Grant Thornton

An instinct for growth™

Global

Intelligence

Technology

What is blockchain?

Introduction

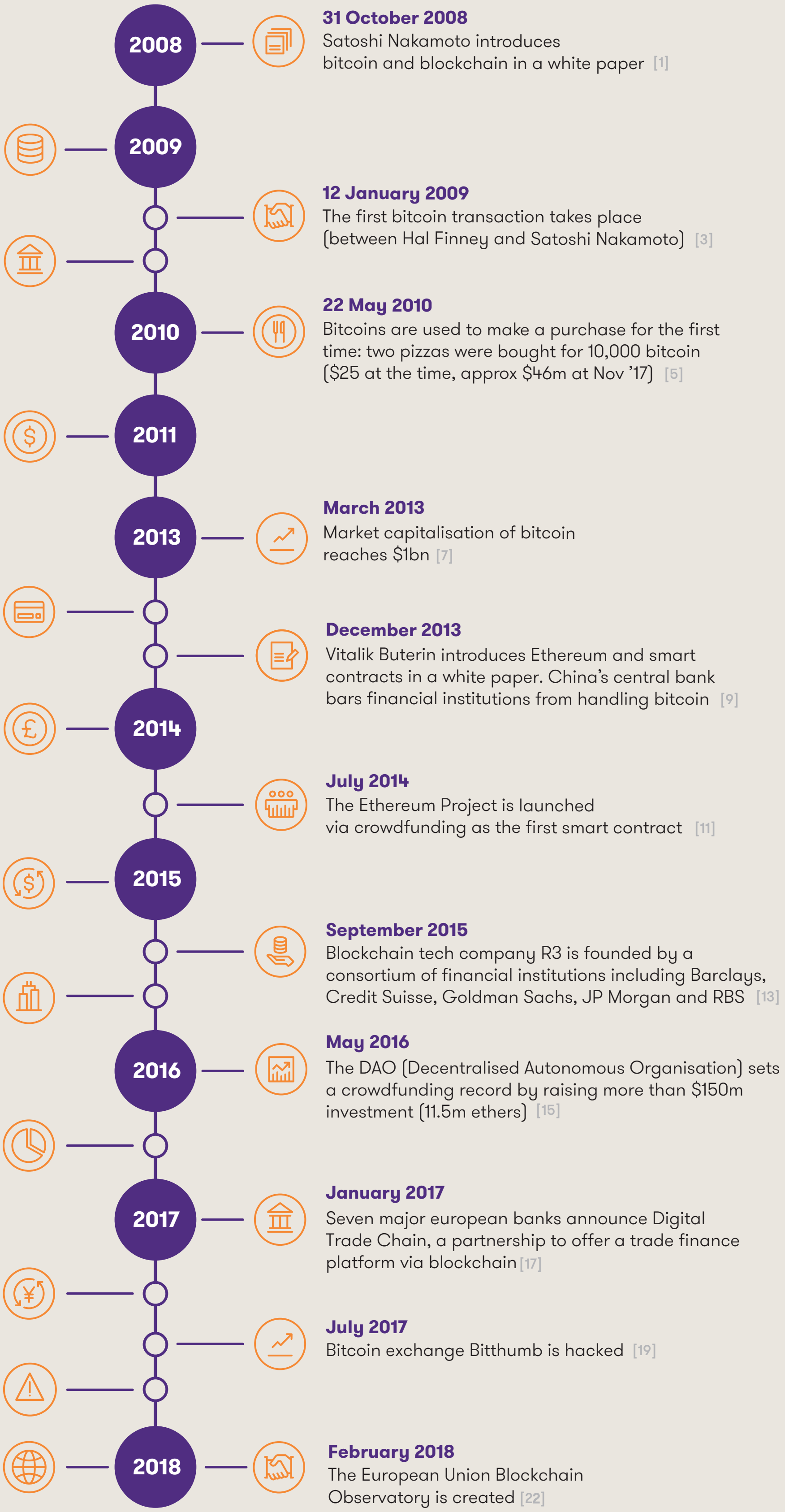
Blockchain technology is designed for the exchange of information and transactions between two or more participants through 100% secure and irreversible coding. A centralised middleman is not required to identify and certify the information being exchanged, rather this information is distributed among a number of independent blockchain network participants (nodes) who each record and validate the information without the need for trust between each other. Each participant has an exact copy of the information, which allows them to carry out transactions that are traceable and cannot be forged.

Blockchain's potential stretches beyond its obvious impact on the banking and financial sector and industries such as insurance, energy, construction and pharmaceuticals, etc. are effectively applying this technology.

Contents

The blockchain timeline

From inception to maturity



2008

31 October 2008
Satoshi Nakamoto introduces bitcoin and blockchain in a white paper [1]

2009

3 January 2009
The first bitcoin transactions – the 'Genesis Block' – are mined [2]

12 January 2009
The first bitcoin transaction takes place (between Hal Finney and Satoshi Nakamoto) [3]

31 October 2009
The first bitcoin exchange, the Bitcoin Market, is established [4]

2010

22 May 2010
Bitcoins are used to make a purchase for the first time: two pizzas were bought for 10,000 bitcoin ($25 at the time, approx $46m at Nov '17) [5]

2011

9 February 2011
Bitcoin exchange value reaches parity with the US dollar [6]

2013

March 2013
Market capitalisation of bitcoin reaches $1bn [7]

June 2013
The first major virtual currency theft: 25,000 bitcoin stolen from Bitcoin Forum founder's wallet [8]

December 2013
Vitalik Buterin introduces Ethereum and smart contracts in a white paper. China's central bank bars financial institutions from handling bitcoin [9]

2014

February 2014
HMRC in the UK classifies bitcoin as private money: VAT will not be charged on the mining or exchange of bitcoin. Bitcoin exchange Mt. Gox is hacked [10]

July 2014
The Ethereum Project is launched via crowdfunding as the first smart contract [11]

2015

April 2015
NASDAQ begins a blockchain trial [12]

September 2015
Blockchain tech company R3 is founded by a consortium of financial institutions including Barclays, Credit Suisse, Goldman Sachs, JP Morgan and RBS [13]

December 2015
The Linux Foundation establishes the Hyperledger Project [14]

2016

May 2016
The DAO (Decentralised Autonomous Organisation) sets a crowdfunding record by raising more than $150m investment (11.5m ethers) [15]

June 2016
The DAO loses a third of its ethers – approx $50m – in a vulnerability attack [16]

2017

January 2017
Seven major european banks announce Digital Trade Chain, a partnership to offer a trade finance platform via blockchain [17]

April 2017
Virtual currencies are officially recognised in Japan [18]

July 2017
Bitcoin exchange Bitthumb is hacked [19]

August 2017
The number of bitcoins in circulation reaches 16.5m [20]

2018

January 2018
Switzerland to begin accepting tax payments in bitcoin [21]

February 2018
The European Union Blockchain Observatory is created [22]

References

1. http://nakamotoinstitute.org/bitcoin/
2. https://en.bitcoin.it/wiki/Genesis_block
3. https://blockexplorer.com
4. https://en.bitcoin.it/wiki/Bitcoin_Market
5. https://en.bitcoin.it/wiki/Pizza
6. https://blockchain.info/charts/market-price
7. https://en.bitcoin.it/wiki/Category:History
8. https://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency
9. http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
10. http://www.ibtimes.co.uk/hmrc-re-classify-bitcoin-private-money-1432718
https://www.wired.com/2014/03/bitcoin-exchange/
11. http://ethdocs.org/en/latest/introduction/history-of-ethereum.html
12. https://www.coindesk.com/nasdaq-becomes-latest-firm-to-trial-blockchain-technology/
13. https://www.r3.com/about/
14. https://en.wikipedia.org/wiki/Hyperledger
15. https://bitcoinmagazine.com/articles/the-dao-raises-more-than-million-in-world-s-largest-crowdfunding-to-date-1463422191
16. https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cyber currency-project.html
17. https://www.cryptocoinsnews.com/7-major-european-banks-form-blockchain-platform-digital-trade-chain
18. https://www.cnbc.com/2017/09/29/bitcoin-exchanges-officially-recognized-by-japan.html
19. http://uk.businessinsider.com/south-korean-bitcoin-exchange-bithumb-hacked-ethereum-2017-7?r=US&IR=T
20. https://blockchain.info/charts/total-bitcoins
21. https://news.bitcoin.com/chiasso-switzerland-to-allow-citizens-to-pay-taxes-in-bitcoin
22. https://ec.europa.eu/digital-single-market/en/eu-blockchain-observatory-and-forum

Blockchain glossary

Blockchain A type of distributed digital ledger to which data is recorded sequentially and permanently in 'blocks'. Each new block is linked to the immediately previous block with a cryptographic signature, forming a 'chain'. This tamper-proof selfvalidation of the data allows transactions to be processed and recorded to the chain without recourse to a third party certification agent. The ledger is not hosted in one location or managed by a single owner, but is shared and accessed by anyone with the appropriate permissions – hence 'distributed'.

Chain A package of data containing multiple transactions over a given period of time.

Block The cryptographic link that keeps blocks together using a 'hash' function.

Data mining The process of solving cryptographic problems using computer hardware to add newly hashed blocks to a public blockchain such as bitcoin. In fulfilling this function, successful data miners keep the blockchain actively recording transactions and, as an incentive, are awarded newly minted bitcoins for their trouble.

Ethereum A public blockchain system developed as an open-source project, its architecture running remotely on the Ethereum Virtual Machine. It uses 'ethers', a cryptocurrency, as its token and supports the storage and execution of 'smart contracts'.

Hash The result of applying an algorithmic function to data in order to convert them into a random string of numbers and letters. This acts as a digital fingerprint of that data, allowing it to be locked in place within the blockchain.

Hyperledger An umbrella project set up by the Linux Foundation comprising various tools and systems for building open-source blockchains.

Node A copy of the ledger operated by a participant with a blockchain network.

Oracle A bridge from a blockchain to an external data source that allows a smart contract to complete its business by referencing timely real-world information. An oracle might allow a smart contract to access consumer energy usage, live train timetables, election results, and so on.

Peer-to-peer (P2P) The direct sharing of data between nodes on a network, as opposed to via a central server.

Permissioned ledger A large, distributed network using a native token, with access restricted to those with specific roles.

Private blockchain A closely controlled network operated by consortia in which the data is confidential and is accessed only by trusted members. Private blockchains do not require a token.

Private key A unique string of data that represents proof of identification within the blockchain, including the right to access and own that participant's wallet within a cryptocurrency. It must be kept secret: it is effectively a personal password.

Proof of stake The mechanism by which participants earn the right to add new blocks and so earn new tokens, based on how much of that currency they already hold.

Proof of work Repeatedly running a hash function, the mechanism by which data miners win the right to add blocks to a bitcoin-style blockchain.

Public blockchain A large distributed network using a native token (such as bitcoin), open to everyone to participate and maintain.

Public key A unique string of data that identifies a participant within the blockchain. It can be shared publicly.

Smart contracts Custom software logic that executes automated events when data is written to the blockchain according to rules specified in the contract.

Token The means of exchange to give value to a transaction,; typically a native cryptocurrency. Some non-currency blockchain architectures can be tokenless.

What is blockchain? Exploring the fact and fiction

Distributed ledgers have grown beyond their cryptocurrency roots and the once-emerging technology is at last ready for your business to put it to work right now.

An alternative currency

Blockchain, the technology behind the bitcoin digital currency, has broken loose from its origins. Given the explosion of interest in blockchain beyond financial services across utility, transportation, business and governmental industries - it is gaining momentum.

The days of talking about blockchain's potential have passed and organisations around the globe are not just building proofs of concept but many are already using it for live applications. Blockchain is being rolled out across sectors from energy supply and property sales to facilities management, environmental provenance and container shipping. However, the technology remains surrounded by a mist of uncertainty.

To bring some clarity and pragmatism to our understanding of the technology, and evaluate how it can benefit an organisation, we need to remove it from its digital currency origins.

The genesis of bitcoin

In 2009, in the wake of the worldwide financial meltdown, an anonymous developer(s) using the moniker Satoshi Nakamoto created an alternative, digital-only financial currency called bitcoin.

Bitcoin was designed to enable simple financial transactions to take place between its participants, completely independently of banking institutions. Each transaction is recorded and validated not by a bank, but by the software architecture of the transaction system itself.

This underlying transaction technology system is blockchain.

What is blockchain technology?

It's essentially a live ledger that records the transactions of a 'token' – in this case, the bitcoin currency – arranged in data batches called 'blocks' that use cryptographic validation to link themselves together. Put simply, each data block references and identifies the previous block using a 'hash' function, forming an unbroken chain, hence the name.

This approach to recording data boasts a significant advantage over traditional financial ledgers and databases. By having every data block validate its direct predecessor, the ever-lengthening ledger is strictly sequential and permanent: it's not possible to amend, mask or delete transactions that have already been recorded. Any attempt to do so would break the cryptographic chain and be immediately flagged to all participants.

In principle, a blockchain ledger is a tamper-proof database with built-in validation.

The distribution of blockchains

The second key feature of blockchain is that the ledger is not maintained in a single location or managed by a single, monopolistic third-party. Instead, it is said to be 'distributed', existing on any number of computers at the same time in such a way that anybody with an interest can obtain a live copy of it.

As such, blockchain is sometimes referred to as a 'mutual distributed ledger' or MDL. It employs this mutual consensus mechanism across the network to guarantee trust in the whole system.

"Blockchain is based on a distributed, decentralised paradigm technology which allows the exchange of any kind of value between peers without using intermediaries" summarises Luis Pastor, partner of IT consulting and innovation at Grant Thornton Spain.

"The magic here is that you don't need a third party to make sure that what is happening in the network between peers is correct."

> “Blockchain is based on a distributed, decentralised paradigm technology which allows the exchange of any kind of value between peers without using intermediaries.”

Luis Pastor
Partner, IT consulting and innovation
Grant Thornton Spain

Staying with the digital currency concept, this would enable you to send money from, say, one country to another without having to pass through a clearing house. Rather than taking two or three days for the transaction to be validated by a third party, the sender and recipient are automatically identified by their encrypted digital signatures, the money is transferred from one wallet to another and the transaction is recorded to the ledger within seconds.

Blockchain networks

“With blockchain,” says Pastor, “we can represent any kind of value through tokens. In the financial world that could be a bond or a share, or property such as a house. The whole network, using its consensus mechanism, would validate the transaction to transfer the ownership.

It would be possible to represent any real-world asset as tokens on a blockchain. Once a network is created with different parties, these assets are going to be unique. The concept of ownership is really strong and made clear to everyone playing by these rules on a blockchain network.”

Applications beyond so-called cryptocurrencies were first proven with the development of the Ethereum blockchain platform in 2013. Although the Ethereum eco-system encompasses its own digital currency known as ethers as its token, the platform introduced the ability to include not just basic numeric records but also small logistical programs into your ledgers.

These are known as ‘smart contracts’.

Smart contracts

“These allow you to make arrangements or agreements between parties,” says Pastor, “for example, to send funds on a certain date or to make changes to an asset’s properties.

Another classic example of a smart contract in action might be the concept of insurance for delayed airline flights. When a traveller buys travel insurance for a specified flight, the purchase could be recorded in a blockchain. This smart contract is designed to check automatically with an external data source whether that flight suffers any delay and, if appropriate, pass a compensation payment straight to the traveller’s wallet without the usual administrative overhead.

The potential for business-oriented blockchains has attracted the interest of big names in the IT industry far beyond its hacker roots. Microsoft customers, for example, can try out their own blockchain proofs of concept on its Azure cloud.

It’s important, then, to recognise that there is more than one way to implement blockchain.

Privacy concerns around blockchain

A key concern with raw blockchain is that its distribution aspect can be a disincentive. That is, a group of parties with an interest in establishing a blockchain to record industry-wide transactions may well be competitors willing to share limited privileged data flow with each other, but not with the public at large.

This need has led to the development of private blockchains, sometimes referred to as ‘permissioned ledgers’. These are protected by security barriers and made available only to interested parties with permission to access the data.

With a private blockchain, richer data can be recorded into the ledger that might otherwise breach data security requirements laid down by regulatory bodies. Bitcoin's blockchain, for example, records transactions and wallet references as public keys but contains no personal information as to whom the wallets belong.

Bitcoin and energy consumption

One concern about blockchain is that it is energy-intensive. Being the first major system based on the technology, bitcoin is arguably the worst offender.

Trust in blockchain is centred around data miners to keep the system up and running, for which they earn a small fraction of newly minted bitcoins, but the server farms employed in the relentless data mining process are said to chew through as much energy as a small city. Many of these server farms are operated in China, whose rising carbon emissions are a matter of record.

Add to this the energy requirement of every bitcoin owner to keep their wallets updated with the current version of the ledger, to which new blocks are added every few seconds, and you're talking about a lot of electricity. It has been estimated that a bitcoin transaction can be as much as 5,000 times more energy intensive than a Visa credit card transaction.

That said, these costs are offset given that blockchain allows for real time transactions and information sharing and, hence, little or no intermediary costs.

Moving forward

Blockchain can be designed to be leaner and less energy-intensive. A well-designed blockchain should be able to process tens of thousands of transactions per second and cost less than 0.00001c each – a far cry from bitcoin's seven transactions per second costing anything up to $2.50 each.

As a result, organisations that have been spending the last couple of years investigating blockchain have now begun taking their systems live and bringing customers and competitors alike into the fold. With the promise of speeding up data flow and removing administrative overheads, blockchain is as much about streamlining processes as just cutting costs.

In our next two articles, we look at the businesses currently active in the roll-out of real-world, commercial blockchain solutions, as well as practical steps explaining how to set about introducing blockchain into your own organisation.

There used to be a joke that the most common software employed in blockchain development was PowerPoint.

Not any more.

The business realities of blockchain, today

How has blockchain been put into practice as part of live, commercial business solutions?

"[Blockchain] spells the death of the invoice," proclaims Lee Pruitt, co-founder and CEO of spend-control-as-a-service provider InstaSupply.

"There's a huge amount of inefficiency today in business-to-business transactions," he continues. "There are a lot of steps involved when businesses place orders with suppliers and how they match them with the supplier's invoices in order to be able to pay them.

"When the accounts payable department goes through an invoice, someone has to check they received all the items being invoiced for. And is it the right price? Did the goods arrive on time? When is the supplier asking for payment? Are the payment terms correct? Is it even the right supplier?"

If there's the slightest query, the invoice is pushed to another department to get reviewed again at length by another human. Business-to-business is one of the sectors in which making and settling a transaction can involve a massive amount of manual work. In some cases, suppliers are forced to wait up to 90 days to get paid.

"Blockchain eliminates all of that," says Pruitt, "because you have a digital form of trust and verification that takes out a lot of these transactions being handled today manually."

Blockchain and data optimisation

InstaSupply is not alone in making use of blockchain in this fashion: the likes of Barclays, Maersk and Microsoft are among the very large enterprises leading the charge.

Maersk is not the only shipping company throwing its weight behind blockchain networks. Marine Transport International has developed a marine supply network using blockchain to connect stakeholders, comprising ports, shipping lines, land-based haulers, freight forwarders and other interested parties.

Marine Transport's CEO, Jody Cleworth, recounts how it came about: "Around July of 2016, there was a regulatory change in the shipping industry. This enabled us to create connectivity inside the land-side supply chain – that's before the container gets to the terminal: the truck, the load point, the shipper, the physical asset-on-asset loading of those goods inside the container.

"We realised that we could create an application which would create an ecosystem amongst these different actors to accelerate data along the land-side supply chain to meet this change. We could communicate the specifics of that container to the terminal before it was allowed into the terminal or allowed on board the ship."

Streamlining through blockchain

Having considered and quickly dismissed the bitcoin blockchain, the company came across tech specialists Agility Sciences which was offering an enterprise-grade blockchain-as-a-service that anyone can connect to. Marine Technology discovered it could connect both legacy systems and new age EDI (electronic data interchange) protocols alike into the network, creating what Cleworth calls "a democratised connectivity".

"Now as containers are loading, data comes into the network, we process it with smart contracts, each a billable event. Then we update the applications so that users such as ourselves get notified with the various events that are going on in the container, and we push that data outside the network to the ports and the shipping lines before the truck driver has even changed into second gear to get out of that load point."

The barrier to entry to the network is low since participants themselves power it and provide its storage, whether that be via Amazon Web Services, Google, IBM Bluemix, or even their own office server. Marine Transport then earns specific fees automatically when milestones are reached in the smart contracts.

Blockchain and energy

Using blockchain to level the field was also the key driver behind a distributed energy trading system rolled out in Australia earlier this year by Power Ledger.

"I was looking at the proliferation of photovoltaic (PV) solar panels which many people have installed onto their rooftops over here," recalls Power Ledger MD and co-founder David Martin.

“The potential for blockchain business solutions is now out there, it’s just about utilising it.”

Markus Veith
Partner
Grant Thornton US

“The problem is that there’s no way of guaranteeing that you will get the benefit of the investment you make in rooftop PV. I might be working from 7am ‘til 7pm, so the sun’s gone down by the time I get home from work but my next door neighbour works from home, so he’s getting all the benefit of that free electricity off the roof.”

This scenario is a serious disincentive to install rooftop PV panels on blocks of flats, which account for 35 per cent of the housing stock in Australia. A big chunk of the population is therefore excluded from the distributed energy economy.

“What we needed was a technology platform able to demonstrate where energy was coming from at a distribution level and reward the person whose generation was being sold,” says Martin. “Blockchain provided us with the ability to do that: it allows us to identify the provenance of every kilowatt hour that is generated on-site or at a consumer’s premise and through a transactive platform and trading algorithm that energy is allocated to a particular consumer.”

Blockchain and trust

The immutable qualities of blockchain also ensure any trading arrangement can be trusted according to terms, conditions and a financial agreement tied into it.

One property making use of this system right now is a 14-unit development in Fremantle, Australia, designed for people on low-income support. The owners, a housing association, already owned the PV and battery system, and wanted to provide the cheapest electricity to their tenants in a fair manner.

The Power Ledger system sits behind the master meter of the property, identifying the consumption of energy per flat, where that energy came from and how it is priced; if one tenant uses more energy than his neighbour, he will exhaust his own discounted allocation from the rooftop PV without taking anyone else’s automatically switching to energy from the network and paying the full retail price for it.

Martin feels that blockchain’s boost to the growing distributed energy economy will ultimately force the major energy companies to adapt their own approach to the market.

A cultural shift

Markus Veith, partner at Grant Thornton US shares this view of blockchain as a driver for cultural change. He uses the analogy of the appearance of smartphones: they didn’t make us work faster so much as change the way we do things.

The real-world example he gives is cross-border peer-to-peer payments technology company, Circle, a rising star with whom he has been working over the last three years. Using Circle’s smartphone app, you can transfer money between users across borders free of charge and instantaneously.

Veith outlines a scenario: “Let’s say you’re a student originally from Brazil studying in the US and you ask your parents to send you money, say $500. Your parents in Sao Paolo then go in the app and send the equivalent of $500 in the Brazilian currency Real translated into dollars, and it arrives in a split second in your account. And it’s free.”

Blockchain acts as a trusted recording system, validating the transfer of funds without further intermediaries and automating the settlement between accounts. Once Circle customers have established their identities on its blockchain, trust and validation are a given.

The blockchain platform reduces the risk of collusion, fraud and cyber-crime in financial services. “It’s much more difficult to hack into a blockchain ledger than a traditional ledger in which you have one server,” observes Veith. “With a blockchain you have multiple servers and every server validates the blockchain. If someone tries to hack a server or fake a transaction, all the others will kick it out.”

The potential for blockchain based business solutions is now out there, it’s just about utilising it.

Contact

Our blockchain specialists have a diverse range of experience. They constantly research and stress test new blockchain technologies to understand their practical business application.

This knowledge means they can help you prepare for the future by integrating blockchain into your business with minimal disruption. To understand whether blockchain is right for your business, please contact:

Wayne Pisani
Partner, tax and regulatory corporate and
financial services
Grant Thornton Malta
T +356 20931000
E wayne.pisani@mt.gt.com

Grant Thornton

An instinct for growth™

grantthornton.com.mt

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions. This publication has been prepared only as a guide. No responsibility can be accepted by us for loss occasioned to any person acting or refraining from acting as a result of any material in this publication.

EPI.248