THE FUTURE IS DECENTRALISED

**BLOCK CHAINS, DISTRIBUTED LEDGERS, &
THE FUTURE OF SUSTAINABLE DEVELOPMENT**

THE FUTURE IS DECENTRALISED

The potential of block chains to disrupt industrial sectors, commercial processes, governmental structures or economic systems seems to know no bounds. We suggest that the transformative power of block chain technology should not be seen as a threat to existing systems of governance; rather, it should be seen as an opportunity for national and international institutions to defend the rights of those they represent and to accelerate our collective progress towards meeting the United Nations' Sustainable Development Goals.

Block chains can bring transparency to opaque or corrupt systems, and verifiability and immutability to commercial processes. They can bring security and resilience to vulnerable infrastructure, ensure individual privacy whilst guaranteeing autonomy, and encourage cooperation and engender trust where they are needed most.

Block chains can ease the frictions that prevent a vast array of sustainability, humanitarian, and environmental initiatives from fulfilling their potential.

This white paper explains how this unconventional technology works and how it is already being used to pursue conventional ends. It illustrates how block chains have brought new levels of efficiency and effectiveness to the fields of development aid, supply chain management, renewable energy, economic growth, and several others.

Our aim has been to show how governments, NGOs, and citizens are working together, exploiting the versatility of block chain technology to form new, powerful partnerships. We address the risks posed by this nascent technology and suggest how these risks should be managed.

BOB WIGLEY
Founder Commissioner, Blockchain Commission

NICOLAS CARY
Co-Founder, Blockchain

CONTENTS

INTRODUCTION

SARAH MEIKLEJOHN
Assistant Professor at UCL, specialising in computer science, security, & cryptography

NICOLAS CARY
Co-founder of Blockchain

WHAT IS A BLOCK CHAIN?

As with many new concepts, block chain technology provokes much optimism and also a substantial amount of intrigue. Just what is it good for?

In short, block chains may improve any process where people need to access, verify, send or store information securely. This information could be a person's identity, a product's shipment history or a digital asset like money.

Typical databases, spreadsheets, and ledgers store information about objects, people, and the interactions between them. Much of the world's information, from credit card transactions to medical and financial records, is stored in these types of systems.

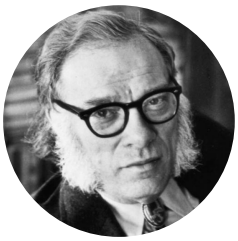
These types of systems have considerable, well-documented weaknesses that stem from their being centralised. A centralised record is opaque and vulnerable to unauthorised access or distribution. It is also, because it is a 'master' copy, vulnerable to irreversible alteration or deletion.

Block chains are also used to store information. Crucially, however, they differ in two ways.

First, information is parcelled up into blocks and sealed. Bitcoin, for example, which relies on a block chain, stores all transactions across the network every ten minutes or so in a single, newly formed block. Each block is then added to the previous one to form a chain.

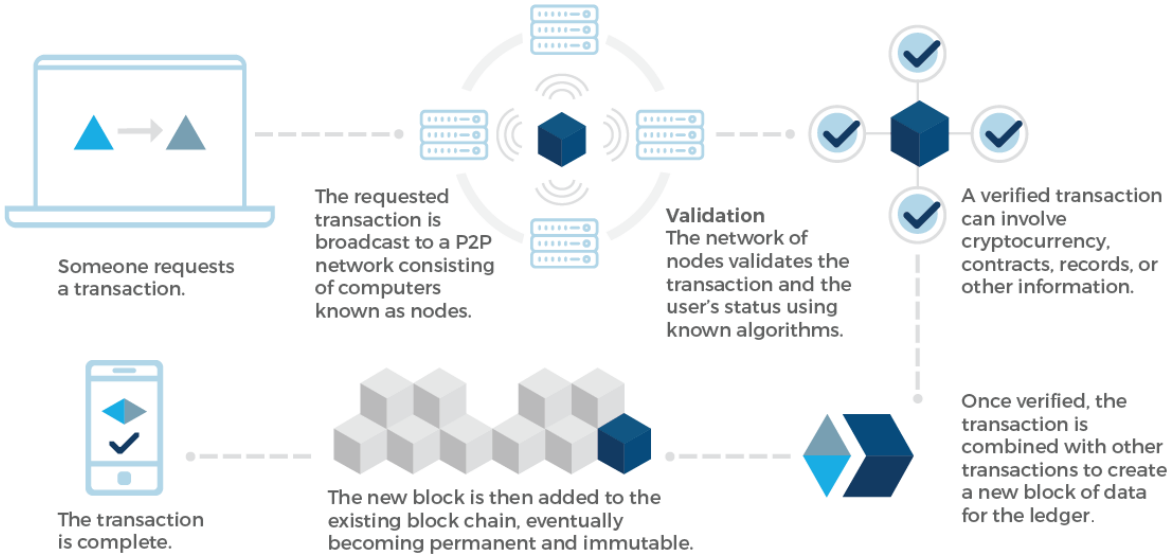
Second, this 'chain of blocks' is not stored centrally. Instead, each block is copied and distributed around an entire network of peers - be they individuals, public institutions, NGOs or businesses - using distributed ledger technology. (The terms 'block chain' and 'distributed ledger' are often used interchangeably; for the sake of clarity, block chain technologies tend to employ distributed ledger technology.)

Each time someone adds a new block to the chain, it is added to everyone's copy simultaneously.



"I discovered, to my amazement, that all through history there had been resistance [...] to every significant technological change that had taken place on earth. Usually the resistance came from those groups who stood to lose influence, status, money [...] as a result of the change, although they never advanced this as their reason for resisting it. It was always the good of humanity that rested upon their hearts."

- Isaac Asimov, lecture at Newark College of Engineering, 1974



BENEFITS

This system of organising and storing information ensures a number of benefits.

Immutability

Since multiple copies of a block chain are kept and managed by consensus across a peer-to-peer network, no one peer can alter past transactions.

Security

It is a fundamental cryptological law that it is relatively easy to set a problem that is very, very difficult to solve. What is relatively easy for a network of computers to do is, in practice, impossible even for much larger networks to undo.

Verifiability

The combination of transparency and immutability also allows us to satisfy full public verifiability: anyone in the world can check for themselves that the rules of the system - in the case of digital currencies, that coins should be spent only once - are being followed. Whilst information cannot be manipulated, it can be easily verified thanks to the size and power of the network.

Resilience

The distributed nature of the ledger makes it resilient. Even if many peers go offline, the information is still accessible.

Transparency

The fact that all transactions are broadcast to all peers also makes the ledger transparent. However, the encrypted nature of the transactions means that privacy is also assured.

These benefits can be tuned and block chains tailored to their specific functions to ensure that issues such as privacy, accountability, and transparency are tightly managed.

A land registry, for example, must be universally visible for it to be useful. The distribution and use of government funding, on the other hand, may need to be publically verifiable without certain sensitive details being available to all. Similarly, an individual may wish to establish their identity with a bank, hotel, airline or doctor without the other party knowing more than is absolutely necessary.

Taken individually, these benefits would mark the block chain technology as an extraordinary system. But it's when we consider how these benefits combine that the technology's truly transformative potential is revealed.

TRUSTLESS COLLABORATION

The decentralised, transparent, verifiable nature of the system means we can trust people and organisations precisely because trust is no longer an issue. The integrity of the system, of every participant, and of every transaction is underpinned by the network as a whole. Trust, like the information, has been distributed and secured.

This combination of decentralisation, resiliency, transparency, and immutability on a trustless protocol is why the technology is so promising across so many use cases from finance and property rights to development and humanitarian aid.

BLOCK CHAINS ARE NOT 'MAGIC BEANS'

Despite the many possible applications and benefits, it is important to remember that block chain is still an experimental and evolving technology. It has vast potential, but it is neither perfect nor universally applicable.

Even beyond the inevitable risks of using nascent technology, the property of trustless, fully public verifiability currently comes at a significant cost in terms of computation, storage, security, and coordination.

It is thus vital to understand what the most efficient solution is for any given setting, and to acknowledge that often it is not a block chain or distributed ledger. Even in settings where a block chain may be appropriate, such as the ones put forward in this paper, it would still be necessary to decide between different variants.

WHAT ARE PEOPLE USING BLOCK CHAINS FOR?

Block chains are best known for underpinning digital currencies like Bitcoin, but many people have started to realise their broader applications. For example, some services take advantage of the immutability of block chains to notarise or witness documents whilst others employ them to issue and transfer licenses for digital art. In finance, block chains can streamline existing infrastructures and enable faster post-trade settlement of securities as well as cheaper payments. In supply chains, they can deliver transparency. In telecommunications, they can help verify website certifications and provide secure communication.

Some of the most advanced block chain platforms such as Ethereum power specialised computer programs - so-called 'smart contracts' - that execute autonomously between several parties once certain pre-set conditions are met. The greatly expanded functionality this provides has enabled developers to provide services for things like crowdfunding, censorship-resistant microblogging, and identity management.

Beyond these immediate use cases, angel, venture, and growth investment in digital currency startups has hit record levels inspired by an abundance of opportunities. According to CoinDesk, over $2.5 billion has been allocated to projects and companies working in the block chain industry (CoinDesk, 2017).

In addition, academic institutions like MIT, Cornell, and the Digital Asset Research Lab at Imperial College are increasingly collaborating on open-source development.

This open-source aspect is fundamentally necessary to security and trust, and it also encourages innovation. Open-source platforms allow for greater flexibility and freedom when it comes to designing, adapting, and using block chain technology, and the overall value of a given initiative increases in line with its potential to scale beyond the local or even national context. And though value may increase, it is vital that accessibility remain low; since so many of the issues to which block chain technology can be applied affect the poor with disproportionate severity, it is essential that affordability is not a barrier.

Finally, governments and central banks are also keen to learn about and participate in the block chain ecosystem. The combined efforts between the private, public, and academic sectors are creating a strong foundation for powerful new public-private partnerships that bring together political power, third-sector ambition, and commercial experience with the necessary funding and technical expertise.

"...there are at least seven billion mobile phone subscriptions in the world (four and a half billion people have access to a flush toilet). So more than twice as many people have a mobile phone as have access to a bank account. If your phone can give you access to the things you would need from a bank, well, you've just disinvented the need for banks, and fundamentally changed the operation of the money system, across whole swathes of the developing and emerging world."

- 'When Bitcoin Grows Up', London Review of Books, April 21st, 2016

...AND WHAT *COULD* THEY BE USING THEM FOR?

Block chains and the distributed ledger technology they employ are often most useful in situations where there is insufficient infrastructure or where there is no natural candidate for a trusted operator.

For example, block chains may help billions of people without access to banking facilities enjoy financial services. This isn't necessarily because big, international banks are inefficient or greedy, but because they're not able to deliver services affordably to everyone equally. John Lanchester makes the point that two and a half billion adults in the world do not have a bank account. Therefore something like five billion people who are members of households are cut off from the financial system that most take for granted, walled off from the global economy.

Similarly, block chains can be put to use in countries that lack robust government infrastructures for records like land registries, or in supply chain systems in which many parties are distrusting of or simply unknown to one another.

TRUST, NOT MONEY, MAKES THE WORLD GO ROUND

Imagine a world where everyone can trust everyone - or where trust isn't even an issue any more.

We would see aid organisations able to receive funds instantly from many individual donors and then distribute these funds efficiently and effectively to people who can prove their identity without a piece of paper.

We would see a world where a hard-working mother in Dubai can send payments to her family back in India without any of them needing a bank account; where a consumer can verify the exact provenance of their food; where voter fraud is a thing of the past and citizens can have absolute faith in the democratic process; where anyone can prove what property they own, allowing for completely new types of capital formation and entrepreneurship.

We are not there yet, but block chains are already helping us reimagine the world in ways that may have seemed like science fiction just a few years ago.