BLOCKCHAIN - BEYOND BITCOIN

CONFERENCE REPORT

Rustat Conference
Jesus College Cambridge
Thursday, 29 September 2016

Table of Contents

Conference report by Jordan Burgess

BLOCKCHAIN - BEYOND BITCOIN

Rustat Conference Agenda
Jesus College, Cambridge - Thursday, 29 September 2016

08.45-09.25 **Registration - Prioress's Room, Cloister Court, Jesus College**
Refreshments served. When moving to Upper Hall please take all bags and coats

09.30-09.35 **Welcome and Introduction - Upper Hall, Jesus College**
Professor Ian White *Master, Jesus College, Cambridge; Chair, Rustat Conferences*

09.35-10.10 **Keynotes**
Chair: Dr Garrick Hileman *Senior Research Associate, Cambridge Centre for Alternative Finance, University of Cambridge*
Dr Balaji S Srinivasan *CEO and Cofounder, 21; Board Partner, Andreessen Horowitz*
Professor David Yermack *Albert Fingerhut Professor of Finance and Business Transformation, New York University Stern School of Business*

10.15-11.15 **Session 1**
Central Bank Issued Digital Currencies, Impact on Banking
Chair: Jeremy Wilson *Vice Chairman, Corporate Banking, Barclays*
Cordelia Kafetz *Senior Manager, Future of Money Team, Bank of England*

11.15-11.40 **Break - Gallery, Upper Hall**

11.40-12.50 **Session 2**
The role of Government. Blockchain and Government Services. Pilot programmes and proving the concept. Government partnerships with private sector and academia
Chair: Iain Gravestock *Partner, Central Government, KPMG*
Nick Davies *Director, Universal Credit Programme, Department of Work and Pensions, DWP*
Dr Tom Wilkinson *Senior Data Scientist, Home Office*
Dr Anil Madhavapeddy *Lecturer, Cambridge Computer Laboratory; Engineer, Docker, Inc.*

12.50-13.50 **Lunch - Prioress's Room, Cloister Court**

13.50-15.00 **Session 3**
Blockchain applications beyond finance. The investor's perspective
Blockchain in energy sector: a trading platform for a new market. Humanitarian Blockchain
Chair: Richard Muirhead *GP OpenOcean*
Paul Ellis *CEO and Founder, Electron;* Jo-Jo Hubbard *COO, Electron*
Alejandro Julio *CEO and Founder, Humanitarian Blockchain*

15.00-16.00 **Session 4**
Blockchain and the law: accountability, responsibility and trust - who will regulate?
Governance of large, unregulated, decentralized systems. Privacy, identity and security
Chair: Alex Bulkin *Co-founder, CoinFund*
Simon Polrot *Lawyer, Fieldfisher LLP*
David Firth *Cryptographic Security Consultant, NCSC*

16.00-16.30 **Conference Close and Tea - Gallery, Upper Hall**

We thank the Bank of England, Fieldfisher and Cambridge Centre for Alternative Finance for their support.

#blockchain #Rustat @JesusCollegeCam
JESUS COLLEGE
CAMBRIDGE

RUSTAT CONFERENCES
JESUS COLLEGE
CAMBRIDGE

The Rustat Conferences is an initiative of Jesus College, Cambridge, and chaired by Professor Ian White FREng, Master of Jesus College. The conferences provide an opportunity for decision-makers from the frontlines of politics, the civil service, business, the professions, and the media to exchange views on the vital issues of the day with leading academics. Since 2009, Rustat Conferences have covered a variety of themes including: *The Economic Crisis*; *The Future of Democracy*; *Cyber Security*; *Financial Technology*; *Inequality*; *Manufacturing in the UK; The Future of Research-Intensive Universities; The Geopolitics of Oil and Energy; Drugs Policy; Organisational Change in the Economic Crisis; the Revolution in Cyber Finance; the Understanding and Misunderstanding of Risk; Food Security; Transport and Energy; the UK North South Divide; Superintelligence and Machine Learning.*

In addition to acting as a forum for the exchange of views on a range of major and global concerns, the Rustat Conferences provide outreach to a wider professional, academic, student and alumni audience through the publication of reports online. The conferences are held at Jesus College, Cambridge and are named after Tobias Rustat (d.1694), a benefactor of Jesus College and the University.

We thank the **Bank of England** and **Fieldfisher LLP** for their support of the Rustat Conference on Blockchain - Beyond Bitcoin. We thank the **Cambridge Centre for Alternative Finance (CCAF**) at the Cambridge Judge Business School for their collaboration.

Rustat Conferences Foundation Members
The Rustat Conferences are supported through a mix of sponsorship and a membership scheme that was launched in 2013-14 - see www.Rustat.org. We thank the Rustat Conferences Members for their generous support:

Dr James Dodd - James's career has concentrated on the founding, financing and governance of companies in the areas of telecommunications and technology. He studied physics at the universities of London, Oxford and Cambridge, and began his career in the areas of scientific and financial analysis for both government and industry. He serves on a number of boards and is active in supporting academic projects and charities.

Harvey Nash - is an executive recruitment and outsourcing group. Listed on the London Stock Exchange, and with offices across the world, we help organisations recruit, source and manage the highly skilled talent they need to succeed in an increasingly competitive and innovation driven world.

KPMG is a global network of professional firms providing Audit, Tax and Advisory services. It has more than 155,000 outstanding professionals working together to deliver value in 155 countries worldwide.

McLaren Racing Ltd has a reputation for efficiency and professionalism. Working within a fast-paced environment and to the highest standards, our highly skilled workforce operates primarily in the areas of manufacturing, engineering and race team as well as logistics and support.

Mr Andreas Naumann is a senior executive in the financial industry. Outside the professional sphere, he is keenly interested in subjects like urbanisation, youth unemployment, education and foreign policy. He supports the Rustat Conferences as a private individual.

Sandaire - Sandaire and Lord North Street came together in April 2014 to combine their businesses, both of which specialise in looking after the investment assets of very wealthy families, charities and endowments.

Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF CAMBRIDGE
Judge Business School

The **Cambridge Centre for Alternative Finance (CCAF)** is a research institute established within Cambridge Judge Business School, University of Cambridge.

The CCAF conducts research across three broad, yet interconnected, research streams:
I. **Online Channels and Instruments** including crowdfunding and peer-to-peer lending
II. **Credit Analytics** and new forms of data analytics to inform credit decision-making
III. **Payments Systems** and distributed ledger technology

CCAF is an internationally renowned centre of excellence, noted for its pioneering research in alternative finance. CCAF's benchmarking and industry reports are widely recognised as the most reliable, independent and comprehensive sources of information and market data in crowdfunding, peer-to-peer lending and other forms of alternative finance.

CCAF's research is made freely available to policymakers, regulators, industry practitioners, academia and the wider public via the CCAF website: www.jbs.cam.uk/ccaf

Since its inception in January 2015, the CCAF's funding has come from corporate donations, sponsored work, and contract work. We are an academic institute within the University of Cambridge and adhere to the principle of academic independence, while following stringent research ethic guidelines.

The CCAF has unparalleled capacity and reputation in the field of alternative finance, evidenced by the depth and breadth of its data depository, and its policy and media impact:

I. Data The CCAF has the world's largest data depository in alternative finance, with market data gathered from 1,200 + alternative finance platforms from across the Asia-Pacific region, the Americas, Europe, Africa and the Middle East. The Centre has also collected survey data from over 15,600 users of alternative finance and a granular level transactional database of 25 million micro-transactions totalling £1.2 billion.

II. Policy Impact The CCAF has engaged and is widely cited by a plethora of regulators and policymakers including: the *FCA, HMT, the European Commission, the World Bank, IDB, Bank of England, Hong Kong Monetary Authority, Singapore Monetary Authority, Malaysia Securities Commission, DFID-FSD, Kenya CMA, Uganda CMA, Rwanda CMA, Tanzania CMA, British Business Bank, BIS* and the *Cabinet Office.*

III. Press and Media The CCAF has been extensively covered in the media, including: the *Financial Times, Reuters, BBC, CNBC, The Economist, The Guardian, Bloomberg, The Times, The Independent, City A.M., Wired, Le Monde, Les Echos, Forbes, Der Spiegel,* the *Daily Telegraph* and the *Sunday Times.*

For information about the Cambridge Centre for Alternative Finance and the opportunities to collaborate in its research programmes, please contact:

Robert Wardrop *Exec Director, Cambridge Centre for Alternative Finance* r.wardrop@jbs.cam.ac.uk

BLOCKCHAIN - BEYOND BITCOIN

Rustat Conference - Jesus College, Cambridge
Thursday, 29 September 2016

EXECUTIVE SUMMARY

Background – Beyond Bitcoin

Blockchain is the technology that underpins bitcoin. It is a public ledger of all bitcoin transactions, visible to all and distributed among thousands of computers over the world. It is a computational proof of the chronological order of transactions, secure against attack as long as honest nodes collectively control more computational power than any cooperating group of attacker nodes.

Blockchain is also a new data structure, whose impact is expected to be far greater than that of bitcoin alone. Its potential applications include programmatic loans, bonds and payments; more efficient supply chains, and even identity management and verification. It is an emerging way for businesses, industries and public organisations to make and verify transactions and it is the cornerstone for enabling the next trillion devices to communicate and transact.

Its impact is likely to be a more open, transparent and publicly verifiable system that will fundamentally change the way we think about exchanging assets, enforcing contracts and sharing data across industries.

However, blockchain also presents an existential threat to our institutions. By design, no single institution should be able to control a public distributed ledger. We're seeing governments and industry attempting to co-opt the technology with private blockchains and centralised digital cash in order to control the market or protect the individual. Bitcoin operates outside the traditional rule of law, and for the first time we're beginning to see market competition to the traditional role states and financial institutions play. As societies fail or succeed based upon the quality of their institutions, this technology represents a disruptive force to the established world order.

Overview of the discussions

The conference brings together researchers and entrepreneurs developing blockchain technologies, with lawyers anticipating the legal implications, and figureheads from banks and governments. The day's events largely covered three main areas:

Applications of the blockchain

Bitcoin is the first application of the new internet infrastructure called blockchain. Bitcoin is viewed as digital cash, and a complement to fiat currency, specialising in transactions that are very small, very large, very fast, very international or very automated. This bitcoin ecosystem will likely be based around micropayments and information economy. Distributed

electronic cash, embedded within each device, is needed to enable the next machine-to-machine communication at a scale not possible with humans or the cloud.

Once payments happen at scale, we'll begin to see smart contracts denominated in the same tokens. This enables automated escrow, complex transactions and completely new types of financial instruments yet to be imagined.

Beyond finance, a distributed, immutable ledger can be used in other industries and for other types of goods. It can record provenance along a supply chain, or act as incorruptible proof of record. The privacy, legal and security implications of blockchaining the land registry or documents of identity remain underdeveloped. The blockchain can also be used for humanitarian purposes, with examples provenance trails reducing slavery, and distributed records protecting against authoritarian regimes. We're beginning to see how blockchain disrupts democracy, with communities of libertarians using it to create new forms of society, and new possibilities for social networks to turn capitalist.

The role of established trusted third parties

The invention of bitcoin was to remove the role of trusted third parties – they're "corruptible, uninformed, expensive and self-interested". However, many industries and banks are trying to co-opt the technology for their own needs with private blockchains they can control. There are potential benefits of this, such as removing the energy-intensive proof-of-work requirement, increased efficiency and automation, however, it remains to be seen how the centralised model survives. If everyone were given access to digital cash, one of the biggest roles banks play would be removed. In what capacity will banks survive in ten years?

Governance and legal implications

Governance of a blockchain is encoded in the open-source software that powers it and the will of the community that runs it. However, the design of bitcoin appears inadequately prepared for the game-theoretic considerations of decentralised management. There is a continuing struggle between making decisions that benefit the ecosystem, and the status quo that profits many of the decision makers. Furthermore, when the operational code is found to be inadequate, such as with *the DAO* hack, thousands of people may be harmed with little to no protection provided by any regulatory bodies. As this system operates outside existing jurisdictions, it is currently unclear what, if any, laws apply and how one could possibly achieve enforcement.

Reputation may substitute for regulation but we may also see systems that privilege certain third parties in exchange for increased protection of the customer. The challenge is to strike the balance between safeguarding the interests of participants and society at large, whilst not stifling innovation with excessively rigid structures. Ultimately, the market will decide which system it prefers.

BLOCKCHAIN - BEYOND BITCOIN KEYNOTES

DR BALAJI SRINIVASAN

CEO and Cofounder, 21; Board Partner, Andreesen Horowitz

While there are many developments of the blockchain technology that we can expect to see in the future, it will be a while before we transcend bitcoin. New coins, private blockchains, smart contracts all start with bitcoin as their reference. Therefore, it is important to first understand what is bitcoin is, what it is good for today and why it will be important.

What is bitcoin?

Bitcoin is a way to transfer rather than copy digital assets over the internet. It is a programmable digital representation of scarcity.

What is it good for?

While it was invented as a competitor to fiat currencies, bitcoin can be thought of as a complement to the existing system, specialising in transactions that are:

- **very large**: you can send $1M or more easily with Bitcoin with negligible fee
- **very small**: you can also send fractions of a cent (feasible with payment channels)
- **very fast**: you can send money and settle it such that the other party has full custody and can spend it within 60 minutes (much faster than typical SWIFT times, especially for international transfers)
- **very international**: you can send money across borders between any two parties with an internet connection
- **very automated**: you can programmatically send money without setting up a bank account

Any use case that hits two or more of those categories would be near impossible with the legacy financial system. For example, the world's first unbannable lottery: 100k people sending $1 worth of bitcoin to an automated smart contract address which selects one entrant to receive $100k of bitcoin. This has very small, fast international payments *in*, with very large, automated payments *out*. Even if jurisdictions would allow this to exist, with the existing infrastructure the wire fees alone would be prohibitive. This is an example of a new type of financial activity possible with bitcoin.

What is used for today?

The primary application today is speculation – which gets a bad rep but can be considered as "borrowing against the future to build the present infrastructure needed" - it's a great way to bootstrap the currency.

Speculation, like Google search, is a single player application. You don't need anyone in the vicinity to also be interested in it for it to work. Speculation was an excellent application in recent years, other than 2014, and has led bitcoin to a $10bn market cap. For a 'startup' founded in 2009, bitcoin's $10bn valuation compares favourably with Dropbox, Airbnb and Uber. The first blockchain unicorn is "bitcoin".

As the percentage *p* of people that have access to the technology increases, new applications become viable. When *p* reaches 25-50% we can have apps that rely on pairs of connections, p^2, such as payments in bitcoin, or Facebook and email on the internet. As we near full penetration, apps that rely on many-to-many interactions are possible.

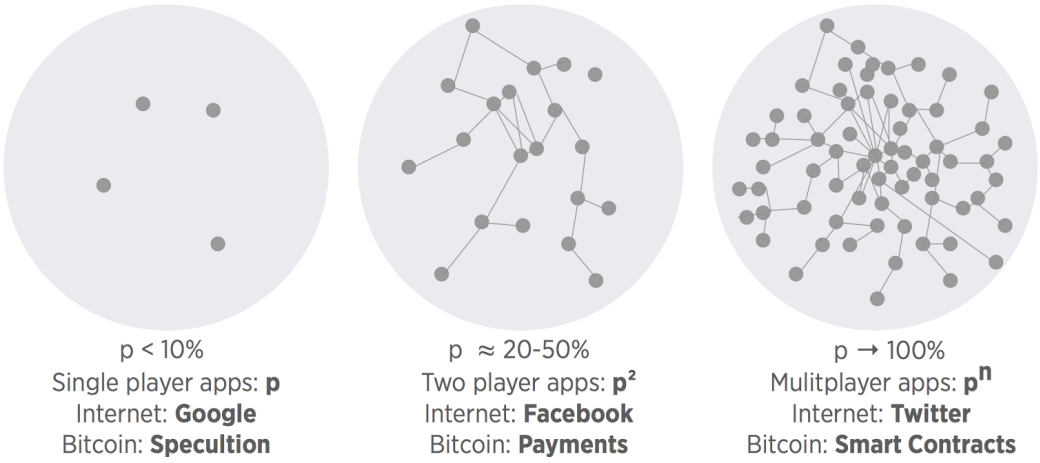


Figure 1 — Viable 'killer apps' depend on market penetration

Bitcoin will see adoption in the dead space of the current financial system. Not taking things that are already done and simply adding blockchain. VoIP wasn't *the* application of the internet because telephone calls already existed. Instead, it was the new technologies such as search and social, which were as the killer apps of the internet.

As contracts are an abstraction built over payments, we will need to see digital currency payments at scale before we see smart contracts. It is unclear if there's value in having contracts in a blockchain which refer to tokens outside the blockchain. We should expect that the first applications of smart contracts to be for use cases where traditional legal overheads would be prohibitive, such as machine-to-machine payments of around $10.

Why will bitcoin continue to be important?

Bitcoin is a gateway drug. All new blockchain tech starts with bitcoin as the reference:

- private blockchain – "bitcoin without the mining"
- IPFS ('inter-planetary file system') – "bitcoin with more data on the blockchain"
- ethereum – "bitcoin with better smart contracts"
- Zcash – "bitcoin with better financial privacy"

Every time someone hears one of these new technologies, they're also hearing about bitcoin. Even this conference: "blockchain – beyond bitcoin". All these new technologies begin with bitcoin interoperability – e.g. you buy ethereum with bitcoin.

What would be necessary to 10x bitcoin's market cap?

Bitcoin's price comes from market balance. Price boost would come from people buying bitcoin and never selling and this would only be the case if there was a bitcoin economy. By nature of the current users, who are distributed about the world, likely means it will be digital economy. The fact that they have varying, but small balances, likely means it will be

micropayments. The fact that early adopters are information workers and those interested in fintech, likely means it will be an information-work based economy.

DAVID YERMACK

Albert Fingerhut Professor of Finance and Business Transformation, New York University Stern school of Business

Financial economics is at a real turning point, more important than in 1973 when Black and Scholes took finance into a new mathematical paradigm. We've seen a soft takeover of finance by information systems departments, which for many is a rude awakening forcing us to adapt. For people in the real world, this is a very threatening time.

> *In 10 years, probably half the big banks will be gone and stock exchanges may be either closed altogether or greatly reduced in size – David Yermack*

There were two events that happened this summer, each in their own way raises troubling questions about the nature of assets in the digital economy.

Bitfinex hack

In August 2016, one of the largest bitcoin exchanges, BitFinEx had 36% of its bitcoin stolen from its accounts, worth $60 million. As a response, the firm performed an effective *bail in*. They mutualised the loss such that all depositors lost 36% of their deposits, replaced with some IOU tokens if the exchange recovers. However, as bitcoins are uniquely identifiable, it is not unreasonable to ask "did they get mine?". Democracy of users would have voted against this yet the 'benevolent dictator' decided what was "fair". As a customer, who could you complain to? What court could you bring this to? And even if the court decided in your favour, who would ensure enforcement? It's a legal void.

Satoshi (Nakamoto - the name used by the person who designed bitcoin) architected these systems to be beyond the reach of sovereign states. This creates a competition between the existing system of law and this new type. But this hack is an example of one of many things that will go wrong to which there is no good answer. We'll be thrown back into a 19th century world where private organisations make their own rules and their reputation defines whether they attract customers or not.

The DAO hack

The DAO was one of the first examples of a decentralized autonomous organization. A 'robot venture capitalist' which received over $160mn in ethereum tokens. Despite the code being audited by the community, an unintended vulnerability allowed hackers to automatically 'invest' a third of its fund into their own accounts.

After the hack, the Ethereum community voted to perform a hard-fork – rewinding the blockchain to the day before the vulnerability was exploited.

This move was controversial. It violated almost every principle behind the technology. Blockchain and DAOs are supposed to be immutable with no possibility of human intervention. Around 15% of the community refused to go along with the hard fork on principle, affirming "code is law" and that any mutation sets a bad precedent. So they carried on the blockchain with the lost funds. So we now have two versions of ethereum, ETH (ethereum) and ETC (ethereum classic) – like having the pope in Rome and in Avignon.

The DAO

The DAO is the first example of a decentralised autonomous organisation (DAO) on the ethereum blockchain. It is a investor-directed venture capital fund with no conventional management structure or board of directors. Instead, it is managed through code ("code is law") and the voting of its investors.

In May 2016, the DAO raised over 160 million USD of ether (14% of all ether tokens issued) from over 11,000 investors – making it the largest crowdfunding project to date.

In October 1929 there was bad day of the stock exchange. What percentage of traders would have voted for a do-over? Had that happened the stock exchange may have dropped even more when it reopened. Humans deciding to interfere and rewrite the rules on the fly discredits the Ethereum project. The same thing could probably happen on *any* blockchain. Who has the authority to do this? What's the threshold for deciding how to do this? And if you're victimised by this decision, who could you apply to for relief?

What law applied and how do you get enforcement?

Architecture is done by brilliant engineers and computer scientists, but they didn't talk to enough economists and lawyers. Right now, with bitcoin, the block size needs to increase to handle the growing number of transactions. However, it's been impossible to get consensus as there's an entrenched group of people profiting from the current system.

Rather than modify bitcoin, we'll likely need to invent a future platform with a better understanding of game theory and incentives.

The issue with mining

A proof of work of guessing random numbers with no greater social purpose is a real issue. There's not enough electricity in the world to take the current bitcoin platform to any significant scale. To get 10x its current value, we would require a lot more power.

"Currently about 350 megawatts according to my own calculations, which is roughly equivalent to the electricity demand of 280,000 American households."

What do blockchains look like in the future?

The enemy of Satoshi is a trusted third party – they're corruptible, uninformed, expensive and self-interested. The classic blockchain is open-source network which anyone can join with no gatekeeper to control entry/exit. However, the model that seems to be taking hold, recreates many of these problems it was trying to solve. In industry we're seeing governments and banks trying to co-opt the technology for their needs. We're seeing permissioned blockchains that they can control. The *R3* consortium contains about 50 banks by invitation only. This looks like a cartel, which government should potentially be opposed to with regards to consumer protection – only market competition will reverse this powerful trend.

DISCUSSION

The discussion was joined with Session 1, and is in the following section.

SESSION 1: IMPACT ON BANKING

CORDELIA KAFETZ

Senior Manager, Future of Money Team, Bank of England

This roundtable is called "Blockchain Beyond Bitcoin". The Bank of England first starting researching these topics in 2014 looking at the economics of digital currencies and innovations in payment technologies. We published two Quarterly Bulletin Articles in 2014 which concluded that non-fiat digital currencies did not pose a risk to monetary and financial stability in the UK, at that time. However the increase in digital innovation, in particular distributed ledger technology, had the potential to transform elements of the financial system and reopened an old debate over who should have access to electronic central bank money.

Since then the Bank has been expanding its work on the impact of FinTech on our objectives of maintaining monetary and financial stability. In June 2016, in his Mansion House speech, Governor Mark Carney set out the five initiatives the Bank was working on. The Governor publicised the Bank's FinTech Accelerator which is working with FinTech firms to help solve central bank questions and announced the extension of RTGS to Payment Services Providers.

The speech also referred to our ongoing research on central bank digital currencies, where in extremis everyone could have access to electronic central bank money. The speech noted that on some levels this is appealing. For example it would mean people have direct access to the ultimate risk-free asset. In its extreme form, it could fundamentally and perhaps abruptly re-shape banking.

Broad access to electronic central bank money, via CBDC, is, if at all, many years away. As Deputy Governor Ben Broadbent noted in his speech in February 2016, it raises some important questions that will take many years to research. Key areas the Bank is seeking to explore include:

- If people took money out of commercial banks into a central bank:
    - Could this cause a run on commercial banks?
    - Would this be a good thing if it made the commercial banks less important in the payment system?
    - Will a market emerge for credit provision? A central bank would be unlikely to lend to small businesses and households.
- Money markets
    - Is there a monetary stability benefit of broadening access to the central bank's balance sheet?
    - What would be the impact on companies that hold gilts if we exchange gilts for central bank money?
    - Who would have incentives to come into the market and provide accounts for a central bank digital currency?

- Legal and regulatory questions around how to determine identity digitally – required if giving access to CBDC and who would have responsibility for anti-money laundering and know your customer checks.
- Distributed systems concerns:
    - Is a distributed ledger necessary for a central bank digital currency?
    - Bitcoin mining is costly and inefficient. It is possible to have a permissioned distributed ledger but there are lots of questions over which consensus mechanism it would use and what this means for scalability?
    - Privacy. How can we have a resilient ledger and ensure that those that have copies or access to the ledger cannot see commercial or private information?

In Feb 2015, the BoE publicly announced that it had embarked on a multi-year research programme on these issues and in July 2016 published a detailed research agenda.

http://www.bankofengland.co.uk/research/Documents/onebank/cbdc.pdf

We are looking for more academic collaborators as we want diversity of thought on these wide ranging topics.

JEREMY WILSON

Vice Chairman, Corporate Banking, Barclays

We could be facing such fundamental changes as a result of this technology not just to business models, but models by which society interacts, that we're going to need some form of governance. Blockchain technology is fundamentally changing the nature of money. If this runs amok, the coherence of how society operates could be undermined.

Alongside regulators, central banks are charged by society to make sure nothing goes wrong. They will need to work *with,* not against, the distributed way things operate otherwise it will just happen without them. We should also understand that the big infrastructures which everything operates won't change quickly because democratic governments and elected officials move slowly by design. Dictatorial regimes can run with this technology as quickly as possible to the extent it helps them.

Barclays understands that this is an existential issue – but it equally understands that it is a custodian of people's money. It has to keep pace with what is going on, but not lose sight of that responsibility.

As we move forwards, it will become apparent that we have changed the way that an individual is identified. The old method of identification is the passport which contains just a few pieces of key information. Detailed records are given to specialists only: health records to doctors, finances with banks. This is what society is comfortable with. We are now transitioning to world where due to data sharing, we can accumulate it all in one place. We can get a near minute-by-minute account of someone's actions. This change has significant implications for civil liberties and the privacy of the individual and we should expect a scandal at some point soon which will cause the custodians of the safety of society, the government, to take note. We can't anticipate this or we'll stifle innovation, but we need be ready for the fact that this will cause us to face some critical issues in society and how governance and government should operate.

DISCUSSION OF KEYNOTE TALKS AND SESSION 1

Adam Wethered asked **how are central banks and tax collectors cooperating to centralise what the tech is trying to decentralize**. The BoE are having informal sharing groups with other central banks on a regular basis and it was noted that the heads of the world's central banks are well informed about distributed ledger technology.

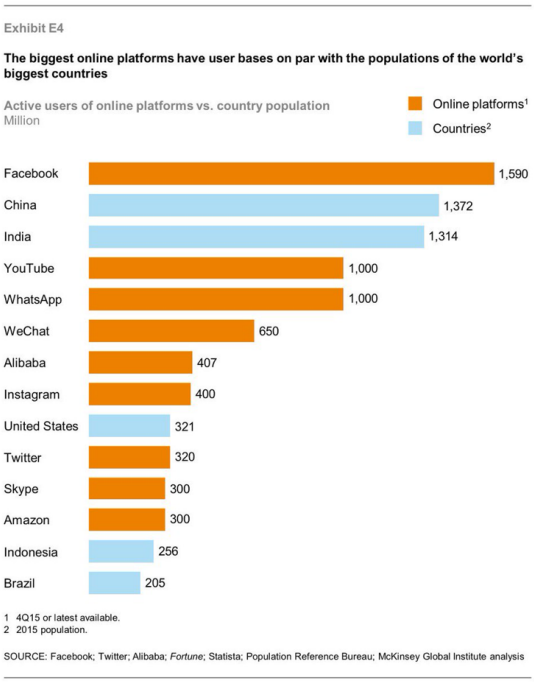
Jeremy Wilson wondered **if any increasing political fragmentation (Brexit / Trump) is going to threaten this co-operation?**

Generally, there was no expectation that it would. Fintech is forcing regulators to do a better job and communicate with each other more.

Balaji Srinivasan divides the Trump/Brexit phenomena into 3 groups of people:

- **Nationalists** – broadly anti-pluralistic people who want to return to the "glorious past";
- **Bureaucrats** – want to hang on the status quo (/improve it gradually);
- **Technologists** – those who want to go to the future as quickly as possible.

The technologist's viewpoint is less appreciated. By population, Facebook is now bigger than China. But economically, Facebook generates $1-10 per-person per-year, whereas China makes $1000/person and the US $10 000.



This shows internet hasn't gotten started yet – we have 100 to 1000x the headroom for monetisation of these massive online populations. Right now these people are liking, tweeting, poking for no remuneration. In the next 10 - 20 years, digital currencies are going to become the lubricant for people to trade digital goods and consulting time. The social networks will transition to capitalist networks. They'll start monetising beyond $100 and $1000 per person and will become serious competitors to nation states — but with distributed models. They will become one of the earliest focal points for digital currency and blockchain – governments will react to that and we're starting to see that now.

Alejandro Julio brought up the topic of Zcash, a new coin with far higher standard of privacy and anonymity to bitcoin. **What's the role of central banks when cash is completely untraceable?**

The panel discussed many legitimate reasons for wanting financial privacy but accepted that this opens up new avenues for nefarious transactions – cash however is still the dominant means for financing crime and terrorism.

David Yermack brought up a 20 year old paper 'Money is Memory' with the thesis that money is only valuable because we believe someone obtained it for doing something valuable. Zcash seems to contradict that. If I can't track it, and authenticate it, how do I know it's real? Why would I accept it? This raises some philosophical questions over what money is.

Jon Crowcroft asked **why banking/centralisation is going to survive**. Changes happening exponentially quicker and disintermediation is what the internet is all about, pointing out the disintermediation of music companies by iTunes, and film companies by Netflix. Wilson emphasized that this tech is a much more fundamental risk than telephones/VOIP. It could affect all our lives.

Discussing what survival for the banks might look like, David Yermack thinks the central banks' best survival strategy might be in introducing a sovereign digital currency. In general, the role of banks will shrink, expecting this to be great for consumers, potentially good for tax collecting but bad for bankers and awful for auditors.

Balaji Srinivasan suggested a model where central banks become like the postal service; USPS still exists but email is where most of the action is. More and more transactions will be done online and the internet technologies will scale. China might have the only government able to stop digital currencies in their tracks because they censor the internet, but generally governments do not have the incentives to do this.

Tim Bird suggested that banks could become custodians of our tokens, identity. Jeremy Wilson agreed. Banks recognise this existential threat and are looking now at their core competencies. Most people "trust banks to keep the information confidential". However, history shows that most dinosaur enterprises die.

Xen Baynham-Herd expects we'll see a debundling of banking tasks by fintech.

SESSION 2: ROLE OF GOVERNMENT

NICK DAVIES

Universal Credit Programme, Department of Work and Pensions (DWP)

Why should government be involved in blockchain technology?

There is a fundamental (re)distributive function in government. Not just financial redistribution, but the distribution of law, defence and infrastructure. The blockchain, which enables new paradigms for distribution, should therefore be a major concern to government.

Government works with the will of people, but with policies in mind. Job seekers allowance is provided to achieve the policy of supporting individuals and their family when they're out of work. Our current method of distribution, through fiat currency, does not meet our policy objective in most cases. Most claimants immediately withdraw the payment in cash. If this is stolen or used for self-destructive habits, this is a policy failure. Furthermore, as many do not use a bank account, individuals pay a 'poverty premium' (around at £1300 / year) for only using cash. This is failure of government.

We need smarter money that is used for what the policy intends. This doesn't mean food stamps, but we should consider that 'benefit pound' could go further with less spent on being poor.

There's plenty of innovation in mobile wallets, so is blockchain necessary? We need to research this. Crucially, the technology used is irrelevant if we don't get people to use it. DWP initiated a beta program of mobile payments, which recorded any transactions on a blockchain. Making data available to government when required should improve the relationship between government and citizen and lead to better policy outcomes.

We don't want to repeat mistakes of internet era. It took 10 years since the advent of the world wide web for tax inspectors to have internet access and another 10 to develop a digital service. We also need to be much more imaginative: "digitalisation" was considered putting a paper form on a screen. We should take this opportunity not just to consider how to improve what we currently do, but to rethink the whole business of governance. We need to look to the future of a fully blockchain enabled world and work back from that.

How do we get to that position? Talking about the Government's attitude to blockchain is probably a category error. We need more trials that tap into social and government issues. Leadership can and should come from private sector initially, with Government being a fast follower once we've figured out the use. A bigger public policy debate needs to be triggered, so that concerns that this technology throws up are considered by ministers.

TOM WILKINSON

Senior Data Scientist, Home Office

Government does more than just redistributing wealth; it has a fundamental role as an arbiter of relationships – providing the rule of law. Blockchain is naturally relevant for mediating P2P relationships.

We're not actively developing implementations, but we are questioning the implications of blockchain for use cases, such as:

- **Data protection**: securing systems against attack e.g. could evidence chains be made incorruptible?
- **Provenance**: secure traceability in supply chains, e.g. could blockchain enable trust in the origin of food?
- **Land registry**: even if there was an incorruptible record, how would one allocate property in the first place?
- **Educational attainment**: preventing people misrepresenting themselves would provide value to society. Government already does so indirectly through fraud laws, but we question whether blockchain could do a better job? In this case though, who keeps a list of valid institutions, and does this render the decentralisation through blockchain redundant? Could decentralised mechanisms, complementary to blockchain, do the same job of identifying trusted awarders and penalising grade inflation/misrepresentation - like negative feedback from tracking how well individuals go on to perform?
- **Identification**: many peer to peer interactions rely on trusting particular individuals, and this makes unique accountable IDs essential. Could blockchain tech prevent

capture of ID by private monopolists (as might be favoured by the current openID model), through mechanisms like Web of Trust?

- **Generally:** it seems complementary decentralised mechanisms might be needed for these P2P applications.

Still, why should governments be involved at all, if everything is going to happen in a decentralised way? Even with the 'inevitable disintermediation' of various services, where we're reducing the cost of transacting, there's potential for monopoly to emerge. This is because there is a danger that the network effects with any entity that intermediates P2P interactions will lock users into that system. This entity can potentially start charging rents and it is a responsibility of government to prevent rent-seeking behaviour.

But once government is looking after it, why not use single central database? Ignoring the issue of corruption, there are strong arguments which suggest that a single decision maker is not well placed to steer a complex system. For similar reasons to why we separate monetary policy from Government to avoid political incentives interfering in the short term, there's reason to decentralise things on the blockchain while working with development teams to decide not how to steer the system, but how the system can steer itself. 'System stewardship', as proposed by the Institute for Government, is putting the rules in place such that people behave in a way that steers society along a desirous path - an extension of what laws and courts already do.

DR ANIL MADHAVAPEDDY

Lecturer, Computer Laboratory, University of Cambridge; Engineer, Docker Inc.

How did savant hackers 40 years ago build the internet network of over a billion hosts? With open source technology. They define a policy on how the software can be used and give it away for free. If the technology is useful, others will take it, embed it in their products and build an 'economies of code' network effect.

The hacker ethos is as follows:

- "fail fast, succeed faster" – run experiments as quickly as possible;
- "move fast and break things" – seek forgiveness not permission;
- solve problems that you have today, without pre-agreeing on the thing you want to build;
- and crucially, leave behind code.

The open source community is creating a huge amount of innovation by putting blockchain technologies into the fabric of machine-to-machine (M2M) communication. Within the last year, we've released open source technology based around making all M2M communication using distributed ledgers; we've made 'immutable infrastructure', so that we have a complete provenance trail for every line of code; we've seen extremely accurate dynamic pricing; and individually mathematically verifiable components through unikernels.

The cloud is almost a lost battle these days for full decentralisation. Microsoft, Amazon and Google have a defendable oligopoly on developer attention with their cloud APIs. The next frontier for decentralisation is your own personal data – but this doesn't involve talking to you, but talking to the cloud of devices around you. They form a shell around you that talks to other systems and acts as your representative online.

Blockchain is looking at M2M communication for the next trillion devices because It is simply impractical to expect a single cloud provider to ever scale to these levels. We're fundamentally limited by the speed of light. If my Internet-of-Things pacemaker goes wrong, I want it to react within milliseconds, rather than wait for a response from the cloud.

Humans will never scale to the speeds we're working at. The open-source community is building blockchain-based technologies that can create decentralised services with the same experience as large centralised services but are delay-tolerant, with highly secure, non-critical individual nodes and a framework to support mechanised contracts. Bitcoin enables completely new approaches that we should experiment with. We could instantly invent new coins, give every individual their own currency. We could encode social capital and tie it to every interaction online.

It is extremely important that as we're building prototypes, that failures leave behind code artefacts which can be built upon for the next experiments. Internet succeeded through open source. The uncountable failures in trying to build distributed systems, cloud services etc. paved the way for the next experiments to succeed.

As we build self-organising consortia, I encourage everyone that's building these systems, in academia, private industry and government, to not try to build a big framework. Instead find a simple, cheap intellectual property framework that allows the use of existing off-the-shelf technologies. Then find the grassroots hackers and empower them to build a network effect around the system you're building. They'll be many failures, but keep it open source, leave residues in the technology and overall there will be success.

DISCUSSION

Asked how government is going to change over the next ten years, Nick Davies replied that continuity in the institutions is required for Government to function. The institutions that make up Government – ideas of personal freedom and rule of law – go back centuries and tamper with those at your peril. Yet technology is already doing so. Government should look out 10 years hence and consider what role does the Government need to take up when the world is behaving like Anil described.

Irene Ng brought up the difficulty of modularising transactions. Transactions happen because of a resource need, however the remodularisation needed to enable it is not trivial. For example, overstretched new parents may decide to bring in a nanny, but to do so they have to remodularise how they deal with the baby so that the nanny can take on tasks.

Anil Madhavapeddy: the bad news is that when you sign up to online services, you implicitly agree to over 100 SLAs between distributed services and that network of dependencies is only getting worse. The good news is that, our knowledge of programming languages and how to mechanise this has improved. The next generation of blockchain technologies can run code directly in the fabric of the currency – so we can modularise transactions in the way we modularise source code. We should be concerned about bugs, but our ability to reason about software mathematically is also improving.

Tom Wilkinson: As the transaction rate increases between mechanical agents, some of which belong to you, there's a difficulty in checking your preferences for these interactions. With our current legal architecture, you'll be liable for your avatars. We're asking for people to encode their preferences for possible eventualities in a way that the machines can then reference when they interact with each other. People not capable of giving the recipe are therefore risking loss of agency.

Discussing identification, Nick Davies brought up the idea that ID is the new money. If you're convinced who someone is, all you need to know is that they're good for it. Maybe we have blockchain from birth? Tom Wilkinson pointed out that Facebook is already guaranteeing ID through a 'web of trust'. It's very hard to fake your trail of online transactions – so putting people on the blockchain may not be necessary.

Anil pointed out that there's a massive flaw in the idea that we have a single online identity. The internet is based around the idea of rapidly created pseudonyms and tying them together creates a resilient identity graph of who you are.

Tom pointed out that the internet works pseudonymously because we have an effective legal infrastructure behind it based on the idea of having a single fixed identity. A criminal record follows you around. If everyone suffered as few repercussions as a YouTube commentator, civilisation would collapse rapidly.

SESSION 3: APPLICATIONS BEYOND FINANCE

RICHARD MUIRHEAD

General Partner, OpenOcean

Comparing blockchain, we're still very early. On one hand people we have people looking for the killer application that will take off, and on the other hand we have people doing extraordinary things with the technology – we're still waiting for that moment when they come together.

PAUL ELLIS AND JO-JO HUBBARD

CEO and Founder, Electron; COO, Electron

There are parallels between the financial service industry and the energy sector. Both are heavily regulated, highly competitive, and carried out on common physical and virtual infrastructure. However, whereas the financial sector recognises being a custodian of records as a core task, the energy sector does not. As such the finance industry appreciates the threat and opportunity of blockchain technologies, whereas energy industry does not (yet). Nevertheless, the earliest non-trivial use case for blockchain are as likely to be in the energy sector as in financial services.

Central service monopolies

The energy sector has de jure monopolies in order to maintain their central shared infrastructure, such as settlement and switching services. However, effort has to be spent on regulating what these companies can do and charge. A consortium blockchain could be more efficient, innovative and cheaper to operate, enabling competitively priced service based on usage and the ability to retrofit economic benefit for good behaviour.

Club goods

	Excludable	Non-excludable
Rivalrous	**Private goods** food, clothing, cars, parking spaces	**Common-pool resources** fish stocks, timber, coal
Non-rivalrous	**Club goods** private parks, cinemas, satellite TV	**Public goods** free-to-air TV, air, national defence

Goods are categorised *private*, *public*, *club* or *common*. Most work on blockchain has focused on private goods. There are other types of goods where blockchain may offer interesting mechanisms for transactions which should be explored.

Electron is developing a trading platform for a club good: *demand-side response capacity* – a scheme in which energy consumers are incentivised to turn down or shift their energy usage to provide flexibility to the grid and lower the cost of operating the system.

This service is increasingly important as supply is becoming more and more inflexible, intermittent and distributed due to the increase of renewable energy sources such as solar and wind, and electricity demand will increase due to electrification of vehicles and heating. Rapid growth targets have been set for this market in the UK: although only 5% of grid balancing services come from the demand side right now, targets have been set for >30% by 2020 and >50% by 2030.

Blockchain is well placed to address the challenges of this industry because:

- transparency: market requires full collaboration between players therefore a public ledger will allow the customers to trust the value allocation method
- flexibility: blockchain makes it easier to evolve methods of value allocation between participants as the market itself evolves
- competition: a service operated by competing consensus nodes removes i) the risk of monopoly rent-seeking behaviour and ii) incentives to create competing trading venues that would fracture liquidity

Question for discussion: is it easier to create a blockchain platform in a completely new market, or more difficult without the pre-existing infrastructure and protocols?

JULIO ALEJANDRO

Founder and CEO, Humanitarian Blockchain

What are the world's most successful use cases of blockchain for humanitarian, social, and political purposes in developing countries and for ethnic minorities?

- Provenance.org is solving slavery in Indonesia's fishing industry.
- Taqanu: world's first bank for refugees.
- Agriledger famine in Kenya, Myanmar, and Papa Guinea.
- Alice.io homelessness in London.
- Libertarian Tiffany Haden the Flint, Michigan water crisis affecting Black Lives Matter.

Where are these ideas brewed, projects manufactured? Those regarding violence and systems of intangible injustices –as White supremacy or islamophobia- not within Fintech or Bitcoin meetups, but within "Intentioned Communities".

- World's largest is the Free State Project, with 2,000 crypto-libertarians residents in New Hampshire.
- BitNation largest Blockchain online community.
- Anarchast & Free Talk Live their media channels.

Vinay Gupta, Susanne Tarkowski, Jeffrey Tucker are recognised as their Blockchain political gurus. Common topics of conversation: holocracy vs democracy; voluntary decentralisation versus forced forms of association; multiple reputation digital identities versus legal biometrics.

Banks and Fintech – despite their knowledge of economics - tend to disregard or ignore the three core philo and axiological foundations of Blockchain ecosystem and technology.

- Friedrich Hayek's "spontaneous order", "distributed use of knowledge", and his price theories are Austrian basics to Bitcoin, entrepreneurship, and scalability.
- Milton Friedman "Social Market" approach towards the poor and oppressed is of common concern in Ethereum N.O.M.A.N.-like groups in London.
- Ayn Rand "natural law" theory, important in Smart Contracts. Her laissez-faire approach on Silk Road dark market and the right to disassociate ("to discriminate") and oppose your "nationality", government, system of law, of trade, or of ethno-religious identity is compatible with her theory of selfishness and rational decision-making objective mechanism.

Alejandro also mentioned his three "failed" Blockchain for refugee project/pilots: Blockchain in Calais four "liberating technologies", e-Salam geo-location token card, and Match and Teach Me for Social and Cultural Integration, which was shortlisted in the Top 20 out of 1,600 by MIT University with the United Nations in October 2016.

DISCUSSION

Xen Baynham-Herd asked how these technologies could potentially be used negatively. Alejandro said he has travelled and lectured in thirty cities and universities this year and asked the audience "Apart from ISIS trading Bitcoin & dark market activities, are you aware of any extremist group/individuals using it for evil?".

He said those audiences aren't aware and government regulation upon nonexistent cases will only hinder entrepreneurship and innovation. He referred to Hayek's theory.

However example, 'D'Apps' (decentralised apps on the ethereum blockchain) could be eventually used to create social media posts that are impossible to remove, which could be used for SEO, national security leaks, or revenge porn.

Richard Muirhead asked whether Electron will develop their own coin. Paul talked about creating a token that represents capacity that is to be turned off. The vision might be to later automatically verify on the blockchain that that capacity has been turned down.

SESSION 4: BLOCKCHAIN AND THE LAW

ALEKSANDR BULKIN

Cofounder, CoinFund

Crypto assets are new and very subtle and hardly anyone is more concerned with these subtleties than the regulators. This last panel is to discuss the law and governance of blockchain.

SIMON POLROT

Lawyer, Fieldfisher

Studying the legal issue around bitcoin and blockchain as a whole is a big area as there are many diverse use cases. On blockchain, the saying goes that "code is law" but that does not mean the use cases are beyond legal territory; this only refers to fact that the transactions are executed automatically by the code on the blockchain.

There have not yet been many adaptations of the law to the blockchain, so we are trying to look at how the existing law may be applied for certain use cases; and what can we propose so that other use cases can be applied in real life.

This raises the following legal questions:

- **Cyptocurrencies:** How should we define bitcoin? As an asset, as money? Regulators are observing closely and things are changing quickly in the field. E.g.: most states now require exchanges to collect the identity of the purchasers.
- **Blockchain as proof**: using inscriptions on the blockchain to prove something in the real world raises issues over how to demonstrate to a judge what the data means and how to link it to your identity.
- **Smart contracts**: automated crowdfunding, DAOs, automatic escrow, prediction markets are complex use cases with many legal issues. We may be able to proceed by analogy for some use cases, however a specific regulatory framework seems desirable.

Significant obstacles:

- **Identity**: many uses cases require linking transactions on a pseudonymous blockchain to a real identity. Private solutions (e.g. uPort) may become a future standard.
- **Regulations**: lack of regulation will hold back established companies from deploying new models, yet true disruptors will prefer to face potential penalties (c.f. Uber and Airbnb)

Regulations are often to protect people. With The DAO, a lot of poorly-informed investors were hurt for not really understanding what they were getting into and the risks involved.

DAVID FIRTH

Cryptographic Security Consultant, National Cyber Security Centre (NCSC)

Blockchain is currently very popular in government as a possible solution for providing services which may be better, cheaper, more efficient. NCSC's focus is to be ready to give security advice to governments considering blockchain projects.

What's weird about bitcoin:

- first crypto technology that if you were building a system to attack it, would literally pay you to do so
- the proof of work of finding hashes with leading zeros is worthless
- miners are building up the precisely the same hardware as that which would be used for 'recovering' hashed passwords

NCSC are looking at the implications of using a distributed ledger for:

- **Land registry**: possible benefits for transparency, efficiency, constraining the rules on how land can be traded, and a hands-off approach to running the service. Similarly, it could be applied to passports and driving licences.
    - What's the balance between transparency and privacy? Land trades public? Driving test failures not public? If selective transparency, you have to share keys and then one would have to manage public key infrastructure (losing claims of efficiency)
    - By owning the service, Government is in a privileged position to be able to print new paper to make new identities, such as for witness protection programs. Blockchain would remove that privilege.
- **Provenance solutions**: for example, tracking meat from cow to supermarket.
    - Only true up to the interface between the digital statement and the physical reality.
- **Smart contracts:**
    - They're not contracts but code. Evaluating code is *very* difficult, even with something very constrained, yet alone code which is nearly Turing-complete.

For many use cases the need is for a better database, not necessarily a distributed ledger. And the extra infrastructure costs of using a distributed ledger with immutable history may be overkill.

Finally, a note on the fragility of cryptography. Putting things on immutable ledgers, even if encrypted, should be considered vulnerable to the future. SHA-256 seems likely to survive but 10 years ago we probably would have said the same about SHA-1. Sane people expect a practical quantum computer within a lifetime. Private information may lose its privacy and that should be prepared for.

DISCUSSION

David Firth discussed the implications of a viable quantum computer. A lot of bitcoin relies on public key signatures, therefore a quantum computer would be able to sign things on your behalf. A bad guy would keep this secret, yet even a public release would undermine all

confidence in the system. NCSC are looking in to post-quantum encryption schemes, but haven't evaluated their viability.

Discussing The DAO hacker(s), Simon Polrot said that they acted in bad faith, therefore are enough legal grounds to charge. David Firth contested whether it was lawful to reverse the code? Code runs as intended and it was checked by the community. Simon: When you sign an agreement, you don't agree precisely on every detail but to the intent. You have bad faith judgments that can be determined by a judge. The hacker didn't only execute the code, but exploited a weakness in the code.

What's your advice to a lawmaker or policy maker of what they should do now?

More and more uninformed individuals are entering into this scheme so it may be the time to have a look at what's going on. Not harsh measures to try and stop it, which would be counterproductive and hinder the development of the technology. The main issue is that cryptocurrencies laws are trying to reinvent the wheel. If you buy bitcoin, it's essentially the same asset as buying gold – there are a lot of regulations about buying gold that you're not allowed to give when buying bitcoin. It's not easy because bitcoin is a free network that anyone can join without any relation to an authority, but most happen through exchanges that are lightly regulated.

Aleskandr Bulkin concludes the day:

We started the day with the question 'what is money', then approached 'what is government?' and 'what is law?'. The mere fact that we're asking these fundamental philosophical questions again after thousands of years of thinking about them and thinking we have the answers, is indicative of the significance of this technology.

Public blockchain technologies are the first class of "hybrid technologies": containing a combination of technology and human motivation and willpower in a non-trivial way. They possess a kind of primordial motivation of their own, which makes us wonder where this is going.

BLOCKCHAIN - BEYOND BITCOIN

Rustat Conference
Thursday, 29 September 2016

Speaker and Chair Bios

Professor Ian White Master, Jesus College, Cambridge and Chair, Rustat Conferences
Prof Ian White is currently Master of Jesus College, van Eck Professor of Engineering, and Head of Photonics Research at the Department of Engineering, University of Cambridge.

He gained his BA and PhD degrees from the University of Cambridge, in 1980 and 1984. He was then appointed a Research Fellow and Assistant Lecturer at the University of Cambridge before becoming Professor of Physics at the University of Bath in 1990. In 1996 he moved to the University of Bristol as Professor of Optical Communications and became Head of the Department of Electrical and Electronic Engineering in 1998, before returning to the University of Cambridge in October 2001. In 2005 he became Head of the School of Technology and subsequently Chair, leaving the School of Technology to take up the position of Pro-Vice-Chancellor for Institutional Affairs in 2010.

Ian is a Fellow of the Royal Academy of Engineering and of the Institution of Electrical Engineers and the Institute of Electrical and Electronics Engineers. He is an Editor-in-Chief of Electronics Letters, has published in excess of 250 journal papers, and received the Aron Kressel Award from the Institute of Electrical and Electronics Engineers in 2011. He is a co-founder of Zinwave Ltd and PervasID Ltd.

Julio Alejandro CEO, Humanitarian Blockchain
Julio Alejandro, the"Leonardo da Vinci of Fintech" (CoinTelegraph, 2016), is the Founder and CEO of Humanitarian Blockchain, an e-governance and human rights consultancy, and the current US & UK Foreign Correspondent of Excelsior, the largest Mexican newspaper. He has appeared on Fox News, Foreign Affairs and The New Statesman. He frequently lectures in North American, European and British universities (LSE) and institutions (Google), and has undertaken globalisation and immigration studies in Sciences Po (Paris) and Cambridge. He lives in London.

Tim Bird Partner, Fieldfisher
Tim Bird is a partner in Fieldfisher's top ranked corporate and tech practice working with companies of all sizes and stages of development from startups to global consolidators. He focuses on tech transactions involving M&A or fund raising and a lot of his clients are tech consolidators in the US or Japan. In recent years Tim has been spending an increasing amount of time with companies in the FinTech sector and he regularly mentors at Barclays' FinTech accelerator at Rise London.

Alex Bulkin
Alex has 13 years of experience in developing pricing, risk management, and high-frequency trading software at Goldman and Sachs Group, Inc. Holding a dual degree in Mathematics and Computer Science from New York University and a Masters Degree in Organizational Psychology from Process Work Institute in Portland, Oregon, Alex bridges technological insight with social science and psychology. He is passionate about social innovation and integrative multidisciplinary thinking.

Paul Ellis CEO, Electron
Paul Ellis is the CEO of Electron, a blockchain company focused on applications in the Energy market. After a degree in Physics from Imperial College and a spell in the military, Paul spent 13 years in investment banking working in debt capital markets and structured derivatives. He then set up MTL, a fintech incubator and software development business. He subsequently founded and ran CreditTrade, a global interdealer electronic trading platform for credit derivatives. After the sale of CreditTrade he became Head of Europe and Asia for MarketAxess, an institutional e-trading platform, before taking up his current position.

Iain Gravestock Partner, KPMG
Iain Gravestock is a Partner in KPMG's Government and Infrastructure (G&I) practice. As a member of the G&I Leadership team Iain is constantly looking for new capabilities and ideas to take to his clients.
Iain joined KPMG from the Civil Service where he worked in a Technology role as a Mathematician. After qualifying as a Chartered Accountant he has pursued a career in Central Government helping his clients deliver benefits and improvements by implementing new systems and solutions often involving commercial and technological innovation. In this role, Iain has led KPMG's contribution to major multi-year programmes in HMRC, FCO, DCMS, the Valuation Office Agency and other Agencies. He know leads KPMG's relationship with the Department of Work and Pensions (DWP) and is interested in the use of technologies such as Robotic Automation, Cognitive, Predicative Analytics and Blockchain in increasing the efficiency, effectiveness and customer experience of delivering public service outcomes.

Dr Garrick Hileman Senior Research Associate, Cambridge Centre for Alternative Finance
Dr Garrick Hileman is a Senior Research Associate at the Cambridge Centre for Alternative Finance and a Researcher at the Centre for Macroeconomics. He was recently 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 the FT, BBC, CNBC, WSJ, Sky News, and other media. Garrick has been invited to present his research on monetary and financial innovation to government organisations, including central banks and war colleges, as well as private firms such as Visa, Black Rock, and UBS. Garrick has 20 years' private sector experience with both startups and established companies such as Visa, Lloyd's of London, Bank of America, The Home Depot, and Allianz. Garrick's technology experience includes co-founding a San Francisco-based tech incubator, IT strategy consulting for multinationals, and founding MacroDigest, which employs a proprietary algorithm to cluster trending economic analysis and perspective.

Jo-Jo Hubbard COO Electron
Jo-Jo Hubbard is the COO of Electron. Her background in energy comes from four years of renewable & cleantech merchant banking at Augusta & Co, over which period she watched renewable assets climb out of the speculative market and land on the balance sheets of pension funds. She then spent a couple of years investing in cleantech and software as a service for a private fund and, most recently, worked as a management consultant at McKinsey, specialising in digital & the consumer journey. She studied English Literature at Christ Church, Oxford.

Cordelia Kafetz Future of Money Team, Bank of England
Cordelia manages the Future of Money team at the Bank of England. She is responsible for the Bank's research on the future of cash, central bank digital currencies and distributed ledger technology. Prior to taking up this role last year, Cordelia has 10 years of experience in banking regulation, supervising a number of retail banks throughout the financial crisis.

Dr Anil Madhavapeddy University Lecturer, Cambridge Computer Lab; Engineer, Docker, Inc.
Anil Madhavapeddy is a University Lecturer at the University of Cambridge, based in the Systems Research Group, and an engineer in Docker, Inc. He was on the original team that developed the Xen

hypervisor, and also founded Unikernel Systems (Computer Lab Company of the Year 2016), later acquired by Docker. Prior to obtaining his PhD, Anil had a diverse background in industry at NetApp, NASA and Internet Vision. He founded and directs the OCaml Labs group at Cambridge, and leads the MirageOS unikernel project, and is involved extensively with open source projects such as OpenBSD and OCaml.

Richard Muirhead GP OpenOcean

OpenOcean is a European fund focusing on software at the Series A. Its five partners started and/or scaled MySQL, MariaDB, Nokia's mobile ad business, Automic, Tideway and Orchestream. OpenOcean's current portfolio includes Truecaller, Nosto, and Rapidminer. Richard led their investment in Dataloop and HeavenHR.

Richard co-founded Firestartr, a seed investment firm (Adbrain, ClusterHQ, Gojimo, Peak, Tray.io and Yoyo). Richard is an angel investor/advisor (Citymapper, Fanatix, Acunu (Apple), Radiant Minds (Atlassian) and Pusher). He led Pantera's investment in Bitstamp. With EQT he bought Automic, with around €150m revenue and double digit growth, the world's largest IT automation company. He joined/built a board of Henning Kaggerman (SAP), Mäns Hultman (Qlik), Bernard Bourigeaud (Atos) and served as Interim CEO. From 2002 to 2009 he was founder, chairman & CEO of Tideway, now a category-leading part of BMC. Richard was EIR at the establishment of Accel Partners. Co-founder, President Orchestream with a $1.4Bn IPO, now a category-leading part of Oracle. He established the Moscow office of Monitor Company. He is a We Are Family Foundation governor and WEF Technology Pioneer. MA Eng from Cambridge, Australian/UK citizenship. He rowed for Cambridge, GB and South Australia. He is 3/7ths of an Ironman™ triathlete. He is married to a Norwegian, two daughters.

Simon Polrot Lawyer, Fieldfisher

As a lawyer working with Fieldfisher LLP in France, Simon Polrot provides assistance on legal and tax issues. He has been interested in the blockchain technology since 2012, particularly with respect to its legal and tax issues and opportunities and has developed specific expertise in this field by bringing together his legal training and actual practice of the blockchain technology. He advises clients on specific legal and tax issues relating to blockchain use cases, with a specific focus on contract law, corporate law, rules governing evidence and taxation. He has also developed a prospective approach on the possible adaptation of the law to this technology. In this perspective, he created in 2016 the leading French website on Ethereum, ethereum-france.com, on which he notably publishes articles about law and tax-related issues on the blockchain.

Dr Balaji S. Srinivasan CEO 21.co; Board Partner, Andreessen Horowitz

Balaji S. Srinivasan is the CEO of 21.co and a Board Partner at Andreessen Horowitz. Prior to taking the role of CEO at 21, Dr. Srinivasan was a General Partner at Andreessen Horowitz. He was named to the MIT TR35, was the cofounder and CTO of Founders Fund-backed Counsyl, and taught a MOOC with 200k students at startup.stanford.edu. He holds a BS, MS, and PhD in Electrical Engineering and an MS in Chemical Engineering from Stanford University.

Dr Tom Wilkinson Senior Data Scientist, Home Office

Tom graduated in maths from Magdalene College, Cambridge and has a PhD in complexity economics at Cardiff. His research modeled the macroeconomy through centralised, hierarchical, and decentralised, peer to peer, enforcement of agreements. To make this empirical he also wrote on the philosophy of science and statistics within economics, and this led him to machine learning. He joined government as an applied mathematician, founded the government practitioners network around machine learning, and then became the first Home Office data scientist. "Since joining government I've been promoting the agenda of understanding decentralised alternatives to our civic institutions, like bitcoin. I became a named contributor to the Chief Scientist's report, proposed and coordinate the Community of Interest for Distributed Ledger Technology".

Jeremy Wilson Vice Chairman, Corporate Banking, Barclays
Jeremy Wilson is Vice Chairman, Corporate Banking, responsible for engagement at Board or ExCo level with Barclays' major corporate and institutional customers, for Barclays' representation on industry initiatives, and as a representative of the financial services sector on global and regional industry bodies. Prior to assuming this role Jeremy Wilson was responsible for the operational banking needs of Barclays financial institution business and, before that, of the large corporate clients at the Group's Head Office. He also worked in the group's credit risk unit following 10 years overseas - in the United States, as personal assistant to the Chairman of Barclays' principal subsidiary; in Vanuatu, as manager of Barclays finance centre interests there; and in Australia, as a corporate account executive. He began his career at Barclays as a graduate of Durham University on the group's Management Development Program.

He is also Chairman, Barclays Bank Egypt; Chair, UK Government Engagement & Advisory Group; Chair of the Banking Industry Environment Initiative Working Group; and a Trustee of a number of charitable Trusts covering the banking industry and education in the UK and overseas. He is also Chair of the Whitechapel Think Tank, established as a vehicle for government, regulators and the private sector to consider issues arising in the emerging distributed ledger and related blockchain eco-systems.

Jeremy Wilson has been Chair of Bloomsbury Publishing PLC; a Director of TheCityUK and Chair of TheCityUK Audit Committee; Chair of CHAPS Clearing Company Limited; Chair of BAFT; a Board Director of BAFT and Chair of BAFT Nominations Committee; a Chair of the Barclays Group Credit Committee, a Director of Barclays Pension Funds Trustees Limited, a Director of the Bankers' Benevolent Fund , Chair of the International Finance Conference (IFC) and Co-Chair of BAFT Europe Council. He was born in South Africa, brought up in Kenya, and now lives in England. He is married with four children.

David Yermack Albert Fingerhut Professor of Finance and Business Transformation and Chairman, Finance Department, New York University's Stern School of Business
David Yermack is the Albert Fingerhut Professor of Finance and Business Transformation and Chairman of the Finance Department at New York University's Stern School of Business, where he has been a member of the faculty since 1994. He is also an Adjunct Professor of Law at the NYU School of Law, Director of the NYU Pollack Center for Law and Business, and a Research Associate of the National Bureau of Economic Research law and economics program.

Since 2014 Professor Yermack has co-taught a full semester course at NYU on digital currency and blockchains, the first course of its type offered by a major research university.

In addition to his recent research on blockchains and digital currencies, Professor Yermack has published some of the most cited papers in the fields of executive compensation and corporate governance. He has also written papers on such diverse topics as options in baseball player contracts, incentive compensation for clergymen, tobacco litigation, fraudulent charitable contributions, CEOs' mansions, and the fashion industry. Professor Yermack was awarded AB (1995), MBA (1991), JD (1991), AM (1993) and PhD (1994) degrees, all from Harvard University. He has been appointed as a visiting professor at 12 international universities, a visiting scholar at the Federal Reserve Banks of New York and Philadelphia, and has given invited research seminars at more than 100 universities and institutes worldwide.

Participants - Rustat Conference on Blockchain - Beyond Bitcoin
Jesus College, Cambridge - Thursday, 29 September 2016

Julio	Alejandro	*Founder and CEO*	*Humanitarian Blockchain*
Prof Jean	Bacon	*Cambridge Computer Laboratory; Fellow*	*Jesus College, Cambridge*
Xen	Baynham-Herd	*MD*	*UBS*
Tim	Bird	*Partner*	*Fieldfisher*
Dr Aeron	Buchanan	*Head of Research & Development*	*Ethcore*
Aleksandr	Bulkin	*Co-Founder*	*CoinFund*
Jordan	Burgess	*Queens' College, Cambridge*	*Rustat Conference Rapporteur*
Scott	Burgess	*Assisting Rustat Conferences*	*Rustat Conferences, Jesus College, Cambridge*
Jonathan	Cornwell	*Director, Rustat Conferences*	*Jesus College, Cambridge*
Prof Jon	Crowcroft	*Marconi Professor of Communication Systems*	*Computer Laboratory, University of Cambridge*
Nick	Davies	*Director, Universal Credit Programme*	*DWP Department of Work and Pensions*
George	de Courcy-Wheeler	*Deputy Chief Investment Officer*	*Sandaire; Rustat Conferences Member*
Peter	Deming	*Director*	*Warburg Pincus*
Paul	Ellis	*CEO and Founder*	*Electron*
Jess	Ferguson	*Head of Art*	*Everledger*
David	Firth	*Cryptographic Security Consultant*	*NCSC*
Christina	Frankopan	*CEO*	*Protozoa*
Dr Phil	Godsiff	*Senior Research Fellow, Surrey Centre for the Digital Economy*	*Surrey Business School, University of Surrey*
Rayan	Goutay	*Regulatory Advisor*	*Lykke Corp UK*
Paul	Graham	*Partner*	*Fieldfisher*
Iain	Gravestock	*Partner, Central Government*	*KPMG*
Helen	Harris	*Communications Manager*	*Jesus College, Cambridge*
Dr Garrick	Hileman	*Cambridge Centre for Alternative Finance*	*Judge Business School, University of Cambridge*
Jo-Jo	Hubbard	*COO*	*Electron*
Dr Tudor	Jenkins	*Director*	*WideEyedVision*
Cordelia	Kafetz	*Senior Manager, Future of Money Team*	*Bank of England*
Robert	Kay	*CEO*	*GovCoin Limited*
Sheharbano	Khattak	*Research, Security Group, Computer Laboratory*	*University of Cambridge*
Dr Anil	Madhavapeddy	*Lecturer, Computer Laboratory; Engineer, Docker Inc.*	*University of Cambridge; Docker Inc.*
Dr Cecilia	Mascolo	*Computer Laboratory, and Fellow, Jesus College*	*University of Cambridge*
Richard	Muirhead	*GP*	*OpenOcean*
Daniel	Murrell	*Co-Founder*	*Duo Money*
Prof John	Naughton	*Emeritus Professor of Public Understanding of Technology, OU; Senior Research Fellow, CRASSH*	*University of Cambridge*
Prof Irene	Ng	*Professor of Marketing and Service Systems; Director, International Institute for Product and Service Innovation*	*Warwick University, Warwick Manufacturing Group*
Dr Grant	Passmore	*CEO; Life Member, Clare Hall, Cambridge*	*Aesthetic Integration*
Simon	Polrot	*Lawyer*	*Fieldfisher*

Dr Jat	Singh	*Senior Research Associate, Computer Laboratory*	*University of Cambridge*
Dr KC	Sivaramakrishnan	*Research Associate, Cambridge Computer Laboratory*	*University of Cambridge*
Dr Balaji	Srinivasan	*CEO and CoFounder 21; Board Partner, Andreeseen Horowitz*	*21.co*
Andrew	Stanger	*Financial Accountant; Assisting Rustat Conferences*	*Privilege Finance*
Peter	Walker	*Director*	*Capita Asset Services*
Dr Adrian	Weller	*Senior Research Associate, Computational & Biological Learning Lab*	*Dept of Engineering, University of Cambridge*
Adam	Wethered	*Senior Adviser; Rustat Conferences Member*	*Sandaire*
Prof Ian	White	*Master, Jesus College; van Eck Professor of Engineering; Chair, Rustat Conferences*	*Jesus College, Cambridge*
Dr Tom	Wilkinson	*Senior Data Scientist*	*Home Office*
Jeremy	Wilson	*Vice Chairman, Corporate Banking*	*Barclays*
Prof David	Yermack	*Albert Fingerhut Professor of Finance and Business Transformation; Chair, Finance Department*	*NYU Stern School of Business*

CONTACT

Jonathan Cornwell
Rustat Conferences
Jesus College
Cambridge
CB5 8BL
www.Rustat.org

Conference Rapporteur

Jordan Burgess
Email: jordanburgess@gmail.com
Bitcoin: 1DHt4oKGFt8ewk9pyKe7WVufrHagAeuZMp
Twitter: @jordnb