1st International Conference
on Mathematical Research
for Blockchain Economy

CONFERENCE PROGRAMME

6-9 May 2019
Santorini, Greece

Sponsored by

Imperial College Business School | Brevan Howard Centre for Financial Analysis

ASSETH

aventus

ORGANISERS

General Chairs
Yike Guo, Imperial College London
Panos M. Pardalos, University of Florida

Programme Chair
William J. Knottenbelt, Imperial College London

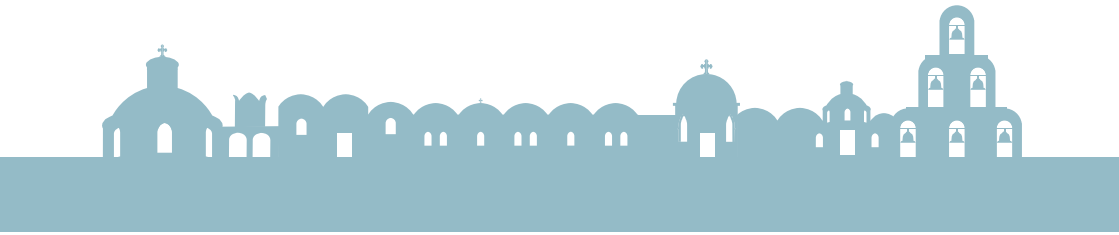
Organising Chair
Kai Sun, Imperial College London

Local Chair
Ilias S. Kotsireas, Wilfrid Laurier University

Finance Chair
Diana O'Malley, Imperial College London

Publicity Chairs
Anna Frankowska, Distributed Academy
Sam Werner, Imperial College London

Technical Programme Committee Members
John Conley, Vanderbilt University
Phil Godsiff, University of Exeter
Zeynep Gurguc, Imperial College London
Aggelos Kiayias, University of Edinburgh
Mario Larangeira, IOHK/Tokyo Institute of Technology
Robert Learney, Digital Catapult
Pedro Moreno-Sanchez, TU Wien
Catherine Mulligan, Imperial College London
Paolo Tasca, University College London
Andreas Veneris, University of Toronto
Edgar Weippl, SBA Research
Katinka Wolter, Free University of Berlin
Alexei Zamyatin, Imperial College London
Qipeng Zheng, University of Central Florida



CHAIRS' WELCOME

It is our pleasure to welcome you to the 1st International Conference on Mathematical Research for Blockchain Economy (MARBLE), being held in Santorini, Greece from May 6 to 9, 2019. In contrast to most blockchain conferences and forums which are dedicated to business applications, product development or ICO launches, MARBLE focuses on the mathematics and economics behind blockchain, seeking to bridge the gap between practice and theory. It aims to provide a high-profile, cutting-edge platform for mathematicians, computer scientists and economists to present latest advances and innovations in key theories of blockchain.

The call for papers solicited 24 research papers across a number of themes including incentives, governance, topological analysis, cryptoassets and security. Of the submissions, 15 were accepted for publication and presentation, and of the accepted paper, four of the top-ranked submissions have been chosen for consideration for the Best Paper Award, which will be presented in a special session and voted on by conference attendees. The winner will be announced during the conference banquet, which is to be held in the atmospheric setting of the Volcano Blue restaurant.

The technical program also features keynotes by the following distinguished speakers: Roman Beck, Jihan Wu, Ambre Soubrian, George Giaglis, Patrick McCorry and Garrick Hileman, and tutorials on the subject of smart contracts (Jerome de Tychey) and zero knowledge proofs (Alexandre Pinto). There is also an industry panel focused on the challenges of blockchain-led transformation of economies, which will be chaired by Naeem Aslam.

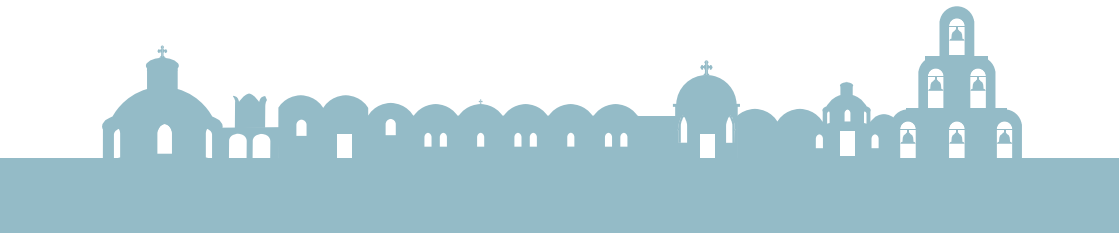
We thank all authors who submitted their innovative work to MARBLE 2019 this year. In addition, we thank all members of the Technical Programme Committee and other reviewers, everyone who submitted a paper for consideration, the General Chairs, Prof Yike Guo and Prof Panos Pardalos, the Organising Chair Kai Sun, the Local Chair Ilias Kotsireas, the Finance Chair Diana O'Malley, the Publicity Chairs Anna Frankowska and Sam Werner, and members of the Centre for Cryptocurrency Research and Engineering who have contributed in many different ways to the organisation effort, particularly Katerina Koutsouri and Lewis Gudgeon.

We are grateful to our sponsors, the Brevan Howard Centre for Financial Analysis, and Asseth for their generous support. Finally, we thank all participants of MARBLE 2019, as we rely on you to make this event interactive, engaging, and thought-provoking for everyone involved. We hope you will not only enjoy the technical programme but will also enjoy the social events including the conference reception, volcano tour and banquet.

William Knottenbelt
Programme Chair
Imperial College London

Yike Guo
General Chair
Imperial College London

Panos Pardalos
General Chair
University of Florida



MAP OF MARBLE 2019 LOCATIONS

Accomodation Information

Santorini Palace
Address: 84700, Firostefani, Santorini, Greece
Tel: +30 22860 22771

Splendour
Address: 84700, Firostefani, Santorini, Greece
Tel: +30 22860 21600

Dream Island
Address: 84700, Firostefani, Santorini, Greece
Tel: +30 22860 24122

Kafieris Apartments
Address: 84700, Firostefani, Santorini, Greece
Tel: +30 22860 22059

King Thiras
Address: 84700, Firostefani, Santorini, Greece
Tel: +30 2286 02388

Conference Venue Information

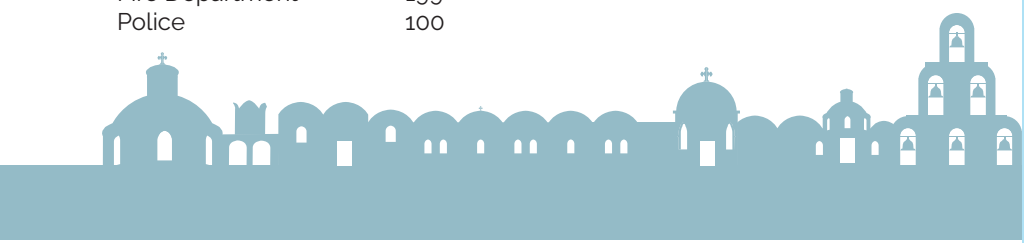
Petros M. Nomikos Conference Centre
Address: 84700, Firostefani, Santorini, Greece
Tel: +30 2286 023016-7

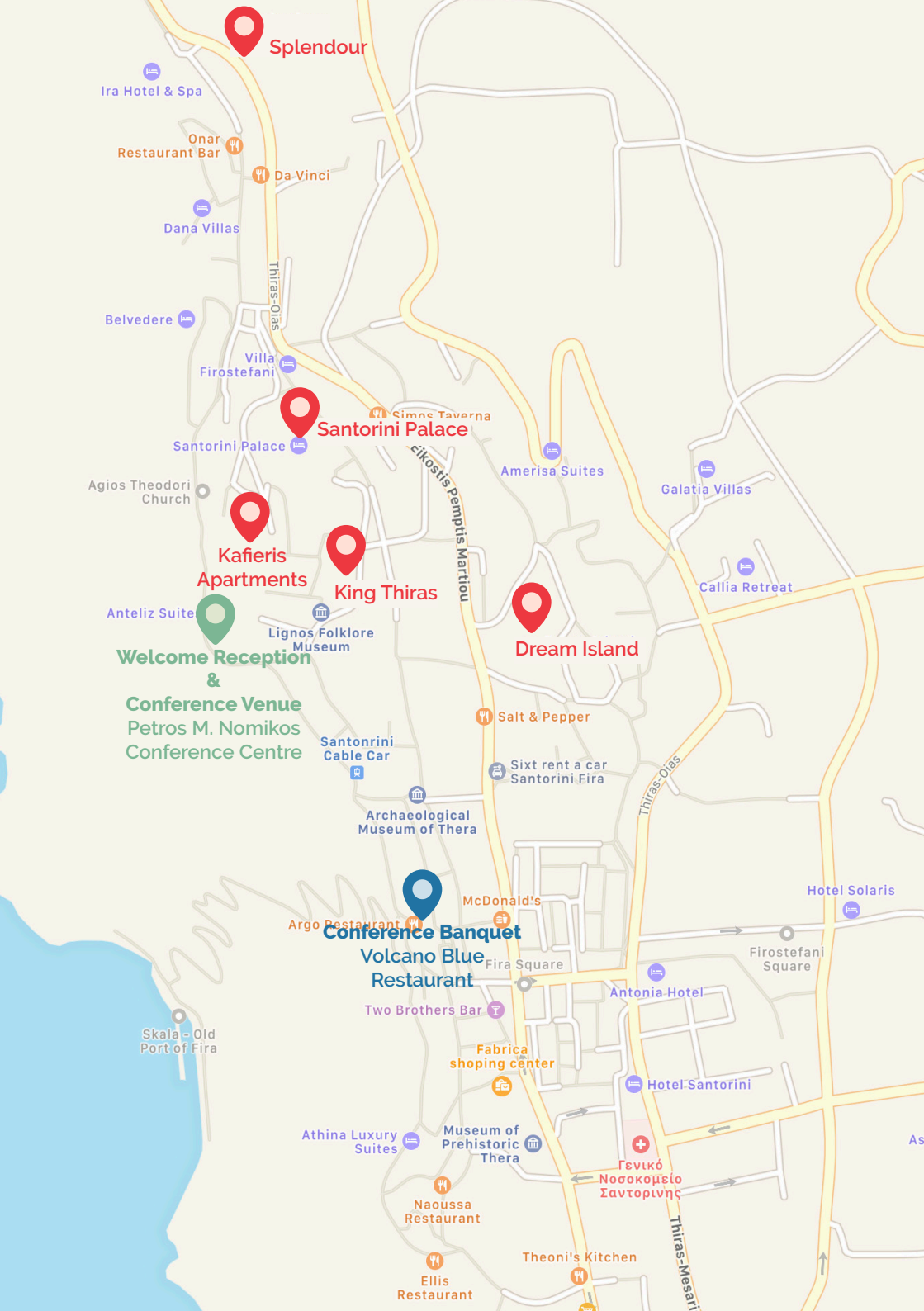
Taxis

Aegean Taxi Santorini	+30 21 5215 4000
Stathmos Taxi	+30 2286 022555
Santorini.cab	+30 2286 021858

Emergency Numbers

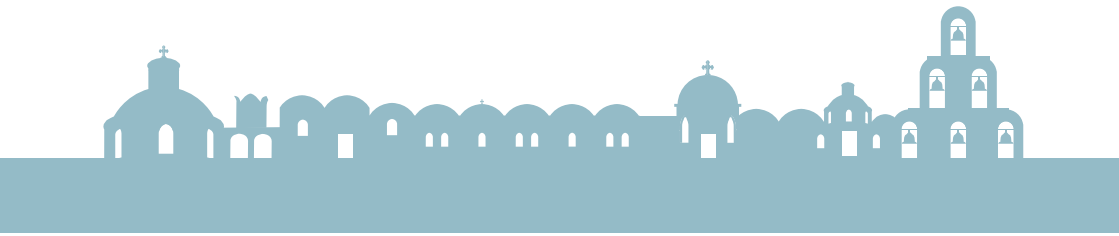
Emergency	112
Ambulance	166
Fire Department	199
Police	100



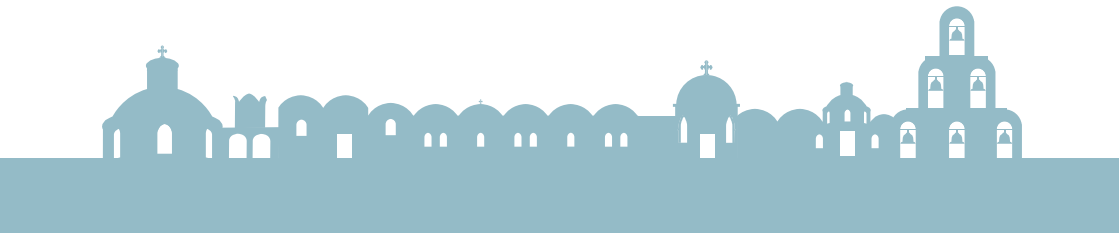

Splendour
Ira Hotel & Spa
Onar Restaurant Bar
Da Vinci
Dana Villas
Thiras-Oias
Belvedere
Villa Firostefani
Santorini Palace
Simos Taverna
Santorini Palace
Agios Theodori Church
Eikostis Pemptis Martiou
Amerisa Suites
Galatia Villas
Kafieris Apartments
King Thiras
Callia Retreat
Anteliz Suite
Lignos Folklore Museum
Welcome Reception & Conference Venue
Petros M. Nomikos Conference Centre
Dream Island
Salt & Pepper
Santonrini Cable Car
Sixt rent a car Santorini Fira
Archaeological Museum of Thera
Thiras-Oias
McDonald's
Hotel Solaris
Argo Restaurant
Conference Banquet
Volcano Blue Restaurant
Fira Square
Firostefani Square
Antonia Hotel
Two Brothers Bar
Skala - Old Port of Fira
Fabrica shoping center
Hotel Santorini
Athina Luxury Suites
Museum of Prehistoric Thera
Γενικό Νοσοκομείο Σαντορινης
Naoussa Restaurant
Theoni's Kitchen
Ellis Restaurant
Thiras-Mesari

CONFERENCE AGENDA

Time	Mon, 6/5/19	Tue, 7/5/19
8:30 AM		Registration and Coffee
9:00 AM	Registration and Coffee	Keynote Talk (Ambre Soubrian)
9:25 AM	Opening	
9:30 AM	Keynote Talk (Jihan Wu)	
10:00 AM		Paper Session (Cryptoassets)
10:30 AM	Keynote Talk (Roman Beck)	
11:00 AM		
11:30 AM	Coffee break	
11:35 AM		Coffee Break
11:40 AM		
12:00 PM	Best Paper Candidates Session	Keynote Talk (Garrick Hileman)
12:30 PM		
1:00 PM		Smart Contracts Tutorial (Jerome de Tychey)
1:30 PM		
2:00 PM	Lunch	Lunch
2:30 PM		
3:00 PM		
3:30 PM		
4:00 PM		
4:30 PM		
5:00 PM		
5:30 PM		
6:00 PM	Welcome Reception (Start)	
6:30 PM		
7:00 PM		



Time	Wed, 8/5/19	Thu, 9/5/19
8:30 AM	Registration and Coffee	Registration and Coffee
9:00 AM	Keynote Talk (George Giaglis)	Keynote Talk (Patrick McCorry)
9:30 AM		
10:00 AM	Paper Session (Incentives)	Paper Session (Security)
10:25 AM		
10:30 AM		
11:00 AM		
11:30 AM		Coffee Break
11:35 AM		
11:40 AM	Coffee Break	
12:00 PM	Zero Knowledge Proofs Tutorial (Alex Pinto)	Industry Panel (Chair: Naeem Aslam)
12:30 PM		
1:00 PM	Lunch	Lunch
1:30 PM		
2:00 PM		
2:30 PM		
3:00 PM		
3:30 PM		
4:00 PM		
4:30 PM		
5:00 PM		
5:30 PM		
6:00 PM		
6:30 PM		
7:00 PM	Conference Banquet (Start)	



PAPER SESSION PROGRAMME

Best Paper Candidates Session

Monday 6 May, 12h00-14h00
Chair: William Knottenbelt

- István András Seres, László Gulyás, Dániel A. Nagy and Péter Burcsi. **Topological Analysis of Bitcoin's Lightning Network**
- Kostis Karantias, Aggelos Kiayias and Dionysis Zindros. **Storage of Superblocks for NIPoPoW Applications**
- Richard Gardner, Philipp Reinecke and Katinka Wolter. **Performance of Tip Selection Schemes in DAG Blockchains**
- Nikos Leonardos, Stefanos Leonardos and Georgios Piliouras. **Oceanic Games: Centralization Risks and Incentives in Blockchain Mining**

Paper Session: Cryptoassets

Tuesday 7 May, 10h00-11h35
Chair: Katinka Wolter

- Stamatis Papangelou. **Digital Currencies: A Multivariate GARCH Approach**
- Aikaterini Koutsouri, Francesco Poli, Elise Alfieri, Michael Petch, Walter Distaso and William Knottenbelt. **Balancing Cryptoassets and Gold: A Weighted-Risk-Contribution Index for the Alternative Asset Space**
- Emmanouil Christoforou, Ioannis Emiris and Apostolos Florakis. **Neural Networks for Cryptocurrency Evaluation and Price Fluctuation Forecasting**
- Luis Montesdeoca and Mahesan Niranjan. **On comparing the Influences of Exogenous Information on Bitcoin Prices and Stock Index Value** (Short Paper)

Paper Session: Incentives

Wednesday 8 May, 10h00-11h40
Chair: István András Seres

- Sam Werner and Daniel Perez. **PoolSim: A Discrete-Event Mining Pool Simulation Framework**
- Paul Merrill, Thomas Austin, Justin Rietz and Jon Pearce. **Ping-Pong Governance: Token Locking for Enabling Blockchain Self-Governance**
- Arinjita Paul, Vorapong Suppakitpaisarn and Chandrasekaran Pandurangan. **Smart Contract-driven Mechanism Design to Mitigate Information Diffusion in Social Networks**
- Oguzhan Ersoy, Zekeriya Erkin and Reginald Lagendijk. **Decentralized Incentive-compatible and Sybil-proof Transaction Advertisement**

Paper Session: Security

Thursday 9 May, 10h00-11h30
Chair: Daniel Perez

- Dragos Ioan Ilie, William Knottenbelt and Iain Stewart. **Committing to Quantum Resistance, Better: A Speed-and-Risk-Configurable Defence for Bitcoin against a Fast Quantum Computing Attack**
- Subhasis Thakur and John Breslin. **Collusion attack from hubs in the blockchain offline channel network (TBC)**
- S. Sharmila Deva Selvi S, Arinjita Paul, Siva Dirisala, Saswata Basu and Chandrasekaran Pandurangan. **Sharing of Encrypted files in Block Chain Made Simpler**

KEYNOTE SPEAKERS

Jihan Wu

Jihan Wu graduated from Peking University with Bachelors' degree in both Economics and Psychology. Jihan is the first person to have translated the Bitcoin whitepaper into Chinese and subsequently co-founded 8btc.com, now one of the most popular Bitcoin news sites in China, in 2011. In 2013, Jihan founded Bitmain as the lead angle investor, director and Co-CEO, in charge of marketing, sales, investments and investor relations. Before this he was a financial analyst and investment manager of private equity fund of funds.

Decentralization and Centralization in PoW

Monday, May 6th
Chair: Yike Guo

Proof of Work (PoW) is a wonderful economic model which was reinvented by Satoshi Nakamoto to solve the double-spending problem without a central authority or without trust. It is PoW that made Bitcoin, the world's first cryptocurrency. Under the consensus mechanism of PoW, people are incentivized to create a real market economy based on open and fair competition. In this presentation, I will briefly describe PoW, its essence, its shortcomings and the factors that cause these shortcomings, resulting in lesser decentralization. Furthermore, I will also discuss some misconceptions about what causes centralization of PoW and the role of specialized hardware such as ASICs.

Roman Beck

Roman Beck is Professor at the BusinessIT department at IT University of Copenhagen. He is Head of the European Blockchain Center and Blockchain Summer Schools. Roman is Head of the Danish delegation to ISO TC 307 Blockchain & Distributed Ledger Technology standardization group and Convenor of ISO TC 307 WG5 Blockchain Governance standardization. He works as Blockchain expert for the EU commission and the German parliament.

Blockchain Market Engineering

Monday, May 6th

Chair: Panos Pardalos

The Bitcoin protocol illustrates the first prototype of a cryptographic economic system, which is organized both autonomously and distributive, without any point of central control or single point of failure. More precisely, it showcased the worldwide first economic system on autopilot, which might not only change the "Nature of the Firm", but also the nature of economic value creation and development itself, on the foundation of a digitally transformed economy. In this presentation, I will discuss current and future blockchain-based research trying to answer the question how we can engineer new markets and economies using blockchain.

KEYNOTE SPEAKERS

Ambre Soubrian

Ambre Soubiran is the CEO of Kaiko, a technology company providing market data to the digital assets space, currently covering all traded pairs accross 100+ crypto exchanges distributed over the world. Prior to joining Kaiko, Ambre spent eight years at HSBC in London and Paris, structuring equity derivatives and equity-based financing solutions, first in the Global Markets then in the Equity Capital Markets division. There, she was successively covering private banks, institutional, and corporate clients. She has been personally interested in cryptocurrencies since 2013, and has invested in a few tech start-ups in the fields of 3D printing, foodtech, and blockchain/crypto. Ambre holds a Bachelor and a Masters in Applied Mathematics from the Université Paris Dauphine. She has also studied Entrepreneurship and Management courses at the Solvay Business School in Brussels.

A New Measure of Crypto Asset Liquidity

Tuesday, May 7th

Chair: Sam Werner

Today we look at daily traded volume (based on transactional data on exchanges) and market cap (based on # of tokens * last price) but perhaps a more accurate indicator would be to look at the volume that is "at stake", based on order-book data. After introducing the notions of fluidity / viscosity, we see how the volume at stake changes vs. share price.

Garrick Hileman

Garrick Hileman is one of the world's most-cited cryptocurrency and blockchain technology researchers. He developed and taught the first UK class on blockchain technology at the University of Cambridge. Garrick is the author of a recently published stablecoins research study, the first University of Cambridge "Global Cryptocurrency Benchmarking Study" and the follow-on "Global Blockchain Benchmarking Study". He also created and published the CoinDesk "State of Bitcoin" and "State of Blockchain" reports from 2013-2016. He was ranked as one of the 100 most influential economists in the UK and Ireland and he is regularly asked to share his research and perspective with government organizations and the FT, BBC, CNBC, WSJ, NPR, and other media. He is currently the head or research at Blockchain, one of the world's largest cryptocurrency companies, and a researcher at the London School of Economics, where he also received his PhD.

Stablecoins: Design Principles, Incentives and Tradeoffs

Tuesday, May 7th

Chair: Stefanos Leonardos

The notorious volatility of digital assets has incentivized the creation of stablecoins, which are cryptocurrencies that are designed to minimize price volatility. This minimization of exchange rate volatility (most commonly against the US dollar) places stablecoins in stark contrast with bitcoin, which lacks an inbuilt price stability mechanism. Today, stablecoins are primarily used by cryptoasset traders to address market volatility. However, they also open up a number of new use cases (e.g., smart insurance) and are seeing demand where it is simply impractical or impossible to use national 'fiat' currencies (e.g., trust-minimized escrow). At present, the largest stablecoins are rather simplistic in design (e.g., US dollars stored by a trusted banking custodian), while more complex 'algorithmic' stablecoins have experienced growing pains (e.g., Maker Dai) or been abandoned (e.g., Basis). Have stablecoins been over hyped? This presentation will highlight key findings from a recently completed empirical study of stablecoins, along with a discussion of different stablecoin designs and their tradeoffs.

KEYNOTE SPEAKERS

George M. Giaglis

George M. Giaglis is the Director of the Institute For the Future (IFF) at the University of Nicosia, Cyprus. He has been working on digital currencies and blockchain applications since 2012, with his main focus being on new forms of industrial organisation and the sharing economy. George is one of the first academics to research and teach on blockchain, having: designed the curriculum of the world's first full academic degree on blockchain; led the development of blockchain credentialing technology that has resulted in the first ever publishing of academic certificates on the blockchain; taught on the disruptive innovation potential of blockchain, both at academic programs and in executive seminars worldwide; organised a number of prominent blockchain conferences and events.

What's next for blockchain research? From M2M commerce to self-sovereign identities for machines

Wednesday, May 8th
Chair: Dragos Ilie

The first wave of blockchain research, innovation and implementation has been under way for almost ten years now. Distributed ledgers have created new paradigms for disintermediated value exchange and, in the process, have given rise to (sometimes irrationally inflated) expectations about their potential impact to economy and society. Today, as we move toward a more in-depth appreciation of blockchain capabilities and limits, new research challenges arise that will demand the attention of the research community, as well as industrial practice, in coming years. In this talk, I will go through three such challenges, discussing ways in which they might influence our future research and technology development agendas:

1. Blockchain converging with other exponential technologies: As the fourth industrial revolution gets under way, we should expect more research to be devoted to the interplay of blockchains with other exponential technologies, most notably the Internet of Things (IoT) and artificial intelligence
2. Blockchain fueling a world of object identities: huge opportunity for paradigmatic shift exists in the ability of distributed ledgers, again coupled with IoT-based architectures, to create worlds in which we develop self-sovereign identities for objects and software. Such abilities will vastly redefine the limits of who (or what) can participate as autonomous agents in our future economy
3. Blockchain enabling new forms of industrial organization: with blockchain, we can start conceiving new notions that deviate from traditional paradigms for corporate structure, for example organizations that exist only as software, coordinating resources through smart contracting and operating autonomously from their human owners with pre-programmed business logic

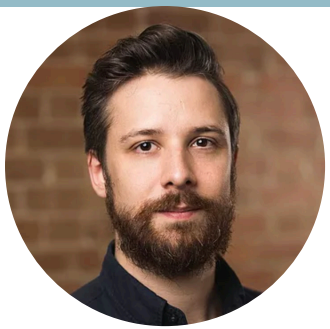
Patrick McCorry

Patrick McCorry is an Assistant Professor at King's College London. His focus is cryptocurrencies, smart contracts, cryptography and decentralised systems. Patrick is the UK's first PhD graduate in Cryptocurrencies and his work has recently appeared at Devcon3 & 4, Scaling Bitcoin 2017, Breaking Bitcoin 2017 and BPASE 2018 alongside numerous academic venues.

Scaling Cryptocurrencies via Off-Chain Protocols

Thursday, May 9th
Chair: Dan McGinn

Cryptocurrencies do not scale. Bitcoin supports around 7 transactions per second and Ethereum supports 14 transactions per second. The community are trying to scale the network by investigating new sharding and blockchain protocols. However by strictly increasing the network's throughput, it hinders the network's public verifiability as it reduces the diversity of peers with the computational power to verify transactions in real time (and thus hold the miners accountable). Off-chain protocols are an alternative scaling approach that simply reduces the network's load as parties transact amongst themselves instead of sending every transaction to the global network. Off-chain protocols are promising as they offer low/no fees and faster transaction finality. In this talk, we'll provide an overview of the off-chain protocol landscape and highlight future problems that must be solved before it can become a reality.



Smartcontracts, from Hello World to Basic Cryptoeconomics

Tuesday, May 7th
Speaker: Jerome de Tychey

Abstract: This tutorial is a hands-on introduction to the Solidity language for smart contracts on Ethereum. The attendees will deploy and interact with basic smart contracts. They will then interact with an application based on non-fungible tokens that illustrates how smart contracts can be used in the context of game theory.

Biography of the Speaker: Jerome is executive director at ConsenSys Solutions which helps organizations across the globe build, test, and deploy public and private blockchain applications. He has a background in economics and used to be an assistant professor at Sorbonne and Paris Dauphine. He jumped into the blockchain space in 2013 and has a particular interest in cryptoeconomics and mining. He founded and is the current president of Asseth which is the largest blockchain oriented non-profit in France. Asseth organises weekly free coding workshops and supports several education and research oriented initiatives.

Zero-Knowledge Proofs

Wednesday, May 8th
Speaker: Alexandre Miranda Pinto

Abstract: ZK-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) are an exciting area of cryptography that has recently generated much interest in the cryptocurrencies community. Although Zero-Knowledge proofs have been around since the 1980s, the first practical ZK-SNARK dates from only 2013, and shortly after, a variant thereof has been applied to the Zerocash protocol and the creation of the private cryptocurrency ZCash. In 2017, the Ethereum Foundation introduced support for the ZK-SNARKs used by ZCash at that time and interest in the technology is surging since then. This session will give a tutorial on ZK-SNARKs, including a high-level view of ZK-SNARKs and some mathematical background. The second part of the session will include a demonstration of the actual process of implementing a full ZK-SNARK journey, from the specification of the kind of statement to be proven, key and proof generation to the verification of a proof.

Biography of the Speaker: Dr Pinto graduated at the close of the 90s in Software Engineering from the University of Porto, Portugal. After some years as a professional developer, he went to grad school and earned a PhD in Computer Science from the same university, specializing in Cryptography and Complexity. Dr Pinto became a lecturer in software development and security, until he took an opportunity as a Post-Doc researcher with the Information Security Group in Royal Holloway, University of London. Currently, he works in the blockchain arena, developing , researching and writing to improve awareness of blockchain technologies and help other developers in this field.

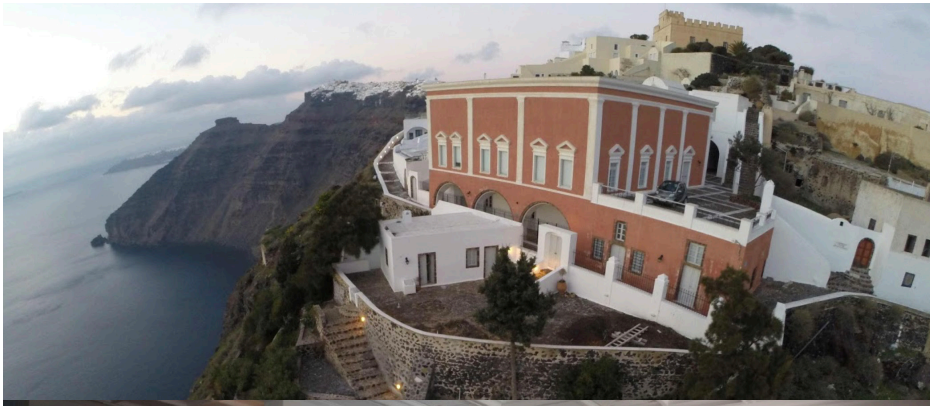
SOCIAL EVENTS

Welcome Reception - Monday, May 6th

Petros M. Nomikos Conference Centre

The MARBLE 2019 Welcome Reception will be held at the Petros M. Nomikos Conference Centre, located in the capital of Santorini, Fira, overlooking the caldera and the volcano. This neoclassical mansion with its characteristic red colouring has been transformed into a modern, operational Conference Centre, preserving its traditional character with its cellars, terraces, pots filled with flowers and parterres.

84700, Firostefani, Santorini, Greece
+30 2286 023016-7



Conference Banquet - Wednesday, May 8th

Volcano Blue Restaurant

The MARBLE 2019 Conference Banquet will be held at the Volcano Blue Restaurant, located on the cliff of Fira in Santorini and built on different levels to ensure uninterrupted views of the sea and the volcano at any table in the restaurant. The menu of Volcano Blue restaurant emphasizes in Greek seafood with fresh fish, and a wide variety of seafood, authentic Greek specialties and many suggestions for vegetarians.

84700, Firostefani, Santorini, Greece
+30 2286 022850

1st International Conference on Mathematical Research for Blockchain Economy

Sponsored by

Imperial College Business School | Brevan Howard Centre for Financial Analysis

A S S E T H

aventus