The Good, The Bad and The Bitcoin: Cryptoassets as a phenomenon

The McNeil International Symposium on Laws and their Applications for Sustainable Development, Cyprus

Amalia Neenan

Civil & Commercial Researcher

Peters & Peters Solicitors LLP

24.10.19

Sound and Fury Signifying Nothing?

'The major concern is the potential for VCs to help criminals, terrorist financiers and sanction evaders to move and store criminal funds.'*

- Cryptocurrencies and Blockchain are the latest challenge facing the legal industry

- This new tech raises issues for a variety of different sectors including:
  - General crime
  - Terrorism
  - Corporate & Commercial Transactions
  - Banking Law & Finance
  - Litigation
  - Real Estate
  - White Collar Crime / Fraud
  - Asset Recovery & Tracing
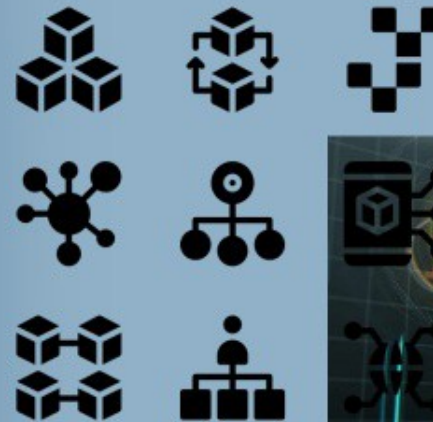
*Mark Kalderon, Ferdisha Snagg, Claire Harrop, 'Distributed ledgers: a future in financial services?' (2016)
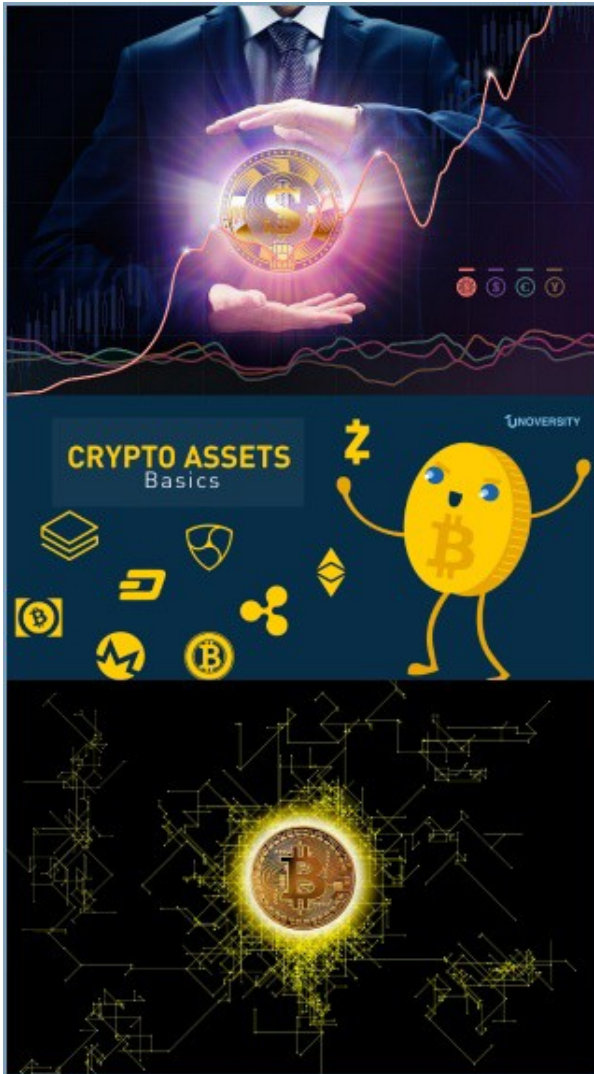
Down into the Crypt?

'Cryptoassets are cryptographically secured digital representations of value or contractual rights that use some type of distributed ledger technology (DLT) and can be transferred, stored or traded electronically.'

- The Financial Conduct Authority, 2019

CRYPTOCURRENCY

No standard definition, but....

'A Virtual Currency is a digital representation of value, this is neither issued by a central bank or public authority nor necessarily attached to a fiat (conventional) currency, but is accepted by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically.'

– The European Banking Authority 2014

FAST FACTS

THE PROS

✔

THE CONS

✗

Blockchain/ Distributed Ledger Technology

- Is the most common form of DLT.

- An expanding list of public records. The record sets are called 'Blocks'. Each 'Block' is linked using cryptographic code and contains a mathematical equation that maps the data contained in the previous block (a cryptographic hash), a timestamp, and transactional data.

- Basically: A system in which a record of transactions made in bitcoin or another cryptocurrency are maintained across several computers that are linked in a peer-to-peer network.

- An independent and continually updated database by each party in a network. There is no central authority. Every network participant processes and holds every transaction. Each participant then votes on the accuracy of the outcome of these processes. Once there is a consensus, the ledger gets updated and each participant holds an identical copy of the ledger.

Digital Wallet/ E-Wallet

- An electronic device or online service that enables electronic transactions.

- Hot Wallets: Connected to the internet

- Cold Wallets: Kept offline

- Does NOT store cryptocurrency – instead allows for the sending and receiving of cryptocurrency.

- Contains a matching pair of the user's Private/Public Keys

Public & Private Keys

- Part of the encryption mechanism to protect data and conceal transaction identities.

- Public Key: Allows information to be encrypted. It turns information into a random string of numbers, that everyone can see but not everyone can read. It also serves as a locator. Everyone in the Blockchain can see everyone's Public Key and can send transactions to specific participants by encrypting the data for transactions using a specific Public Key.

- Private Key: Decrypts information sent via the Public Key. Only the owner of the Private Key knows what this is. Works as a mathematical pair with a Public Key. Think of it as a cypher.
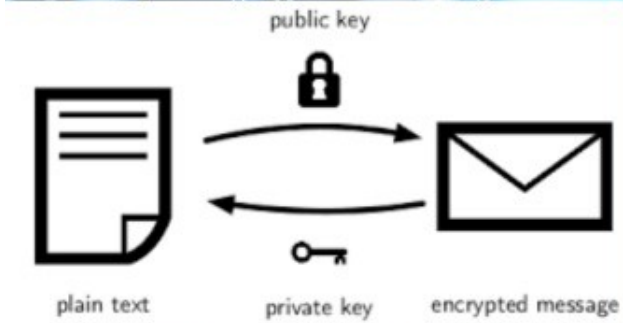
FAST FACTS

- Cryptocurrencies have no intrinsic value – they are not linked to an underlying commodity or sovereign currency.

- Value is derived from the ability to transfer it from point A to B within its *"electronic ecosystem."*

- Started to properly pick up speed in 2008 after Satoshi Nakamoto (an anonymous programmer or group of programmers) published a White Paper introducing bitcoin as a *"peer- to-peer electronic cash system"* that forgoes the need for financial intermediaries such as centralised banks etc.

- One of the first transactions using bitcoin was to order two pizzas from Papa John's for 10,000 bitcoins. In today's market value that is the equivalent to nearly $81 million.

THE BUBBLE

CONCERNS

SIPS2019: McNeil Intl Symp. on Laws and their Applications for Sustainable Development

Has the Bitcoin Bubble Burst?

- In December 2017, the price of one bitcoin was in excess of $19,300, having increased from $0.06 in July 2010.

- As of October 2019, the price of one bitcoin has dropped to $7961.41.

- In November 2018, the Crypto Market lost more than $60 billion in under a week - plummeting prices to their 2017 levels.

- The rise returns?

CONCERNS

"Is crypto the future or a fad? Golden ticket or Ponzi scheme? Amazon 2.0 or tulip mania? And what good is it for, anyway?"

- Nick Paumgarten 2018

THE PROS:

- Speed

- Lower transaction costs

- Fraud prevention?

- *"The... most obvious beneficiaries are said to be the disenfranchised and the so-called unbanked – the billions of humans around the world with no passports or access to any reliable kind of financial system."**
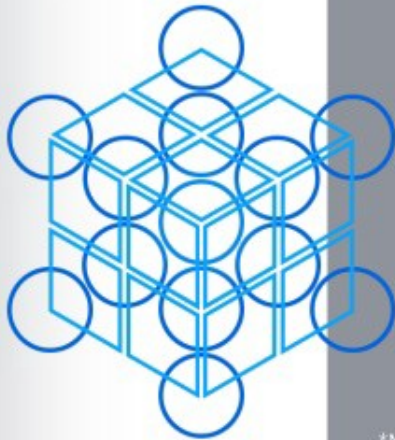
*Nick Paumgarten, 'The Prophets of Cryptocurrency Survey the Boom and Bust', The New Yorker, October 22 2018

BLOCKCHAIN:
THE ANSWER?

Blockchain: The Answer?

- Banks may disappear in the next few decades.

- Peer-to-Peer networks would outmode 3rd Party intermediaries.

- Distributed Ledger Technology = the way forward?

- Public, shared record of transactions in real-time.
    - Greater transparency
    - Overview of all capital flows
    - Easier to identify suspicious transactions

- Avoids failings of trust!

The Cons:

[Cryptocurrencies are] "a fraud".

- Jamie Dimon, CEO JPMorgan

"rat poison squared."
- Warren Buffett

- Despite, the supposed *'transparency'* of Blockchain technology, where each user is able to see every transaction to attest its validity and reduce financial impropriety, theft still occurs.

- Virtual Currencies can be stolen. One way involves *'Bitcoin Phishing'*, where cybercriminals attempt to procure users login details for exchanges or online wallets, to steal coins.

FOR EXAMPLE

CYBER SCANDALS

- The Silk Road: *'The eBay of vice'.* Used cryptocurrency to shield consumers who were purchasing contraband goods.

- Mt. Gox - Bitcoin exchange: Repeatedly hacked, filed for bankruptcy having lost 850,000 Bitcoins ($6.8 billion worth in today's market value), coins also stolen by company agents – riddled with fraud and embezzlement.

- IT team at a *'large Italian bank'* had been concealing one in ten of the company's computer servers under the office floorboards to mine cryptocurrencies for their own personal benefit - known as *'cryptojacking'.*

A RECENT SPEED BUMP?

Crypto company can't access $137M because dead owner didn't share passwords

Canadian Crypto Exchange QuadrigaCX Owes $190 Million To Customers Per New Court Filings

£145m cryptocurrency password goes to grave with QuadrigaCX co-founder Gerald Cotten

QUADRIGACX

FORTUNE — Cryptocurrency Owners Can't Access Funds After Exchange C...

Cryptocurrency Owners Can't Access Funds After Exchange CEO Dies—Because No One Knows the Password

- Died, taking the only password for a digital account containing £145 million worth of cryptocurrencies, for 115,000 account holders, with him.

- Kept a large proportion in a cold wallet (disconnected from the internet to prevent hacking).

- Ernst & Young gained access, to discover the account had been cleared out months before his death.

- Speculation that the CEO faked his death after the company ran into trouble.

- Quadriga CX filed for creditor protection in Nova Scotia in February 2019.

Crypto: The Highs?
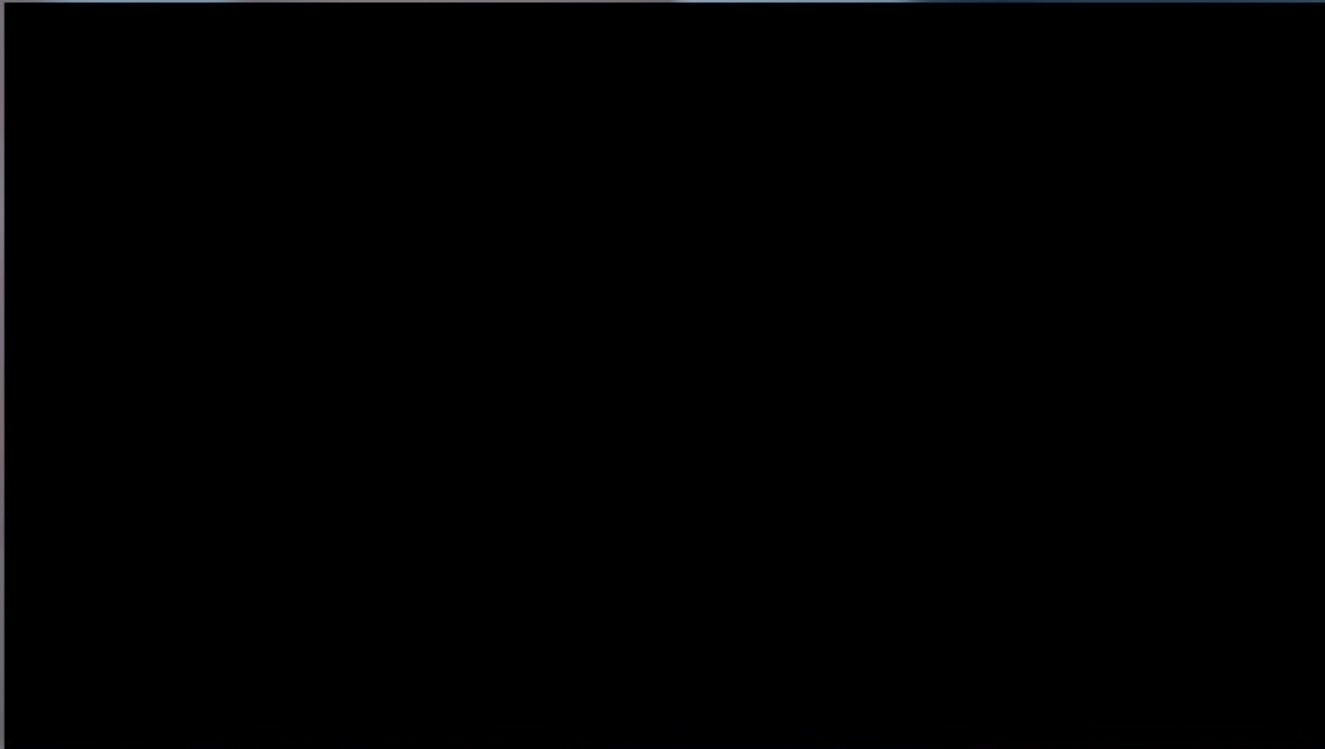
Why the Bad Rap?

- The Media Frenzy?

- Nomenclatorial Discrepancies?

- Lack of understanding?

- Sophistication of the tech?/Sophistication of fraudsters?

- Lack of a codified framework?

- Whatever the problem, there is a solution ... it's just a matter of fitting them with the right digital *'upgrades'*.
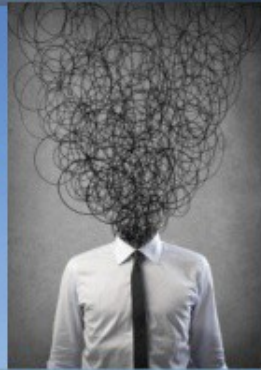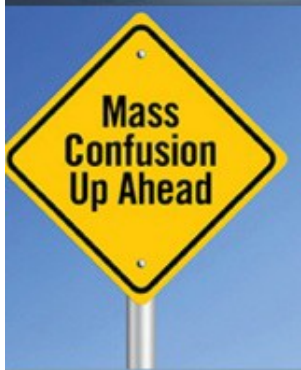
What's in a Name?

'Although bitcoin and similar VCs have some of the characteristics of currency, they also have characteristics of a commodity or other property. Their legal treatment varies from jurisdiction to jurisdiction, and regulators within the same jurisdiction may even take differing approaches depending on the regulatory context being considered. Some jurisdictions have been actively regulating entities carrying on business involving VC (New York) whereas in others trading in VCs remains unregulated (the UK).'
Phoebus L. Athanassiou

- One easy solution would be to broadly class cryptocurrencies as property, as HMRC and the IRS already do for tax purposes.

- *'Providing a basis for the recognition of property rights in assets of this nature is essential to harnessing the enormous potential this technology offers.'* Luke Von der Heyde

- *'Bitcoins clearly have a value. There are no immediate policy reasons why they should not be considered property.'* Misha Tsukerman

- By classing these assets as property, this entitles the holder to certain rights and remedies - removing part of the difficulty the sector faces in the first place.

- It would simply be a case of using the existing provisions in the UK legal toolkit used to deal with the theft of traditional property, to cross-apply to curtail crypto-criminality.

Act on it!

The Theft Act 1968

Section 17(1) stipulates that falsifying an account or document occurs when *'a person **dishonestly**, with a view to **gain for himself or another** or with intent to **cause loss** to another...destroys, defaces, conceals or **falsifies any account or any record** or document made or required for any accounting purpose.'*

The Fraud Act 2006

Section 2 provides for the offence of fraud by false representation, which involves the **dishonest and intentional making of a false representation** either to **make a gain** for the maker or to **cause loss** to another.

Falsified Records
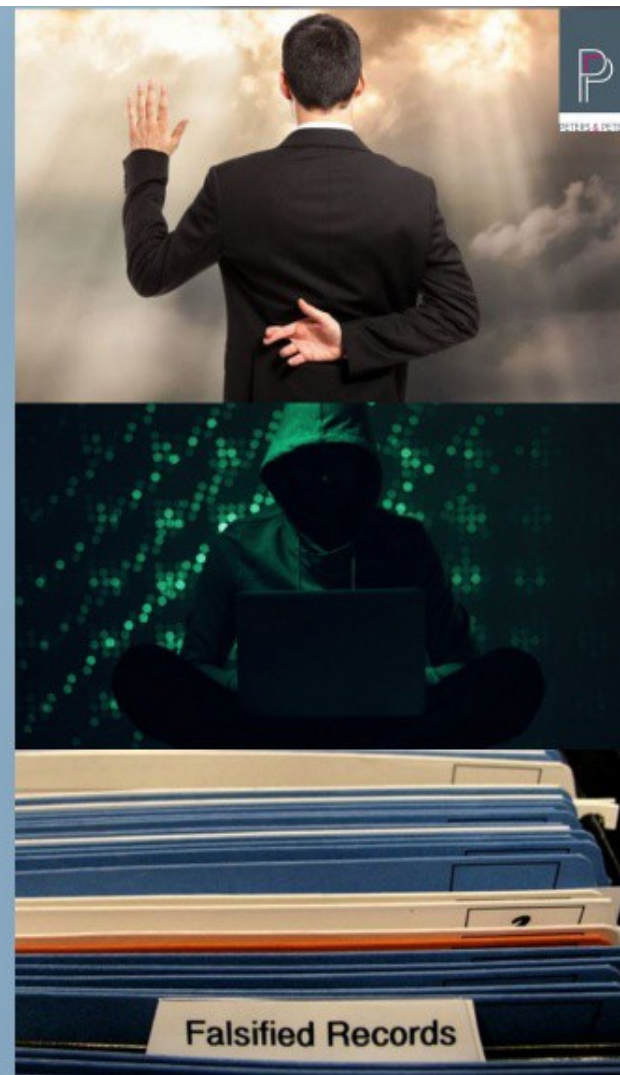
Inherent Vice?

'Governments and other legal authorities are afraid of virtually untraceable transactions that might be connected with illegal activities or even financing terrorist organisations.'
Jozef Bucko, Dana Palová & Martin Vejacka

- Anonymity characteristics can present significant hurdles.

- As the Public Key address is the only information available, this presents a significant hurdle for enforcement agencies when tracing illegal activity.

- This, compounded with decentralization, adds another layer of complexity to prosecution and asset recovery.

- While it may be possible to trace the location of misappropriated funds to an encrypted Public Key address, the question remains as to who can be served with court orders to oblige them to divulge identification information?

- Yet, anonymity and decentralization are also key advantages of the tech!

- They paint a picture of a future where individuals are in complete control of how they transact. Fiscal privacy would be absolute in a world where privacy itself is the latest commodity.

A New Toolkit?

CMOC Sales & Marketing Limited v Person Unknown and others [2018] EWHC 2230

- Concerned an alleged fraud, committed by *'Persons Unknown'* infiltrating the email account of a senior official at a company.

- The fraudsters then sent payment instructions purporting to come from the manager.

- As a result, a total of £6.3 million was sent out from the company's bank account, at Bank of China in London, to various other banks around the world.

- The Claimant did not know who was responsible, or where the money was.

- Obtained WWFO and disclosure orders:
  - Against *'Persons Unknown'* and third-party banks.
  - In circumstances where it was not known where the assets were. Allowing disclosure orders to be made against overseas banks under Bankers Trust.
  - Key: The dicta discussed alternative methods of service when there are grounds to believe that the Defendant will evade service/where urgent relief is necessary. Then it is appropriate to consider forms such as email, Facebook, WhatsApp and by access to a data room.

Cases like this take into account the reality of tech. The new realities of the modern world.

Hot off the Press

- Exchange hacking may be a thing of the past.

- Cryptocurrency security firm CipherTrace, report that $1.2 billion has been stolen through various cryptocurrency-based frauds in just the First Quarter of 2019.

- While crypto-frauds can take many forms, exchange hacking is one of the most prevalent.

- Enter, a new platform .... Nash!

- Traditionally, customers have to deposit funds onto trading platforms, prior to trading, with the exchange platform becoming custodians of the funds.

- It is at this point that hacks are most likely to occur.

- Nash however, does not require users to transfer cryptoassets to a third-party exchange pre-trade.

- Enhancing security, certainty and productivity!

Sustainability

- Mining takes a vast amount of computational power and energy.

- In 2017, Blockchain used more power than the power consumption of 159 individual nations including Nigeria and Ireland.

- Bitcoin accounted for 0.5% of the world's energy consumption in 2018 (*A. Cuthbertson, The Independent, 2018*)

- The first-fix would be to use mining systems that only use renewable or green energy.

- Icelandic company, Genesis Mining, uses 100% renewables and is one of the largest miners worldwide.

- Better incentives are needed to make this practice widespread. E.g. more cryptocurrency could be given to miners who use green energy sources.

- Proof of Work vs. Proof of Stake?

Raising the stakes?

Proof of Work

System most commonly used to authenticate transactions on the Blockchain. '*Miners*' race to solve a mathematical equation embedded in the transactional block to validate the transaction. The first one to solve the equation is rewarded (normally in cryptocurrency).

Proof of Stake

'*Validators*', first '*stake*' cryptocurrency in return for the right to validate transactions and add '*blocks*' to the chain. Validators are chosen by an algorithm that factors in their stake.

Energy Conservation

- PoW requires lots of machines racing to solve the same problem - wasting energy.
- PoS allows each machine in a PoS system to work on one problem at a time, which is a better distribution of energy.
- Ethereum is already working towards transitioning to PoS systems.
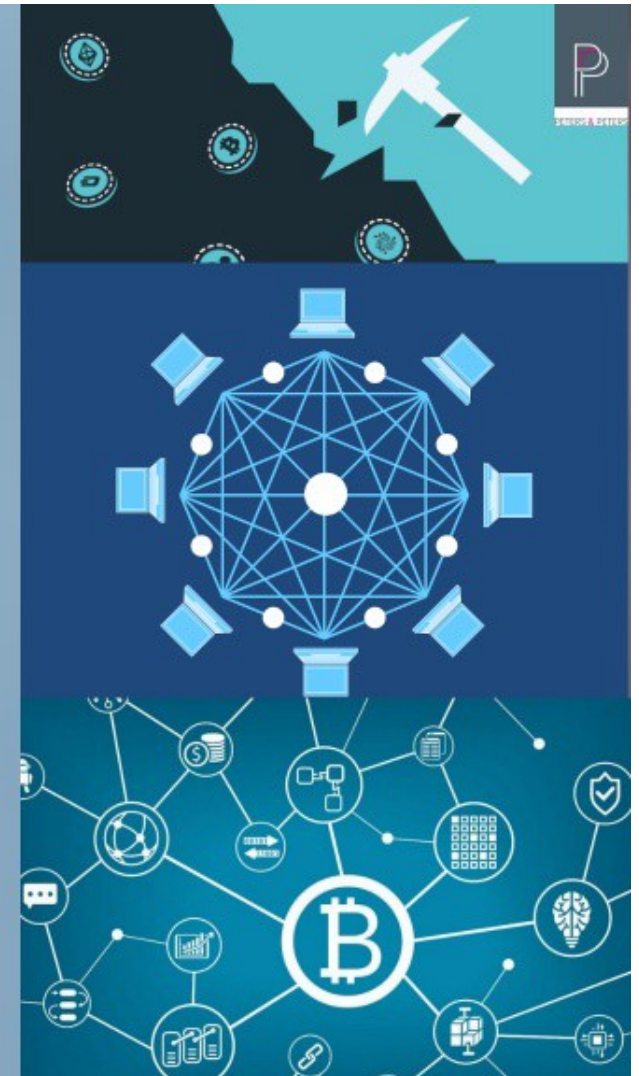
Put to good use?

- Dadiani Fine Arts in London was the world's first art gallery to accept multicurrency cryptocurrency.

- Owner Eleesa Dadiani, through the Dadiani Syndicate, set up the UK's first crypto-transactions for bloodstock, gems, bullion, private jets and yachts.

- For example, one of her clients bought four Formula 1 cars, collectively valued at £4 million (HK$41.9 million), in Litecoin.

- Furthermore, Andy Warhol's *'Fourteen Small Electric Chairs'* (1980), recently *'fractionally'* auctioned a £1.3 million stake in the piece in exchange for cryptocurrencies. *'The millionaire is changing...[there is a] big shift happening in consciousness, money and culture.'*

Vive la révolution!

- Agatha Bacelar, candidate for the United States House of Representatives in 2020, is accepting campaign donations in five major cryptocurrencies, including Bitcoin and Ether.

- In justifying this novel move, Bacelar states that the current political system is built to stifle a future *"where economic freedom is afforded to all."*

- Born out of the ashes of our collapsed financial system in 2008, cryptoassets have revolutionised our concept of transactional trust.
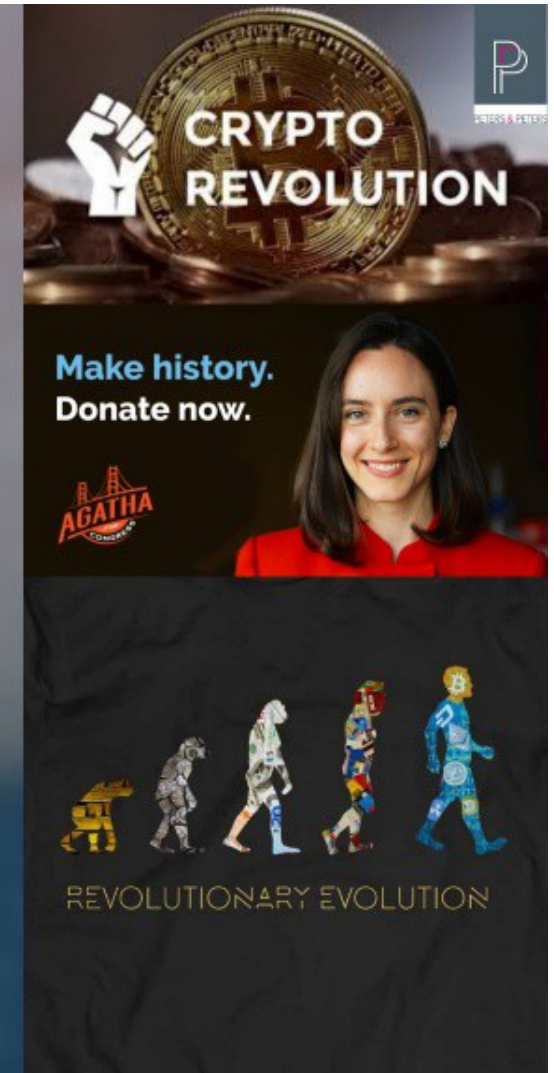
Questions?

Contact

Amalia Neenan

aneenan@petersandpeters.com

Tel +44 (020) 7822 7777

15 Fetter Lane

London

EC4A 1BW

United Kingdom