Blockchain and Cryptocurrencies

Report

October 2017

UoG Fintech Society
info@uogfintech.com
http://uogfintech.com

Introduction

Welcome to another published Report of the University of Glasgow FinTech Society with title “Blockchain and Cryptocurrencies”. In this report, we provide an entry-level and easy-to-understand introduction to Blockchain, Cryptocurrencies, Smart Contracts, ICOs. Lastly we analyse and discuss the current regulations around the FinTech sector regarding these new distributed ledger technologies.

About the UoG FinTech society

Founded in summer 2017, we are the first student-led FinTech Society in Scotland. We bring together University of Glasgow students of any degree who are interested in technological innovations that are likely to disrupt the financial services sector. We recognise the need for developing FinTech awareness among students before their graduation as a number of surveys indicate that FinTech and FinTech technologies will play a key role in a number of industries in very near future. We also aim to give members opportunities to develop useful employability skills.

We believe we can achieve our goals by running a series of workshops throughout the academic year, which are characterised by students' cross-faculty collaboration, peer learning and engagement with industry professionals.

About the “Blockchain and Cryptocurrencies” report

This report and presentation slides accompanying this report were created by members of the UoG FinTech Society, namely Antreas Pogiatzis, Zi Qin Wong, Aleksandra Waluga, Santiago Ramirez and Kamal Chauhan.

This report aims to explain in simple terms how blockchain, smart contracts and ICOs work. Firstly, we introduce some basic concepts and background that are essential for understanding cryptocurrencies blockchain technology and continuously we provide a definition.

Moreover, we dive into deeper concepts such as Smart Contracts and ICOs. AS such we analyse advantages and disadvantages of real life examples.

Furthermore we discuss the current regulations around that context and examine the existing legal frameworks that are in place.

Lastly, along with the report we provide a link for instructions and code on how to create your own ERC20 tokens.

Glasgow University FinTech Society

Table of Contents

Blockchain Fundamentals:

History

Blockchain technology has been getting some serious attention by press, social media and corporations lately. Interestingly though, the technology has survived for 7 years in stealth since its discovery. More specifically, a person with the nickname Satoshi Nakamoto whose identity is still unknown published a whitepaper explaining Bitcoin in 2009 [1]. A possible explanation for that would be the bad reputation that was initially developed around it due to the illegal use of Bitcoin. Indeed, Bitcoin was the currency of the dark web. It was used for buying guns, drugs, leaked data and even hiring hackers. Unlikely for blockchain, which was the underlying technology of Bitcoin, this reputation was overshadowing its potential and kept innovators away from it for many years.

2017 is the golden year for Blockchain. The term is all around the internet and big players across many industries have started to identify the possibilities and experiment with it [2]. Although, many people have heard the term, very few of them understand its functionality and how it works. As a result, the further sections we be focusing on explaining in simple terms how this fascinating technology works.

Ledger

One of the core components of blockchain is a ledger so it's essential to you know what a ledger is before you proceed reading. One of the simplest definitions of a ledger is the following. A ledger is a list of ingoing and outgoing transactions in chronological sequence to keep track of an account balance. This is also how your bank keeps a record your account.

Blockchain definition

At its simplest, blockchain is a *distributed ledger*. You may be wondering why it is called a blockchain if it is just another ledger. The truth is, it's not only called blockchain. Another more formal name given is *distributed ledger technologies* which is more commonly used in the academic context. Nevertheless, as you may have guessed is called blockchain because it is exactly that! A chain of blocks where each block points to the previous one and contains a set of transactions - just like a ledger – along with some other extra properties which are mostly utilised for technical purposes.

The above definition is mainly what you will encounter by doing a google search on blockchain. However, this is only a partial definition covering the data structure aspect of the blockchain technology. Probably, that may be the reason why people fail to understand the whole concept.

Apart from the data structure itself, blockchain as a technology encapsulates another three components.

One of the most basic is *cryptography*. The internal functionality is heavily depended on one-way mathematical functions called hashes and asymmetric encryption. Some more advanced blockchain networks even utilize cutting edge cryptography breakthroughs such as zero knowledge proofs. To give you an example, a blockchain user can use his public key as a wallet address and his private key to sign transactions *i.e. sending money*. Moreover, the blockchain is ultimately a *P2P network* and thus, relies on P2P node discovery and data sharing. In other words, blockchain uses the same algorithms that are applied on peer to peer distributed systems. Another key component of a blockchain network is the *consensus mechanism*. In simple words, the consensus mechanism is the methodology that the peers use to identify the order and validity of information in an environment where not all nodes are trusted. Namely some of the most common consensus algorithms used by the blockchain are, Proof-of-Work, Proof-of-Stake and PBFT.

Conclusively, blockchain technology is not just a ledger scattered around. It is a P2P network which uses cryptography and consensus algorithms to distribute and validate transactions on a shared ledger.

Types of blockchain

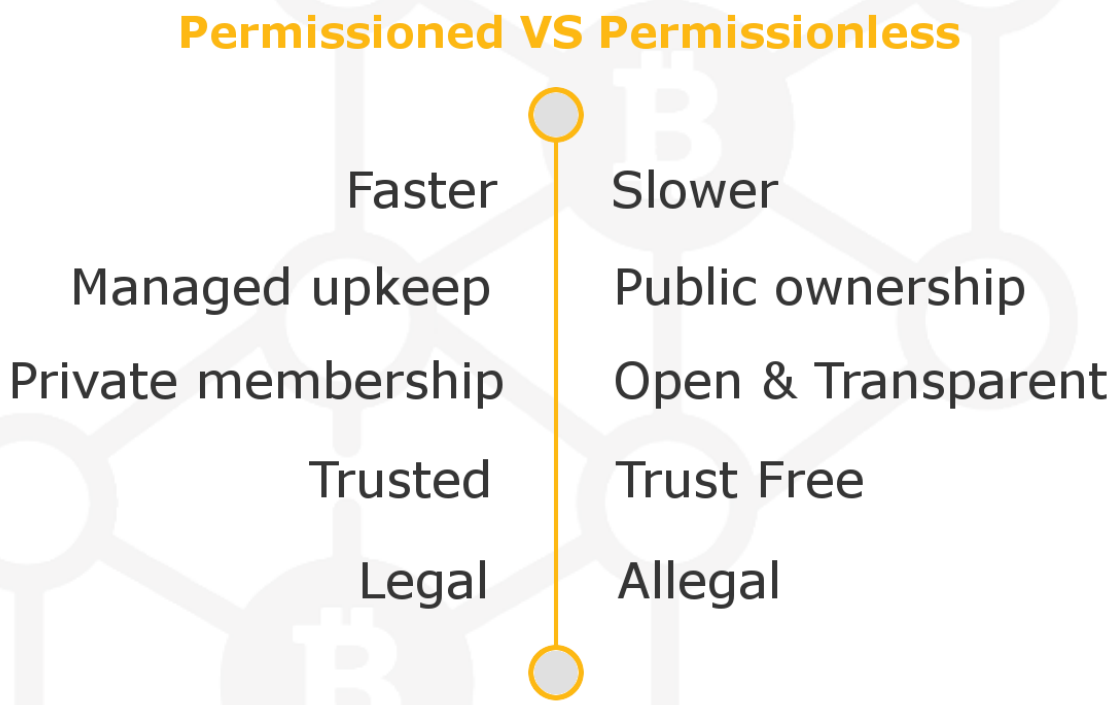
There are 3 types of blockchains. *Public*, *Private* and *Permissioned*.

Public is a blockchain that doesn't have any limitations. Anyone can join the blockchain network and all of the nodes can participate in the process of adding a block to the network. However, this comes with the caveat of high transaction verification time. Examples of public blockchains are Ethereum and Bitcoin.

A Private blockchain is used only internally by a specific organization and that organization has write access to the blockchain. As a result users have to trust the organization entities that verify transactions. Something which, on one hand reduces the verification time but it also requires some amount of trust by the nodes. Many argue that private blockchains do not provide any value as they can simply be replaced with a simple database [3]. On the contrary, others claim that a traditional database lacks other features that blockchain provides such as disintermediation and robustness. [4]

Lastly, permissioned blockchains can be considered as a hybrid of these to balance block confirmation time and immutability/disintermediation. A good example would be multiple

organizations that work on the same blockchain network but maintain a permission model to achieve privacy within the network.



Adapted and modified from: https://www.slideshare.net/gavofyork/blockchain-what-and-why

Best type of blockchain

A ubiquitous question floating around the internet is "What kind blockchain should I use?" or "Which one is the best?" The answer is simple. There is not a "best" blockchain. All different types of blockchains come with their pros and cons. An accepted notion across the blockchain community is that the publicity of the blockchain is directly proportional to the security that it provides but indirectly proportional to its scalability. For instance Bitcoin blockchain is public and permission less. Anyone can join and use it, however, it allows only 7 transactions per second. Compared to the scalability of the VISA network which is currently handling thousands of transactions per second this rate cannot cope with the demands of the consumers. Apparently, this limitation is one the main reasons that we have not seen blockchain technology applications dominating the enterprise. On the contrary Hyperledger platform allows the creation of a permissioned blockchain network where only several authorized nodes are responsible for validating transactions. This can enable rapid

validation and therefore more transactions per second. Nevertheless it is easier to compromise the security of the network because a malicious attacker only needs to target that subset of nodes that the rest of the network is putting trust into.

The potential

Although blockchain technology started off as an unwanted technology it evolved to a trend and some can argue that is the invention of the century. Undoubtedly the potential is huge. Already companies and big corporations started experimenting and adopting blockchain to satisfy their demands. Even outside of the Fintech industry the applications are endless, from supply chains, to medical records, insurance and e-residencies. [5] More specifically, the ability to have a set of people agreeing on a piece of information without any intermediaries is the most fascinating part. Blockchain has the power to shift the control from the centre to the nodes and this provides hope for a better society in the near future. To put it into context, Internet set the foundations for freedom of speech and gave the ability for anyone to express his opinion. Equally, blockchain can give to everyone equal rights of being heard.

Cryptocurrencies

Cryptography primer

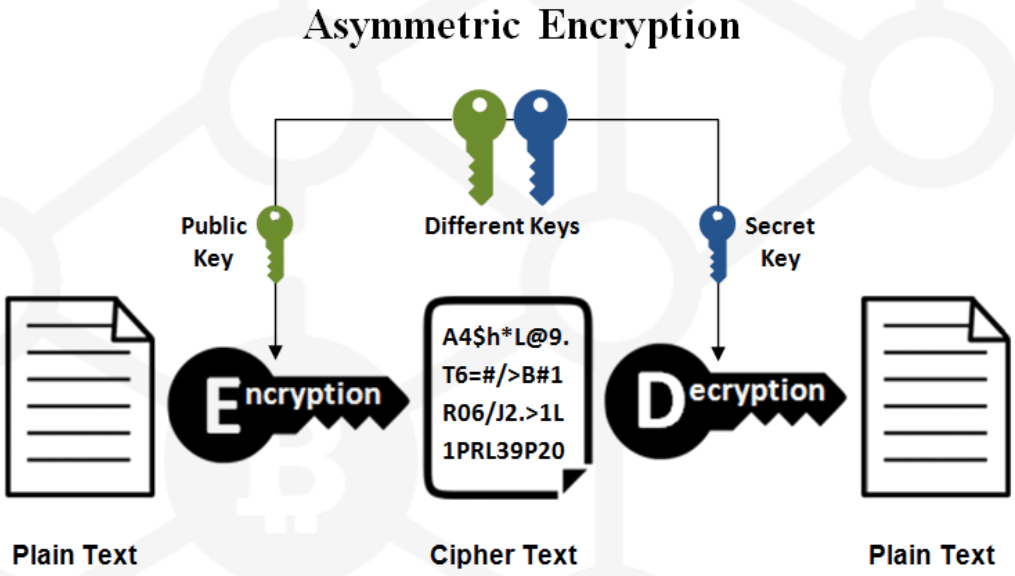
Cryptography is “the practice and study of techniques for securing communication and data in the presence of adversaries”. In other words, it’s a way to scramble up information so that only the appropriate entity can unscramble it. Usually it involves a key which is used for encryption and decryption (symmetric encryption). In more advanced cases it includes two of those keys (private and public keys i.e. asymmetric encryption) to secure information through a communication channel. Using asymmetric encryption and hashes a digital signature can be created, which can be used to validate messages, software, or a digital document.

Hash Functions

Hash functions are one-way mathematical function which are extensively used in cryptography to verify that a digital piece of information has not been tampered. A hash function gets a piece of information as input and it returns a fixed length hexadecimal value (most of the times) that is guaranteed to be unique for every input, or more precisely the likelihood of having the same hash output for two different inputs is enormously small. Some popular hash functions are SHA, RIPEMD and Tiger.

Asymmetric cryptography

Cryptocurrencies use asymmetric cryptography to ensure that a unit of a currency is only used in one transaction at a time. This involves the use of two 'keys' that are essentially a pair of different, large numbers (hence the name 'asymmetric'). Each user has a unique private key that only they have. The public key, on the other hand, is made available to everyone. When a transaction occurs, a user's private key takes the data and essentially signs it before it is sent back to the network. It is then decrypted using the public key, and verified by a hash function.



How keys are used for asymmetric encryption Source: Blockgeeks.com

Cryptocurrency definition

A cryptocurrency is digital currency that uses cryptography, to secure transactions to control the issuance of new currency units. Unlike physical currencies, cryptocurrencies use a peer-to-peer network. This means that there is no central command server, and that users are able to share data with each other. Transactions are secure and anonymous, due to the use of cryptography and blockchains. More specifically, the blockchain is secured by the peers that are using it so the more participants in a blockchain network the more secure it is.

In order to remain secure, a wallet owner has two keys- a public key and a private key that are used to verify transactions. When a transaction occurs, the private key takes the data and essentially signs it before it is sent back to the bitcoin network. This is then checked and verified by the public key to make sure that the private key matches the public key.

Here is an example of how a transaction works:

In this example we will use 'Alice' 'Bob', and 'Carl' as users. Imagine Alice wants to send Bob 10,000 bitcoin. When she does, the private key is used to sign the data, and publish it onto the bitcoin network. All other participants including Bob can verify that it was Alice that made the transaction using her public key. Now in order for the Bob to actually receive the money the transaction has to be verified by other participants, Carl in this case. In the case of Proof-of-Work that Bitcoin uses that would be a 'miner'. Miners, add transactions into blocks and use hash functions to verify them. Once a block is verified it is added to the blockchain and from that point and onwards it is almost impossible to change.

Bitcoin and the History of Bitcoin

The first cryptocurrency to be created was Bitcoin, created anonymously under the pseudonym Satoshi Nakamoto in 2009. It is the most popular cryptocurrency to date, with a market capitalization of around $45 billion as of July 2017. The progress it has made since its founding is immense and could potentially shape the future of the way we spend money. Large-name companies like Microsoft, PayPal, Subway, Expedia, and many others accept bitcoin as payment, acknowledging it as a legitimate currency.

On May 22nd, 2010, the first real-world interaction using bitcoin was made. Laszlo Hanyecz bought two Papa John's pizzas in exchange for 10,000 bitcoins. At the time, that was only worth around $30, but at the time of writing this it would be worth approximately $57 million. That was probably the most expensive pizza in the world.
Here are a few other key events for Bitcoin:

January 9th, 2009: The announcement of Bitcoin was made anonymously by Satoshi Nakamoto

January 3rd, 2009: The Genesis Block was created by Nakamoto. This is the first block of transactions that all other subsequent blocks build upon

October 5th, 2009: A currency rate is established for bitcoin at $1 = 1,309 BTC

February 6th, 2010: The Bitcoin Market is established

November 6th, 2010: The bitcoin economy is now worth $1 million

2011: The website Silk Road opens, selling illegal drugs using bitcoin

April 23rd, 2011: The value of Bitcoin is now on par with the Euro and British pound

June 12th, 2011: The Great Bubble of 2011 where the exchange rate dropped from US$31.91 to $10 in four days

May 9th, 2012: An FBI report is leaked, showing concern that bitcoin is used for illegal transactions

October 2nd, 2012: The FBI shuts down the Silk Road, obtaining $3.6 million worth of bitcoins

November 19th, 2013: The bitcoin value surges from $125 in September to $1242

2016: Bitcoin is the 'best performing currency of 2016', with a 126% increase in value over the year

(Add something about the current good public use of bitcoin) i.e. University of Nicosia accepts tuition fees to be paid with bitcoin

Other Cryptocurrencies

Apart for Bitcoin, there are a few other popular cryptocurrencies and platforms that have been developed.

Litecoin: Developed in 2011, this currency is similar to bitcoin, but has faster payments and therefore has faster transactions

Ether: Founded in 2015, this currency is the second most popular cryptocurrency, on the Ethereum blockchain.

Ripple: Created in 2012, this currency exchange network supports not only cryptocurrencies, but also commodity money, or any other unit of value (like frequent flyer miles). It has been used by banks such as Santander.

The Potential

The unique characteristics of cryptocurrencies can, in some ways, be more beneficial than those of physical currencies. They have the potential to shape the future of how we exchange money and live on a day-to-day basis.

Secure and anonymous

As explained before, each transaction uses a public key and private key for verification. On top of that, there are many users who monitor the blockchain, to make sure that nothing is out of order. Since transactions can't be faked, it also means that cryptocurrencies tend to be more reliable than physical currencies.

Unaffected by inflation

In addition, the value of bitcoin or other cryptocurrencies are immune to inflation. Currencies like bitcoin have a fixed amount of 21 million in the system (with 15 million currently in circulation), the currency cannot be devalued because more bitcoins can't suddenly be created. This also means that the value of cryptocurrencies is more susceptible to external factors. While this could be a bad thing, it also means that small investments could easily have large turnouts, under the right circumstances.

Easy access and usage

Since cryptocurrencies use a peer-to-peer network, all users are connected with each other, and can access everyone in the market. There are also lower transaction fees than those of physical currencies as there is no "middleman" facilitating transactions.

The Downsides

Despite the promise that cryptocurrencies hold, they also have some downsides.

External shocks

Since cryptocurrencies such as Bitcoin are decentralized, this means that there is no one governing the value of the currency. Thus, the value of the currency relies entirely on the demand and supply of bitcoins. This means that external shocks can create a huge impact on the value,

Illegal activity

The anonymity and security that cryptocurrencies provide makes it ideal for illegal activity to take place. For example, Silk Road was an online black market that mainly sold illegal drugs, where all sales were made using bitcoins. In addition, some have hacked Bitcoin to launder money. In July of 2017, Alexander Vinnik was arrested for laundering $4 billion in bitcoin. In the history of Bitcoin, the company has been subject to around 40 thefts, indicating that the security is not entirely fool-proof.

Questionable legitimacy?

Lastly, although some cryptocurrencies are used for real-life transactions, some still claim that they are illegitimate, and it is absurd for people to think that they have any real value. One of these people is Jamie Dimon, CEO of JPMorgan. In an interview conducted recently, he stated that "The currency isn't going to work. You can't have a business where people can invent a currency out of thin air and think that people who are buying it are really smart". After this interview, the value of bitcoin dropped by 10%. However, he does support the use of blockchain technology, and has shown support for government-backed digital currencies like crypto sterling, euro, and yen.

Smart Contracts

What is a smart contract?

A smart contract is a computer program that can facilitate and enforce the terms of a contract, without the need for third party intermediaries. Developments in blockchain technology since the invention of Bitcoin have created a new platform for smart contract; the most popular of which currently being Ethereum.

On their most basic level, blockchains are databases which can be shared between parties, without the need for a trusted third party. Ethereum places another layer on their blockchain, which additionally allows for software programs, or decentralised apps (Dapps) to be run. Ethereum is therefore both a Bitcoin-like exchangeable currency, and also a platform for Dapps.

Applications of smart contracts

The benefits of combining smart contracts and blockchain programming are clear:

Immutability
Once a contract is executed, all parties will be safe in the knowledge that it cannot be stopped or changed, and will function as programmed to do so.

Lower costs
Setting up and ensuring correct enforcement of traditional contracts can be costly. Through automation, smart contracts can significantly reduce costs.

Security
The validity of a smart contract based on the blockchain, can be viewed and verified by all interested parties.

Currently smart contracts are only widely used for Initial Coin Offerings (ICOs), and peer-to-peer gambling programs, although as the technology grows, new use cases are emerging. ICOs on Ethereum are currently experiencing a bubble-like growth, they involve creating your own "ERC20" token on Ethereum, which creates your own cryptocurrency or Dapp. These tokens can then be offered to the public, in exchange for Ethereum (the cryptocurrency), through a smart contract (run on the Ethereum platform), in the form of an ICO. These tokens can then be then easily traded on external cryptocurrency markets in exchange for Bitcoin or other cryptocurrencies.

One recent ICO, Bancor, recently raised $153m in three hours, and currently there are 707 Dapps being developed on the Ethereum platform. One of these applications is peer-to-peer gambling, that allows for "provably fair" games with fixed odds, which can be verified by the user, and negate the need for third party auditing.

Voting system
The blockchain provides a public verifiable, yet anonymous ledger, so you nobody could link you to your vote but you could verify your own vote through your public key.

Management functions
Performing tasks such as submitting and approving expenses may currently take several layers of management to approve. Smart contracts could provide efficiency.

Supply chain
Simply taking online payment for a product could trigger a smart contract to perform a series of tasks to ensure the product is delivered, or specially manufactured for the consumer.

Property
In the future Bitcoin may become the standard way of conducting property transactions as it provides a public transaction that is verifiable by all parties. The land registry may also be on a smart contract on the blockchain.

DAOs:
Combining smart contracts and blockchain technology has led to a new type of company – the Decentralised Autonomous Organisation. DAO's are smart contracts that act like companies or investment vehicles. Existing without traditional managers and directors, DAO's exist only in code, the idea is that they would act only as programmed to do so, and could only be changed by consensus of members or token holders.

Security issues

An important aspect of smart contracts is their security which is also an active area of research. In essence if you can trust a smart contract and avoid using intermediaries, essentially means that you trust the programming skills of the developer who developed it. Consequently, there is research being conducted on how the code of smart contracts can be formally verified which can on one hand ensure security but one the other had make development more difficult.

An example which highlights the importance of this issue is "The DAO" hack which refers to an Ethereum based investment fund that was created in May 2016 and raised over $250m (when

Ethereum was trading at $20 – would now be worth $3.75 billion if they had just held ETH!). Before any significant actions could be taken a hacker found an exploit in the smart contract and began to drain the DAO of its funds. So in July 2016 the community voted for a "hard fork" to refund the investors of the DAO with their funds. The fork meant that the blockchain would be in effect "rewound" to a point pre-hack. This caused division and controversy within the community as some believe that this action undermined some of the fundamental concepts of smart contracts and blockchains– namely decentralisation, immutability and the code being "the law". The argument was the code was faulty and the hacker potentially had a legitimate claim on the funds by finding the exploit.

Tokens

What are ERC20 Tokens?

ERC20 tokens are crypto tokens on top of the Ethereum blockchain that comply with the ERC20 interface [6]. ERC20 interface was introduced as an improvement for a common interface for tokens [7]. In result, this would benefit wallet and blockchain developers working with crypto tokens because they would essentially have the same basic functionality which can be extended. In simple words, ERC20 defines a smart contract with a specific set of functions that a token must implement.

Real world applications

Crypto tokens are widely used in different blockchain applications. A common one is to represent company shares as a token and distribute them through an ICO (see ICO section). Also tokens can be thought as another form of crypto currency and be traded in market exchanges for fiat money. Lastly a crypto token can represent any form of asset from property to mortgages which allows for a wide new range of disruptive applications.

ICOs

A Kickstarter for crypto-nerds

Blockchain technology is reshaping the way in which start-ups can raise capital. A new fundraising model has been dominating headlines this year: an ICO (Initial Coin Offering) is the process of issuing digital tokens and selling them to a global crowd for cryptocurrency (Ether, Bitcoin), or at times even for regular money[8].

The crypto tokens are created on an indelible distributed ledger, which means that the digital coupons can be easily traded, however, unlike company stock, they don't confer ownership rights [9]. It has become a popular way for tech companies to obviate the struggle of seeking venture capitalists and surrendering any decision-power to them.

The misleading name draws parallels to IPOs, but in fact, it can entail multiple offering rounds, and involves tokens rather than coins in their ordinary currency meaning. In effect, many issuers opt for different terminology now, including "token sale", "software sale," or "donation event." [10]

Monopoly money?

ICOs begin with a team of technologists generating an idea for a capital-intensive project, which they explain further in a white paper that describes the business and technical dimensions of the venture.To many the ICO structure is essentially raising munificent funds for merely a promise of a hypothetical future piece of code.[11]

In reality, ICOs benefit from their ability to form a smart contract on a token with codified terms of trade. The holders can be entitled to a portion of profits, a platform utility enabler, or almost anything else, as evidenced by Ethereum.[12]

There are also instances of ICOs being run for non-digital ventures: Mikhail Shlyapnikov, a Russian farmer, issued *Kolions* that serve as an investment into his local Kolionovo ecosystem. His cryptocurrency is directly connected to actual product – Kolions holders can purchase some of Kolionovo farm produce with a discount of up to 100%, and the proceeds are re-invested into growing the existing local production.[13]

The tokens also tend to become mini-currencies traded for fiat money or cryptocurrencies at blockchain marketplaces. While the initial price of the crypto tokens is determined by the issuing team's idea of how much they are looking to raise and the amount of tokens they are willing to emit, the secondary market price obeys the supply and demand laws. As with the regular company stocks, the price changes are strictly attached to the trust in the team, reactions of the current investors and other project information[14]. This dynamic attracts a pronounced amount of speculation, and ICOs' impact on the real world is increasing every day.

ICO speculative frenzy

The ICO mechanism has debuted in 2013, but really surged in 2017 – only in the first half, cryptocurrency offerings attracted an estimated $1.3B, up from the 'modest' $260M raised in the

whole of 2014-2016. Interestingly, in June 2017, for the first time more money has been raised in the blockchain sector through ICOs than traditional VC investments ($327M vs $295M) [15][16].

The most notable completed offerings which all raised over $100M were done by:

Filecoin (2017, $260M) – a decentralised storage network that runs on a blockchain with Filecoin that miners can earn by providing storage to clients, raised $200M in just 60 minutes;
Tezos (2017, $230M) – a 'self-amending' blockchain driven by governance rules where protocol upgrades are to be approved by stakeholders;
Bancor (2017, $150M) – a platform for launching new blockchain tokens which can hold other cryptocurrencies;
The DAO (2016, $150M) – a smart contract system designed to function as a community-managed venture fund, ceased to function after a system hack.

What investors hope to get out of the investment is strong and quick returns from the tokens' appreciation. To give an example, Ether was issued at $0.3-0.4 per token in 2014, with the price reaching $19 already in 2015, now at over $300. The success of the project on which the token value is dependent in many cases is a risky bet, and the recent ICO hype might be reflecting the pressures in the larger financial market. Investors are desperately seeking higher yields, and with fewer and expensive equity securities they turn to gambling on the cryptocoin market. The growing speculative ICO environment may be then a result of the post-crisis era of low rates, de-equitisation and central banks-led ample liquidity. Yet, in finance, speculative hysteria and innovation are known to appear side by side.[17]

90's are back

People from across the globe flock into investing in cryptocurrencies hoping to take a shortcut to riches, allowing projects with no more than a whitepaper to show raise funding at an exuberant scale. Looking back at the history, it doesn't have to sound as absurd as it does.

In the 90's, companies needed as much as just the word 'internet' in their business model to see their market caps soar after going public. The fear of missing out on the soaring valuations took hold of investors, further driving the prices up. This irrational ebullience led many people to lose vast sums of money when the bubble burst, yet, tremendous value was built as a result too: the Internet and companies like Google, Amazon, PayPal have changed our lives forever.[18]

The crucial point that needs to be raised in this debate is that the funds raised in the top cryptocurrency projects will be spent on developing cutting edge technology. These innovations will become the infrastructural backbone of the future autonomous and decentralised

organisations. What we see on the surface, the enthusiastic investor crowds, who swayed by grand visions don't analyse the fundamentals, may look like just another recipe for a bubble about to pop. However, that is how disruptive technologies emerge – they need enough money to make it possible to face the small odds, spread the risk through selling a variety of tokens, and just push the frontier further.

Some estimate that the current state of ICOs looks rather dim: 40% are fraudsters, 50% are not thoroughly knowledgeable about blockchain or decentralisation, and 9% don't understand the problems of building a business [19]. Many people will lose their investments and learn their lesson the hard way, but that hopeful 1% will succeed, and the emergent giant technologies will revolutionise the world yet again.

Regulations

Current regulations

Legislation of cryptocurrencies and ICOs differs from countries to others. Few countries currently have a legal framework regarding these new technologies.

We can identify three current legal level of regulation: legality (or semi-legal), legal status and regulatory frameworks.

Legality or semi-legality

In most countries, the use of cryptocurrencies and ICOs is not illegal itself, which mean that it is possible to purchase, sell, exchange or use cryptocurrencies as a way of payment in specific platforms.

Some countries have a hybrid position, where cryptocurrencies are semi-legal. For instance, in Russia, cryptocurrencies are not forbidden. However, it is illegal to buy anything with a currency other than the national Ruble, which automatically makes any purchase with a cryptocurrency illegal.

As well, China established a ban plan over ICOs and cryptocurrencies exchanges within its national territory. Nonetheless, private owning of cryptocurrencies isn't prohibited, which means that Chinese users of cryptocurrencies are still able to buy and sell their cryptocurrencies on foreign platforms.

Legal status

Among the countries where it is not illegal, it can be said that their use is permitted because they don't have a legal status yet. To put in another way, cryptocurrencies and ICOs do not correspond to any statutory provision nor any precedent in each national legal system. As a result, it cannot be *expressly* illegal.

Authorities across the world are trying to give a legal definition to ICOs and cryptocurrencies. The United-States consider cryptocurrencies as intangible assets for tax purposes, as well as the United-Kingdom. Other countries may consider it as money, other not etc.

Some regulator (SEC in the USA; CSA in Canada; HKFSC in Hong-Kong; MSA in Singapore), consider ICOs as securities. It enables regulators to have jurisdiction over specific cases where ICOs or cryptocurrencies are involved. However, giving a legal definition or status doesn't mean that cryptocurrencies and ICOs are regulated. It's just a first step toward a complete legal framework.

Regulatory framework

A legal framework is the most advanced legal stage for cryptocurrencies and ICOs. Through regulation, a country establishes specific laws regarding ICOs and cryptocurrencies. These rules can provide: authorisations for fintech professionals doing business with these technologies, power of control and sanctions to authorities or regulators, protection for consumers etc. Basically, regulation enables a country to have some control over cryptocurrencies, ICOs, but also platforms of exchanges. This is not the case when there is merely a legal definition. Control involves a complete legal framework.

Almost no countries have a regulation system for ICOs and cryptocurrencies. Japan and Mexico adopted laws regarding cryptocurrencies and Fintech professionals in 2017.

Lack of regulation is mainly due to the newness of ICOs and cryptocurrencies and because authorities are still wondering whether prohibit or authorise them.

Financial regulators are getting really concerned about it because of the considerable amounts of ICO transactions during the year 2017. More than 2,2 billion USD had seen raised since January, including 537 million USD solely in September [20]. Another element that increased worries in the financial sector was the ban of ICOs and trading of cryptocurrencies in China at the beginning of September 2017. Both circumstances urged regulators to publish guidance, advice notes, or simple statements about the risks related to ICOs and cryptocurrencies, or simply to express their willingness to regulate them:

- In September 2017, the Australian Securities and Investments Commission (ASIC) issued some guidance for ICO issuers and warned investors about the potential risks of scams. The guidance specifies that ICOs may be subjected to different areas of law depending on the type of ICO issued. [21]

- The Monetary Authority of Singapore (MAS) aims to adopt a different approach. Indeed, the regulatory body plans to regulate firms providing payment services through cryptocurrencies instead of regulating cryptocurrencies themselves. The objective is to control these services to prevent money laundering and terrorism financing. The chairman of the MAS also announced that tokens issued through ICOs will be deemed as securities, making them subject to securities requirements. [22] [23]

Few examples of the current legal framework regarding ICOs and cryptocurrencies across the world. [24] [25]

Country	Legality of cryptocurrencies ICOs and platforms of exchange	Legal framework or legal status of ICOs and cryptocurrencies
Mexico	Authorized	A *'FinTech'* law has been presented by the Senate on the 10th of October 2017, to regulate cryptocurrencies and fintechs. [26] [27]
United-Kingdom	Authorized	Cryptocurrencies are considered as 'private money'. Any purchase with a cryptocurrency will be subject to VAT, and any profit or loss on cryptocurrencies are subject to capital gains tax.
Russia	• Owning, selling and buying cryptocurrencies is authorized. • Purchases with cryptocurrencies is illegal.	No legal framework has been adopted yet, but the government is considering to regulate cryptocurrencies as securities before the end of the year 2017, but the Bank of Russia and its governor are sceptical about cryptocurrencies and seem opposed to any legalization. No consensus has been found between the Ministry of Finance, the Central Bank of Russia and the Federal Financial Monitoring Service. [28] [29]
Bolivia	Forbidden	The use and trade of cryptocurrencies is illegal in Bolivia. The country has been the first to totally prohibit it. In May 2017, the Bolivian Financial System Supervision Authority (ASFI) arrested 60 *'cryptocurrencies promoters'*. [30]

To sum up, regulations as well as legal status of cryptocurrencies and ICOs varies from one country to another with no single trend:

- In most countries, buying, selling, exchanging cryptocurrencies and purchasing with them is legal, as well as ICOs.
- Some countries have adopted ban policies over ICOs and sometimes cryptocurrencies, to prevent frauds. However, these prohibitions seem temporary awaiting the adoption of a legal framework.
- Few countries have adopted laws regulating cryptocurrencies, ICOs, exchanges platforms and Fintech professionals, but none of them covers every single aspect of these new technologies.

Nonetheless, this situation should change soon. The interest of national regulators is increasing and most of them are working on the set up of rulings. [31] [32] [33]

Need for regulations

There are many reasons justifying the necessity to regulate cryptocurrencies. [34] [35].

Prevent criminal activities

Cryptocurrencies are pseudonymous, encrypted and decentralized thanks to the blockchain technology, which makes tracking difficult for authorities. The most significant problematic about unregulated cryptocurrencies, is that it eases the development of cybercrime and illegal activities such as:

Frauds

Money laundering

Through the blockchain technology, any transaction realized is public permanently for anyone. However, it can be easy for a criminal to use an anonymous ID and purchase tokens in a market which is non-cooperative with authorities. In these type of markets, criminals can exchange their dirty money into tokens which are not related to criminal activities, and exchange these tokens for conventional currencies.

Funding of terrorism

Gambling in countries where it is illegal, such as China.

'*Darknet* markets'

More broadly speaking, cryptocurrencies are significantly used in the Darknet markets, where drugs, cyber-arms, counterfeit currencies, stolen credit cards, fake identity documents, child pornography and other type of illicit goods can be purchased. For instance, bitcoins were massively used in the online black market *Silk Road*, which has

been shut down in 2013 and in 2014. [36] Cryptocurrencies absolutely need to be regulated to prevent the expansion of these activities, even though it will never totally shut them off.

Tax purposes

The use of cryptocurrencies can also be motivated by a desire to evade taxes. Exchanges made with cryptocurrencies do not transit through central banks or any other third parties, which eases tax evasions for individuals.

Some countries are aware of this tax issue. In 2014, the Internal Revenue Service (IRS) of the United-States ruled that Bitcoin will be deemed as a property (virtual asset), which means that the cryptocurrency will be subject to capital gain tax, unlike conventional currencies. [34]

Other tax issues have been raised, regarding VAT. The Court of Justice of the European Union stated that the conversion of bitcoin into conventional currency should not be subject to VAT, because the cryptocurrency should be considered as a mean of payment. Nonetheless, VAT is still applicable to any transaction involving the purchase of good or service in exchange of cryptocurrency, as a regular transaction with conventional currencies. [35]

Protection of investors

One of the major issues regarding ICOs is the probability of frauds and scams, the value of a token may not genuinely represent the economic results of a company …

Even worse, an ICO may be a total scam, and no project or real company stands behind the fund raising. (see: *ICOs that went wrong*.) Investing in a company through ICO is riskier than buying stocks or securities of a company.

- In a regular IPO (*Initial Public Offering*) investors are much more protected. In an IPO, investors can assess in the most accurate way the viability of a business plan thanks to balance sheets, CRA (Credit Rating Agencies) reports, and other diverse information available about a company. After the IPO, shareholders are granted three rights: information (at least one mandatory general meeting per year), vote (control), and dividend (return of investment). Through their right of information and control, shareholders are protected and can properly decide whether they should keep or sale their stocks.

- As well, an investor can buy securities such as bonds from a firm. In this type of investments, security-holders benefit from preferential rights over shareholder, mainly in case of insolvency.

In the opposite, during ICOs, investors are granted merely no rights (*i.e.* vote or information), except the possibility to purchase good or use the services provided by the start-up. In case of

insolvency, they do not benefit from preferential rights enabling them to recover their investment. In other words, tokens issued through an ICOs do not provide sufficient protection to investors.

Though, investors can assess the viability of the business plan through the *white paper* provided by the company seeking to raise funds. It could be compared to a *prospectus* issued by traditional firms during IPOs. Since white papers are not regulated, some start-ups do not provide sufficient information permitting to scrutinize the feasibility of the funded project, or sometimes they are not even provided to investors.

This situation is dangerous for investors, because the lack of legislation restricts their security and their possibility to sue an unlawful firm.

Cryptocurrencies

Protection of investors doesn't relate only to ICOs transactions, but more generally to any owner of cryptocurrencies. Here are some examples of incident within cryptocurrencies markets:

- In February 2014, the world's largest bitcoin exchange, *'Mt. Gox'*, declared bankruptcy with a loss of 473 million USD of bitcoin.

- In 2014, the company *'MyCoin'* based in Hong-Kong, built a Ponzi pyramid by using bitcoin. The investment firm disappeared with 387 million USD worth of bitcoin. Two suspects were later arrested in Taiwan during the summer 2015. [37] [38]

When this type of incidents occurs, it is almost impossible for cryptocurrencies owner to recover their loss, because there is no way to legally pursue the company who lost or stole the coins.

- After The DAO attack, the alleged hacker threatened to sue anyone who tried to recover the stolen *ethers*. His main argument was this one: *'The Code is law'*. The computer code should be the only rule to be respected, and not the legal statutes. Following this principle would mean that this cyber robbery is not fraudulent, because the smart contract had a security flaw that enabled the hijacking. [39]

To resolve the problem, the *Ethereum* community decided to reverse the transaction history to give back *ether* to affected coin holders, and that decision lead to a huge controversy within the community.

Legitimacy

Trust is generally essential in business affairs. If regulated, cryptocurrencies will be granted a certain legitimacy and considered as safer than if they were unregulated. As a result,

cryptocurrencies could be used by a broader number of persons, because they would be more confident regarding this new technology rather than being sceptical.
This is what happened in Japan. The 1st April of 2017, Japan decided to give a legal framework to both cryptocurrencies and ICOs, which lead to a soaring use of it. [40] [41]

ICOs that went wrong

System hack: *CoinDash* (July 2017)

A start-up called *CoinDash* tried to raise funds though an ICO in July 2017. Investors could purchase *'CoinDash tokens'*, in exchange of the *Ether* cryptocurrency. To do so, they were asked to send the funds to the token's smart contract address. Apparently, the sending address have been modified into a fraudulent address by unidentified hackers. In only 30 minutes, investors sent to the fake address an amount of *Ether* equivalent to 7 million USD.

The start-up announced that it will provide tokens to people who have been affected by the hack before the shutdown of the website. [42]

Fraudulent ICO: *REcoin Group Foundation & DRC World* (September 2017)

In September 2017, the Securities and Exchange Commission (SEC) filed a complaint against *REcoin Group Foundation* and *DRC World*, two companies who raised funds through ICO. Both companies were supposed to invest in the real estate market and in diamonds. [43] [44]

However, the two ICOs were scams lead by the founder of the companies, Maksim Zaslavsiy:

- The *white papers* provided false information to investors.
- No tokens were given to investors.
- High returns were promised to investors, and the founder declared that brokers, lawyers and accountants had been hired, but all of this was totally false.
- Plus, the SEC highlights that the ICOs should have been notified to the regulatory body for registration, since the tokens issued by these ICOs were assimilated to financial instrument.

The crook tried to defend himself by claiming that the transactions were *'IMO'* (Initial Membership Offering), but the SEC didn't take it into account.
300,000 USD have been hijacked during these ICOs.

Technical issues: *AirSwap* (October 2017)

The 11th October of 2017, during an ICO, an investor tried to purchase tokens from *AirSwap* in exchange of 1700 *Ethereum* coin, which is equivalent of 508,000 USD.
However, the purchase failed for an unknown reason and the purchaser lost 236 ethers, which constitute a loss of 70,000 USD. [45]

Examples of China's ban of ICOs & the SEC's attempt to regulate

China

China represents a significant part of the cryptocurrency market. The use of cryptocurrencies is quite popular, since it bypasses the control over money moving out the country and that gambling is popular even though it is illegal in the country. Also, the Chinese government plans to launch its own digital version of the Yuan [46].
However, on the 4th of September, authorities began a ban policy over ICOs and cryptocurrencies. [47] [48] The country decided to ban ICOs, defining *"ICOs as an unauthorized fundraising tool that may involve financial scam"*. More precisely, the government asked the regulators to take a *"zero tolerance approach"* to cryptocurrencies. Basically, it means that Chinese start-ups cannot raise funds through ICOs anymore. As well, regulators forced domestic bitcoin trading platforms (OKCoin, BTCC China and Huobi.com) to *'voluntarily'* shut down, and asked companies to return money to ICO investors. [49]

Nonetheless, the Chinese ban highlights the fact that it is impossible for a government to totally forbid the use of cryptocurrencies. Cryptocurrency users can still use their coins by exchanging them in foreign trading platforms such as Japan. Also, many start-up founders began to register their companies in Singapore or Hong-Kong in order to keep raising funds through ICOs.

The motivation for this ban is quite unclear. Analyst explained these policies not only because of financial reasons, but as well because of political reasons. The Communist single party is seeking for stability [50]. Other assert that national regulator is trying to prevent fraud for the moment, and are planning to establish regulation regarding cryptocurrencies and ICOs in the future.

USA

In July 2017, the Securities and Exchange Commission (SEC) of the United-States proposed some rulings regarding cryptocurrencies and ICOs through a report investigating *TheDAO* [51] [52]. Basically, the SEC ruled that:

"These offers and sales have been referred to, among other things, as "Initial Coin Offerings" or "Token Sales." (…) the U.S. federal securities law may apply to various activities, including distributed ledger technology, depending on the particular facts and circumstances, without regard to the form of the organization or technology used to effectuate a particular offer or sale.(…) Whether or not a particular transaction involves the offer and sale of a security—regardless of the terminology used—will depend on the facts and circumstances, including the economic realities of the transaction (…)."

Even if the report is related to *The DAO* case, the rules is aimed to be applied to ICOs in general.

To sum up, this ruling is unclear [54] [55]. The SEC doesn't formally distinguish in which situation tokens will be considered as securities or not. In other words, it cannot be asserted when the SEC will have jurisdiction over tokens and ICOs, because it depends on *'particular facts and circumstances'*.

The report also mention the fact that cryptocurrencies exchange platforms should be soon regulated as well [53]. If these exchanges trade tokens and cryptocurrencies that are deemed as securities, then these platforms should meet the registration requirements imposed by the SEC.

However, this is a start for a legal framework of the US authorities on these transactions. It shows that whilst regulatory bodies are attempting to give a *'legal existence'* to ICOs and cryptocurrencies, they remain uncertain about which position adopt.

The Japanese example of initiatives to introduce regulation

In April 2017, Japan enacted a *Cryptocurrency Law* [56]. This is a pioneering bill since it is probably the first one across the world to expressly regulate cryptocurrencies. Among rules that have been settled, here are one of the most significant:

- Bitcoins are completely legal and are now accepted as a way of payment within the country, like the official national currency, the Yen.

- Platforms providing services of cryptocurrencies exchanges are now subject to registration requirements with the Financial Services Agency (FSA).

  In September 2017, the FSA accepted to register 11 companies as cryptocurrencies exchanges operators.

- These virtual platforms are required to keep a minimum capital stock of 10 million Yen (≈ 90,000 USD).

- Annual audit will be imposed to companies providing cryptocurrencies exchanges services.

- A new regulatory team of 30 members lead by a *'Chief of cryptocurrencies monitoring'* has been set up within the FSA to control exchanges platforms.

Unfortunately, this law doesn't provide a complete legal framework to this field. Indeed, ICOs have not been regulated by the Japanese authorities. It seems that initial coin offerings are still subject to debate within the FSA, and some point such as accountability rules for ICOs have not been resolved [57]. By adopting these provisions, Japanese authorities try to prevent incidents, such as the sudden shutdown of *Mt. Gox* in 2014, the platform which was the one of the world's biggest exchange and located in Japan.

Optimism for a future regulation

A key element of the blockchain philosophy is transparency. It is an open-source based technology and most of the cryptocurrencies and firms using ICOs aim to bypass the traditional financial system. Auto-regulation is then a core principle in the cryptocurrency system. However, the hack of *TheDao*'s smart-contracts illustrates the potential risk of an auto-regulated solution.

During the next years, regulation will probably be the main challenge for governments regarding blockchain technologies. Though, a wide range of factors should be bore in mind of regulators. Reaching a complete legal framework for blockchain and cryptocurrencies is going to be complex and delicate, because of many reasons [58][59]:

- In many ways, law is not adapted to this technology.

  For instance, Bitcoins raise issues of property law. Bitcoins are just an accumulation of number into a numeric public ledger. *But who the bitcoin blockchain protocol belongs to?* Even though this question would be resolved, English property law would hardly applicable to Bitcoins, because there are neither tangible property nor intangible property. As well, some intellectual property problematics can be raised.

- Regulation operate in a *vertical* way, which means that rules are established for a particular concept, or sector etc. The problem is that blockchain technologies have a

horizontal approach, since they can be applied to various sectors and industries. Consequently, rules will need to cover a broad scope of situations.

- As well, blockchains are decentralized and enable cross border transactions. There might be a potential risk of jurisdictions conflicts to determine which authority is going to be competent to resolve any litigation. Blockchain will have to be compliant with various legal regimes, which involves a consensus among worldwide regulators.

- Plus, blockchain technologies are too new and not many precedents exist, which makes it tricky for regulators to foresee all kind of situations that may arise from a legal point of view. This is even more difficult given that blockchain can be extremely complex for actual regulators to understand.

- At last, authorities should keep a soft approach toward blockchain. If rules are too strict, regulation could have negative consequences on the development of blockchain technologies, which are not only applicable to the financial sector.

It has been illustrated through the last questions that regulation is necessary, and it seems to be the only solution since it is impossible to stop the expansion of cryptocurrencies and ICOs. Indeed, ban isn't efficient because cryptocurrencies users and start-ups seeking funding through ICOs will always be able to bypass prohibitions.

Hopefully, regulators should give a legal framework to the blockchain technology and *in fine* to cryptocurrencies and ICOs. This is an essential stage for blockchain technologies to grow and acquire credit from the public.

Bank of England

In March 2017, the Bank of England linked with *Ripple,* a blockchain specialist start-up, in order to launch a trial program which aimed to test a *'blockchain-based technology that would enable cross-border payments'* instantaneously and without risks [60][61][62].

This type of initiative depicts to what extent national institutions can be eager to adopt blockchain technologies rather than forbid them. It is also an illustration on how central banks can take advantage of blockchain and explore new financial solution, rather than being be outdated by this technology.

IMF

In September 2017, Christine Lagarde, the International Monetary Fund (IMF) managing director, evoked her enthusiasm about cryptocurrencies. The former French Ministry for the Economy and Finance encouraged banks and government not to ignore the potential and the development of cryptocurrencies and blockchain technology [63].

She raised potential scenarios in which cryptocurrencies could be a solution for countries with an *'unstable national currency'* or where payment services are difficult to access for citizens in remote regions. One day, people may prefer these currencies because we could reach a point where cryptocurrencies will be more secured and accessible than conventional currencies [64] [65].

Such statement by a person as influent as Christine Lagarde brings optimism about the future of blockchain and cryptocurrencies. Nowadays, these technologies are too unstable to be completely adopted by national regulators. However, we can hopefully expect governments to carefully pay attention to cryptocurrencies, ICOs, and other blockchain-based technologies and embrace them rather than banning it.

References

[1] Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
Available at: https://bitcoin.org/bitcoin.pdf

[2] Browne, R. (2017). *Blockchain technology being considered by more than half of big corporations.*
Available at: https://www.cnbc.com/2017/07/31/blockchain-technology-considered-by-57-percent-of-big-corporations-study.html

[3] Narayanan, A. (2015). *"Private blockchain" is just a confusing name for a shared database*
Available at: https://freedom-to-tinker.com/2015/09/18/private-blockchain-is-just-a-confusing-name-for-a-shared-database/

[4] Greenspan, G. (2016) *Blockchains vs centralized databases*
Available at: https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/

[5] BlockGeeks (2017) *17 Blockchain Applications That Are Transforming Society*
Available at: https://blockgeeks.com/guides/blockchain-applications/

[6] Ethereum Wiki (2017) *ERC20 Token Standard*
Available at: https://theethereum.wiki/w/index.php/ERC20_Token_Standard

[7] Ethereum Developers (2015) *EIP20: ERC20 proposal*
Available at: https://github.com/ethereum/eips/issues/20

[8] Volpicelli, G. (2017*) The $3.8bn cryptocurrency bubble is a huge deal. But it could break the blockchain*.
Available at: http://www.wired.co.uk/article/what-is- initial-coin- offering-ico- token-sale

[9] The Economist (2017) *The market in Initial Coin Offerings risks becoming a bubble*.
Available at: https://www.economist.com/news/finance-and- economics/21721425-it-may-also- spawn-valuable-innovations-market-initial- coin-offerings

[10] Smith and Crown (2016) *What is an ICO?*
Available at: https://www.smithandcrown.com/wp-content/uploads/2016/06/smithandcrown_ico_handout_v2.0.pdf

[11] Kaminska, I. (2017*) ICOs and the money markets*.
Available at: https://ftalphaville.ft.com/2017/07/18/2191577/icos-and- the-money- markets/

[12] Autonomous (2017) *Token Mania*.
Available at: https://autonomous.app.box.com/v/tokenmania

[13] Naumoff, A. (2017) *Blockchain Is Like Badass Tractor: How Russian Farmer Launched ICO.*
Available at: https://cointelegraph.com/news/blockchain-is- like-badass- tractor-how- russian-

farmer-launched- ico

[14] Benoliel, M. (2017) *Hack your Funding with an Initial Coin Offering.*
Available at: https://medium.com/startup-grind/hack-your- funding-with- an-initial- coin-offering- 2a2a0614bddf

[15] Groden, C. (2017) *Understanding China's Crackdown on Bitcoin and ICOs.*
Available at: https://lawfareblog.com/understanding-chinas- crackdown-bitcoin- and-icos

[16] Sunnarborg, A. (2017) *ICO Investments Pass VC Funding in Blockchain Market First.*
Available at: https://www.coindesk.com/ico-investments- pass-vc- funding-in- blockchain-market- first/

[17] The Financial Times (2017) *In cryptocurrencies, tech and speculation meet.*
Available at: https://www.ft.com/content/83a496fe-995b- 11e7-b83c- 9588e51488a0

[18] Nussbaum, J. (2017) *The ICO Bubble.*
Available at: https://medium.com/@josh_nussbaum/the-ico- bubble-6cadefaf8cbc

[19] Kravchenko, P. (2017) *Is the ICO market currently a ponzi?*
Available at: https://medium.com/@pavelkravchenko/is-the- ico-market- a-ponzi- 34bddefca115

[20] Coindesk (2017) ICO Tracker
Available at: https://www.coindesk.com/ico-tracker/

[21] Financial Times (2017) *Australia regulator warns of ICO 'scams'*
Available at :https://www.ft.com/content/1f60eb3d-2620-3be2-9e59-865b0b62a95c

[22] Haig, S. (2017) *Singapore to Regulate Crypto-Based Businesses, Not Cryptocurrency Itself*
Available at: https://news.bitcoin.com/singapore-to-regulate-cryptocurrency-based-businesses-not-cryptocurrency-itself/

[23] Rose R. (2017) *Singapore's Central Bank Plans to Regulate Bitcoin Payments*
Available at: https://www.coindesk.com/singapores-central-bank-plans-to-regulate-bitcoin-payments/

[24] Wikipedia (2017) *Legality of bitcoin by country or territory*
Available at: https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory

[25] BitLegal (2017) *Legal World Map*
Available at : http://bitlegal.io/

[26] Leyva, J. (2017) *Hacienda turna al Senado proyecto para crear Ley Fintech*
Available at: http://www.elfinanciero.com.mx/economia/hacienda-turna-al-senado-ley-fintech.html

[27] Estanol, A. (2017) *LA LEY FINTECH RELAJA EL USO DE BITCOIN*
Available at: http://expansion.mx/empresas/2017/09/18/la-ley-fintech-relaja-el-uso-de-bitcoin

[28] Rudnitsky, J. (2017) *Russia's Central Bank Is Also Skeptical of Cryptocurrency*
Available at: https://www.bloomberg.com/news/articles/2017-09-14/bank-of-russia-channels-china-in-seeing-cryptocurrency-pyramid

[29] Helms, K. (2017) *Russian Regulators Disagree on Crypto Regulation, Postpone to Next Year*
Available at: https://news.bitcoin.com/russian-regulators-cryptocurrency-regulations-postpone/

[30] Wirdum, A. (2017) *Bolivian Authorities Arrest 60 'Cryptocurrency Promoters'*
Available at: https://bitcoinmagazine.com/articles/bolivian-authorities-arrest-60-cryptocurrency-promoters/

[31] Kharif, O. (2017) *Global Regulators Play Bitcoin Whack-a-Mole as Demand Explodes*
Available at: https://www.bloomberg.com/news/articles/2017-10-11/global-regulators-play-bitcoin-whack-a-mole-as-demand-explodes

[32] Choudhury, S. (2017) *Governments want to control cryptocurrencies — but there's a danger to too many rules*
Available at: https://www.cnbc.com/2017/09/12/regulators-are-turning-their-attention-to-cryptocurrencies.html

[33] Steptoe and Johnson LLP (2017) *Blockchain and Cryptocurrency: The Emerging Regulatory Framework*
Available at: https://www.lexology.com/library/detail.aspx?g=85676d29-5a50-4437-9405-2dd295a69dbd

[34] IRS (2014) *IRS Virtual Currency Guidance : Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply*
Available at: https://www.irs.gov/newsroom/irs-virtual-currency-guidance

[35] Court of Justice of the European Union (2015). *The exchange of traditional currencies for units of the 'bitcoin' virtual currency is exempt from VAT*
Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128en.pdf

[36] Santori, M. (2017) *Silk Road Goes Dark: Bitcoin Survives Its Biggest Market's Demise*
Available at: https://www.coindesk.com/bitcoin-milestones-silk-road-goes-dark-bitcoin-survives-its-biggest-markets-demise/

[37] Southurst, J. (2015) *Hong Kong's MyCoin Disappears With Up To $387 Million, Reports Claim*
Available at: https://cryptofr.com/topic/923/mycoin-disparait-avec-340-millions-d-euros/2

[38] Price, R. (2015) Hong Kong bitcoin exchange disappears with at least $8.1 million
Available at: http://uk.businessinsider.com/mycoin-ponzi-scheme-allegations-losses-2015-2

[39] Thierry Bonneau & Thibault Verbiest *(2017) Fintech et Droit*, pages 78-79, RB Édition

[40] Young, J. (2017) *U.S. May Follow Japan to License Bitcoin and Cryptocurrency Exchanges*
Available at: https://www.cryptocoinsnews.com/the-us-may-follow-japan-to-license-bitcoin-and-cryptocurrency-exchanges/

[41] Norrie, A (2017) *Opinion: How Barclays Seeking Cryptocurrency Regulation Impacts Bitcoin*
Available at: https://www.cryptocoinsnews.com/how-barclays-seeking-cryptocurrency-regulation-impacts-bitcoin/

[42] Levy, A (2017) *Fraudsters just stole $7 million by hacking a cryptocoin offering*
Available at: https://www.cnbc.com/2017/07/17/coindash-website-hacked-7-million-stolen-in-ico.html

[43] Bohic, C. (2017) *Les États-Unis épinglent une fraude aux ICO*
Available at: http://www.itespresso.fr/etats-unis-fraude-ico-172424.html?inf_by=59dcee47681db8d7448b4622

[44] Chaparro, F. (2017) *The SEC comes down on 2 cryptocurrency-based fundraising schemes*
Available at: http://www.businessinsider.com/recoin-group-foundation-drc-world-ico-sec-fraud-charges-cryptocurrency-2017-9

[45] Leising, M. (2017) *Someone Just Lost $70,000 in a Failed ICO Purchase Attempt*
Available at: https://www.bloomberg.com/news/articles/2017-10-11/buyer-beware-as-70-000-goes-up-in-smoke-on-broken-ico-trade

[46] Godwin, A. (2017) *China's Crackdown on Cryptocurrency Trading – A Sign of Things to Come*
Available at: https://thediplomat.com/2017/09/chinas-crackdown-on-cryptocurrency-trading-a-sign-of-things-to-come/

[47] Choudhury, S. (2017) *China bans companies from raising money through ICOs, asks local regulators to inspect 60 major platforms*
Available at: https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html

[48] Rapoza, K. (2017) *What China Ban? Cryptocurrency Market Cap Rebounding*
Available at: https://www.forbes.com/sites/kenrapoza/2017/09/28/china-ico-ban-bitcoin-crypto-currency-market-cap-returns/#10e5785d6c21

[49] Financial Times (2017) *Beijing set to shut bitcoin exchanges to ensure price stability*
Available at: https://www.ft.com/content/b2f1d198-96df-11e7-a652-cde3f882dd7b

[50] Bloomberg News (2017) *Bitcoin Crashes Again After China Moves to Halt Exchange*
Available at : https://www.bloomberg.com/news/articles/2017-09-15/china-is-said-to-call-for-bitcoin-exchange-halt-by-month-end-j7lblmdg

[51] Securities and Exchange Commission (2017) *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934:The DAO*
Available at: https://www.sec.gov/litigation/investreport/34-81207.pdf

[52] Roberts, J. (2017) *The SEC's Big Digital Coin Ruling: What It Means*
Available at: http://fortune.com/2017/07/26/sec-icos/

[53] Financial Times (2017) AlphaVille
Avaialble at: https://ftalphaville.ft.com/2017/07/26/2191851/cryptocurrency-exchanges-could-be-subject-to-sec-regulation-too/

[54] Churchouse, T. (2017) *The SEC is finally starting to regulate Bitcoin and other cryptocurrencies*
Available at: http://www.businessinsider.com/bitcoin-price-security-equity-sec-2017-7

[55] Jeong, S. (2017) *The SEC is throwing a damper on ethereum madness*
Available at: https://www.theverge.com/2017/7/27/16046978/sec-ethereum-cryptocurrency-dao-ico-bitcoin-blockchain

[56] Kharpal, A. (2017) *Bitcoin rallies to hit a one-month high but experts warn of a volatile upcoming event*
Available at: https://www.cnbc.com/2017/10/09/bitcoin-price-hits-one-month-high-volatility-ah ead.html

[57] Asian Review (2017) *Japan to begin supervision of cryptocurrency exchanges*
Available at: https://asia.nikkei.com/Politics-Economy/Policy-Politics/Japan-to-begin-supervision-of-cryptocurrency-exchanges

[58] Eversheds (2016) *Blockchain – Considering the Regulatory Horizon*
Avaialble at : https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/blockchain-%E2%80%93-considering-regulatory-horizon

[59] Filippi, P. (2016) *WE MUST REGULATE BITCOIN. PROBLEM IS, WE DON'T UNDERSTAND IT*
Available at: https://www.wired.com/2016/03/must-understand-bitcoin-regulate/

[60] Burton, L. (2017) *Bank of England trials artificial intelligence and blockchain in bid to stay ahead of the pack*
Available at : http://www.telegraph.co.uk/business/2017/03/17/bank-england-trials-artificial-intelligence-blockchain-bid-stay/

[61] Financial Times (2017) *Bank of England successfully tests new payment method*
Available at: https://www.ft.com/content/a8d997a0-6605-11e7-8526-7b38dcaef614

[62] Zagone, R. (2017) *Results of the Bank of England/Ripple Proof of Concept Published Today*
Available at: https://ripple.com/insights/results-of-the-bank-of-englandripple-proof-of-concept-published-today/

[63] Lagarde, C. (2017) *Central Banking and Fintech—A Brave New World?*
Available at https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world

[64] De, N. (2017) IMF's Lagarde: Ignoring Cryptocurrencies 'May Not Be Wise'
Available at: https://www.coindesk.com/imf-head-christine-lagarde-it-may-not-be-wise-to-dismiss-virtual-currencies/

[65] Hackett, R. (2017) IMF Head: Cryptocurrency Could Be the Future. Really.
Available at: http://fortune.com/2017/10/02/bitcoin-ethereum-cryptocurrency-imf-christine-lagarde/

APPENDIX A

Technical Workshop

Along with the report there are technical instructions and ready code for deploying a Hello World smart contract to the Ethereum blockchain and creating your own ERC20 Token. Please follow the link below to get started.

https://github.com/UoG-Fintech-Society/blockchain-cryprocurrencies-workshop-25-10-2017