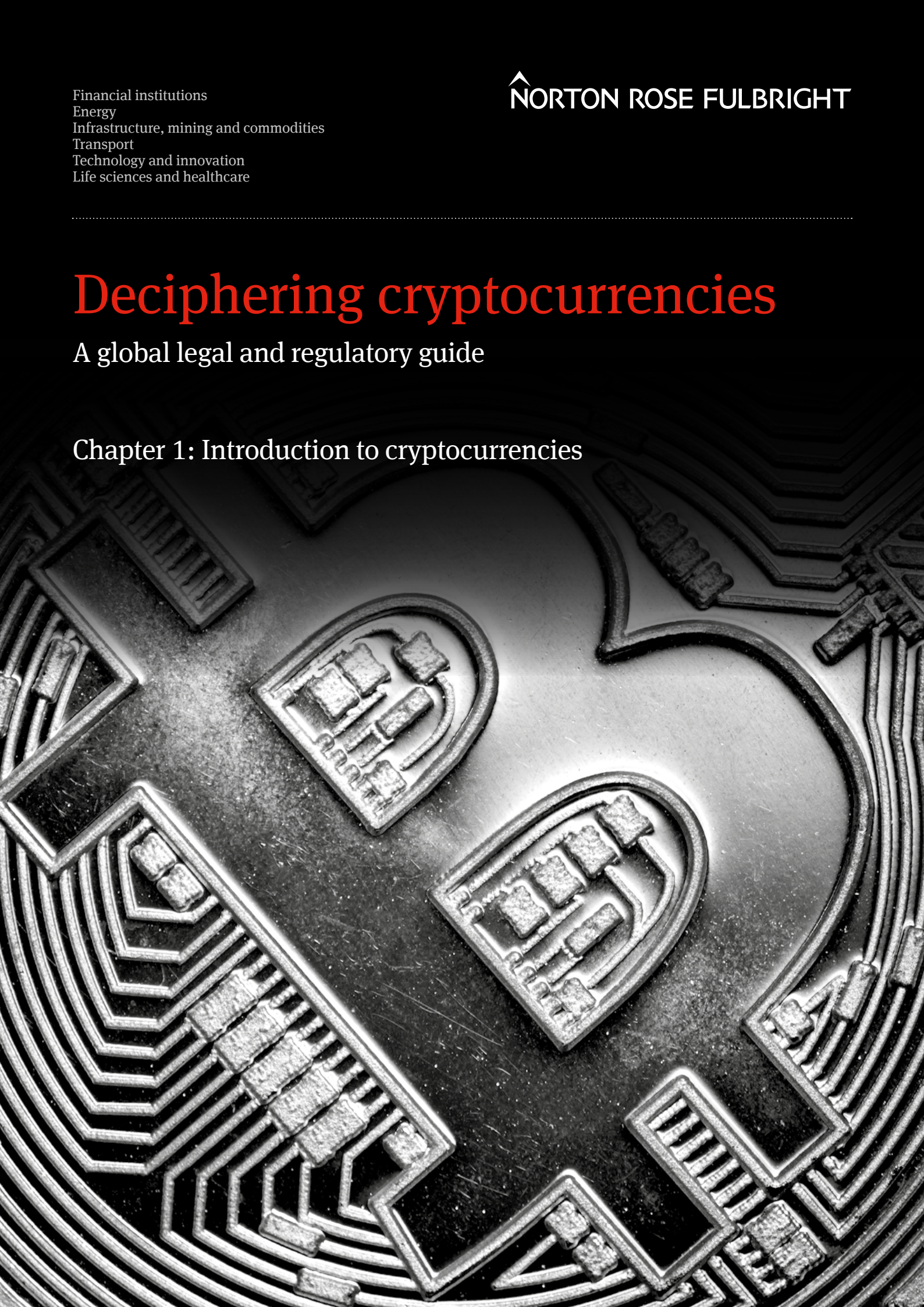
Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

# Deciphering cryptocurrencies

## A global legal and regulatory guide

## Chapter 1: Introduction to cryptocurrencies



# Norton Rose Fulbright

Norton Rose Fulbright is a global legal practice. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3800 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.

# Contents


Overview 04

**Introduction 06**
What is a cryptocurrency? 06
The development of cryptocurrencies 07
Adoption of cryptocurrency 09
Considerations for businesses looking at cryptocurrency technology 10

**How cryptocurrencies work in practice 13**
A decentralised network 13
How to complete a transaction in cryptocurrency 13
Mining 14

Global resources 15

Contacts 16

# Deciphering cryptocurrencies

## Overview

Use of, and interest in, cryptocurrencies and the technology which underpin them has grown substantially in recent years. There has been wider acceptance of cryptocurrencies as a payment mechanism and the underlying decentralised public ledger technology has been applied to an increasing number of areas outside of virtual currencies. This has cemented interest in its potential as a disruptive technology. There has also been significant growth in investment in businesses operating in this sector and increasing interest from financial institutions in the technology and its potential.

Against this backdrop, a number of regulators have been focusing on the benefits, challenges and risks posed by the technology and how it fits within the existing legal and regulatory framework. In addition, a number of regulatory initiatives have been announced across the globe and a patchwork of legislation and regulation has begun to emerge.

In view of these developments, Norton Rose Fulbright's global cryptocurrency team has produced a guide to the legal and regulatory framework within which cryptocurrencies and their underlying technology operate.

The guide will be published in a series of chapters:

**Introduction to cryptocurrencies**

**The legal nature of cryptocurrency**

**Insuring cryptocurrency risks**

**Taxation of cryptocurrencies**

**Cryptocurrency litigation risks**

**Taking security over cryptocurrency**

**Cryptocurrencies – crime and compliance**

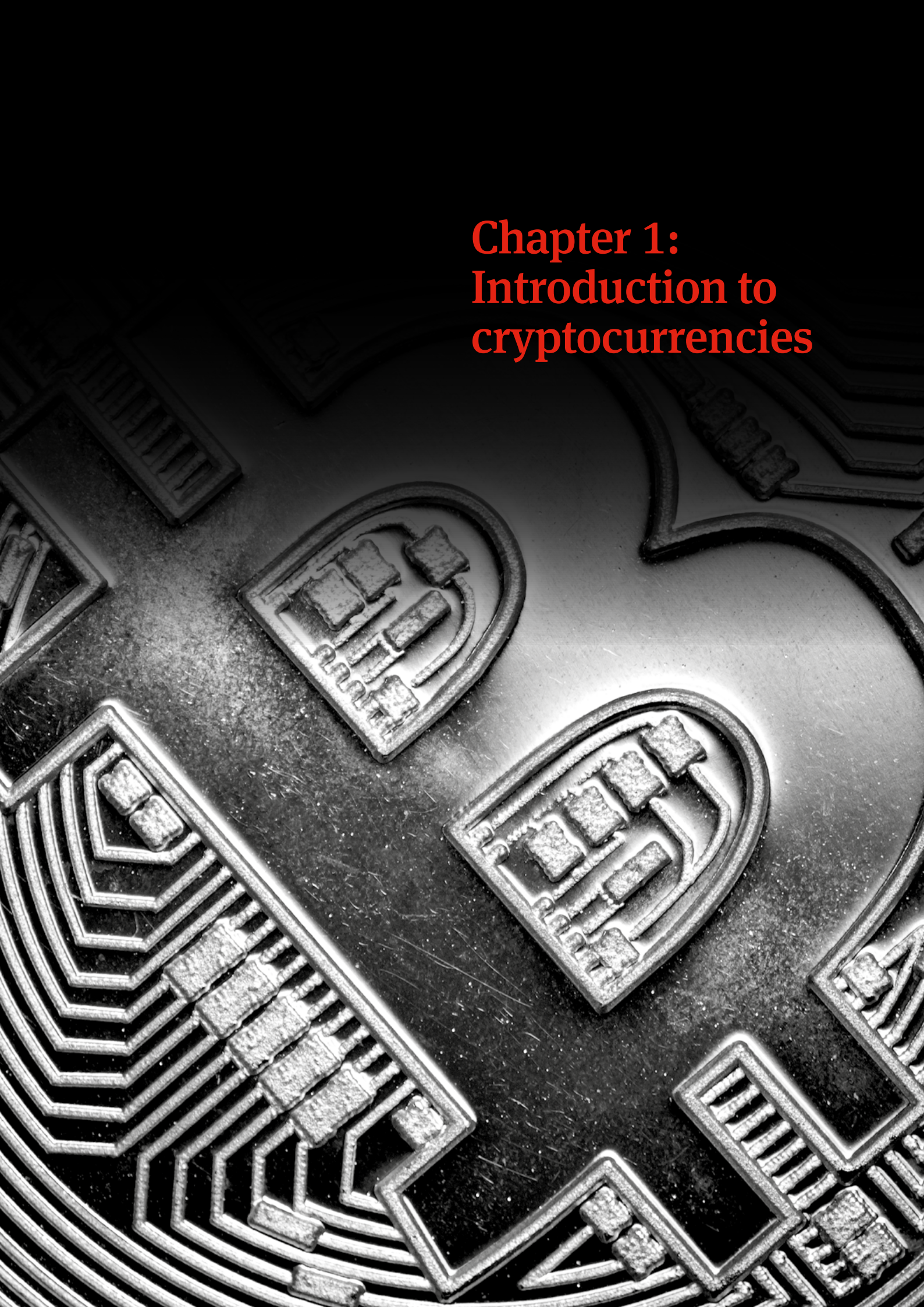
**Regulation of cryptocurrencies**

We hope that you will find this guide insightful and would welcome the opportunity to discuss any aspect with you in greater detail.

**The global cryptocurrency team**
Norton Rose Fulbright

May 2015

# Chapter 1: Introduction to cryptocurrencies



# Introduction

## What is a cryptocurrency?

A cryptocurrency is a form of virtual currency that uses cryptography to verify that any person who attempts to spend some of the currency is the person entitled to do so.

Cryptocurrencies typically use a decentralised peer-to-peer network to verify transactions and to record them on a decentralised public ledger (which is commonly known as a blockchain).

In this series of papers we will look at how cryptocurrencies operate and the laws and regulations that govern their operation. We will also consider potential future developments both in terms of usage and governmental and regulatory proposals for changes to the regulatory framework.

A glossary of some of the key terms used in the cryptocurrency sector and which we will use throughout this series of papers is set out opposite.

## Decrypting the jargon: a glossary of key terms

| | |
|---|---|
| **Blockchain** | A public ledger of all transactions in a particular cryptocurrency (e.g. Bitcoin). |
| **Cold storage** | Holding private keys for cryptocurrency wallets offline and deleting any online copies. |
| **Double spend** | An attempt to spend cryptocurrency that has already been spent in another transaction. |
| **Hash** | A number generated from any data source (such as a block header) that is practically unique to that data source. |
| **Key pair cryptography** | A form of cryptography that gives each user a two-part cryptographic key made up of the public key and the private key. |
| **Miners** | Persons or legal entities who run computer systems to repeatedly calculate hashes with the intention to create a successful new block for the relevant blockchain. |
| **Nonce** | An arbitrary number added to a message before encryption. Nonces are used in 'proof-of-work' systems (such as Bitcoin) to generate alternate alternative hashes in the search for a valid hash. |
| **Private key** | The secret code which allows a user to prove his ownership of his units of value. The private key is generally used to decrypt ciphertext or to create a digital signature. |
| **Public key** | The code used to encrypt plaintext or to verify a digital signature. |
| **Unconfirmed transaction** | A cryptocurrency transaction that has not yet been included in the public ledger and is still reversible. |
| **Wallet** | A software programme that stores the information necessary for the user to transact in cryptocurrency, i.e. it stores the digital credentials for the user's cryptocurrency holdings. |

## The development of cryptocurrencies

The most widely-recognised cryptocurrency, Bitcoin, was first proposed in a 2008 white paper written by Satoshi Nakamoto (widely presumed to be a pseudonym for either an individual or group of individuals working in concert). The paper (the 'Bitcoin White Paper') discussed the creation of 'an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party'[1].

Following the launch of Bitcoin, hundreds of cryptocurrencies have emerged, each possessing different characteristics and created for a variety of reasons: some as a joke, some as a user/community engagement token, some to circumvent internet censorship, and others as alternatives to existing national currencies.[2] Similarly, the number of networks and exchanges on which cryptocurrencies are created and traded has grown significantly.

As use of the technology has increased, a number of regulators and public bodies have begun to express interest in the legal and regulatory framework within which cryptocurrencies operate. In July 2014, the New York Department of Financial Services proposed a licensing regime for cryptocurrency businesses – the BitLicense regime (with subsequent revisions proposed in February 2015). The UK government stated support for the technology in its 2015 Budget in which it announced an intention to apply anti-money laundering regulations to digital currency exchanges in the UK, the creation of a research initiative into the technology and an initiative to work alongside the British Standards Institution and the digital currency industry to develop voluntary standards for consumer protection. Tax authorities have also been active in this space and the European Court of Justice is currently reviewing a referral from the Swedish tax authorities in respect of the VAT liability of Bitcoin exchanges.

A number of public authorities and central banks have also begun to consider the possibility of issuing centralised cryptocurrencies. In the UK, the Bank of England recently stated that

'While existing private digital currencies have economic flaws which make them volatile, the distributed ledger technology that their payment systems rely on may have considerable promise. This raises the question of whether central banks should themselves make use of such technology to issue digital currencies.'[3]

In the US, the Vice President of the Federal Reserve Bank of St Louis recently wrote a thesis on a government-backed 'Fedcoin' that would use a Bitcoin-style protocol with the US dollar as the monetary object, thereby combining both cryptocurrency technology and fiat currency.[4] Similarly, in the Philippines, draft legislation has been proposed to introduce a national cryptocurrency.[5]

1 Satoshi Nakamoto. 'Bitcoin: A Peer-to-Peer Electronic Cash System'
2 See Auroracoin (Iceland) or Spaincoin
3 Bank of England: One Bank Research Agenda: Discussion Paper
4 David Andolfatto, 'Fedcoin: On the Desirability of a Government Cryptocurrency'
5 Electronic Peso or E-Peso Act of 201.

## Some key dates in the development of cryptocurrency

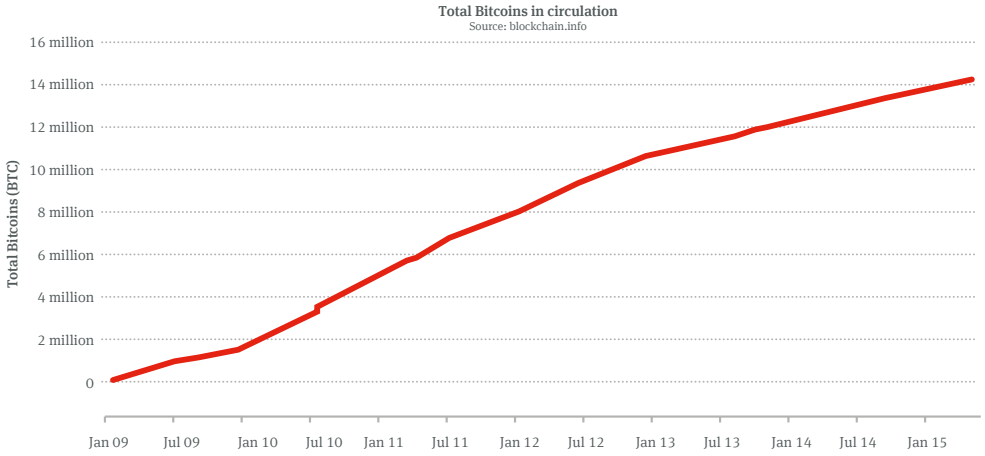
| | |
|---|---|
| Nov 1998 | Wei Dai publishes the 'B-money proposal', a precursor idea to Bitcoin in which the use of a 'proof-of-work' function is proposed as a means of creating money |
| Nov 2008 | Satoshi Nakamoto publishes *Bitcoin: A Peer-to-Peer Electronic Cash System* |
| Jan 2009 | First Bitcoins released |
| Oct 2011 | Litecoin is released |
| Aug 2012 | Peercoin is introduced |
| May 2013 | US Department of Justice charges Liberty Reserve with operating an unregistered money transmitter business and money laundering |
| Oct 2013 | First Bitcoin ATM unveiled in Vancouver, Canada |
| Dec 2013 | Bitcoin's value peaks at just over US$1,200 |
| Dec 2013 | Chinese authorities instruct the country's banks and other financial institutions not to accept Bitcoin; Bitcoin's value drops to c. US$870 |
| Feb 2014 | Mt. Gox exchange files for bankruptcy |
| July 2014 | European Banking Authority issues an opinion on virtual currencies |
| July 2014 | New York Department of Financial Services (NYDFS) proposes the BitLicense regime (revised Feb 2015) |
| July 2014 | Dell announces that it will accept Bitcoin |
| Sept 2014 | TeraExchange, LLC, receives approval from the US Commodity Futures Trading Commission to begin listing an over-the-counter swap product based on the price of a Bitcoin |
| Jan 2015 | Coinbase launches a licensed US Bitcoin exchange and the Winklevoss twins announce Gemini (a regulated Bitcoin exchange traded fund) |
| Feb 2015 | Ross Ulbricht (founder of Silk Road) convicted of (amongst other things) narcotics trafficking, computer hacking and money laundering conspiracies |
| Mar 2015 | HM Treasury issues Response to Call for Information on digital currencies |

## Adoption of cryptocurrency

Use of cryptocurrency has grown substantially since Satoshi Nakamoto published the Bitcoin White Paper and as of April 7, 2015, the total market capitalisation of Bitcoin was judged to be about US$3.5 billion. Bitcoin has experienced a very high degree of volatility since its inception (its market capitalisation plunged by more than 50 per cent in 2014), but usage is on the increase with the number of Bitcoins in circulation rising to about 14 million in April 2015 and daily Bitcoin transactions surpassing 100,000 for the first time in the last quarter of 2014[6].

There is also increasing acceptance of the technology by retailers. A number of major retailers have begun to accept cryptocurrency as payment, such as Dell, Microsoft and Expedia and a report by Boston Retail Partners found that about 8 per cent of US retailers intend to start accepting Bitcoin as payment by the end of 2015.

There is also increasing venture capital investment in the cryptocurrency space with venture capital funding for Bitcoin businesses tripling to US$315 million in 2014. Financial institutions are also paying increasing attention to the technology with the New York Stock Exchange and BBVA participating in a US$75 million funding round in Coinbase (a Bitcoin wallet and exchange service) and the licensing of Nasdaq's X-stream technology to Noble Markets (a platform for trading Bitcoins). In April 2015, UBS announced that it intends to open a London-based research lab to explore the application of blockchain technology in the financial services industry.




6 Blockchain.info

## Considerations for businesses looking at cryptocurrency technology

Set out below are some of the benefits and risks that businesses should consider when looking at cryptocurrency technology.

### Potential benefits

**Costs**

Traditional payment systems typically rely upon trusted third parties to transfer, convert and process money. These services can incur a variety of fees, such as SWIFT payment fees, credit card processing fees and foreign currency exchange fees. In each case, the transfer, conversion, or processing fees charged by the intermediary may amount to a significant portion of a transaction's overall value.

By comparison, peer-to-peer cryptocurrency transactions can be made on many networks without users incurring a transaction fee. This does not necessarily mean, however, that there is no cost associated with the processing of these transactions. For example, on some networks (such as Bitcoin) considerable computing power is required in order to update the relevant blockchain. At the moment users of Bitcoin are not required to pay fees to have their payments processed because the network subsidises miners through the issuances to them of new Bitcoins. However, a number of networks and exchanges do charge transaction fees, for example, to incentivise miners to process transactions more quickly. That said, these fees are typically lower than traditional banking charges and are usually fixed without reference to the transaction size.

It is important to note, however, that there are concerns that transaction fees in the cryptocurrency space are unlikely remain low, particularly if the technology is subject to greater regulatory and compliance scrutiny. Similarly, intermediary fees may still be incurred by users, for example, at the point at which the cryptocurrency is converted into fiat currency.

**Timing**

Cryptocurrencies can also speed up transaction processing times. Transactions involving existing inter-bank payment systems can take significant periods of time to complete even, particularly in the case of cross border transactions, several days. Similarly, conventional payment services are often only available during banking hours.

By comparison, the average time it takes to update the blockchain to complete a cryptocurrency transaction is typically between 10 seconds and 10 minutes and the networks and exchanges are available 24 hours a day.

**Micropayments**

Unlike many traditional currencies, it is possible to spend cryptocurrencies in minute denominations. This creates the possibility of monetising very low cost goods and services and accepting micropayments for online content. This has already been seen in a number of chat platforms, such as Telegramchat and Slack.

There is also the possibility of other forms of micro-transactions, such as internet tipping, charitable giving and even micro-payrolls (whereby employees can receive their salaries on an hourly or daily basis) and the opportunity to charge nominal amounts to users who wish to send content, which may be relevant to anti-spam technology.

**Privacy**
Unlike many conventional payment methods, cryptocurrency transactions are 'pushed' by the payer rather than 'pulled' by the recipient. This means that the recipients of cryptocurrency payments do not need any data from the payer in order to be able to request the transaction. This may be beneficial to merchants who currently incur costs and risks associated with securing customer data. That said, merchants would typically still need enough information to be able to pair the payment with the purchase and, therefore, with the delivery address (even if it is a digital address). This requires a link to be made between the public key of the payer and an address.

In addition, transactions are typically sent to public keys and so, without further information linking all of an individual's public keys together and then linking to the individual, the total account balance of that individual is private.

**Financial inclusion**
Cryptocurrencies potentially provide access to payment and other financial services to those persons who lack access to traditional banking. This could be particularly relevant in emerging markets which lack an established banking infrastructure and where large proportions of the population are unable to access a bank account.

## Potential risks

**Criminality**
Due to the pseudonymous nature of cryptocurrency technology, there is a concern that it facilitates criminal activity. For example, the use of cryptocurrency as a payment vehicle for the buying of and selling of illicit goods and services, such as in the Silk Road case and cases of 'ransomware' where criminals have demanded payment in cryptocurrency from owners of computers that they have infected.

The UK National Crime Agency reported in October 2014 that it did not believe that digital currencies had been widely adopted as a means of payment by the broader criminal community and that the majority of illicit digital currency spends were for low-value transactions. Similarly, the transparency and visibility of transactions on the blockchain, price volatility and the relatively small number of individuals and businesses accepting cryptocurrencies may deter the use of the technology by criminal participants.

A number of jurisdictions have also begun to reinforce the regulatory framework surrounding cryptocurrencies to restrict its attractiveness to the criminal community, particularly in respect of anti-money laundering legislation. For example, the Isle of Man has amended existing legislation to bring digital currencies within the scope of anti-money laundering requirements and the UK government has announced its intention to do the same.

**Valuation**
A key area of concern for businesses using cryptocurrency is the value that should be attributed to their cryptocurrency units. This is partly because most cryptocurrencies are not backed by any central authority or pegged to any other currency or commodity. In addition, although the value of cryptocurrencies has risen since its inception, the price has not remained constant – for example the value of Bitcoin has dropped from over US$1,000 in late 2013 to around US$260 at the start of April 2015 with fluctuations in the interim.

In order to protect against fluctuations in value, merchants often contract with a third-party payment processor to immediately convert the cryptocurrency into local currency. By using such a process agent to immediately convert cryptocurrency into local currency, the merchant avoids the valuation risk in exchange for the fee paid to the third-party payment processor.

**Deflation**
Many cryptocurrencies have a capped or fixed number of units that can be created. For example, the number of potential Bitcoins is capped at 21 million. This creates a risk of liquidity problems and deflation.

There is, of course, no requirement that cryptocurrencies have a deflationary feature and a number of unlimited cryptocurrencies have also been released, such as Dogecoin.

**Security**
The irrevocable nature of cryptographic payments and the absence of an overarching authority with control over transactions means that there is no recourse to a bank, payment scheme company or regulator in the event of erroneous or fraudulent payments, such as in the case of a 51 per cent attack (where an individual or pool of miners control a sustained majority of the computing power and are thereby able to 'double spend' cryptocurrency). In addition, there is no recourse for users who lose funds as a result of exchanges and wallet providers being hacked or becoming insolvent, as was the case in the Mt. Gox failure.

A number of technological innovations have been introduced recently to reduce the risk posed by exchange security, such as multi-signature authentication, escrow accounting and 'cold storage' used digital currency firms. In addition, there have been a number of regulatory initiatives to improve regulatory oversight of exchanges, such as the BitLicense regime.

**Consumer protection**
There is also concern that many elements of consumer protection legislation do not apply to transactions in this space, such as charge-back rights for credit card holder rights under section 74 of the Consumer Credit Card Act in the UK and Regulation Z of the Truth in Lending Act in the US.

A number of regulators are reviewing the application of consumer protection legislation to cryptocurrency transactions. For example, in the UK, the government has announced an initiative to work alongside the British Standards Institution and the digital currency industry to develop voluntary standards for consumer protection.

# How cryptocurrencies work in practice

## A decentralised network

Transactions using a cryptocurrency are typically made over a decentralised peer-to-peer network without recourse to a bank or central authority.

Each transaction is recorded on a public ledger (or blockchain) that is publicly available to all users. A user wishing to make a payment issues payment instructions which are disseminated across the network. Cryptographic techniques (which are described below in more detail) are then used to enable the network to verify that the transaction is valid (i.e. that the would-be payer owns the currency in question).

This contrasts to a traditional bank deposit where the relevant bank will hold a digital record of transactions and is trusted to ensure the validity of that record.

## How to complete a transaction in cryptocurrency

### Key pair transactions

Commonly, cryptocurrency networks use a cryptographic mechanism known as key pair cryptography to enable its users to transact with each other.

'Key pair' cryptography gives each user a two-part cryptographic key (known as a 'key pair'). One part of the key pair is known to its owner only (the 'private key') while the public key is used for the purpose of communicating with the wider public.

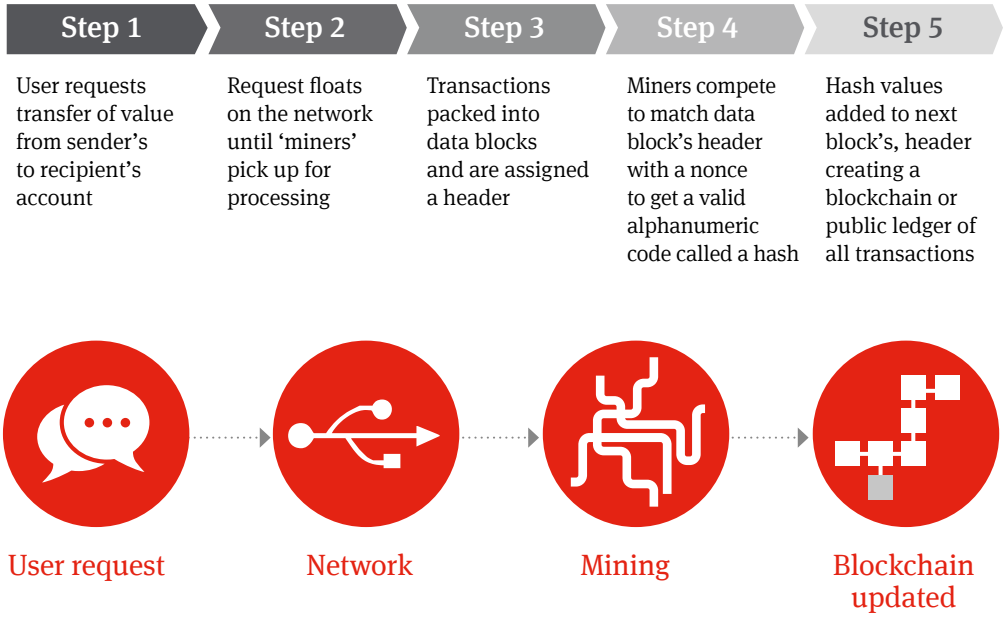
Key pair cryptography can be used to encrypt messages or to authenticate them, or both at the same time. In cryptocurrencies key pair cryptography is typically used to authenticate (rather than to encrypt) payment instructions. The payer digitally 'signs' the payment instruction using their private key and the recipient verifies the authenticity of the payment instruction using the payer's public key.

### Confirming and recording each transaction

In its simplest form, once a 'spend' has been made, a message is sent to the network requesting that the relevant amount be deducted from the payer's wallet and added to the recipient's wallet.

The request remains on the network while 'miners' compete to process blocks of transactions and update the blockchain accordingly. It is the point at which the blockchain is updated that the transaction is deemed to be confirmed and irreversible. This process can take a period of time, which is on average anywhere from ten seconds to ten minutes depending on the cryptocurrency in question.

### The process for updating the blockchain




## Mining

Cryptocurrencies typically use 'miners' to process and verify transactions broadcast upon the relevant decentralised network.

When a transaction occurs it is packed into a data block which is assigned a header. The miners then compete to match the data block's header with a nonce to get a valid alphanumerical code called a hash. The hash values are then added to the next block's header updating the blockchain accordingly.

As discussed above, on many networks (for example Bitcoin) miners have to deploy very considerable computing power in order to update the relevant blockchain. This computing power has a cost associated with it. Therefore, miners are usually rewarded for updating the blockchain either through the issuance to them of new cryptocurrency units or in the form of a transaction fee.

**Click here to visit our dedicated cryptocurrency webpage and register to receive subsequent chapters.**

# Global resources

Norton Rose Fulbright is a global legal practice. We provide the world's pre-eminent corporations and financial institutions with a full business law service. We have more than 3800 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Our office locations

**People worldwide**

7400

**Legal staff worldwide**

3800+

**Offices**

50+

**Key industry strengths**

- Financial institutions
- Energy
- Infrastructure, mining and commodities
- Transport
- Technology and innovation
- Life sciences and healthcare

**Europe**

- Amsterdam
- Athens
- Brussels
- Frankfurt
- Hamburg
- London
- Milan
- Moscow
- Munich
- Paris
- Piraeus
- Warsaw

**United States**

- Austin
- Dallas
- Denver
- Houston
- Los Angeles
- Minneapolis
- New York
- Pittsburgh-Southpointe
- St Louis
- San Antonio
- Washington DC

**Canada**

- Calgary
- Montréal
- Ottawa
- Québec
- Toronto

**Latin America**

- Bogotá
- Caracas
- Rio de Janeiro

**Asia**

- Bangkok
- Beijing
- Hong Kong
- Jakarta[1]
- Shanghai
- Singapore
- Tokyo

**Australia**

- Brisbane
- Melbourne
- Perth
- Sydney

**Africa**

- Bujumbura[3]
- Cape Town
- Casablanca
- Dar es Salaam
- Durban
- Harare[3]
- Johannesburg
- Kampala[3]

**Middle East**

- Abu Dhabi
- Bahrain
- Dubai
- Riyadh[2]

**Central Asia**

- Almaty

1 Susandarini & Partners in association with Norton Rose Fulbright Australia
2 Mohammed Al-Ghamdi Law Firm in association with Fulbright & Jaworski LLP
3 Alliances

# Contacts

## Asia

**Stella Cramer**
**Partner, Singapore**
Norton Rose Fulbright (Asia) LLP
Tel +65 6309 5349
stella.cramer@nortonrosefulbright.com

**Barbara Li**
**Partner, Beijing**
Norton Rose Fulbright LLP
Tel +86 10 6535 3130
barbara.li@nortonrosefulbright.com

**Charlotte Robins**
**Partner, Hong Kong**
Norton Rose Fulbright Hong Kong
Tel +852 3405 2465
charlotte.robins@nortonrosefulbright.com

## Australia

**Warwick Andersen**
**Special counsel, Sydney**
Norton Rose Fulbright Australia
Tel +61 2 9330 8050
warwick.andersen@nortonrosefulbright.com

**Tessa Hoser**
**Partner, Sydney**
Norton Rose Fulbright Australia
Tel +61 2 9330 8083
tessa.hoser@nortonrosefulbright.com

## Canada

**Anthony de Fazekas**
**Partner, Lawyer, Patent Agent, Toronto**
Norton Rose Fulbright Canada LLP
Tel +1 416 216 2452
anthony.defazekas@nortonrosefulbright.com

**John Jason**
**Of counsel, Toronto**
Norton Rose Fulbright Canada LLP
Tel +1 416 216 2964
john.jason@nortonrosefulbright.com

## Europe

**Sean Murphy**
**Partner, London**
Norton Rose Fulbright LLP
Tel +44 20 7444 5039
sean.murphy@nortonrosefulbright.com

**Victoria Birch**
**Of counsel, London**
Norton Rose Fulbright LLP
Tel +44 20 7444 2124
victoria.birch@nortonrosefulbright.com

**Roberto Cristofolini**
**Partner, Paris**
Norton Rose Fulbright LLP
Tel +33 1 56 59 52 45
roberto.cristofolini@nortonrosefulbright.com

**Jamie Nowak**
**Partner, Munich**
Norton Rose Fulbright LLP
Tel +49 89 212148 0
jamie.nowak@nortonrosefulbright.com

**Floortje Nagelkerke**
**Senior associate, Amsterdam**
Norton Rose Fulbright LLP
Tel +31 20 462 9426
floortje.nagelkerke@nortonrosefulbright.com

## Latin America

**Ramón Ignacio Andrade Monagas**
**Partner, Caracas**
Despacho de Abogados Miembros de Norton Rose Fulbright, S.C.
Tel +58 212 276 0014
ramon.andrade@nortonrosefulbright.com

## South Africa

**Rohan Isaacs**
**Director, Johannesburg**
Norton Rose Fulbright South Africa Inc
Tel +27 11 685 8871
rohan.isaacs@nortonrosefulbright.com

**Nerushka Deosaran**
**Associate, Johannesburg**
Norton Rose Fulbright South Africa Inc
Tel +27 11 685 8691
nerushka.deosaran@nortonrosefulbright.com

## United States

**Kathleen A. Scott**
**Sr counsel, New York**
Norton Rose Fulbright US LLP
Tel +1 212 318 3084
kathleen.scott@nortonrosefulbright.com

**Susan Linda Ross**
**Sr counsel, New York**
Norton Rose Fulbright US LLP
Tel +1 212 318 3280
susan.ross@nortonrosefulbright.com

NORTON ROSE FULBRIGHT

Law around the world
nortonrosefulbright.com