DESIGN OF RELIABLE DECENTRALISED APPLICATIONS ON BLOCKCHAINS

PhD Project Proposal -- Andrea Bracciali

Abstract. This is a multi-disciplinary proposal on a hot research topic and developing technology. It enables collaboration across different faculties at the University of Stirling, with a high potential impact on the flourishing fintech Scottish sector, in collaboration with industry and supported by a large international network of academic expertise.

Context. Blockchain technologies (BCT), widely renown after the advent of the Bitcoin virtual currency (2009 – with a current market cap of about 20USD billion), make decentralised consensus possible, i.e. agreement between untrusted players, without the need for a central certification authority, In the case of Bitcoin and other virtual currencies, BCT allow a coherent history of monetary transactions to be agreed by independent parties. Consensus is generated by cryptography-enabled algorithms running on a distributed network of peers, a.k.a. *miners*, and enabling, in this case, virtual currencies that do not depend on the existence of a central bank. BCT have then triggered the development of innovative decentralised applications, a.k.a. *dapps*, for trading services and payments, bankability and clearing, certifiable sensitive data, e.g. health data, identity management, smart property, "ownerless" ride-sharing systems, intellectual property, estate and land registry, fraud prevention. More recently, BCT also support the decentralized execution of code, e.g. the Ethereum blockchain, defining a new model of decentralised computation and enabling *smart contracts*, i.e. self-enforcing agreements expressed as executable code to be published, invoked and run on BCT.

BCT are currently generating strong interest in academia, particularly in the UK, e.g. the foundation of the "Centre for Cryptocurrency Research and Engineering" at Imperial College, and the very recent “Blockchian Lab” at Edinburgh University; private companies and the government, e.g. believing that BCT will lead to "... powerful, disruptive innovations that could transform the delivery of public and private services and enhance productivity" in several sectors (Distributed Ledger Technology: beyond block chain, UK Government, Office for Science, 2016). BCT are extremely relevant for Scotland, the second financial area in the UK, where the fintech sector is flourishing with 1000+ companies, the presence of major banking multinationals and financial institutions, top tech universities and governmental support, e.g., the recent RSB fintech accelerator and the event http://www.scotchain16.com/.

However, BCT are still in the thriving phase of multiple proposals competing for their market share and not yet mature enough for widespread and safe adoption, as some recent highly disruptive attacks—first and foremost the DAO attack (June 2016) worth about 50USD million—have demonstrated.

Research programme. The multi-layered and multi-disciplinary structure of BCT poses several, highly intertwined, open research questions: scalability and efficiency of the framework, robustness of decentralised trust, security of dapp programming languages, data analytics of BCT information, and, noticeably, the economics of incentives and virtual currencies which are at the bases of BCT. In the words of Ethereum founder, Vitalik Buterin, *“Arguably, the true genius behind the success of Bitcoin, Ethereum and similar systems was not the specific design of their blockchain, or their use of algorithms that resemble forms of distributed consensus in order to maintain security; rather, it is the innovation of cryptoeconomics - the art of combining cryptographic techniques and economic incentives defined and administered inside a protocol in order to encourage users to (correctly) participate in certain roles in the protocol, and thereby preserve and maintain certain desired properties …” (WTSC17).* Indeed, associated virtual currencies provide the incentives for maintaining the BCT execution environment alive, and affect program execution (fees are typically associated to dapp execution), and are traded by programs in execution. Accordingly, the main research goal of this proposed PhD is to define a multidisciplinary framework, drawing from computer science and economics, which will support (relevant aspects of) software design for trustable dapps, properly accounting for the effects of the economics of the associated virtual currencies on the execution environment. The definition of such a framework is currently a recognized open research problem.

The project will comprise the following main phases, roughly corresponding to the three years of the PhD programme (details will need to be finalized in due course): a) Survey of the state of the art, study of BCT, and critical evaluation of competing proposals. Selection of reference blockchains and language(s) of interest. Identification of use cases of interest. b) Focus on dapp programming languages and econo-computational properties of interest. Study of "economics-aware" software design for selected language(s) (and specific properties). c) Prototyping of supporting tools. Validation of the proposed framework, with respect to selected properties and use cases.

Supervisory arrangements. The project will be carried out under multidisciplinary and industry-supported supervision (please see attached support letters). Dr. Andrea Bracciali will be the main supervisor, and Dr. Jingpeng Li, CSM, expert in data analytics, and Dr Theodoros Diasakos, Economics, expert in economic theory and bounded rationality, will support the student as second supervisors, making a suitable multidisciplinary supervising team. Wallet.Services ltd will contribute industrial expertise and provide a very effective pathway to impact for the findings of the student's research. Dr. Davide Grossi, Computer Science, University of Liverpool, expert in decision theory and shared agreement, Dr. Massimo Bartoletti, Computer Science, University of Cagliari, expert in the theory of BCT, Prof. Nicola Dimitri, Economics, University of Siena, expert in economic dynamics, and Prof. Massimiliano Sala, leader of the Crypto-Lab, University of Trento, have all expressed their interest in supporting and contributing to the proposed project, complementing the supervising team with a very complete set of expertise of big value for the multidisciplinary approach that we propose to tackle the research questions of interest.

Sustainability and fitting with University Reasearch Strategy This project proposal lies within a larger effort to build research capacity on the BCT theme, examples include the organization of Blockchain@Stirling and WTSC17 featuring Vitalik Buterin as invited speaker, and strengthening research links with Liverpool, Glasgow, King's College, Trento, Siena and Cagliari (a PhD student is currently visiting Stirling). The several colleagues that have expressed interest in a direct involvement in the project set ideal working conditions for the student and the success of the project. This will lead to reciprocal visits and new collaborations.

Being part of such a network is valuable for the strategic goals of the University, for supporting joint application for funds, European networking and PhD exchanges, further contributing to the internationalization goals of the University.

At the University level, having a PhD student carrying out work on BCT will contribute to aggregate researchers with an interest in BTC from different faculties: initial talks have started with staff in Economics, Mathematics and Law aiming to the creation of a cross-faculty group of interest. A first outcome was a pre-proposal for a Leverhulme Doctoral Studentship (1M), and the possibility of a MSc on BCT is under consideration. These initiatives will largely benefit from the contributions that a PhD student can give in terms of competence and expertise.

Finally, considering the impact aims of the University, this proposal benefits from an established promising collaboration with Wallet.Services, one lively start-up on BCT. A joint application for funds, potentially contributing to the research on BTC at Stirling has been submitted to the DataLab Innovation Centre. The results of the research here proposed are of great interest for the WalletServices products and services. The company is willing to collaborate to the student's research programme and provide use cases of interest, further strengthening the success chances of our project. The approval of this PhD project proposal will further strengthen our developing industrial collaboration, from which further applications for industrial funds will stem (DataLab, KTP are possible targets).

Person specification This is an interesting research project on a currently developing breakthrough technology. Blockchain-based applications are still in the early phase of definition and the several competing proposals carry open research questions. This PhD will focus on how to enhance our capability to develop secure and reliable blockchain-based applications, enabling direct interaction between individuals without the need for a supervising centralised authority.

We propose a multi-disciplinary approach, supported by a large international network of co-investigators with expertise in economics, game theory, cryptography, security and

verification, keen to collaborate on this project. Furthermore, companies from the fintech sector will provide use cases of industrial interest.

The proposed project is suitable for a student curious about technological innovation and interested in carrying out a scientific investigation of blockchain technologies and applications. Within the proposed framework, ranging from theory to development, the PhD research plan can be adapted to the specific interests and expertise of the PhD student.

- urls for the above links:

http://tcs.unica.it/news/blockchain-day-stirling
http://fc17.ifca.ai/wtsc/
https://en.wikipedia.org/wiki/Vitalik_Buterin

Peter Ferry
Director
Wallet.Services
3 Lady Lawson Street,
Edinburgh
EH3 9DR

March 30th 2017

Statement of Support

Dear Sir or Madam,

this letter is to express support and interest for the research proposed in the PhD fellowship application to the CSM division the University of Stirling, entitled “DESIGN OF RELIABLE DECENTRALISED APPLICATIONS ON BLOCKCHAINS ” by Dr Andrea Bracciali.

Wallet.Services are an Edinburgh-based Scottish SME, founded in 2016. Its core business is to provide a simplified access to BCT through a highly scalable, validated, trusted, cloud 'Platform as a Service'. Such an approach manages risk and complexity, and allows users to focus on business model and innovation. Wallet.Services mission is key in strengthening the development of the Scottish fintech sector, as well as the broader eco-system that is, or will soon be, adopting BCT for their business, including large companies, banks, and governments.

Wallet.Services consider the research envisioned by this proposal of extreme relevance and timeliness and are interested in the potential results of the proposed programme, which might have an impact on our products. Wallet.Services are happy to collaborate on industrial use cases, providing our expertise and experience as in-kind contribution to the project (this can be roughly estimated in 10 man-hour/4 meetings per year – roughly equivalent to 5000GBP over the three years).

Please feel free to contact Wallet.Services for any further question you may have.

Kind regards,

Peter Ferry

UNIVERSITY OF LIVERPOOL

Dr. Davide Grossi

Department of Computer Science
Ashton Building
Ashton Street
Liverpool
L69 3BX

T 0151 7954245
E d.grossi@liverpool.ac.uk

www.csc.liv.ac.uk

Liverpool, Januari 6th 2017

Statement of Support

Dear Sir or Madam,

this letter is to express support and interest for the research proposed in the PhD fellowship application to the CSM division the University of Stirling, entitled “DESIGN OF RELIABLE DECENTRALISED APPLICATIONS ON BLOCKCHAINS ” by Dr Andrea Bracciali.

I am a senior lecturer at the University of Liverpool and my research focuses on smart technologies for coordination and cooperation. I consider the research envisioned by this proposal of extreme relevance and timeliness. I believe that the current proposal, if supported, could contribute substantially to a rigorous understanding of blockchain technologies and their deployment through Dapps development. I am most interested in interacting with the project and collaborate with the project partners on these themes.

I am at disposal for answering further enquiries you might have.

With kind regards,

Dr. Davide Grossi

Massimo Bartoletti
Università degli Studi di Cagliari
Dipartimento di Matematica e Informatica
Via Ospedale 72 — 09124 Cagliari (Italy)

March 31, 2017

Subject: **Statement of Support**

Dear Sir or Madam,

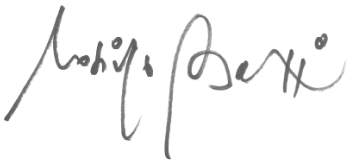
this letter is to express support and interest for the research proposed in the PhD fellowship application to the CSM division the University of Stirling, entitled "DESIGN OF RELIABLE DECENTRALISED APPLICATIONS ON BLOCKCHAINS " by Dr Andrea Bracciali.

I am a researcher at the department of Computer Science and Mathematics at the University of Cagliari, IT, where I lead a group carry out research on Blockchain Technologies. I believe that the research envisioned by this multidisciplinary proposal is extremely relevant, and I am interested in taking part to the proposed programme and in hosting the PhD student for a research visit on shared research themes.

If approved, this fellowship will foster and strengthen the developing international collaboration I am developing with Dr. Bracciali.

Please feel free to contact me for any further question you may have.

Kind regards,



(Massimo Bartoletti)

Siena, March 30th 2017

Statement of Support

Dear Sir or Madam,

this letter is to express support and interest for the research proposed in the PhD fellowship application to the CSM division the University of Stirling, entitled “DESIGN OF RELIABLE DECENTRALISED APPLICATIONS ON BLOCKCHAINS ” by Dr Andrea Bracciali.

I am a Full Professor at the Department of Economics and Statistics at the University of Siena, IT, where I carry our research on consensus in economics.

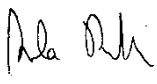
I believe that the research envisioned by this multidisciplinary proposal is extremely relevant and of interest for my work, and for possible future collaborations.

I am interested in contributing to the proposed programme via research collaboration, as appropriate.

Please feel free to contact me for any further question you may have.

Kind regards,

Prof. Nicola Dimitri



University of Siena
Piazza San Francesco, 7/8
53100 Siena
nicola.dimitri@unisi.it
+39 0577 232695