch, “Contesting Digital Futures: Urban Politics, Alternative Economies, and the Movement for Technological Sovereignty in Barcelona,” *Antipode*, vol. n/a, no. n/a, 2019.

[22] H. March and R. Ribera-Fumaz, “Barcelona: From corporate smart city to technological sovereignty,” in *Inside Smart Cities*, Routledge, 2018, pp. 227–242.

[23] J. Potts, E. Rennie, and J. Goldenfein, “Blockchains and the crypto city,” *It - Inf. Technol.*, vol. 59, no. 6, pp. 285–293, 2017.

BEHAVIOURAL ANALYSIS OF CRYPTOCURRENCIES INVESTORS

Hai Yen TRAN
Accounitng, Finance and Economics
Griffith University
Brisbane, Australia
haiyen.trh@gmail.com

Tracey WEST
Accounitng, Finance and Economics
Griffith University
Brisbane, Australia
T.West@griffith.edu.au

Victor S.H. WONG
Accounitng, Finance and Economics
Griffith University
Brisbane, Australia
V.Wong@griffith.edu.au

***Abstract*— This study investigates the behavioural of cryptocurrencies investors using Vector Autoregression (VAR) technique, along with Granger Causality and Impulse Response Function.**

We question if the recent volatility and trading activities behaviours of cryptocurrencies share the familiar momentum of Dotcom Bubble 1980 whereat tech-based gained market overconfidence, which consequently, yielded spurious share prices of these firms and their products. Motivated by overconfidence-theories to understand the 2017 crypto-phenomena, this thesis investigates the lead-lag relationship between turnover and return of cryptocurrencies market, in general and three largest market cap coins including Bitcoin, Ethereum and Ripple, in particular.

The findings show that cryptocurrencies market activity suggest the overconfidence's explanatory power is significant statistically, but subtle economically, during its tremendous volatility last year. In particular, statistically speaking, the research finds the presence of overconfidence bias in Bitcoin and Ripple investment as well as in crypto-market at a whole while Ethereum individuals trade for disposition effects. We also perceive that, Bitcoin, Ethereum and Ripples are different in fundamental drivers and investment intentions, which justify for particular economical insignificances when performing joint interpretations.

***Keywords*— Cryptocurrencies, Behavioural, Investments**

I. INTRODUCTION

While traditional theories and principles in finance emphasise modern portfolio theory (MPT) and the efficient-market hypothesis (EMH), the emergence of the behavioural finance field investigates the cognitive factors and emotional issues impacting the decision-making processes pertaining to the systematic investment errors made by investors (Asad, Khan, and Faiz, 2018). In the same vein, Shefrin (2007) defines that bias is nothing else but the "predisposition towards error". Stated alternatively, a bias is a prejudice or a propensity to make decisions while already being influenced by an underlying belief. In financial decision making, a study by Bateman and Schwenk (1986) indicated that investors inaccurately interpret information and fail to comprehensively search for information due to their limited cognitive capacities, resulting in cognitive biases. To date, research has just covered the influence of these cognitive biases in traditional markets such as in real estate market (Salzman and Zwinkels, 2013), in corporate bond market (Wei, 2017) and largely in the stock market.

A working paper by Obryan (2018) provides the initial groundwork on crypto-market participants' irrationalities through investigation into the herding bias. However, among cognitive biases, overconfidence is one of the most-studied biases since it is linked to other biases and, notably, it includes the exogenous and endogenous dimensions of risk perception (Fabre and François-Heude, 2009). Studies on overconfidence bias greatly enhance people's understanding of investors' reactions. Following this research stream, the current study attempts to investigate the overconfidence bias within the crypto-market and also test it on the three coins with the largest market capitalisation, represented more than 71.8 percent of the crypto-market's value at the time writing. The rationale for the study is that we conjecture that the high volatility and trading activities in crypto-market are driven mainly investor sentiments, particularly, by overconfidence bias rather than fundamental supports. The intuition behind the conjecture emerges from our two observations. First, theoretically, Shefrin (2007), along with Barber and Odean (2001), provided support for the notion that male investors exhibit higher levels of overconfidence compared with females as they are more competitive (Niederle and Vesterlund, 2007), they invest more often and more aggressively than women when facing financial opportunities (Barber and Odean, 2001). It is worth noting the majority of crypto-participants are overwhelmingly male. Hence, crypto-market is suspected to exhibit the overconfidence bias.

Second, crypto-market is possibly unfolding like the Dot-Com crash, in which people were overconfident about website-based firms and bet big on a seemingly revolutionary technology; hence, suffered a painful reality check. The similarities in price moves and trading volume between these two market events could be signs that history is repeating itself. Specify the particular of BTC and Amazon, BTC is the crypto-market leader, accounts for more than 54 percent of total market capitalization at the time writing, and Amazon was the NASDAQ market leader and also a biggest loser during the crash. We observed that their price movements have followed a similar path. Amazon's share prices has eventually recovered and lifted to approximately USD$2,000, became the second public company to reach a one trillion-dollar valuation. Accordingly, positively speaking, there is the fact that many companies survived the Dot-Com bubble, have climbed to prices exponentially higher than those during the bubble, which anchor a great hope on crypto-market perspectives. In other words, the crypto-market and Dot-Com similarity offers much more than a simple parallel comparison, it offers a precedent of hope which entirely impacts the world built around them.

To expand our analysis, this study is also based on the fundamental idea presented in Obryan (2018) on the behavioural familiarities between the crypto-market and the Dot-Com bubble. Recent studies have suggested overconfidence was (and continues to be) a major cause in numerous historical disasters namely, the Iraq War, Vietnam War, WWI, climate change, and Hurricane Katrina, as well as the Global Financial Crisis in 2008 in particular (Johnson and Fowler, 2011) and stock market bubbles in general (Luuk, 2016). Such historical events demonstrate that bubbles are the result of overconfident behaviours. In this regard, it is the aim of this study to determine whether there is a close relationship between crypto-behaviour and the Dot-Com bubble, thus establishing the existence of the overconfidence bias in the current crypto-market.

To the best of our knowledge, the hypothesis presented in this thesis attempts to understand crypto- market movement with an investigation into the overconfidence bias by examine the relationship between past market returns and current trading activities. We seek to draw conclusion on overconfidence in existence if the positive inter-relationships are found. Additionally, we also expect to provide a universal empirical explanation of the anomalies observed in CCs in 2017. To broaden our research and to firmly root it in previous studies, this thesis presents general ideas around anticipating the future of CCs based on historical data.

A. *Significance and Contributions*

When the Internet was first adopted in the 1990s, no one expected it would have the reach and impact that it currently has. FinTech shares a similar position to this today. Indeed, the financial services industry is undergoing rapid transformation due to innovations in technology, which now include CCs and several other digital assets. Importantly, as long as technological innovations provide for improved efficiencies, these developments will not only continuously drive significant changes in the way financial service providers operate, but also have significant implications for financial consumers including both macro- and small business relating to the cost and services' security. Indeed, while early developments of the Internet dealt with intangibles, the modern FinTech Internet deals with assets stored in encoded form on a network-to-network chain. One of these assets is cryptocurrency, where money is in digital form. These fast-evolving market dynamics require traditional financial institutions, banks, and financial regulators to play integral roles in closely monitoring and regulating these developments.

Cryptocurrencies have demonstrated their influence, now boasting approximately 2,180 coins equivalent to USD$245.6 trillion market capitalisation and BTC in particular with 17 million BTCs in circulation at the time writing (coinmarketcap.com). Although the bears ruled the crypto-market in late 2018, the market has proven it is going to be here for the long haul. Given the recency of cryptocurrencies and the excitement surrounding them (Narayanan, 2016), it is essential to conduct in- depth reviews of the current crypto-literature.

Cryptocurrency has gained wider mainstream attention since its peak in early 2018, in which the market experienced immense trading activity and volatility. Opinions on CCs are buzzing on the Internet and the market is witnessing greater analysis of these new assets. For decades, understanding anomalies in the stock market has presented significant challenges for economists. Theoretical foundations in financial economics rely ultimately on the assumption of the market efficiency theory. Empirical studies, in the meanwhile, have also found evidence to contradict the assumptions underpinning the market efficiency theory and to better explain anomalies. In such findings, overconfidence is considered a key behavioural factor in gaining a more in-depth understanding of this trading puzzle (De Bondt and Thaler, 1995). To date, empirical studies that have investigated the existence of behavioural biases have generally found there is a lack in cryptocurrency holdings. Based on this background information, the findings of the present study endeavour to add a behavioural dimension to the current discussion on this topic. We expect to contribute insights regarding crypto-market trading activities, as well as the fundamental factors underlying them. We believe such insight will be valuable to those who are currently involved in the market, or to those who are looking to get involved. On the basis of this foundation and in combination with historical data, this study is expected to generate general ideas in relation to future analysis on market performance.

II. Behavioural Literature Review

Many studies on behavioral have demonstrated the definition of the overconfidence bias. Most studies of error-prone *self-assessment* reveals overconfidence. Self-assessments often correlate poorly with objective measures of skill in a variety of domains, such as intellectual abilities (Borkenau and Lieber, 1992), social skills (DePaulo et al., 1997), and job performance (Bass and Yammarino, 1991). For example, drivers (Marttoli and Richardson, 1998), motorcyclists (Rutter et al., 1998) and bungee jumpers (Middleton et al., 1996) tend to overestimate their ability to travel safely in their preferred manner. Moreover, the previous literature on this topic also describes overconfidence as the tendency to overestimate personal skills, abilities and predictions for success (Ricciardi, 2008; Koriat, Lichtenstein, and Fischhoff, 1980). This definition is closely linked with the *better-than-average* effect (Larwood and Whittaker, 1977; Alicke, 1985; Taylor and Brown, 1988). Overconfident individuals strongly believe in their own judgement (Odean, 1998) and tend to overstate the precision probability of their personal assessment and information (Daniel, 1998).

Methodologically, overconfidence has been widely explained by individual information searching strategies. Koriat et al. (1980) conducted experiments with 268 paid volunteers. These volunteers were asked to answer a list of questions and also required to list reasons for and against each of the question prior to choosing an answer and assessing the probability of its being correct. The experiment suggested that the confidence depends on the amount and strength of the evidence supporting the answer chosen. Klayman et al. (1999) found that confidence people have in their judgments exceeds their accuracy and that overconfidence increases with the difficulty of the task. Alternatively stated, there are systematic differences between confidence and accuracy, which also consists of an overall bias toward overconfidence. Motivational factors also contribute to explain overconfidence. such as the correlation between wishful thinking and self-defined level of fanhood (Babad, 1987). Kunda (1990) argued that people's confidence is reduced when they are asked to provide reasons contradicting their responses in particular questions. Conducted a series of 6 studies consisting of 631 adults to elucidate the "*illusion of control*" phenomenon, Langer (1975) defines that expectancy of a personal success probability inappropriately higher than the objective probability would warrant. Tindale (1989) showed that the amount of feedback people expected to receive affected the level of confident they had about their decisions. In detail, people who expected no feedback showed the most confidence in their decisions, on the contrary, those who expected feedback on their chosen alternative expressed an intermediate amount of confidence, and those who expected feedback on foregone alternatives exposed to the least confidence. Overconfidence is also measure by on tendency to choose harder-than-normal questions (Gigerenzer et al., 1991; Juslin, 1993, 1994).

In financial decision making, overconfidence has been well-studied analytically (Barber and Odean, 1999; Benos, 1998, Caballe and Sakovics, 2003), experimentally (Adams at al., 1995; Benos and Tzafestas, 1997; Camerer and Lovallo, 1999) and with field data (Baber and Odean, 2000). The argument that overconfidence results in aggressive trading activities is shared by several researchers (e.g., De Long, Shleifer, Summers, and Waldmann, 1991; Kyle and Wang, 1997, Benos, 1998; Odean, 1998; Wang 1998, 2001; Daniel, Hirshleifer, and Subrahmanyam, 2001; Scheinkman and Xiong, 2003). Consequently, this aggressiveness typically translates into poor return investments (Barber and Odean, 2000). Belsky and Gilovich (1999) refer to this bias as the ego trap.

Overconfidence is common in different professional fields, including clinical psychology (Oskamp, 1965), engineering (Kidd, 1970), investment banking (Stael von Holstein, 1972), medicine (Christensen and Bushyhead, 1981; Baumann, Deber, and Thompson, 1991), law (Wagenaar and Keren, 1986), entrepreneurship (Cooper, Woo, and Dunkelberg, 1988), negotiation (Neale and Bazerman, 1990) and management (Russo and Schoemaker, 1992). In other studies, the relationship between demographic factors and overconfidence has been examined. In this area, psychologists found that men tend to be more overconfident than women, which also aligns with findings by Lundeberg, Fox and Punccohar (1994), and Barber and Odean (2001).

A. *Volatility of Cryptocurrency Prices and its Relationship to Dot-Com Bubbles*

Given the substantial fluctuations observed in BTC, there has been a resurgence in the relevant discussions about bubbles. Orbryan (2018) contextualises the crypto-market phenomenon by referencing its current behaviours against the past speculative bubble. He argues the 2017 event mirrors the Internet bubble (i.e., the Dot-Com bubble) when tech-giants such as Amazon and eBay emerged. At that time, various Internet companies were launched, and investors assumed that a company that operated online was going to be worth millions. They were willing to pour an influx amount of money into Internet start-ups in the hope of those companies would one day become profitable. Notably, many investors and venture capitalists abandoned a cautious approach for fear of not being able to cash in on the growing use of the internet during the 1990s. On the whole, people bought into fads or get-rich- quick schemes, society's expectations of what the Internet could offer were unrealistic, and tech-firms' product prices paradoxically experienced an upsurgence. By and large, these investors were inspired by companies such as Amazon and eBay as they grew and became multi-million-dollar businesses. In other words, Internet-based stock prices essentially deviated from their underlying foundation, namely overconfidence increased, there was a lack in caution, and individuals panicked about "not being part" of the investment occurring at the time. The crashes followed, and Pets.com, GeoCities and Gov.works became synonymous with the Dot-Com bust's most famous flop.

In comparison with crypto-market, bubble warnings potentially exist as it seems the Dot-Com bubble and the 2017–2018 fluctuation in the crypto-market have exposed a similar psychological market cycle. Amazon and BTC, respectively, are two leaders of NASDAQ Composite Index in the late 1990s and current crypto-market, share a similar story. During the Dot-Com bubble, Amazon's stock price plunged from its all-time high of around USD$107 per share, to lows of under USD$6 after the crash, a massive loss of over -90 percent. It took Amazon nearly 14 years to reach highs it once set during the bubble. In comparison, BTC recorded a loss of -80 percent from its all-time high of remarkably USD$19,000 in the late 2017, currently priced at nearly USD$5,300 per share. Hence, imagining the movement of price in BTC against the Amazon crash reveals price patterns that suggest there is much about the crypto- market pointing to a bubble occurring in recent years (Figure 1). In fairness, as these are tech-base businesses, if there exists a strong correlation between BTC and Amazon or eBay in terms of the Dot- Com bubble, then would the never-ending tokens of ICO projects face a similar fate to Pets.com, GeoCities and Gov.works? The bubbles ended eventually, and there is no suggestion of a recurrence of this phenomenon in today's financial markets.

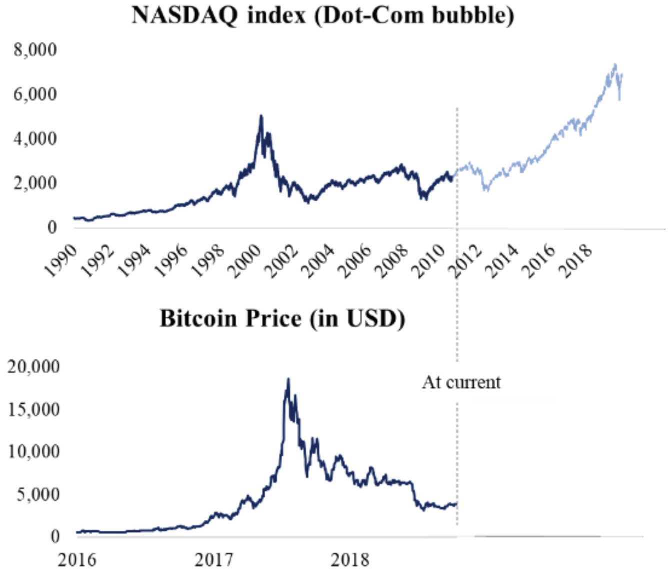


Fig. 1 Degree of familiarity between NASDAQ index and BTC performance

B. *Identified Gap in the Literature*

Traditional economists have failed to understand how the economy works (Posner, 2009). Over the past five decades, the efficient-market hypothesis and rationality fail to explain volatility between stock prices and their fundamental values, as well as excessive trading volume (Lavoie, 2010). Consequently, behavioural economists going back to at least Keynes (1936) explain how psychology drives sentiments to create the gap between stock prices and their fundamental value. Several biases namely, overconfidence, optimism, conservatism, anchoring, and availability biases or belief perseverance, which provide the basis for interpretation of financial decisions (Baker and Wurgler, 2004). Among these biases, insights into overconfidence matter most in terms of gaining a better understanding of decision-making processes in finance (Daniel and Tversky, 2007). Previous scholars have well researched and documented the effect of behavioural biases in general and overconfidence bias in particularly, largely cover in stock market. To date, the study of behavioural impacts on crypto-market is lacking. The crypto-market has currently evolved at unprecedented speed over the course of its short lifespan. Given the current proliferation of crypto-market as well as its evolutionary dynamics, it is essential to conduct in-depth reviews of the current CCs' studies.

There is a comprehensive set of theoretical considerations regarding overconfidence bias based on the relationship between trading volume, return, lagged return and market volatility. However, the majority of interest rests on traditional markets such as stock markets. Empirical research still lacks studies that test CCs. The current crypto-market is experiencing an aggressiveness in trading activity and gaining greater understanding around this phenomenon is essential. If the crypto-market yields the familiar relationship between past returns and current trading volume, there are two significant contributions further studies can make: 1) the acknowledgement of overconfidence bias among crypto-individuals, and 2) the price forecast framework for crypto-market.

III. Data Description

To recall, the collected data attempts to examine the inter-relationship between the turnover and return of a crypto-market index and the three largest market capitalisation coins, BTC, ETH, and XRP, on a daily basis, from the 2nd of March, 2016, to the 30th of April, 2019. This is equivalent to 1,150 observations. The data were downloaded from Coinmarketcap.com and coinmetrics.io as daily prices (in USD), 24-hour exchanged volume (in USD), and daily market capitalisation (in USD). The trading activity is measure along with the turnover for each coin.

The crypto-market is currently composed of 2,180 cryptocurrencies at the time writing. Due to the limitation of fully obtained crypto-market data, we sample ten largest market capitalization CCs to proxy the entire market. These sampled digital coins accounts for approximately 83.7 percent on average of total crypto-market capitalisation at the time of testing, namely BTC, ETH, XRP, LTC, BCH, EOS, XLM, USDT, ADA and DASH.

The rationale to the length of the formation period is that it allows to fully visualize the growth in the overall cryptocurrency by capturing how the top ten cryptocurrencies by market capitalisation have started to change significantly over the last three years. The market rallied in 2016 after the steep crash in 2015. At the time, there were only two CCs valued above USD$100 million, BTC and ETH. At the beginning of 2017, the crypto-market recorded seven coins above the USD$100 million mark. Remarkably, in the late 2017, the market observed all top ten of the largest cryptocurrencies joint into the billion-dollar market cap valuation. Moreover, the paper individually tests overconfidence bias on BTC, ETH and XRP, whose available trading data could be obtained fully within the tested time. The daily return and daily turnover are calculated as follows:

$$Return_t\ (\%) = log(\frac{price_t}{price_{t-1}}) \qquad (1)$$

$$Turnover_t\ (\%) = \frac{24h\ Exchanged\ volume_t}{Market\ Capitalization_t} \qquad (2)$$

In time-series analysis, the use of logarithmic data reduces the gaps caused by absolute values and variability in the data, especially in datasets that contain outlying observations (Feng et al., 2014). Moreover, Wang (1994) and Lo and Wang (2000) provide a justification for their preference towards turnover rather than the use of other volume metrics. The market return and turnover are calculated as weighted-returns of the index compositions and are expressed as follows:

$$\begin{aligned} MRKret_t = {} & w_{BTC,t}\log(BTCret_t) + w_{ETH,t}\log(ETHret_t) \\ & + w_{XRP,t}\log(XRPret_t) \\ & + w_{LTC,t}\log(LTCret_t) \\ & + w_{BCH,t}\log(BCHret_t) \\ & + w_{EOS,t}\log(EOSret_t) \\ & + w_{XLM,t}\log(XLMret_t) \\ & + w_{USDT,t}\log(USDTret_t) \\ & + w_{ADA,t}\log(ADAret_t) \\ & + w_{DASH,t}\log(DASHret_t) \end{aligned} \qquad (3)$$

$$\begin{aligned} MRKturn_t = {} & w_{BTC,t}BTCturn_t + w_{ETH,t}ETHturn_t \\ & + w_{XRP,t}XRPturn_t \\ & + w_{LTC,t}LTCturn_t \\ & + w_{BCH,t}BCHturn_t \\ & + w_{EOS,t}EOSturn_t \\ & + w_{XLM,t}XLMturn_t \\ & + w_{USDT,t}USDTturn_t \\ & + w_{ADA,t}ADAturn_t \\ & + w_{DASH,t}DASHturn_t \end{aligned} \qquad (4)$$

Table 1 presents a statistical summary of the 1,150 observations of the returns and turnovers of BTC (*BTCret, BTCturn1*), XRP (*XRPret, XRPturn*), ETH (*ETHret, ETHturn1*), and the crypto-market (*MRKret*). Empirically, the market-wide model successfully provides solid support for the existence of overconfidence effects through examination of the lead-lag relationship between security turnover and market return. In a study by Shefrin and Statman (1985), the term 'disposition effect' was introduced, which suggests a direct comparison between individual return and market return influences on security turnover. In short, the disposition effect represents a desire to realise gains by selling stocks when their prices have appreciated and, therefore, to delay the realisation of loss. The effects are also explained in terms of the behavioural bias of individual investors towards individual security and, in particular, an investor's attitude towards the individual stock they currently hold, results in holding losers too long. Meanwhile, the term 'overconfidence is believed to be closely related to market fluctuation as a whole.

In other words, if investors overconfident about the ability to generate higher returns by actively trading, they are likely to maintain this belief to the stock market in general. In a nutshell, market return serves as a more precise proxy for overconfidence level. Due to the subjectivity inherent in distinguishing them, we interpret the relevant aspects of our findings as confirmation of the overconfidence bias and the disposition-effect hypothesis separately.

TABLE 1 Descriptive statistics

Panel A:	***MRKret***	***MRKturn***	***BTCret***	***BTCturn1***
Mean	4.035	0.511	0.295	3.900
St Dev.	12.585	17.580	3.987	3.718
Skewness	27.322	3.151	0.337	2.066
Kurtosis	854.494	34.558	8.233	8.499
Panel B:	***ETHret***	***ETHturn1***	***XRPret***	***XRPturn***
Mean	0.121	6.757	0.137	2.427
St Dev.	2.655	9.114	3.339	2.968
Skewness	0.096	2.484	3.017	3.798
Kurtosis	6.575	9.344	40.382	27.221

IV. Methodology

The current study employed the vector autoregression (VAR) model to test the overconfidence hypothesis presented by Gervais and Odean (2001) in their study on cryptocurrency indexes, as well as the disposition effect hypothesis presented by Shefrin and Statman (1985) as it pertains to BTC, ETH and XRP. Please note that due to the length of the paper, please refer to Sims (1980) and Gervais and Odean (2001) for full VAR model description.

The VAR model is considered especially useful in illustrating dynamic economic behaviours and financial time series, as well as macro-economic forecasting. In part, its popularity stems from its flexibilty, simplicity, ability to fit the data, and, undoubtedly, from its success as a forecasting model (Karlsson, 2013). Technically speaking, VAR is built to explore the lead-lag relationships among variables. Moreover, the VAR model is capable of performing an extensive set of equations simultaneously without specifying which variables are exogenous and which endogenous.

Use of the VAR model became widespread after the publication of Sims' (1980) influential paper. After Sims, Dert (1998) employed this model to yield pension-plan scenarios. He created future inflation in prices, wage inflation, stock returns, cash returns and real estate returns, all of which are consistent with historical patterns in terms of means, standard deviations, autocorrelations and cross correlations between selected variables. Carino (1994) performed VAR in generating scenarios for the Yasuda Kasai model. VAR methodology is also used to predict the returns of stocks, bonds or indexes. For example, Brennan, Schwartz and Lagnado (1997) used the Treasury-bill rate, Treasury-bond rate and dividend yield as independent variables in their model. Brandt (1999) used lagged excess return on NYSE over Treasury-bill rate in addition to dividend yield, default spread and term spread.

Statman, Thorley and Vorkink (2006) used VAR and associated Impulse Response Function to perform multivariate time-series analysis on investigating the lead-lag relationship between market turnover and market returns for monthly observations on all NYSE/AMEX common stock. One of their findings is to confirm the formal theories of investor confidence. According to Statman, Thorley and Vorkink (2006), if there is a positive lead-lag relationship between turnover and past returns of the market, the inference on overconfidence bias will be drawn. The rationale is that past returns act as a proxy for overconfidence, as people's levels of overconfidence change according to the previous outcomes they have experienced.

Based on Statman, Thorley and Vorkink's (2006) study, we predicted a statistically significant lead-lag relationship between the turnovers and returns of the whole market would provide confirmation of the overconfidence bias, and that the three largest market cap coins (i.e., BTC, ETH, and XRP) would confirm the presence of disposition effects.

V. Empirical Findings

The VAR model is an ad hoc dynamic multivariate model, treating simultaneous sets of variables equally, in which, each endogenous variable is regressed on its own lags and the lags of all other variables in a finite-order system (Sims, 1980). By employing VAR model, many previous studies have provided strong evidence in support of significant time-series relationships, either in terms of individual stocks or the market, between past return and subsequent trading volume. If overconfidence plays an explanatory role in trading volume, we should find positive and significant coefficients in the regression analysis of market turnover and its lagged returns. More specifically, high past (lagged) returns cause investors to become more confident in trading and, therefore, they tend to trade more aggressively in a subsequent period and, vice versa, investors may trade less after the experience of negative market returns. On the other hand, previous studies on individual stocks have found negligible support for a time-series relationship between past trading volume and returns over different time horizons. For example, Statman (2006) concluded that there was no significant association between lagged turnover and monthly returns over a 40-year sample. Using the daily data of 29 DAX companies, Gurgul (2007) provided support for the minimal impact of trading volume on current stock returns. The findings from these authors align with the efficient-market hypothesis, in which the short-term forecasts on current returns as well as future returns are unable to be improved by observing the trading volume data, and vice versa. On the other hand, Brauneis (2007) finds that high-volume trading tends to yield positive stock returns when applying the VAR model and Granger-casualty analysis on the daily time- series data of individuals' DAX companies with alterations to subjectivity. He also interprets this as confirmation of a high-volume premium existence.

Table 2 summarises the results of the full-sample bivariate VAR on market turnover (*MRKturn*) and market return (*MRKret*). The table is organised into columns for lagged variables and rows for dependent variables. The estimated coefficient values, as well as the p-values are also reported. Consistent with the study by Statman, Thorley and Vorkink

(2006), we refer to coefficients with a p-value of 0.1 or less as significant and of 0.01 or less as highly significant. Significant levels (in parentheses) are rounded to three digits.

TABLE 2 Market VAR estimations

	MRKret		***MRKturn***	
Lagged	Coeff.	Prob.	Coeff.	Prob.
MRKturn(-1)	0.137*	0.000	-0.016	0.707
MRKturn(-2)	0.080*	0.007	0.027	0.535
MRKturn(-3)	0.085*	0.004	-0.045	0.304
MRKturn(-4)	0.083*	0.005	0.016	0.719
MRKturn(-5)	0.050**	0.095	-0.012	0.790
MRKturn(-6)	0.123*	0.000	0.014	0.757
MRKturn(-7)	0.088*	0.003	0.020	0.653
MRKret(-1)	0.017	0.394	0.140*	0.000
MRKret(-2)	0.009	0.661	-0.109*	0.000
MRKret(-3)	0.009	0.676	0.045	0.138
MRKret(-4)	-0.006	0.752	-0.080*	0.008
MRKret(-5)	0.032	0.113	0.011	0.709
MRKret(-6)	0.038**	0.061	0.106*	0.000
MRKret(-7)	-0.017	0.404	-0.021	0.484

* significant at 1 percent confident level

** significant at 10 percent confident level

Table 2 illustrates that market turnovers are autocorrelated with highly significant coefficients for all lags. With reference to the conclusion presented by Amihud-Mendelson, turnovers measure investors' trading frequencies. The consistently positive and significant estimated lagged turnover coefficients produced in this study, therefore, represent the increasing function of market participants' trading frequencies during the test period. These results link the positive dependence of market turnovers to almost all their lagged returns and illustrate the material impacts on the sixth lag, as market participants take the initiative to trade based on the market returns of the previous six days. This relationship represents our first finding and confirms the presence of overconfidence in the market.

A. Discussion of the Results

The study attempted to examine the existence of overconfidence bias in crypto-market by hypothesizing the explanatory power of past market returns to the current turnover ratio of crypto-market in general and of three CCs namely BTC, ETH and XRP in particular. Our initial estimations stemmed from the high degree of familiarity between the recent volatility in the crypto-market, as well as the presence of historical asset bubbles, as these bubbles are mainly driven by overconfidence. After the surge in popularity of cryptocurrencies in 2017, people invested vast amounts into this market people. The seemingly erratic pouring of billions of dollars into the market has raised financial concerns, as such a phenomenon mirrors that of the Dot-Com bubble in the 1980s. Indeed, the appetite of investors for shares of tech-based firms is insatiable, as many are overconfident in terms of the future prospects of these firms.

Although our analysis was initially motivated by overconfidence theory, the findings of this study related to the dependence of trading activities on past market returns. Nonetheless, overconfidence is believed to be an important occurrence both theorists and empirical researchers in this field should acknowledge. We employed a vector autoregression model, Granger-causality tests and the associated impulse response function to test the overconfidence hypothesis on the cryptocurrency indexes used in this study and to test the disposition effect on the three largest market capitalisation coins (i.e., BTC, ETH and XRP). The study also attempted to disentangle overconfidence and the disposition effect by examining the interpretative ability of market returns and individual coin returns to turnover as confirmation of overconfidence and the disposition effect, respectively.

Interestingly, despite notions of the importance of overconfidence-based tests in providing a solid explanation in terms of stock market trading volume and volatility, our analysis of crypto-market activity during the tremendous volatility it experienced in 2018 suggests it played a statistically significant role, but had only minimal economic impacts. This study generated following key findings. Based on VAR tests on the crypto-market, overconfidence bias was found to be present, as current turnover was positively dependent on almost all its lagged returns, with significant impact found on lag six. However, the relationship was not found to be economically significant, as an increase in one standard deviation of the sixth-lagged return resulted in a slight 0.038 percent increase in current trading turnover. Additionally, we observed that BTC returns varied at a consistent rate compared to the returns of the crypto-market. A possible explanation for this is BTC simply acts as a proxy for the entire market.

Overconfidence bias was also found to be present in individuals involved with BTC and XRP, but at different lags. Moreover, the model illustrated that the impact of market return for XRP turnover was larger than that of BTC turnover, wherein we found higher coefficients and more explanatory lags in the regression of XRP turnover and lagged-market returns. In terms of XRP, all regressed variables, except for its own return and associated market return, are inter-related. Besides, it is worth noticing that BTC is a digital currency intended as a mean of payment, while XRP is a more about a payment settling, a currency exchange and a remittance system intended for banks and payment networks (Marr, 2018). In 55 other words, as compared to BTC, XRP is more than a pure cryptocurrency, it is more of a protocol (Marr, 2018). Briefly describe, XRP protocol is specifically designed to utilize blockchain technology which enable to transfer money anywhere around world instantaneously and inexpensively. Over the course of the brief failure in the market, XRP proved itself to be the most battle-tested crypto-asset. Indeed, the recent warm response from the market towards this cryptocurrency is due to its stability, where major central banks and financial institutions are lining up to adopt the payment technology underpinning XRP. There are now over 100 exchanges worldwide that list XRP (ripple.com, 2019).

In term of ETH, our second finding was the presence of disposition effects in ETH investments. Alternatively stated, observation of past returns for ETH helped to explain its associated current trading activity. Notably, we remarked that ETH returns are statistically unexplainable in terms of all variables tested. Therefore, we argue the price of ETH is not significantly driven by fundamental mechanisms. For example, ETH is required when an individual participates in ICOs, which implies that demand is supported by a favourable

ICO climate. Indeed, as compared to BTC, ETH is more than a pure CC. That is, ETH is an advancement based on the blockchain principle that supports BTC but with a purpose that does not compete with Bitcoin (Hayes, 2018). ETH, instead, serves as a platform for smart contracts that makes ICO easier to do. ICO, therefore, are an economy built on top of ETH. ICO projects, in brief, is a new method for companies to create their own digital currency (Robert, 2017) as they will create a certain number of digital tokens that can then be sold to the public, serve as a medium of change for other CCs on a peer-to-peer platform.

Touted by Willet back in 2012, ICO was not a part of the daily crypto-lexicon until ETH-based projects began to emerge in the market in September 2014, where they garnered a whopping USD$19 million – the largest ICO ever completed at that time. This success for ICOs stirred a frenzy of new ICO instruction during this period. Unfortunately, many ICOs failed to live up to the market hype until late 2016, when the Decentralised Autonomous Organisation (DAO), one of the most remarkable and most successful concepts implemented via blockchain technology, first created a smart contract on the ETH blockchain with a value of USD$168 million. Since the late 2016, the size of individual ICO projects has gradually increased.

VI. Conclusion

Given the substantial empirical and theoretical support for the predictability of past market returns towards current turnover stock as confirmation of overconfidence bias in the stock market, this study attempted to understand such bias as it pertained to the crypto-market. In a nutshell, our findings expect to contribute insights regarding crypto-market which we believe that such insights will be valuable to those who are currently involved in the market, or to those who are looking to get involved. First of all, it should be emphasized that findings about the dependence of trading activity and past returns are important empirical fact that should be acknowledged by both theorists and empirical researchers, regardless of one's interpretations. Secondly, understanding the impacts of overconfidence is vitally important. Previous studies proved that overconfidence was a major cause in a number of historical disasters and asset bubbles. In investment decision making, overconfidence bias forms a vicious cycle in which investors buy when they are confident, sell when they get scared, miss the recovery opportunities and re-enter in when the markets bounce back. Regarding to crypto-market, statistically speaking, historical figures confirm the comparison between the price momentum in the crypto-market and in BTC in particular, to the Dot-Com bubble, as well as the presence of overconfidence among crypto-participants. Such findings are expected to yield forecasting capacity in terms of upcoming movement in the crypto-market. Practically speaking, we observed that CCs, particularly BTC, ETH and XRP, are different in fundamentals and investment intentions, which makes joint interpretation of these three cryptocurrencies deficient.

On the basis of this foundation and in combination with historical data, we expect to generate general ideas in relation to future analysis on market performance. That is, rather than attempting to understand the performance of the crypto-market in its entirety in a more traditional sense, the integration level of these digital coins should be the principal concern. Undoubtedly, CCs are still investable assets and actively trading, meaning their prices are partially driven by the daily supply-demand equilibrium. Trading intentions and motivations, however, serve as main research concerns. We initially expected to find a significantly robust conclusion for these concerns upon accessibility of the data related to investor types (i.e., institutional or individual). However, crypto data has only recently been established and it is a relatively intensive exercise to obtain in full. This placed a limitation on our interpretations.

References

[1] Adams, M. E., Johnson, E. J. and Mitchell, D. J. (1995). Your preferences may be hazardous to your wealth: How false consensus and overconfidence influence judgments of product success (Working Paper No. 05). Retrieved from: https://www8.gsb.columbia.edu/researcharchive/articles/5755

[2] Alicke, M. D. (1985). Global self-evaluation as determined by the desirability and controllability of trait adjectives. Journal of Personality and Social Psychology, 49(6), 1621–1630.

[3] Asad, H., Khan, A., and Faiz, R. (2018). Behavioural biases across stock market investors: Evidence from Pakistan. Pakistan Economic and Social Review, 56(1), 185–209.

[4] Babad, E. (1987). Wishful thinking and objectivity among sports fans. Social Behaviour, 2(4), 231-240. Baek, C., and Elbeck, M. (2015). BTCs as an investment or speculative vehicle? A first look. Applied Economics Letters, 22(1), 30–34.

[5] Baker, M. and Wurgler, J. (2004). Handbook of the Economics of Finance. Retrieved from: http://dx.doi.org/10.1016/B978-0-44-453594-8.00005-7

[6] Barber, B. M. and Odean, T. (2000). Trading is hazardous to your wealth: Common stock investment performance of individual investors, Journal of Finance, 55(2), 773–806.

[7] Barber, B. M., and Odean, T. (2001). Boys will be boys: Gender, overconfidence and common stock investment. Quarterly Journal of Economics, 116(1), 261-290.

[8] Bateman, T. S., and Schwenk, C. R. (1986). Biases in investor decision-making: The case of John DeLorean.American Journal of Business, 1(2), 5–12.

[9] Belsky, G., and Gilovich, T. (1999). Why smart people make big money mistakes and how to correct them: Lessons from the new science of behavioral economics. New York, NY: Simon and Schuster Paperbacks.

[10] Benos, A. and Tzafestas, E. (1997). Alternative distributed models for the comparative study of stock market phenomena. Information Sciences, 99(3-4), 137–157.

[11] Benos, A. V. (1998). Aggressiveness and survival of overconfident traders. Journal of Financial Markets 1, 1(3-4), 353–383.

[12] Caballe, J. and Sakovics, J. (2003). Speculating against an overconfidence market. Journal of Financial Markets, 6(2), 199-225

[13] Cooper, A. C., Woo, C. W., and Dunkelberg, C. D. (1988). Entrepreneurs' perceived chances of success. Journal of Business Venturing, 3, 97–108.

[14] Christensen-Szalanski, J. J., and Bushyhead, J. B. (1981). Physicians' use of probabilistic information in a real clinical setting. Journal of Experimental Psychology: Human Perception and Performance, 7, 928– 935.

[15] Daniel, K., Hirshleifer, D., and Subrahmanyam, A. (2001). Overconfidence, arbitrage, and equilibrium asset pricing. Journal of Finance, 51(3), 921–965.

[16] De Long, J., Shleifer, A., Summers, L. H., and Waldmann, R. J. (1991). Noise trader risk in financial markets. Journal of Political Economy, 98(4), 703–738.

[17] Fabre, B., and François-Heude, A. (2009). Optimism and overconfidence investors' biases: A methodological note. Dans Finance, 30, 79–119.

[18] Johnson, D. P., and James, H. F. (2011). The evolution of overconfidence, Macmillan Publishers Limited, 477, 317–320.

[19] Kidd, J. B. (1970). The utilization of subjective probabilities in production planning. Acta Psychologica, 34, 338–347.

[20] Klayman, J., J. B. S., Gonzalez-Vallejo, C., and Barlas, S. (1999) 'Overconfidence: It Depends on How, What, and Whom You Ask'. Organizational Behavior and Human Decision Processes, 79(3), 216–247

[21] Koriat, A., Lichtenstein, S., and Fischhoff, B. (1980). Reasons for confidence. Journal of Experimental Psychology: Human Learning and Memory, 6(2), 107–118.

[22] Kunda, Z. (1990). The Case for Motivated Reasoning. Psychological Bulletin - the American Psychological Association, 108(3), 480 - 498

[23] Langer, E. J. (1975). The illusion of control. Journal of Personality and Social Psychology, 32(2), 311-328. Langer, E. J. (1975). The illusion of control. Journal of Personality and Social Psychology, 32, 311–328.

[24] Larwood, L., and Whittaker, W. (1977). Managerial myopia: Self-serving biases in organizational planning.

[25] Journal of Applied Psychology, 62(2), 194–198.

[26] Lundeberg, M. A., Fox, P. W., and Puccohar, J. (1994). Highly confident but wrong: Gender differences and similarities in confidence judgments. Journal of Educational Psychology, 86, 114–121.

[27] Luuk, G. (2016). The effect of overconfidence on stock market bubbles, velocity and volatility (Unpublished Master's Thesis). Radboud University, Netherlands. Retrieved from: https://theses.ubn.ru.nl/handle/123456789/1768

[28] Marr, B. (28th February, 2018). What Is The Difference Between Bitcoin And Ripple? Retrieved from: https://www.forbes.com/sites/bernardmarr/2018/02/28/what-is-the-difference-between-bitcoin-andripple/#28c92fdc6611

[29] Neale, M. A., and Bazerman, M. H. (1990). Cognition and rationality in negotiation. New York, NY: The Free Press.

[30] Obryan, P. C. (2018). Herding behaviour in cryptocurrency markets (Working Paper). Retrieved from: https://arxiv.org/pdf/1806.11348.pdf

[31] Odean, T. (1998). Volume, volatility, price and profit when all traders are above average. Journal of Finance, 53, 1887–1934.

[32] Odean, T. (1999). Do investors trade too much? American Economic Review,89, 1279–1298.

[33] Oskamp, S. (1965). Overconfidence in case-study judgments. Journal of Consulting Psychology, 29(3), 261– 265.

[34] Ricciardi, V. (2008). The psychology of risk: The behavioral finance perspective. Handbook of finance (Volume 2): Investment management and financial management, John Wiley and Sons, 85–111. Retrieved from : https://ssrn.com/abstract=1155822

[35] Russo, J. E., and Schoemaker, P. J. H. (1992). Managing overconfidence. Sloan Management Review, 33, 7– 17.

[36] Scheinkman, J., and Xiong, W. (2003). Overconfidence and speculative bubbles. Journal of Political Economy, 111(6), 1183-1220.

[37] Shefrin, H. (2007), Behavioral corporate finance: Decisions that create value. New York, NY: McGraw-Hill/Irwin.

[38] Shefrin, H., and Statman, H. (1985). The disposition to sell winners too early and ride losers too long: Theory and evidence. Journal of Finance, 40, 777–791.

[39] Stael von Holstein, C. (1972). Probabilistic forecasting: An experiment related to the stock market. Organizational Behavior and Human Performance, 8, 139–158.

[40] Statman, M., Thorley, S., and Vorkink, K. (2006). Investor overconfidence and trading volume. Review of Financial Studies, 19(4), 1531–1565.

[41] Taylor, S. E., and Brown, J. D. (1988). Illusion and well-being: A social psychological perspective on mental health. Psychological Bulletin, 103(2), 193–210.

[42] Tindale, R. S. (1989). Group vs individual information processing: The effects of outcome feedback on decision making. Organizational Behavior and Human Decision Processes, 44(3), 454-473.

[43] Wagenaar, W., and Keren, G. B. (1986). Does the expert know? The reliability of predictions and confidence ratings of experts. Intelligent decision support in process environments, 21, 87 – 103.

[44] Wei, J. (2018), Behavioral biases in the corporate bond market. Journal of Empirical Finance, 46, 34 – 55 Weinstein, N. D. (1980). Unrealistic optimism about future life events. Journal of Personality and Social Psychology, 39(5), 806–820.

Organising Committee

General Co-Chairs

Raja Jurdak, Queensland University of Technology, Australia
Ryan Ko, University of Queensland, Australia
Vallipuram Muthukkumarasamy, Griffith University, Australia

Organization Co-Chairs

Ernest Foo, Griffith University, Australia
Kamanashis Biswas, Australian Catholic University, Australia
Guangdong Bai, University of Queensland, Australia

Local Co-Chairs

David Tuffley, Griffith University, Australia
Marius Portmann, University of Queensland, Australia
Wee Lum Tan, Griffith University, Australia

Industry Co-Chairs

Katrina Donaghy, Civic Ledger, Australia
Don Sands, Synengco, Australia

Publicity Chair

Ali Dorri, Queensland University of Technology, Australia
Zhe Hou, Griffith University, Australia

Web Chair

Hadrien Bride, Griffith University, Australia

Sponsors

Gold Sponsors

Griffith UNIVERSITY
Queensland, Australia

Silver Sponsors

QUT ife Institute for Future Environments

Bronze Sponsors

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CONSENSYS

PEGASYS

iC integratedCAPITAL
Making smart money more agile

CSIRO

DATA 61

ANONYOME LABS