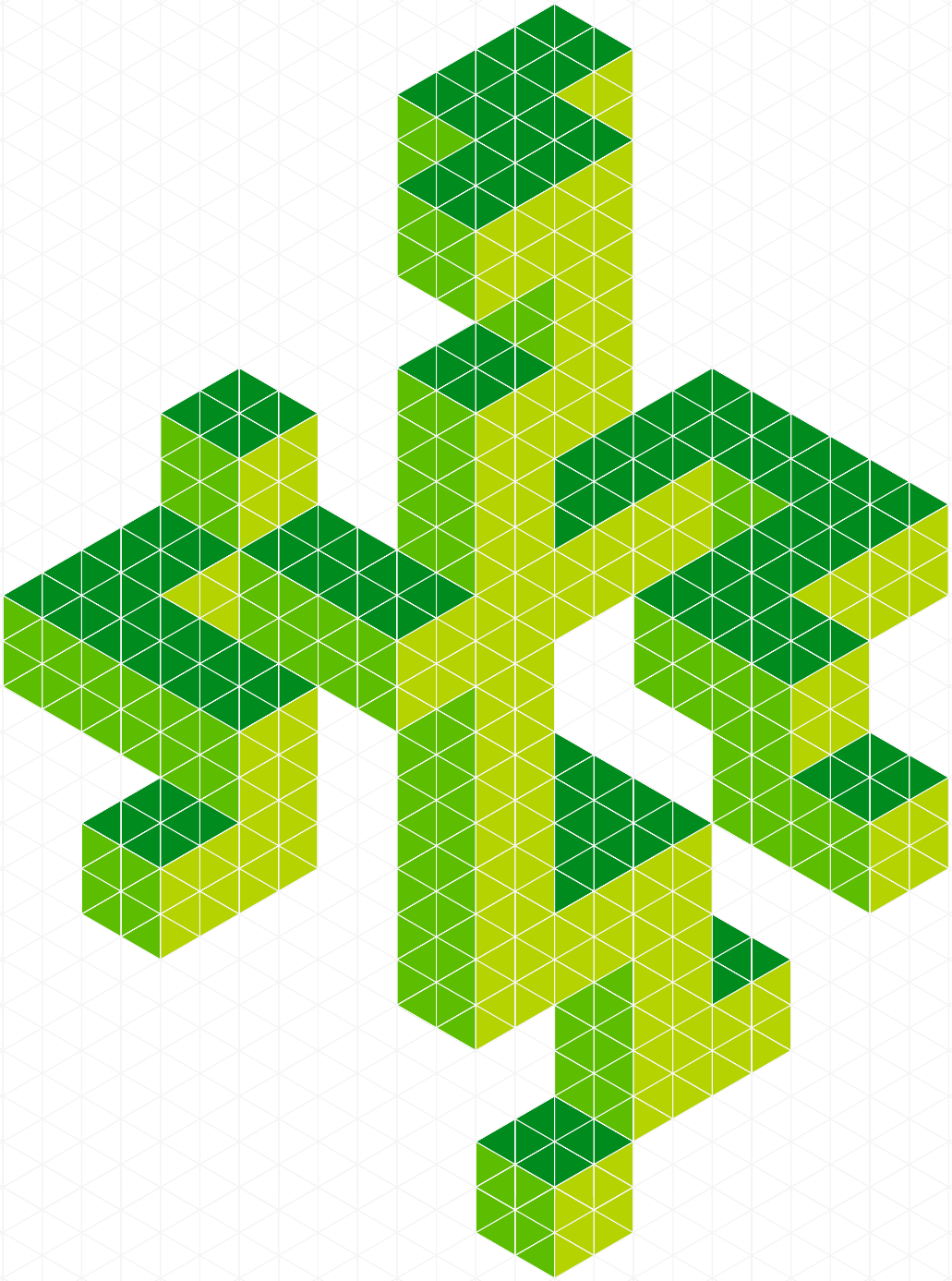
Deloitte.

Bitcoin, Blockchain & distributed ledgers: Caught between promise and reality

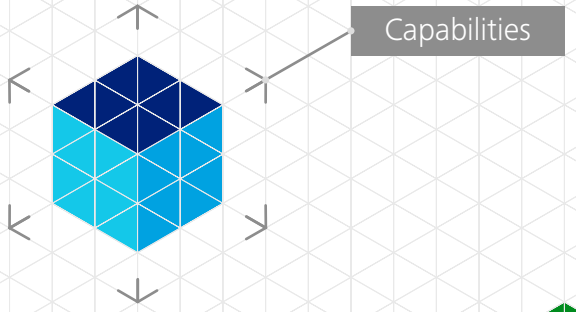
Centre for the *Edge*
Australia



Contents

1. Introduction

Blockchain has become a marketing buzzword making it impossible to talk about the technology. A more productive approach – and the approach we've taken – is to focus on the capabilities and problems

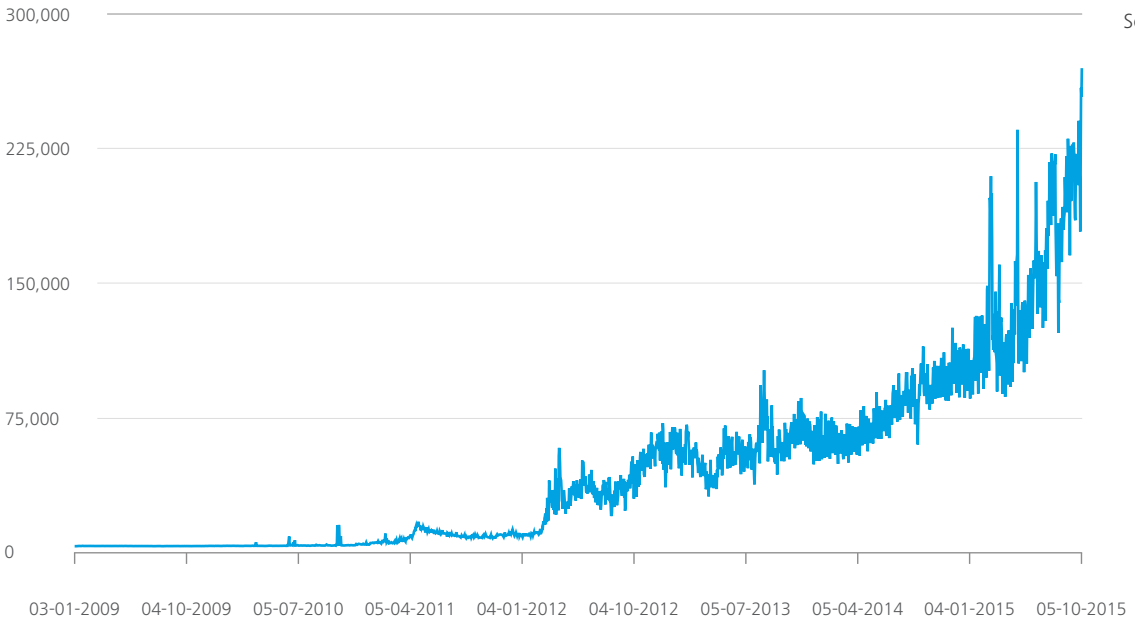


Blockchain's genesis in Bitcoin

In October 2008, Satoshi Nakamoto proposed a combined digital asset and peer-to-peer payments system in his paper, *Bitcoin: A Peer-to-Peer Electronic Cash System*.[1] The first Bitcoin was minted on January 4th 2009,[2] the first payment occurred on January 11th,[3] and the software was released as open source on the 15th,[4] enabling anyone with the required technical skills to get involved.

For a long time, there was little interest in Bitcoin. Then, roughly a third of the way through 2012, the transaction volume started to grow exponentially. In early 2013 Bitcoin's market capitalisation started to follow the same path.

Bitcoin Daily Transaction Volume



Source: blockchain.info

Figure: Bitcoin Market Capitalisation (USD)

Source: blockchain.info

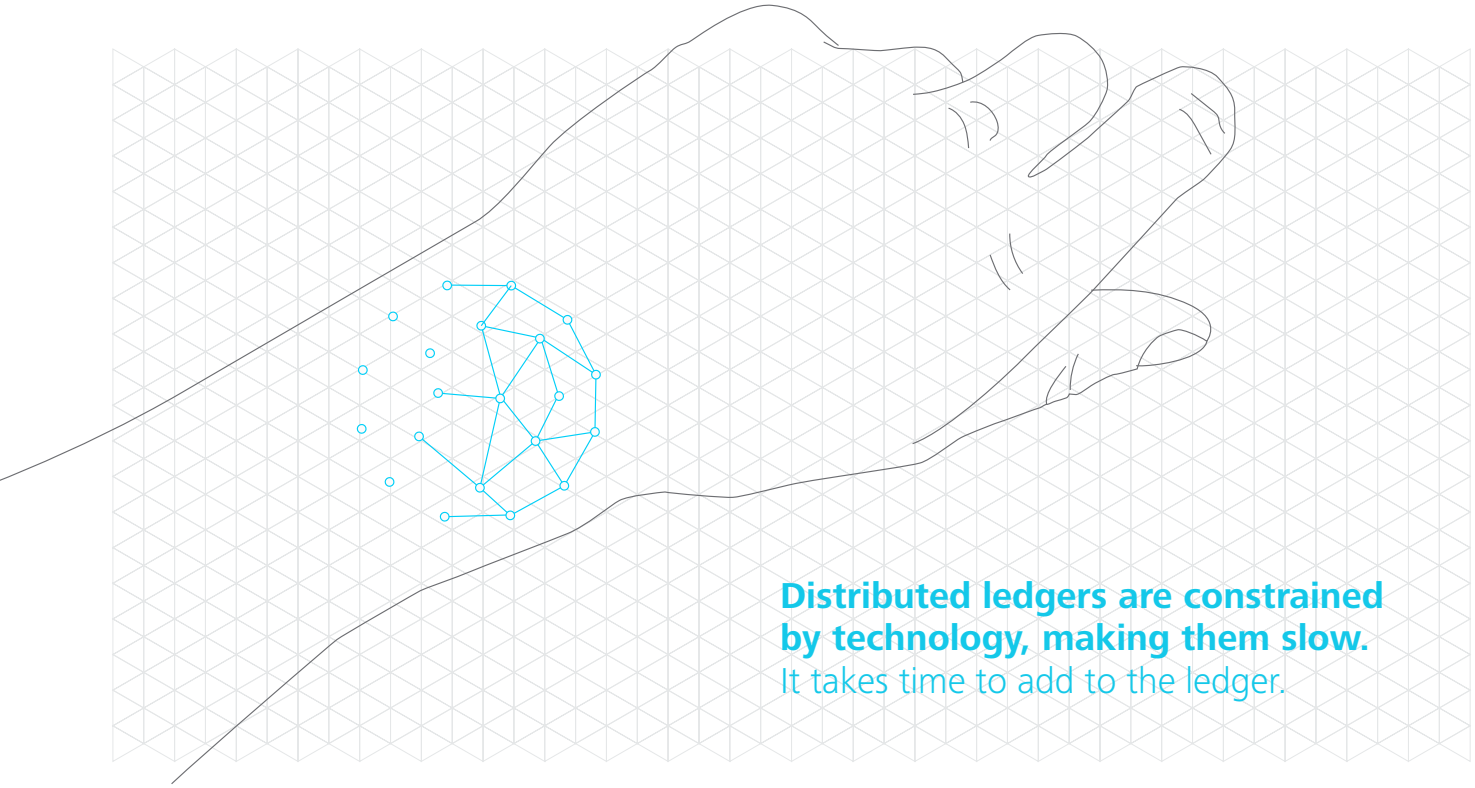
Today Bitcoin has exploded into the mainstream. With a market capitalisation of roughly six billion US dollars and daily transaction volume around 200,000, it dominates water cooler conversations at many firms. Garnering even more interest is *blockchain*, the solution underpinning Bitcoin, with many pundits predicting it has an even bigger future. It is as if no problem cannot be solved by the artful application of blockchain technology. Proposals are flooding the market: from blockchain-enabled payments, through to identity management solutions, and Amazon and Uber killers – all powered by blockchain. Bitcoin and blockchain seem to have triggered a new gold rush.

A new gold rush

The last gold rush was cloud computing. Cloud computing's advocates seemed to argue no problem couldn't be fixed, or at least alleviated, by moving it *to the cloud*. A cynic might claim we're hearing similar refrains today, with *to the cloud* replaced by *on the blockchain*. To take one common example, capital markets will be made faster and more efficient once moved o*nto the blockchain*. There are even proposals for creating ownerless companies that live *on the blockchain*,[5] giving these companies sovereignty over their own assets via technologically enforced contracts – bypassing today's sprawling and inefficient financial back offices and legal systems, and creating distributed autonomous organisations (DAOs) in the process. Tomorrow's electric ridesharing car might not only be autonomous, it might accept fares on its own – while also requesting and paying for its own recharging and servicing when needed.

Blockchain sounds too good to be true, much like cloud computing did in its early days. Excited vendors quickly transformed *cloud* from a well-defined solution with demonstrable benefits (and problems) into a nebulous marketing concept. The same is true with the current gold rush. While Bitcoin is well defined, tied as it is to a currency, blockchain's definition is stretching to the point where it no longer refers to a particular technology or solution and is useful only as a marketing term.

The challenge is that blockchain is a limited technology. Currently, Bitcoin only supports a few transactions per second, with transactions processed in batches ten minutes apart. It relies on a community of anonymous miners to process these transactions, with each miner paid 25 BTC[6] per block (roughly US$8.25 per transaction). Replacing the miners with a consortium, such as established banks, could help solve the problem, but makes the solution look like a private platform, and then you must ask what you've actually gained. Firms are responding to these limitations by developing approaches that don't suffer from Bitcoin's confines. While Bitcoin is narrowly defined with limited benefits, these emerging alternative approaches have significant potential. Many only have a passing resemblance to Bitcoin but are still marketed under the blockchain banner in an attempt to tap into the current gold rush.



Distributed ledgers are constrained by technology, making them slow.
It takes time to add to the ledger.

We believe, like cloud computing, the emergence of blockchain does signal something new. The challenge is to cut through the noise and understand what new capabilities are implied, what new solutions are enabled, and what is beyond the reach of the technology. To put it more succinctly, we need to understand what blockchain can and can't be.

The importance of terminology

Terminology is important. Without a consistent approach to terminology, it is difficult to explore the opportunities a new technology presents. It's not surprising many of us are struggling to understand blockchain's utility when its foundations are built on shifting sand. However, attempting to create a more precise definition is futile. Many definitions have already been offered, with the ensuing arguments about what is and what isn't a blockchain, offering little progress.

A more fruitful approach is to develop an understanding from the solutions Bitcoin enables. Consequently, our strategy is to set aside blockchain as a marketing term and work from the solutions down.

In From Bitcoin to Distributed Ledgers, we compare the Bitcoin's ledger with the more familiar physical ledgers that preceded it, and develop the concept of a *distributed ledger*[7] defined in terms of the problems solved rather than the technologies used.

In A map of the distributed ledger landscape, we identify questions that should be asked when considering a new distributed ledger, creating a map of the solution landscape.

In Regulation, we explore the potential regulatory implications of these solutions, though we only focus on what is different with distributed ledgers. How does one regulate something no single person or organisation is accountable for?

In Applications, we review the strengths and weaknesses identified in the previous two sections to develop an understanding of what a distributed ledger can be and what it can't be.

Finally, in Conclusions, we look at the technology's potential and what the future might hold.

Definitions

The terminology around Bitcoin and blockchain is imprecise and can be confusing for both novice and expert. For clarity, we have taken what we think is a pragmatic approach to the definitions used in this report but we make no claim they are definitive. The following definitions will be used unless otherwise noted:

Bitcoin (upper case) is the well-known cryptocurrency.

bitcoin (lower case) is the specific collection of technologies used by Bitcoin's ledger, a particular solution. We should note the currency itself is one of these technologies as it provides the miners with the incentive to mine.

blockchain (or blockchain technology) is the generic name for the family of technologies and solutions that provide the same functionality as bitcoin, but which use different approaches to realising the functionality, for example via alternate algorithms.

***the* blockchain** (the definite article) is the particular ledger that underpins Bitcoin: the blockchain created by Satoshi Nakamoto.

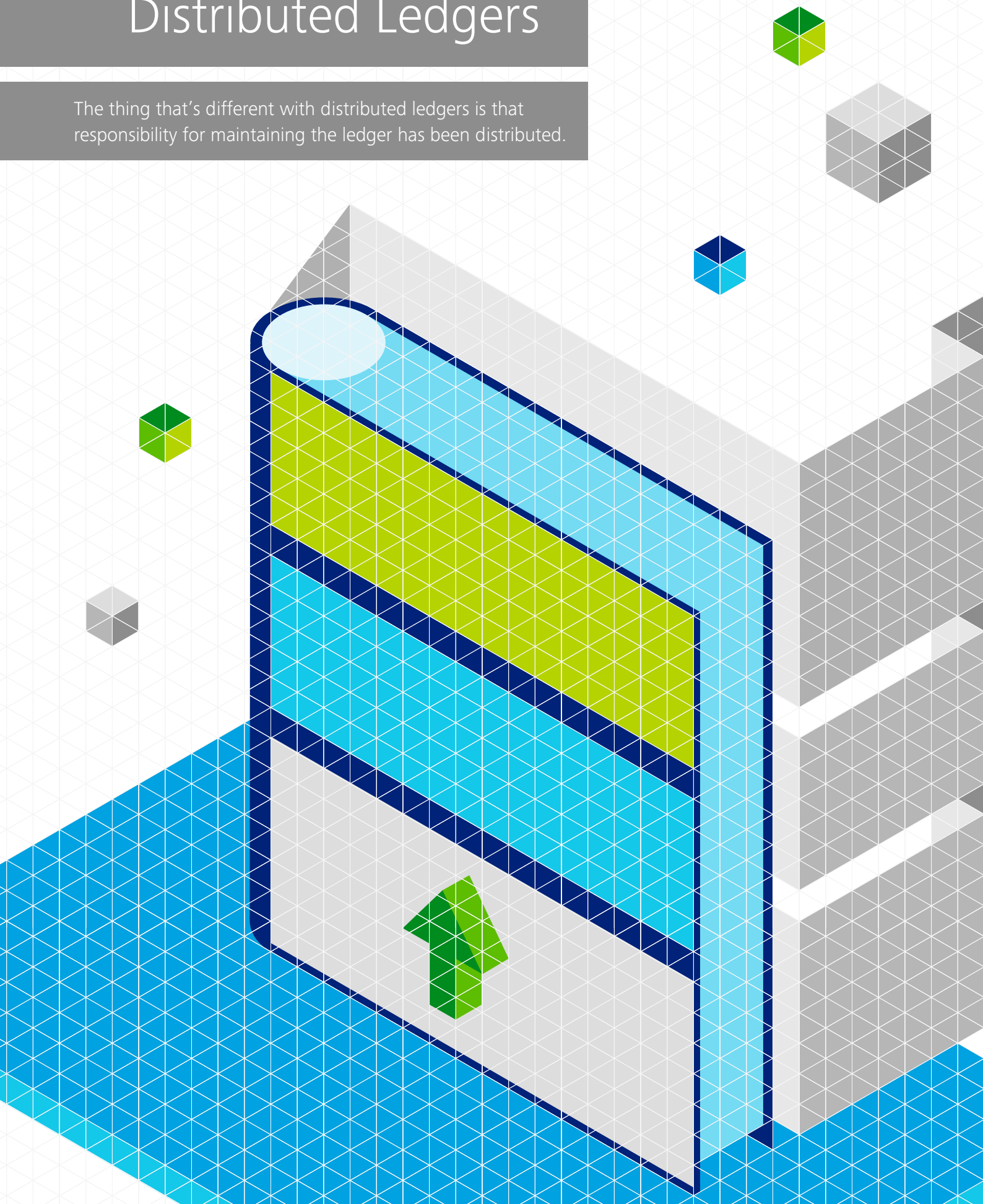
***a* blockchain** (the indefinite article) is a ledger based on blockchain technology, though not necessarily the one used by Bitcoin. This might be as simple as using the same open source code as bitcoin to create a new ledger, through to swapping in alternative implementations or algorithms.

distributed ledger is a generic name for the family of problems that bitcoin and blockchain are one possible solution to.

shared ledger is an alternative generic name.

2. From Bitcoin to Distributed Ledgers

The thing that's different with distributed ledgers is that responsibility for maintaining the ledger has been distributed.



A technology of trust

Bitcoin – the currency – is a technology for managing a lack of trust, just as all currencies are.[8] We use both formal and informal currencies when we want to exchange value with someone we don't know and otherwise wouldn't or couldn't trust.

Commodity currencies imply trust in the inherent desirability or usefulness of the underlying commodity; we have faith demand will hold firm and maintain the commodity's value. Trust in a fiat currency relies on our faith that a government will repay its debts, a faith underpinned by the government's monopoly on taxation.

Bitcoins, like fine art and gold, only have value because we all agree they are valuable.[9] The value of Bitcoin rests on our trust that if we wish to transact our Bitcoins will be accepted by another member of the Bitcoin community. This trust comes in three parts:

One, we have faith Bitcoins are an accurate measure of value; we can accurately and easily convert between Bitcoin and other measures, other currencies, or the value inherent in goods and services.

Two, we have faith the demand for Bitcoins is sufficient in that we can use them as a means to exchange value when needed.

Three, we have faith this demand will not change dramatically while we hold Bitcoins, so their value remains stable and allows us to use Bitcoin as a store of value. Our level of trust will determine how long we are willing to hold Bitcoins.

All three rest on the faith the ledger supporting Bitcoin will maintain an accurate record of the creation and ownership of all Bitcoins.

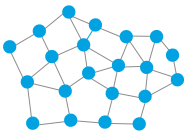
Physical vs. Digital vs. Distributed

Physical: Physical ledgers started in the Bronze Age, often the result of needing to maintain records of agricultural goods. Represented by records stored in a codex, they are 'pages' organised into volumes that form an authoritative source of information.

The identity and integrity of the ledger is ensured by controlling physical access to where the codex is stored. *Image: Early writing tablet recording the allocation of beer.*

Digital: Date back to the development of business computers, in the 50s and 60s. Ledger represented by records stored in a database. Moves the physical ledger to the digital world, but adheres to the same paradigm.

Identity and integrity of the ledger ensured by controlling access to the application that maintains the ledger. *Image: LEO (Lyon's Electronic Office), the world's first general purpose business computer.*



Distributed: Emerged in 2008 with the release of Bitcoin. Ledger represented by the consensus view of a group of peers who share responsibility for maintaining the ledger.

Identity and integrity of the ledger ensured via establishing consensus among the peers who share maintenance of the ledger.

From physical ledgers through digital to distributed ledgers

The ownership of Bitcoins, including transfers of ownership, is recorded in a *distributed ledger:*[10] the Blockchain.[11] For our purposes, we'll define 'ledger' as:

an append-only record store, where records are immutable and may hold more general information than financial transactions.

We can think of distributed ledgers as a consequence of the mass adoption of digital networks, and the logical evolution of physical ledgers (lines of text in a codex) and digital ledgers (rows in a database). Both physical and digital ledgers record entries in a single place; as a central agency is typically responsible for them we might call them central ledgers. Central ledgers allow one authoritative copy of the data. For physical ledgers, this is a single codex, or a volume in a series. Digital ledgers use a single database, a system of record.

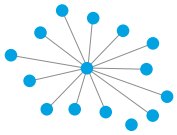
We define central ledgers in terms of the information they contain. They specify how information is to be recorded and where the ledger is stored. Security of central ledgers – ensuring their identity and integrity – focuses on managing access to this stored information. Access to the ledger enables us to add entries as well as read or change existing ones. For example, the Printers' Guild in 16th century Britain stored a codex in a secure room on which printers (members of the guild) could record their intended publications to establish precedence, an early form of copyright.

Distributed ledgers on the other hand, do *not* rely on an authoritative copy. Indeed, one advantage of distributed ledgers is that anyone who wants to review the ledger can easily obtain a copy, as all copies are equal. The disadvantage is that ensuring the integrity of the ledger is more complicated as we can no longer rely on controlling access to an authoritative, central ledger.

Central vs. Replicated vs. Distributed

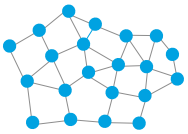
Central: Ledger maintained by a central authority. The current state of the ledger is simply whatever is in the *ledger of record* maintained by the authority. Other actors must travel to the ledger (communicate with the authority) to consult the ledger or to submit records for inclusion. A good example is the ledger maintained by the British Printers' Guild during the 16th century.

Ledger identity and integrity ensured by the central authority by restricting access to the ledger.



Replicated: Ledger maintained by a central authority. The current state of the ledger is simply whatever is in the *ledger of record*. Other actors must travel to (communicate with) the central authority if they want to submit records. Other actors can obtain a copy of the ledger if they want to consult it locally. However, they must take care to ensure their local copy is synchronised with the ledger of record. The Domain Name Service used to manage internet names is a good example.

Ledger identity and integrity ensured by the central authority by restricting access to the ledger of record.



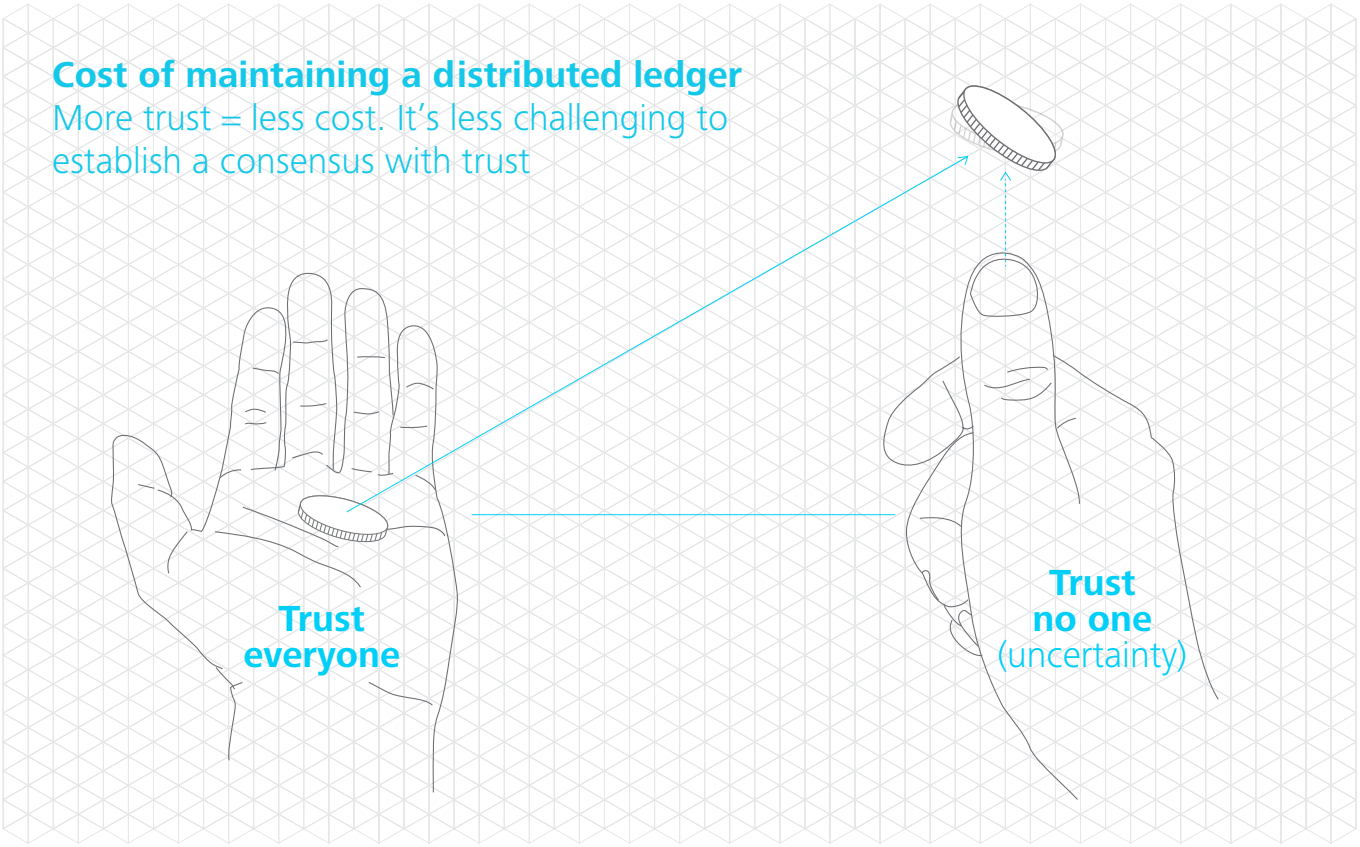
Distributed: Responsibility for maintaining the ledger shared by a group of peers. The current state of the ledger is represented by the peer's consensus on what records the ledger contains. Other actors can obtain a copy of the ledger from any of the peers, as there is no single authoritative copy. Other actors can submit new records to any or all of the peers.

Ledger identity and integrity ensured via the consensus process, that specifies how peers reach consensus.

If we merely wanted to distribute the information in a ledger, we could create what we might call a *replicated ledger*. This ledger would rely on a central authority to maintain its integrity but with other actors able to request copies and subscribe to updates. All additions and changes to the replicated ledger must pass to the central authority. While the information in the replicated ledger may be distributed, due to the magic of digital networks, responsibility for managing it is not.

What has been 'distributed' in a distributed ledger is responsibility for managing the ledger – responsibility for deciding what entries to include and their order, and for ensuring entries once added are not changed. A group of *peers* shares this responsibility, rather than leaving it to a central authority. With no single agent responsible for maintaining the ledger, we must rely on the consensus of the peers involved. The current state of the ledger is simply the peers' consensus view.

Consequently, distributed ledgers aren't defined in terms of how or where the information they contain is stored, indeed each peer may store ledger data how and where they prefer. They are defined instead by the ledger's *consensus process*, the process peers use to reach consensus.



Dealing with trust

Our choice of consensus process depends on how we choose to manage trust within the peer group. We can see the primitive form of this when we consider a central ledger. As we trust a single, central actor (a single peer), the consensus view is simply the actor's view on what information the ledger should contain: i.e. a central ledger, where we explicitly trust a single system of record.

Once we shift to trusting a group of peers to maintain the ledger (two or more actors), we need to consider how trust is spread across this group. The obvious choices are: implicitly trust all in the peer group, only trust some members of the peer group, or trust no-one. The less we trust, the more challenging it is to establish consensus. The practical consequence of this is how the cost of maintaining the distributed ledger increases as trust decreases, making the decision of whom to trust and therefore how to establish consensus, a trade-off of cost and benefit.

Establishing consensus is not typically a continuous process. This would be too expensive and time-consuming, with the peers agreeing on the current state of the ledger record-by-record. It's more common for the consensus process to be periodic, with the peers meeting either after a predefined period of time or when a set number or volume of records are ready to be added to the ledger. The distributed ledger jumps between these *consensus points* where the peers gather to agree the state of the ledger.

We can establish consensus via a range of mechanisms. For example, this might be explicit via a vote or it could also be implicit by providing evidence a majority of peers were working with a specific set of ledger information. This latter approach is the one used by Bitcoin.

Actors wanting to inspect the current state of the ledger only need to ask any of the peers for the result of the latest consensus point. From this, the entire ledger can be reconstructed.

The Byzantine Generals' Problem

Computer scientists have long concerned themselves with the problem of maintaining a consistent and accurate set of records in a large and complex computer system where malfunctioning components give conflicting information to different parts of the system, or where hacked components deliberately lie in an attempt to subvert the system. Bitcoin is subject to this problem because the integrity of the distributed ledger must be maintained in an environment where some of the miners may be actively working to subvert the ledger. This problem is called the Byzantine Generals' Problem as it's often described in terms of a group of generals of the Byzantine army camped with their troops around an enemy city.

The problem is often formulated along the following lines: *'Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if, and only if, more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed.'*

— Leslie Lamppost, Robert Shostak & Marshall Pease, *The Byzantine Generals' Problem*[12]

A definition

We therefore provide a definition of 'distributed ledger':

a ledger maintained by a group of peers, rather than a central agency.

Any member of the group of peers can add records to the ledger. However, records are only accepted when the group agrees the record meets all the ledger's requirements – typically it must be unique, correctly signed, etc.

For a distributed ledger to be trusted, it must have two characteristics:

One, we must be confident the records it contains haven't been tampered with. We do this with cryptography via digital signatures, in much the same way we sign other digital documents, and digital fingerprints using a technique called 'hashing', which is extremely sensitive to any change in underlying data. The use of cryptography is what gave virtual currencies created on digital ledgers the name 'cryptocurrencies'.

Two, we must determine what records are stored in the ledger and their precedence – the ledger's contents. The consensus view of the group of peers represents the contents of a distributed ledger. This consensus must be established in an environment where we assume some of the peers are providing erroneous data.

This may be by accident, such as partial computer or network failures, or it may be deliberate, as when a malicious actor might try to subvert the Bitcoin ledger to rewrite earlier transactions and capture Bitcoins for itself. This is a challenge often referred to as the Byzantine Generals' Problem. Network and computer failures are more frequent than we might expect. For example, Bitcoin commonly experiences problems lasting 10 or 20 minutes with some failures lasting 30 or 40 minutes and one exceptional failure lasting roughly 1 hour.[13] This means that while blocks are added to the Bitcoin ledger every 10 minutes, in exceptional circumstances it can take up to an hour to reasonably confirm a payment.

Finally, as a distributed ledger is represented by the consensus view of the peers maintaining it, the ledger is defined via the process these peers use to reach consensus, rather than by a data schema, technology or place. It is the consensus process we must define and maintain, and which the regulator will want to regulate if we wish to create a distributed ledger.

Bitcoin and proof of work

Ideally, we would use a direct approach to determining consensus, such as polling all the peers. However, in some cases a direct approach is not possible. For example, when we don't trust any of the peers as the peers may be anonymous.

Indirect approaches rely on embedding evidence in the ledger itself of how many peers, or what proportion of the peer community, believe the ledger to be the correct one. This enables us to distinguish between two or more competing instances of the ledger by preferring the ledger supported by the larger proportion of the peer community. Typically, this is evidence of a peer's control of a limited resource used in creating a ledger update. This implies not all peers are equal, as peers who control more resources have a proportionally larger say in which of the competing instances of the ledger should be trusted.

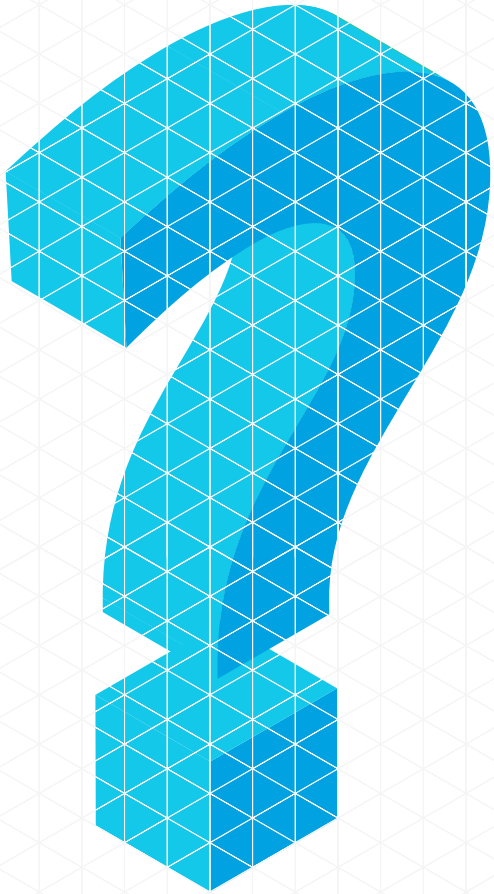
Bitcoin uses *proof of work* as this indirect evidence. Each time a Bitcoin peer, known as a *Bitcoin miner*, submits an update to the Bitcoin ledger, called a *block*, as ledger updates are blocks of Bitcoin transactions, they attach evidence they have solved a challenging cryptographic problem. Solving this problem consumes computer time that incurs real-world costs. Over time, as ledger updates accumulate and the blocks grow into a blockchain, the ledger will contain more-and-more proof of work. If technical problems or an attempt to subvert and rewrite the ledger cause the blockchain to fork separating it into two or more chains that share a common ancestry, the consensus view of the ledger is represented by the longest unbroken chain. The longest chain will have the most 'embedded work' as it required the most computing resources to create and is therefore the ledger supported by the majority of the peer group.

Approaches other than proof of work have been proposed, such as *proof of stake* used in PeerCoin,[14] another cryptocurrency that asks users to prove ownership of a certain amount of currency – their 'stake' in the currency.

3. A map of the distributed ledger landscape

5 questions you need to ask yourself

- Who's involved?
- Who do we trust?
- What is the basis of consensus?
- What does the ledger record?
- How 'smart' is the ledger?



Mapping the problem space

Something of a gold rush has been underway since Bitcoin emerged into the mainstream. As with all new technologies, there is a dash to find new and interesting problems to solve. In many cases, and just like a gold rush, firms have hurried to stake a claim as the default provider for a particular type of solution, and potentially to extract an economic rent by building a thicket of patents around themselves. Some of these solutions are clearly better than the centralised solutions we're familiar with. For others, the wisdom of moving to a distributed ledger is not so obvious.

Forming a map helps make sense of the emerging distributed ledger landscape, the nature of the ledger required, and the trade-offs. It is also a tool to enumerate the possibilities distributed ledgers bring, allowing us to look beyond the first few examples and understand the depth of the capability.

A number of questions shape our map, and while we've already touched on some of these questions, such as 'Who do you trust to maintain the ledger?', others are new.

The complete list of questions we developed to shape our map of distributed ledgers comprises:

- What does the ledger record?
- How 'smart' is the ledger?
- Who's involved?
- What is the basis of consensus?
- Who do we trust?

What does the ledger record?

We need to determine the nature of the records the ledger contains.

→**Native Records** A piece of information – a record – that comes into existence only when it is entered on the ledger. Any virtual good, or a contract that defines rights and/or obligations arising from an agreement, are candidates for native records. Examples include copyrights tied to a ledger, as the copyright only comes into existence when it is entered on the ledger.

→**References References** to external assets or agreements, things that exist separately to the ledger and which the ledger tracks. An obvious example is gold certificates.

How 'smart' is the ledger?

This is an innovation added by Bitcoin. Rather than include a pro forma in each transaction explicitly specifying how value is to be distributed from one set of accounts to another, Bitcoin allows the payer to specify a pair of scripts that when run together determine how the value will be transferred. This is more flexible than the pro forma, as in principle the payer can write a script that includes multiple signatures or impose conditions on the payee. This technique is the foundation of 'smart contracts'. The most widely known smart contracts are the digital rights embedded in ebooks, music and media files. This leads us to ask, how 'smart' do we want the records on our ledger to be?

Smart contracts
Smart contracts are computer programmes that facilitate, verify, or enforce the negotiation or performance of a contract. Proponents of smart contracts claim many kinds of contractual clauses may be made partially or fully self-enforcing.

→**Text Entries** on the ledger are simple text, and are not at all smart.

→**Logic, on ledger** Entries can include logic, via a programming language, that refers to on-ledger data.

→**Logic, off-ledger** Entries can include logic, via a programming language, that refers to on-ledger and off-ledger data.

Who's involved?

How do we define the community supporting and using the distributed ledger? There are two options:

→**Open** The community is open to all, potentially allowing even anonymous or pseudonymous actors to act as peers or participants.

→**Closed** The ledger is closed, where the identity of all entities involved in the ledger is known and they require permission to join the ledger, and possibly separate permission to act as peers.

What is the basis of consensus?

We need to consider the focus of consensus process by asking – what do the peers build consensus around?

→**The Entire Ledger** We can choose to use the entirety of ledger data – every record ever created – as the basis for the peers to reach consensus.

→**Net State** Consensus is based on the net state of the ledger, where any transactions or changes in state are rolled-up. Peers explicitly agree on the current net state of the ledger typically by agreeing on a set of ledger updates to be applied to a previous version of the net state agreed on. This results in a *chain of ledgers*, as each ledger consists of the current net state, a reference to the previous net state, and the set of ledger updates that must be applied to the previous ledger to achieve the new net state. It is easy to determine the current net state but determining the update history requires us to traverse the entire chain of updates. This is the approach used by Ripple.[15]

→**Ledger Updates** Peers explicitly agree on the updates to be added to the ledger, with each update referring to the previous one. Typically, these updates are batched by being grouped into blocks. This results in a *chain of blocks* of ledger updates, hence *blockchain*. It is easy to determine the order updates were applied, but determining the net state is more difficult as one must obtain all the updates and play them forward to determine the net state of the ledger. This is the approach used by Bitcoin.

→**Records** Consensus is based on individual records. Rather than a chain of updates, or a chain of ledgers, this approach allows individual updates to exist in isolation. Whereas the two previous approaches determine precedence by managing the update process, this approach establishes precedence with explicit references between updates. This approach does away with a global definition of consensus, relying on local definitions of consensus.

Who do we trust?

We need to ask which peers from this community we trust to maintain the ledger. The looser our definition – the further along this progression from *trust one* to *trust no-one* – the more expensive it is to maintain the distributed ledger. This rising cost is due to the increased effort required to establish consensus in an ever more distributed environment, an environment where we can rely on fewer peer-to-peer trust relationships.

→**A single peer** We trust a single actor, a central authority, to maintain the ledger, the ledger of record. This is the primitive case of a distributed ledger, one resulting in a physical or digital ledger, a central ledger.

Permissioned vs. unpermissioned

A permissioned ledger is a ledger where actors must have permission to access the ledger.

Permissioned ledgers map to closed *trust-some* or *trust-all* ledgers. Permission is granted in two different ways. The first is via a *white list*, a list of actors allowed to join the ledger's community. The second is via a *black list*, a list of actors who are banned from the ledger's community: a permissioned ledger using a black list would be a closed, trust-some ledger; a permissioned ledger using a white list could be either an open or closed, trust-some ledger.

We note Bitcoin was originally designed to be permissionless, although it is becoming increasingly permission-based as the various services enabling one to access the ledger demand you identify yourself – typically to comply with anti money-laundering or counter-terrorism financing regulations.

The cost of maintaining a central ledger is driven by:

- The cost of maintaining a copy of the data, including the computing infrastructure and organisation responsible for the ledger's maintenance
- The cost of accessing the ledger, either physically or via a digital network.

→**All peers** We implicitly trust *all* members of the peer group, with each peer accepting all valid records from other peers. This approach incurs the additional cost for each peer to maintain a local copy of the ledger data, and the communication overheads implied by distributing this data.

→**Some peers** We can explicitly trust *some* peers and, by extension, distrust the remaining members of the peer group.

Consensus is typically established via voting on what constitutes the ledger, where we only consider the votes of trusted peers. It's important to note trust can be a fluid concept. Different members of the ledger's community might trust different, potentially overlapping or even disjointed, sets of peers. A peer can also move from trusted to untrusted or untrusted to trusted, such as when a peer fails, or leaves or joins the peer group.

This approach incurs the additional cost of a consensus process.

→**No peers** We can distrust all peers, a *trust no-one* situation. Any peer can join in the maintenance of the distributed ledger, and it may be possible for them to be anonymous. Typically, consensus ties to control of a limited and possibly expensive resource. Bitcoin uses this approach.

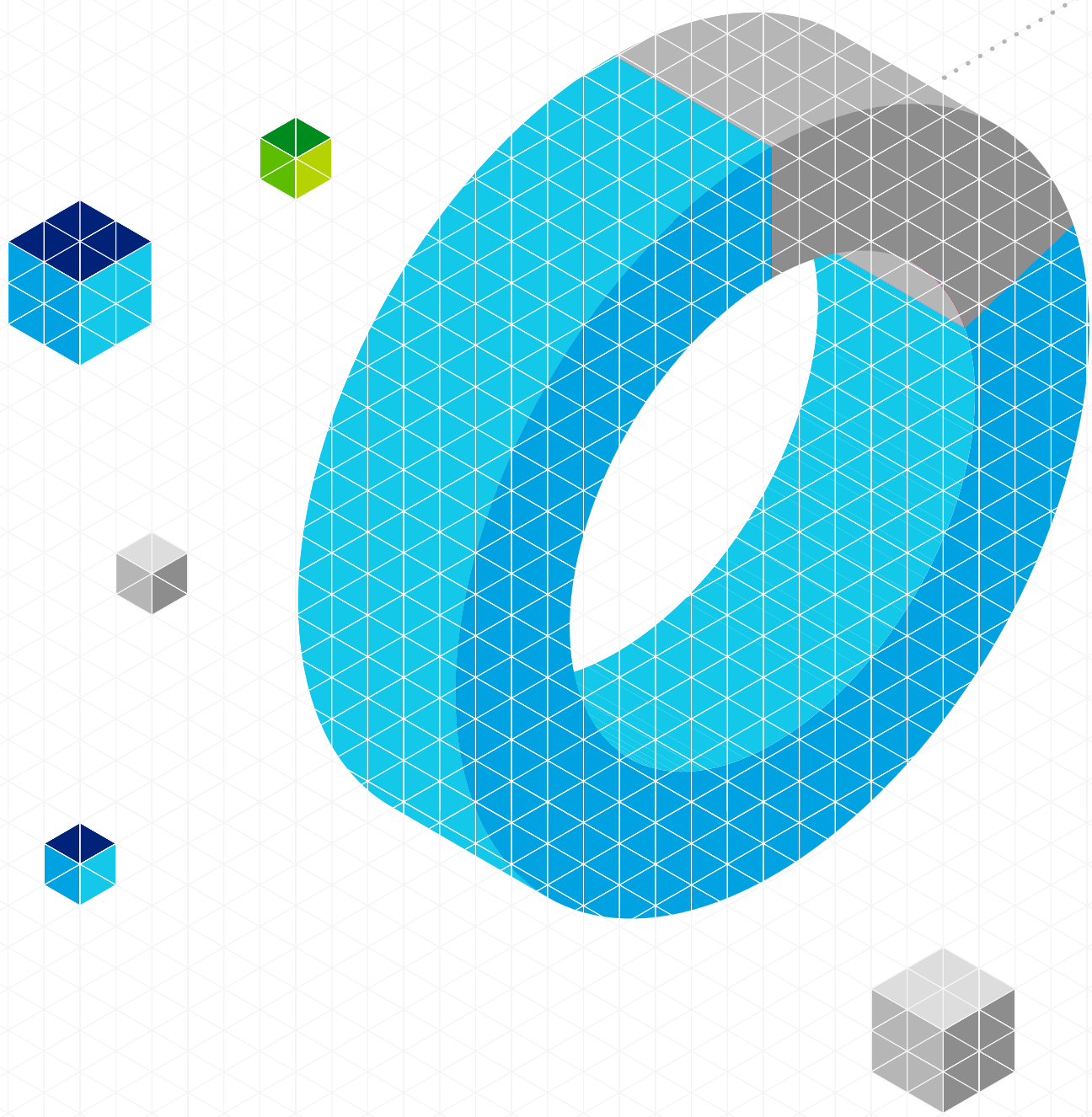
This approach incurs the additional cost of controlling the requisite resources. For example, it was estimated in 2013 that Bitcoin was consuming the processing six to eight times greater than the top 500 supercomputers[16] just to ensure the integrity of the ledger, with an aggregate cost of US$8.25 per transaction. It was also estimated in 2016 that a small number of Chinese miners, possibly as few as 2 but less than 5, control more than 50% of these resources.[17]

Tokened vs. tokenless

The first distributed ledgers – such as Bitcoin – required a native on-ledger currency to operate. These currencies are known as tokens in the nomenclature of the blockchain community. A tokened ledger is a ledger requiring a currency to function, typically to pay the miners or to make denial of service attacks economically challenging. Tokenless ledgers don't require a currency to operate.

4. Regulation

- There is little that is unprecedented that existing regulatory approaches can't cover
- The exception is the corner case where the ledger is outside the regulator's reach, but this can be covered by certifying the ledgers that are allowed to interact with regulated industries.



A new regulatory frontier?

Are distributed ledgers a new regulatory frontier? Our existing frameworks are based on the state's monopoly on violence: do what the regulator says or go to jail. However, distributed ledgers spread responsibility evenly over a number of individuals, with many of the individuals in other jurisdictions or even anonymous. So just who would we put in jail?

A Cambrian explosion of currencies

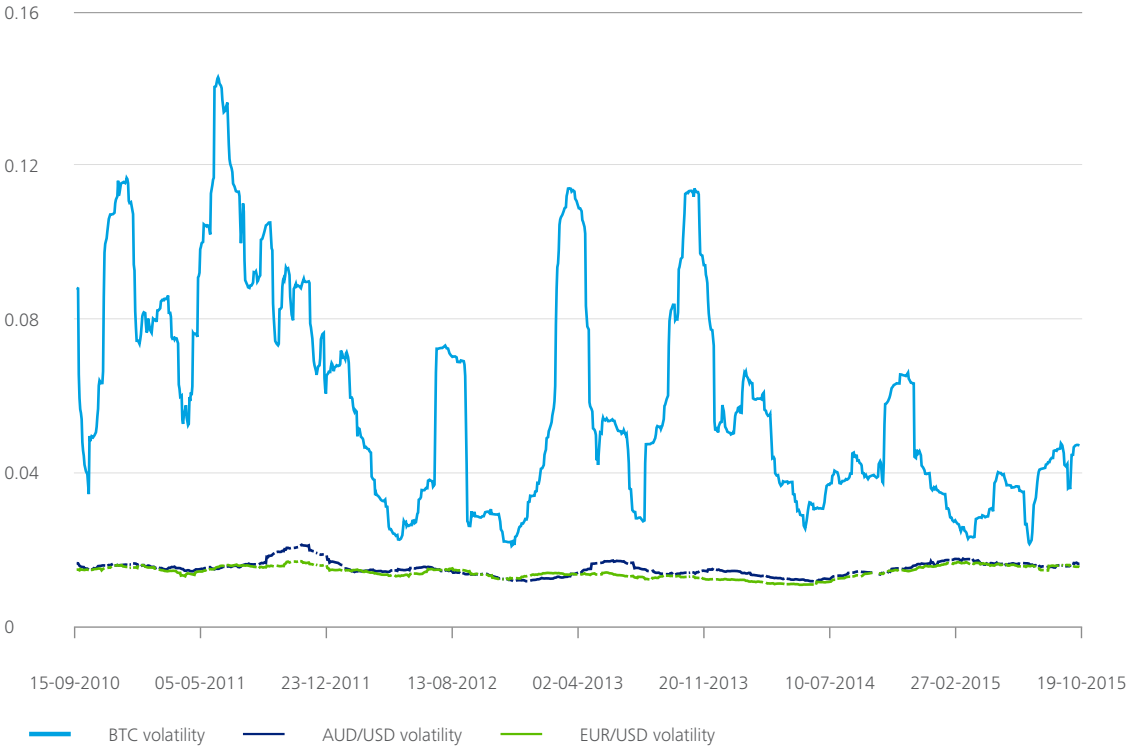
It seems appropriate to deal first with the question of cryptocurrencies. Bitcoin represents the genesis of distributed ledgers, and the particular type of distributed ledger that Bitcoin uses – *the* blockchain – has a currency as an integral part of its solution. The two are not separable, remove Bitcoin from the blockchain and there is no incentive for mining, making the ledger unsustainable.

Regulating a blockchain can imply regulating a cryptocurrency. Before we rush into how we might regulate a cryptocurrency, we need to ask the question: do we need to regulate cryptocurrencies at all?

The currency to support mining in a blockchain is not required to be created on-ledger as Bitcoin is, where the value is created as part of the consensus process. Value can be injected from outside the ledger from an off-ledger currency and either transferred onto the ledger to be accounted for or simply passed directly to miners via records as a fee.

Off-ledger currencies could be either a sovereign currency, fiat or not, or a private currency.[18] Sovereign currencies do not require our attention. Private currencies used for this purpose on the other hand, are conventional electronic currencies and would consist of the uninsured liabilities of private individuals or companies. For example, the IMF could easily use Special Drawing Rights (SDRs) to fund mining if it were to release a blockchain. Free banking[19] taught us that in these circumstances attention must be paid to the importance of the assets into which the private money is convertible and to the issuer's reputation for making the conversion as promised.

Figure: Bitcoin Volatility.



Source: The Bitcoin Volatility Index[20] and FRED.[21]

On-ledger currencies such as Bitcoin are different beasts. Created on-ledger they are fiat currencies that aren't backed by a trusted institution or government with the power to tax, and they cannot be exchanged for specie or commodities – their value is purely a function of demand. This institutionless nature of Bitcoin might be the source of much of its volatility, with the market treating Bitcoin more like an asset than a sovereign currency. And while Bitcoin volatility is in gradual decline, volatility is also positively correlated with trading volume, as it is with all asset markets.

It is easy to forget the purpose of regulating a currency is to provide stability and predictability, and thereby reduce the effort required to exchange value. We work to control inflation so the currency is a stable unit of account and store of value, while the compulsion for merchants to accept the currency makes it a ubiquitous medium of exchange.

So rather than asking how we should regulate cryptocurrencies, we need to ask ourselves two rather different questions:

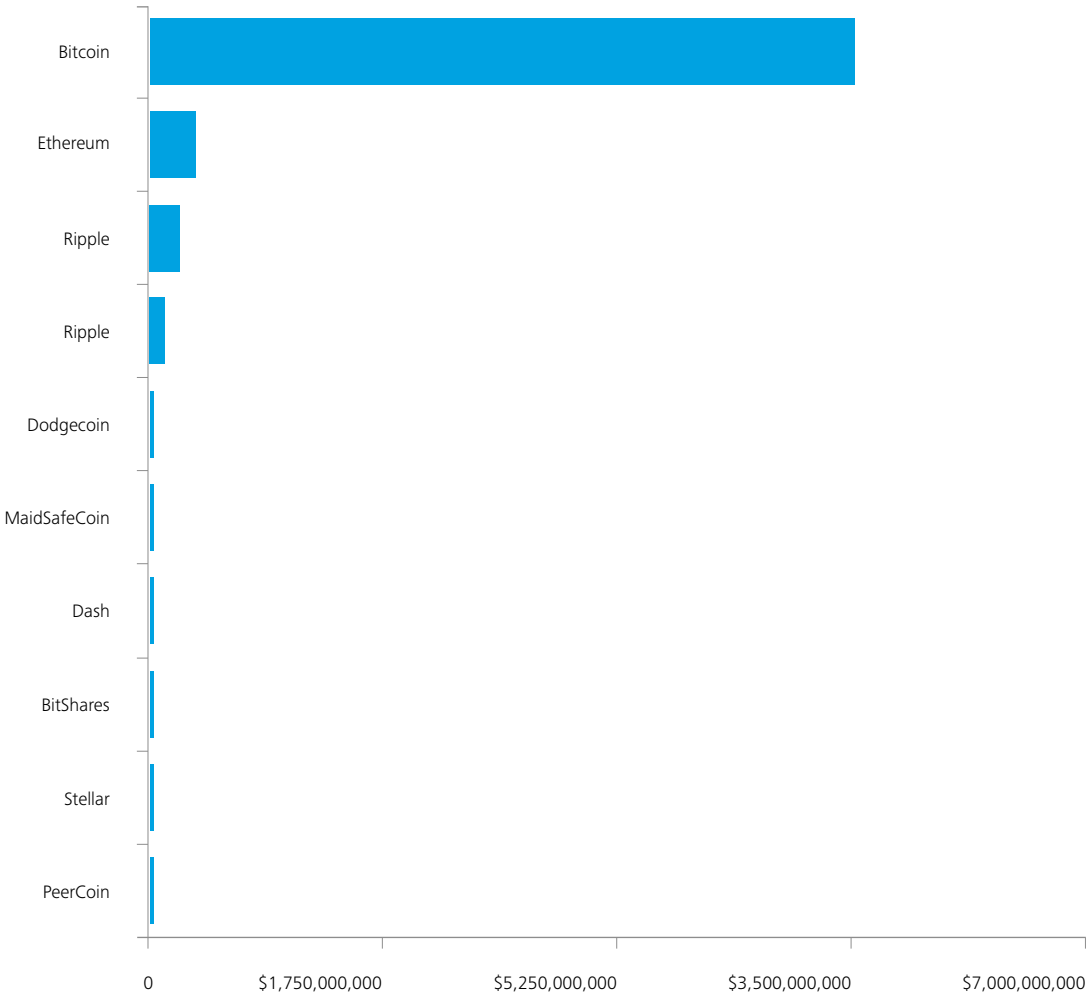
Do we need to ensure the stability of cryptocurrencies?
As long as there is reliable and low-cost information on the relative worth of the various currencies, consumers are quite capable of deciding how to manage the risk for themselves. We saw this in the free banking era in the late 19th century. Bitcoin's volatility, or the volatility of any cryptocurrency, is not a problem for regulators to solve.

Do we need to ensure the currencies used by distributed ledgers are ubiquitous mediums of exchange?
We should reframe this question and consider if we should be concerned that the rise of cryptocurrencies will throw us back to something like the free banking[19] era.

One of the challenges then was managing high transaction cost due to the additional risks and lack of transparency incurred by the many cross-currency transactions. The motivation behind nationalising currencies – creating the Australian pound, US dollar, and even the Euro – was to reduce this cost. A single national currency makes doing business more cost-effective and less risky. However, there are limits to these benefits as we can see with the Euro. Limiting private and cryptocurrencies is as simple as imposing a tax on them, converting them into demurrage currencies.

While it might seem as if we're in the middle of a Cambrian explosion of cryptocurrencies – with more than 710 cryptocurrencies available for trade online – only 10 cryptocurrencies have market capitalisations over $10 million US. Of these 10, Bitcoin currently stands arms and shoulders above the rest.

Figure: Cryptocurrency market caps.



Source: CoinMarketCaps.[22]

New technologies such as Bitcoin attract the early adopters and speculators, but the majority of consumers are more circumspect. As we noted in The Future of Exchanging Value: Cryptocurrencies and the trust economy[23], consumers adopt currencies to manage the risk associated with a lack of trust. This is the opposite of what's often assumed – that currencies are adopted to build new trust relationships. Cryptocurrencies' volatility makes them poor units of account and stores of value, though this doesn't prevent them from being an effective means of exchange. It is unlikely more than a minority of consumers, the early adopters, will choose to store their wealth in cryptocurrencies, relegating cryptocurrencies to a tactical means of exchange with value denominated via other, more stable currencies.

The environment that gave birth to private and state-based currencies was dominated by high communication costs. This is why wildcat banks would base operations 'out where the wildcats are', so it was hard to exchange their currency for scrip, enabling the wildcat banks to maintain low reserves and high returns. Today's low communication costs lead us to believe it's unnecessary for regulators to step in and encourage private and cryptocurrencies to consolidate because consumer preference and market forces will naturally push them in that direction. We can expect distributed ledgers – in most cases – to migrate from cryptocurrencies to private or sovereign currencies, or to a dominant cryptocurrency (most likely Bitcoin), as they attempt to reduce transaction cost and thereby improve adoption.

To address our original question on whether we need to regulate cryptocurrencies – it doesn't appear as if the regulating the currencies embedded in distributed ledgers requires new regulatory approaches.

Distributed governance

The second aspect is to consider the governance of the ledger itself, which we can address in two parts:

First, the regulation of the ledger's contents – supporting regulations designed to change the records in a ledger, such as 'Right to be Forgotten'. Second, the regulation of the governance process that manages the evolution of the ledger – forcing changes into the ledger, or forcing the elimination of unwanted bugs and features.

We define a distributed ledger via its consensus process, rather than its data store like a physical or digital ledger. This means we can only indirectly regulate the contents of the ledger.

Consider how we might implement a 'Right to be Forgotten' law, where the regulation is intended to remove identified records from the ledger. There is no effective way of doing this via the consensus process. We could direct the consensus process to a normative list of records to remove, but then we don't really have a distributed ledger anymore because the list is centralised. If we embed the list in the consensus process itself, then the list becomes public as the

consensus process is public. If we simply compel the minority of peers we can control to remove the record (as they're domiciled in our country), then the integrity mechanisms designed into the ledger will reject the change – just as they would reject similar changes from malicious actors.

We must also consider how the ledger's governance facilitates desirable changes to its consensus process. Any solution has errors that need to be removed or new features to be added. In some cases, the error and feature are the same, as with Bitcoin Mixing where a feature intended to create flexibility also enables money laundering.

While a consensus process might be governed conventionally, it is also quite possible for a distributed ledger to have a distributed governance process. Take the recent schism at Bitcoin as an example. Bitcoin's ledger is protected by an indirect consensus process. Rather than voting on which ledger is correct, with Bitcoin we prefer the ledger containing the most 'embedded work', as this should be the ledger with the support of the largest proportion of the mining community. Bitcoin's definition – its consensus process – is protected via a similar mechanism. Miners are free to adopt any version of the consensus process they choose. We should also remember there is no restriction on who can offer up a version, they don't need to be from a 'core team' or other blessed group of individuals. Subsequently, Bitcoin governance – just like the state of the ledger – is based on the consensus of the miners. The Bitcoin consensus process is simply the process the majority of miners are using.

How do we regulate the consensus process when the governance structure built around the consensus might not be based on the nation state? How would the regulator enforce their will when there is no one to put in jail?

Bitcoin Mixing

It is impossible to trace value across a Bitcoin transaction. Value is added to a transaction from one or more accounts ('addresses' in Bitcoin nomenclature), and is then distributed to one or more accounts. This feature has been used to create industrial scale money laundering services by washing legitimate and illegitimate exchanges through the one transaction for a 0.05% fee.

Concerns over the limitations of Bitcoin Mixers, and the possibility a mixer might abscond with value, spurred the creation of mixing venues, where like-minded individuals can meet others and mix their coins directly. The latest iteration is ZeroCoin,[24] which attempts to change Bitcoin to embed mixing in the transaction definition.

A 2012 Australian Transaction Reports and Analysis Centre (AUSTRAC) report[25] examined digital currencies, including Bitcoin, for use in criminal activities and specifically looked at their use in money laundering. The report concluded digital currencies generally fall outside AML legislation globally and digital currency exchanges could provide criminals with the ability to serially convert their digital currencies to other digital currencies before reintroduction as a fiat currency. However, the report notes that use of digital currencies for illegal activities is not without drawbacks, citing the limited size of the digital currency markets and the limited rate of acceptance for payment.

The scenarios outlined above represent corner cases, exceptions rather than the rule. However, they are exceptions that warrant concern. The challenge for regulators is to find a mechanism that enables them to ensure the safe operation of all distributed ledgers.

While governance of distributed ledgers might at first seem challenging, it also appears to be tractable.

We need to remind ourselves many – if not the vast majority – of distributed ledgers will operate inside established regulatory regimes. The challenge is to deal with those few ledgers sitting outside existing regulation.

When Bitcoin first emerged there was concern the anonymity it provides would enable fraud and money laundering on a previously unimagined scale. These fears proved to be unfounded.

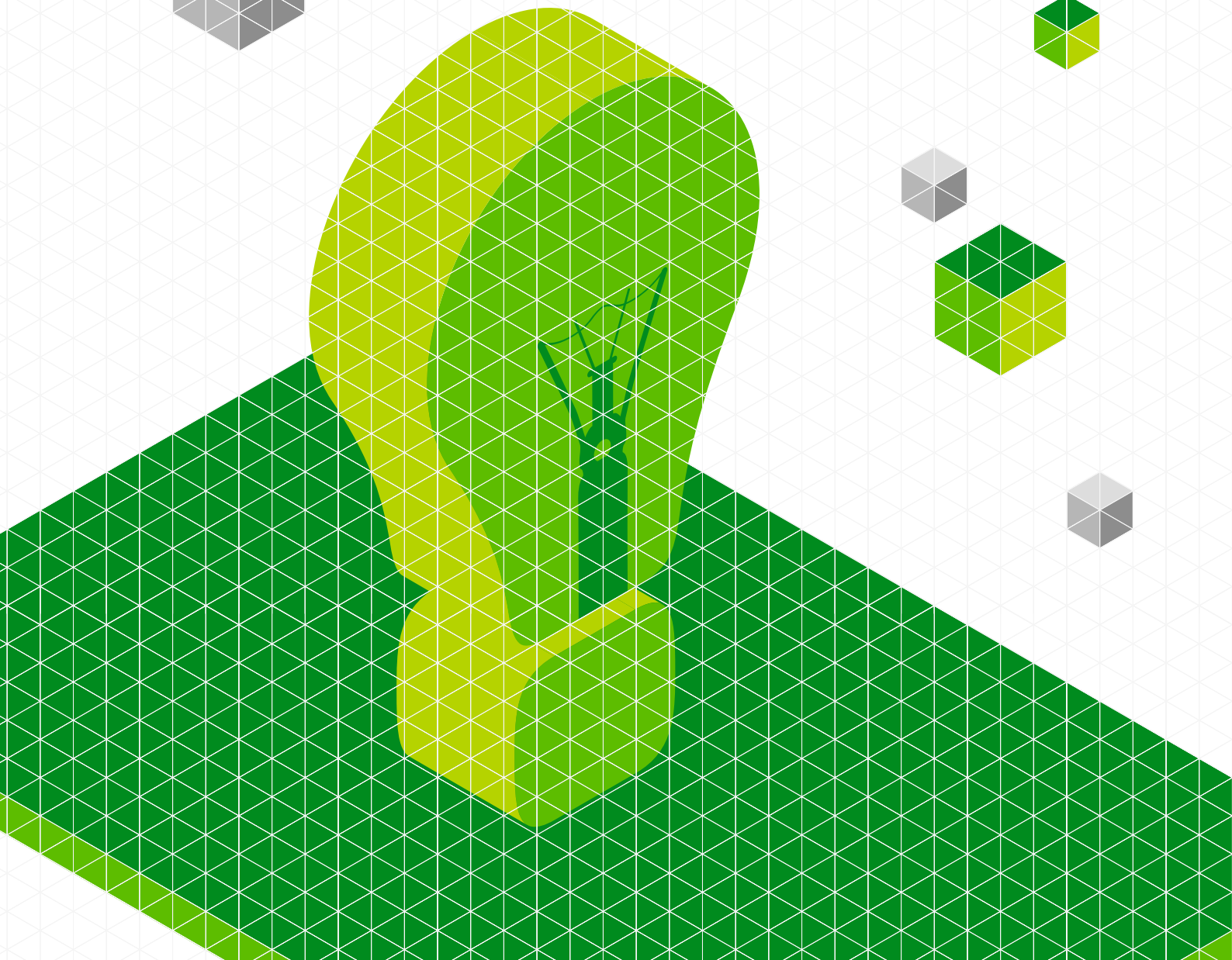
While Bitcoin itself might exist outside regulatory structures, it must touch the real world for the currency's value to be realised. Regulators soon found these on-ramps, the services acting as bridges between Bitcoin and the real world, were subject to existing regulation. Bitcoin exchanges and payment services had the regulators knocking at their door demanding they register as money transfer services and adhere to compliance requirements.

Regulation of the on-ramps to any distributed ledger provides regulators with a powerful tool for managing the ledger itself. This holds true regardless of the ledger's contents – be they assets, contracts, or entitlements. For example, the transfer of ownership of a physical asset recorded on a distributed ledger need only be recognised if the ledger itself is recognised by the legal system.

Consequently, regulation of distributed ledgers is a question of determining which of them will be recognised by the existing legal and regulatory system.

5. Applications

Light bulbs and toasters: they do the same thing (turn electricty into light and heat), the only difference is which we consider the waste product. Similar to distributed ledgers, which have a consensus process, and record of past results from the consesus process.



What distributed ledgers can't be

Software is an incredibly malleable tool, which is wonderful because it means with software everything is possible. The problem is that not everything possible is also is practical, and possibly not even desirable.

Trading platforms responsible for price formation are a good example of where physical constraints have made a possible distributed ledger solution impractical. Recent research by Bank of America Merrill Lynch led the authors to conclude:

It is physically impossible for a distributed solution to reach the performance of even the existing generation of trading platforms. This is a feature not a bug. Price formation will remain centralised – and the existing exchanges seem unlikely to be disrupted.[26]

A distributed ledger will never be as performant as a central ledger as the consistency guarantee they provide will always incur an overhead. This overhead is the result of the need to compare each record with every other record to ensure they are unique. Moving data around takes time and every peer we add to the consensus process incurs additional communication overhead. It's impossible to escape these physical realities, and they limit the rate at which records can be added to a ledger. We can easily do much better than Bitcoin's current performance of roughly 3 transactions per second with transactions released in blocks 10 minutes apart, but it will be impractical to solve high velocity, low (transaction) value, problems with the technology.

What distributed ledgers can be

Focusing on what distributed ledgers can't be is unproductive. It results in blog posts and published articles containing long lists of potential solutions, followed by robust discussions on their technical merits typically ignoring the cost-benefit trade-offs that must be made. Our approach, discussed in the introduction to this report is to develop our understanding of distributed ledgers by working down from potential solutions, rather than up from the technology. Instead of focussing on what is technologically possible, we want to understand – within the usual trade-off of cost and benefit – what seems economically sensible, given the capabilities of distributed ledger. To do this we're going to compare distributed ledgers to toasters and light bulbs.

At their core toasters and light bulbs do the same thing: they transform electrical energy into heat and light. The only difference is which of heat and light is considered the waste product, and which is the desired product.

We can use a similar point of view to understand the potential applications of distributed ledgers.

At their core distributed ledgers convert power into both a consensus among the peers and a durable record of past consensuses. The interesting question is, which one of these is waste?

First, let's focus our attention on the durable record, and consider the consensus process waste. In this scenario we're using the ledger as a public registry, as a place where we can register our claims of ownership or entitlement or where we can publicly attest to agreements or commitments we have made.

Ownership registers track the ownership of physical or virtual assets. Indeed, Bitcoin is based on an ownership registry. Other examples include internet domain names,[27] stock, diamonds,[28] or real estate and other physical property. A recent article by The Economist[29] highlighted the potential benefits of a distributed ownership registry via a rather pointed example:

When Honduran police came to evict her in 2009, Mariana Catalina Izaguirre had lived in her lowly house for three decades. Unlike many of her neighbours in Tegucigalpa, the country's capital, she even had an official title to the land on which it stood. But the records at the country's Property Institute showed another person registered as its owner, too—and that person convinced a judge to sign an eviction order. By the time the legal confusion was finally sorted out, Ms Izaguirre's house had been demolished.

Moving a physical, central property registry onto a distributed ledger has the potential to extend access to property registries into underprivileged areas. By reducing the cost and effort required to access the register in remote locations it could help the people living there secure title to their land. This might not be a problem in mature nations with well develop institutions, but the shift has the potential to bring real benefits to jurisdictions where there is sovereign risk. Distributed ownership registers also bring certainty to the ownership of assets that pass through multiple jurisdictions, such as tracking provenance to prevent 'blood' diamonds from entering the supply chain.[30]

In developed countries we might use ownership registers to streamline complex and slow settlement processes. The US$600 billion leveraged loan market is a good example, where new rules enacted by the regulator change how investors and sellers in non distressed loans are compensated for late-settling trades. The change means buyers will no longer be able to collect loan interest payments made between a loan trade's purchase agreement and settlement, a period currently averaging three weeks. Moving the current complex multi-party settlement process to a distributed ownership register has the potential to slash settlement times.

Entitlement registers track entitlements granted to individuals and organisations. We provide one such example in From Bitcoin to Distributed Ledgers where we discussed the early (physical) copyright ledgers created by the Printers' Guild in 16th century Britain. Moving copyright to the online world via the creation of a distributed entitlement register is an obvious move. We can see the first steps in this direction with Mycelia,[31] a project instigated by musician Imogen Heap, who sees a distributed ledger of music rights as a means to remove overhead from the industry and provide musicians with a more equitable system.[32] Ms. Heap has already released a song – Tiny Human – *on the blockchain*[33] via Ujo Music.[34]

Other examples of potential entitlement registers include individual or business licences (driver's licence, liquor license), government benefits, and so on. Again, there are obvious applications in nations where there is sovereign risk or where the government struggles to reach into every corner of the economy where they will have the potential to reduce fraud, though these benefits will be muted in many developed countries.

Attestation registers are durable records of agreements, commitments or statements, providing evidence (attestation) these agreements, commitments or statements were made.

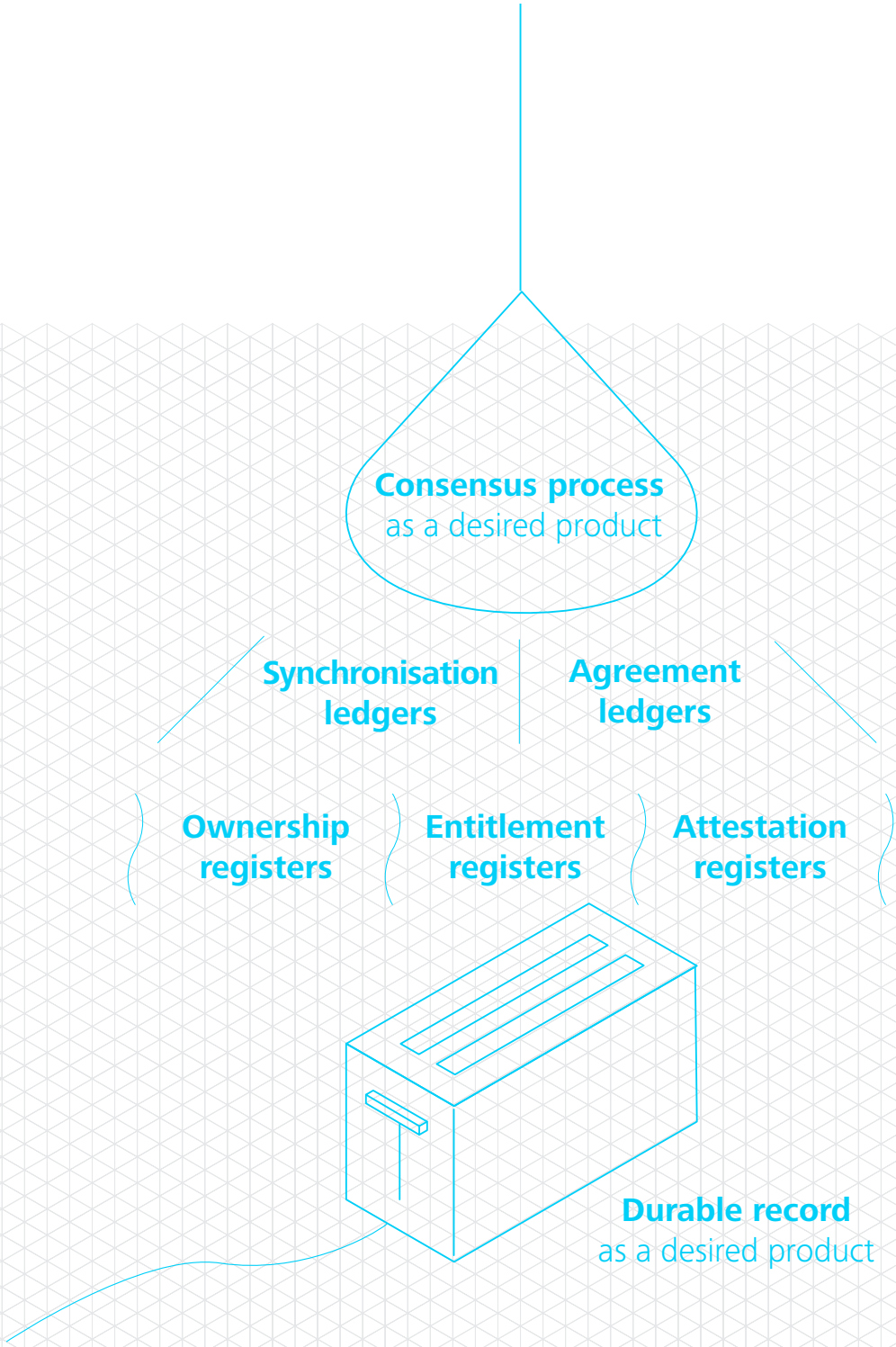
A distributed contract or 'smart contract' ledger is an obvious opportunity gaining support in the technology community. An early example of a smart contract in action was as a form of gambling, where two individuals could agree to bet on the outcome of an event (a horse race, possibly) and record their agreement in a smart (self-enforcing) contract placed on a distributed attestation register, with the final payment made automatically once the outcome of the event is known.

A distributed attestation register can also be used to record deeds, including estoppels and warranties, with the warranty potentially tied to the asset via a distributed asset register, insurance agreements, and so on. Another obvious use case is to provide an impartial record of private agreements: how many times is a contract signed only to have key pages swapped out?

Next let us consider the consensus process as the product, and the durable record as the waste. In this scenario we're using the ledger as a tool to enable two or more actors to reach agreement, with the ledger simply a possibly unneeded record of previous agreements.

Synchronisation ledgers use the consensus process for reconciling the formal records of two or more actors. Indeed, an early uses case suggested for distributed ledgers was to replace existing double-entry accounting reconciliation with a shared, distributed ledger. An example of this would be tying a firm's purchase day book to the sales day book of its suppliers via a distributed ledger where the ordering and reconciliation processes are replaced by a more streamlined consensus process. The callout *Capital Markets* has an example of this usage scenario. The authors expect synchronisation ledgers to be the low hanging fruit for distributed ledgers in industry.

Agreement ledgers use a richer consensus process that enables the actors involved to actively negotiate trading proposals and counter proposals to reach an agreement rather than simply using the process to validate records and ensure the integrity of a share data store. This might even include integrating decision support systems and humans into the consensus process. The callout *Tax and the Audit Process* shows how this approach might streamline and simplify the process of auditing a firm's books and preparing its tax documentation for submission to the local authority.



Economically sensible opportunities

At their core toasters and light bulbs do the same thing: they transform electrical energy into light and heat. The only difference is which of light or heat is considered waste and which is the desired product.

What is practical?

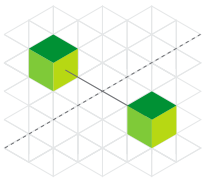
Clearly distributed ledgers can provide us with benefits. As always though, we are caught in a trade-off of cost and benefit, and while a distributed ledger might be technically attractive, it might not be the most practical solution. Adi Shamir (the 'S' in RSA) noted that he was *yet to see a use case for blockchain that can't be solved with an existing simpler technology*.[35] With this in mind we can consider not just which solutions are possible but which might also be practical.

Distributed ledgers are often promoted as technologies to create trust, or even to democratise trust. This is wrong. Distributed ledgers are tools to enable us to more effectively manage risk.

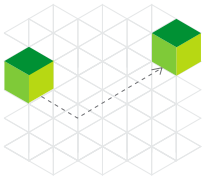
A common theme weaving through the examples in the previous section was the ability for a distributed ledger to take information that was somewhat inaccessible and make it much more accessible, extracting ledgers from inside custodian institutions and making them public where they are easy to view and validate. Actors can use this improved visibility to better manage the risk they are exposed to. However, improved visibility does not increase trust. Storing the records kept on the performance of surgeons on a public ledger doesn't mean you trust the surgeon more – after all, you can 'trust' a poor surgeon to do a botched job! – but it does enable you to manage the risk of undergoing surgery more effectively.

When we're considering the cost-benefit trade-off between a central and distributed ledger, it is this ability to more effectively manage risk that will often nudge us from the central to the distributed solution. We can see three scenarios where the balance might fall on the side of the distributed ledger.

Disintermediation. Trusted intermediaries – such as correspondent banks – can be replaced with a distributed ledger to create a more transparent process that ensures all involved parties are fully informed. Trade finance is a good example.



Cross Jurisdiction. Any ledger that tracks assets, entitlements, and attestations across jurisdictions, and where there is no logical home for a central ledger, can use a distributed ledger to create a shared authoritative source of information. The creation of a distributed diamond (asset) register is a good example. We might also consider synchronisation ledgers, mentioned above, to also fit into this category.



Compliance. Regulatory compliance reporting can be moved from a reporting process to consensus process supported by a distributed ledger, as discussed in the callout *Tax and the Audit Process*, reducing risk by reducing the time between consensus points and avoiding the annual 'and what bad news do you have' conversation with the auditor.

Capital Markets

Capital markets are large, complex and costly ecosystems. Viewed by some as antiquated and overly manual, the industry is an enticing target for technology-based disruptive forces.

There is no doubt that the current operating structure faces challenges. The process is information intensive and yet companies are exposed to risks due to information asymmetries and inefficiencies from multiple intermediaries. Counterparty risk must always be considered as contractual performance cannot be guaranteed. These challenges represent a significant opportunity to pursue new methods of organising the market.

Distributed ledgers represent an opportunity to consider what these new methods might look like. A fundamental aspect of capital markets is the exchange of value, in the form of assets, agreements and undertakings. Currently we use a central, trusted party in many scenarios to transact through, guaranteeing to each party contractual performance. Distributed ledgers enable the removal of the trusted counterparty, replaced with an incorruptible, distributed record of transactions, verified by network participants. Multiple systems can benefit from a transition to a distributed ledger operation:

- Asset transfers (e.g. Securities) currently transacted through a central clearing party would instead transact through updates to a series of ledgers. An asset ledger would enable prompt confirmation a security was owned by a party. Similarly, a cash ledger linked to digital wallets could confirm funds existed to complete an agreed exchange. Through signing individual private keys, the Delivery-Versus-Payment transaction would take place, broadcast through the node network and chained to previous transactions through cryptographic hashing. A central party is no longer required as all confirmation and validation is performed over the protocol, and settlement time is drastically reduced to near-instant
- Events and distributions are handled through smart contracts or alternatively issued directly onto the distributed ledger as assets, with consensus provided by the peer group, rather than the trusted status of a central intermediary
- Contractual agreements, such as OTC derivatives, are executed over the protocol, enabling automation as external sources are accessed and cross-referenced against clauses, providing visibility over exposure and variable margin requirements, while also reducing counterparty risk
- Data management and insight generation is improved as visibility of capital flows increases drastically as all transactions are executed on ledger with full data provided.

The potential uses of blockchain in capital markets represent an opportunity to dramatically reduce cost and risk in the existing capital market structure.

Jonathan Perkinson
Partner, Assurance & Advisory
Banking & Payments

Richard Miller
Director, Payments Advisory

Tax and the Audit Process

Tax offices world-wide, including the ATO, have been working toward a model where lodgement information is received as a by-product of transactions and information stored in customers' business systems. This would reduce or eliminate the need for lodgement from compliant taxpayers with simple tax affairs, enable the tax offices to source tax data from business systems, and use the information to support 'light touch' returns, with even the possibility of moving to a 'no touch' assessment experience. The main enabler for this is the development of Standard Business Reporting (SBR) and the development of a standard chart of accounts.

This is a challenging problem, and we've seen similar problems prove nearly intractable in other industries. A good example is efforts to develop universal health records databases, which typically flounder in their attempts to create a single, workable, health record taxonomy suitable for every (or even just the majority) of stakeholders. Development of a standard chart of accounts faces similar challenges. While it might be technically possible to create a standard chart of accounts, the challenges of integrating the needs of a diverse range of stakeholders will likely result in a chart of accounts that is overly complex and not well suited to any particular situation.

A second challenge is to support the interpretation of complex transactions as they are prepared for submission. As with many similar situations, a 70, 20, 10 rule likely applies. 70% of the transactions require no interpretation – GST transactions are an obvious example – and can be passed directly to the tax office. 20% of transactions might require the application of known policies before they are passed on. The final 10% may involve the development of new policies, which implies intervention from a human expert. While a standard chart of accounts will streamline the process for the easy 70%, the remaining 30% will still require the existing (complex and burdensome) manual process.

Finally, moving to real time, incremental assessment means whenever a problem is identified, the first task is to establish a benchmark that determines what is in and out of scope of the problem, which the experts can work from.

An alternative approach is to consider how a distributed ledger can solve this problem. Rather than support incremental assessment, a distributed **agreement ledger** could be used to create a periodic and on-going assessment process, with the length of time between assessments configurable based on the volume of exception transactions, the roughly 20% and 10% of transactions that require interpretation and therefore approval:

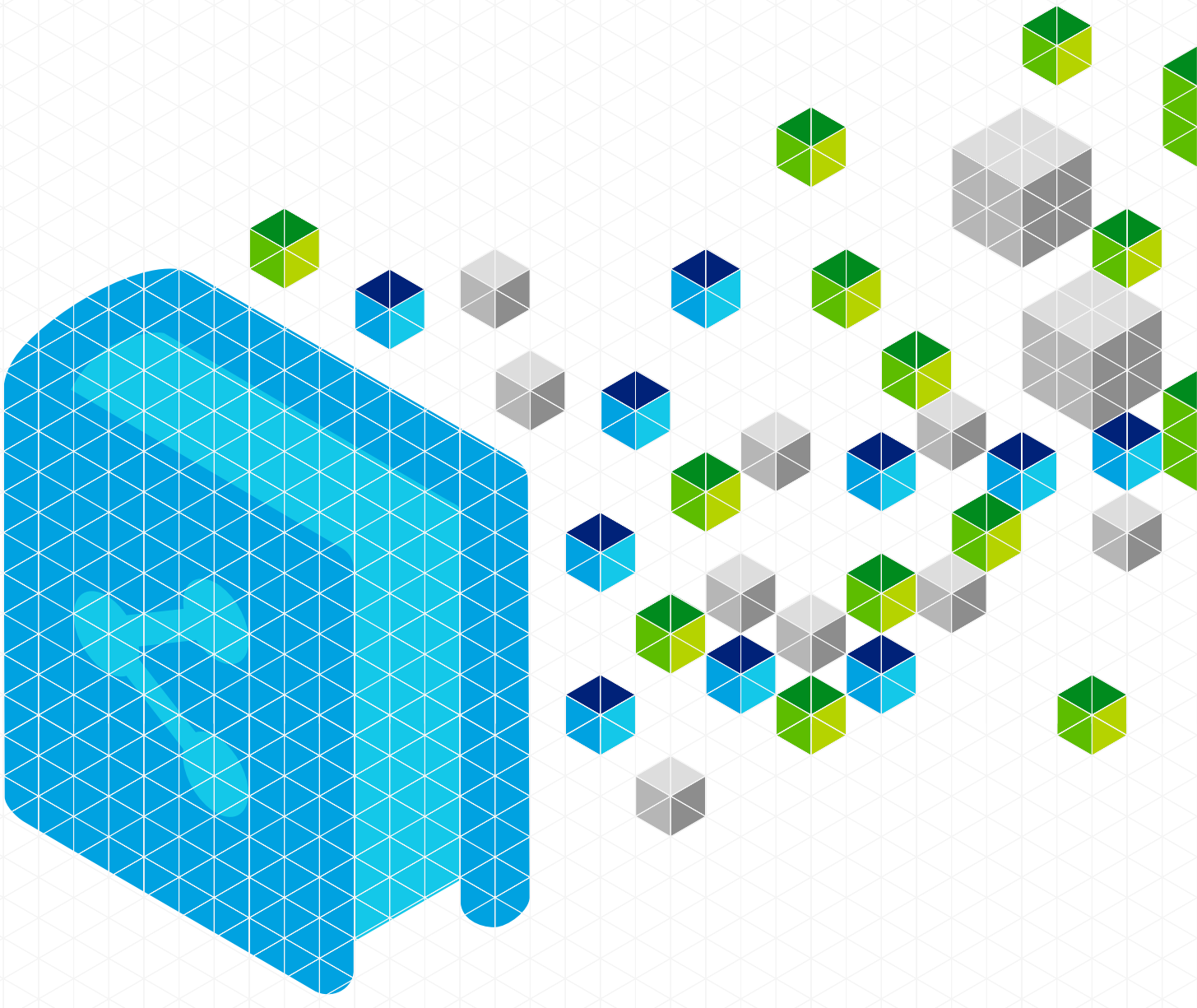
- The **ledger would record financial transactions** suitable for reporting to the ATO
- These records would be simple, containing **only data** and not business logic or the ability to support smart contracts
- The ledger is, by definition, **closed.** All the participants are identified and access to the ledger controlled. The only actors who can access the ledger data are the tax office, regulators or firms directly involved in the tax preparation process. We note this implies the submitting firm's auditor will also be an ongoing participant, due to their expertise in applying policy and developing new policy when submitting exception transactions
- Consensus is built on the **net state of the ledger**, with any transactions rolled up, by agreeing on a set of ledger updates to be applied to a previous version of the net state that was agreed on. An exception process is triggered whenever any of the transactions proposed by the submitting firm are questioned by the tax office
- The ledger follows a **trust some** model, where only the submitting firm and tax office can collectively finalise and approve the ledger. Though the auditor might be also required to attest to the state of the ledger when consensus is reached.

This approach has the benefits that:

- The ledger can be based on a standard, industry based, reporting chart of accounts, creating a middle ground between the single chart of accounts require to enable direct integration, and the individual chart of accounts desired by firms
- Managing exceptions remains an integral part of the reporting process enabling the smooth integration of machine and even human interpretation of the exceptions
- The need to periodically reach consensus means regular baselines are established.

6. Conclusions

Bitcoin and blockchain are limited, niche, solutions, but we see an important role for distributed ledgers.



Search for the killer app

This report has taken a pragmatic approach to defining *blockchain.* Bitcoin begat blockchain – with the unique feature of bitcoin being the idea of using 'proof-of-work' with a currency to incentivise miners[36] – as such we see *blockchain* to be any distributed ledger that uses 'proof-of-work' in tandem with a currency. When the currency and 'proof-of-work' are removed *blockchain* starts to lose meaning and merges with a much more general set of ideas, that solve a set of similar but slightly different problems. Expanding the definition of blockchain to include all of these earlier technologies is a valuable marketing tool, which is probably why *blockchain* is rapidly becoming the new *cloud*: a word whose meaning is nebulous and unspecific but must be important as everyone is using it.

While blockchain is an interesting development, it also inherently a niche solution suitable only for creating an open, trust no-one ledger. The technology is slow, its capacity a handful rather than tens of thousands of transactions per second,[37] and it takes over 10 minutes for a transaction to appear on the ledger. It's expensive to run, with the current mining community consuming US$1.5 million in value a day, placing the average cost per transaction around US$8.25 at current volumes or, if you prefer an environmental measure, roughly 157% a US households daily electricity consumption required per transaction. Blockchain's ability to store data is limited to 80 bytes per transaction. It has also reached its current performance limits at fairly modest transaction volumes, around 1/10,000th of VISA's, which doesn't bode well for a future of incremental refinement. Finally, we should note the nature of blockchain's proof-of-work approach means we can never be sure a transaction we've submitted to the blockchain, but which we haven't yet seen in the ledger, will ever be accepted.

Incremental refinement of the technology will broaden its applicability but only incrementally. The reliance on an on-ledger currency will be a barrier to adoption and it's likely the search for a killer app – the solution that will bring blockchain into the mainstream – will be fruitless.

No new math

Blockchain might be a limited technology, but it might also be a portent of bigger things to come. This is likely the reason why many 'blockchain' advocates may want to distance themselves from a definition tied to proof-of-work and currency.

The novel features in blockchain do not involve any new maths, they are not the result of the incremental accretion of knowledge due to experiment and discovery, something that takes time and which would imply blockchain could only happen when it did. This means there must have been an environmental change, a change in the economics that shifted the idea from impractical to practical. This implies many other existing approaches to distributed consensus have also shifted from impractical to practical. We suspect sometime around 2008 the availability, capacity and cost of digital networks crossed a point where a distributed ledger became more efficient and effective than many of the current batch-based settlement processes built around central ledgers we currently use.

While Bitcoin might be a niche solution it is also a great demonstration of what is possible. The market is responding and a wealth of new distributed ledger platforms and frameworks that don't use proof-of-work with a currency and for marketing reasons might call themselves 'blockchains', but allow more flexible trust models and consensus processes to provide higher performance.

Does this mean blockchain will be yet-another failed technology, Betamax to the VHS of other distributed ledgers? Amusingly the videotape analogy holds, but we shouldn't consider blockchain a dead-end technology, nor should we consider Bitcoin a failed currency. VHS didn't kill the technically superior Betamax, it just took away the consumer market where VHS's playing length was more important than Betamax's picture quality, leaving Betamax the professional video production market where picture quality was more important. Similarly, blockchain and Bitcoin appear to be finding a role for themselves in the international remittance market, though only time will tell.

Opportunities

There are a number of scenarios where a distributed ledger appears to be superior to a central ledger. What is not clear is which of these scenarios will be economically viable. As with all technology adoption, there is a cost-benefit trade-off to be made, and in each case it's not enough for the distributed ledger to be cheaper to build and operate than the existing central ledger, it must be cheaper than the incremental cost of improving the existing ledger. A number of these scenarios will also necessarily require multiple stakeholders to agree on the change, something that might be too challenging politically in some instances.

There's clearly a huge number of potential applications for the technology, but unfortunately we don't have space in this report to do more than touch on a few, though we do intend to pursue this line of inquiry in subsequent reports that focus on applying the technology to individual use cases or sectors.

What is clear is that we're moving to an environment where our old centralised solutions are gradually being replaced by decentralised or distributed solutions. This trend is visible from decentralised power and utilities, through the maker movement and decentralised production and manufacturing, to distributed ledgers and the possibility of distributed finance. Bitcoin and blockchain appear to be the canaries in the coal mine showing us we're at the start of a new era.

Glossary

Agreement Ledger. A distributed ledger used by two or more parties to negotiate and reach agreement.

Attestation register. A distributed ledger providing a durable record of agreements, commitments or statements, providing evidence (attestation) that these agreements, commitments or statements were made.

Bitcoin (uppercase) The well known cryptocurrency.

bitcoin (lowercase). The specific collection of technologies used by Bitcoin's ledger, a particular solution. We should note the currency is itself one of these technologies, as it provides the miners with the incentive to mine.

a blockchain (the indefinite article). A ledger based on blockchain technology, though not necessarily the one used by Bitcoin. This might be as simple as using the same open source code as bitcoin to create a new ledger, through to swapping in alternative implementations or algorithms.

Blockchain (or blockchain technology). The generic name for the family of technologies that provide the same functionality as bitcoin, but which use different approaches to realising the functionality, via alternate algorithms for example, a family of solutions.

the blockchain (the definite article) The particular ledger that underpins Bitcoin: the blockchain created by Satoshi Nakamoto.

Blockchain Technology. See blockchain.

Central ledger. A ledger maintained by a central agency.

Community. The community of actors participating in the ledger. Note actors in the community do not automatically become peers.

Consensus Process. The process a group of peers responsible for maintaining a distributed ledger use to reach consensus on the ledger's contents.

Consensus Point. A point – either in time, or defined in terms of a set number or volume of records to be added to the ledger – where peers meet to agree the state of the ledger.

Distributed ledger. A ledger where responsibility for managing it is distributed.

Entitlement Register. A distributed ledger providing a durable record of entitlements granted to individuals and organisations.

Ledger. An append-only record store, where records are immutable and may hold more general information than financial records.

Off-ledger currency. A currency minted off-ledger and used on-ledger.

On-ledger currency. A currency minted on-ledger and used on-ledger. Bitcoin, for example.

Ownership Register. A distributed ledger providing a durable record of the ownership of physical or virtual assets.

Participant. An actor who can access the ledger: read records or add records to.

Peer. An actor that (shares) responsibility for maintaining the identity and integrity of the ledger.

Permissioned Ledger. A permissioned ledger is a ledger were actors must have permission to access the ledger.

Private currency. A currency issued by a private individual or firm, typically secured against uninsured assets.

Replicated ledger. A ledger with one master (authoritative) copy of the data, and many slave (non-authoritative) copies.

Shared Ledger. An alternative generic name for the family of problems bitcoin and blockchain are one possible solution to. See also Distributed Ledger.

Synchronisation Ledger. A distributed ledger where the consensus process is used by two or more actors to reconcile and align their formal records.

Tokenless Ledger. A distributed ledger that doesn't require a native currency to operate.

Endnotes

1. Nakamoto, S. October 2008, Bitcoin: A Peer-to-Peer Electronic Cash System, bitcoin.org. Available from <https://bitcoin.org/bitcoin.pdf>. [11 March 2016]
2. Bitcoin Block #0, 1 January 2009. Available from <blockchain.info/block-index/14849/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>. [11 March 2016]
3. Bitcoin Block #170, 12 January 2009. Available from <blockchain.info/block/00000000d1145790a8694403d4063f323d499e655c83426834d4ce2f8dd4a2ee>. [11 March 2016]
4. Bitcoin v0.1 released - P2P e-cash, 13 January 2009. Available from <sourceforge.net/p/bitcoin/news/2009/01/bitcoin-v01-released---p2p-e-cash/> [11 March 2016]
5. Frank, A. 16 February 2016, In the Future, Ownerless Companies Will Live on the Blockchain, SingularityHUB. Available from <singularityhub.com/2016/02/16/how-ownerless-firms-will-soon-live-on-the-blockchain/>. [11 March 2016]
6. The Bitcoin block reward, as it is called, is periodically halved, based on a scheduled laid down when the currency was created. This limits the total supply of Bitcoins as the currency is not infinitely divisible. The next such halving is due late in 2016, while the total supply of Bitcoins is expected to run out in 2024, at which point the block reward will drop to zero.
7. The term shared ledger was coined by Richard Brown, formerly of IBM and now Chief Technology Officer of the Distributed Ledger Group. We consider the two equivalent but prefer distributed ledger.
8. Evans-Greenwood, P.; Harper, I.; Hillard, R.; & Williams, P. January 2016, The Future of Exchanging Value: Cryptocurrencies and the Trust Economy, Deloitte Australia.
9. This implies a collapse of Bitcoin, or any other digital currency for that matter, might poison the market for all digital currencies as the collapse could destroy our trust in anonymous networks as a foundation for exchanging value. We can distinguish between governments as they have identity, but all anonymous networks are simply 'anonymous networks'.
10. Some pundits are using shared ledger rather than distributed ledger. We consider the two terms equivalent and prefer the use of distributed ledger.
11. We use 'the blockchain' to refer to the distributed ledger that underpins Bitcoin, and 'a blockchain' to refer to the family of similar solutions, which the Blockchain is a member of.
12. Lamppost L.; Shostak, R. & Pease, M. July 1982, The Byzantine Generals' Problem, ACM Transactions on Programming Languages and Systems,Vol.4, No. 3, pages 382-401.
13. Bitcoin Stack Exchange, What is the longest blockchain fork that has been orphaned to date?, Available from <bitcoin.stackexchange.com/questions/3343/what-is-the-longest-blockchain-fork-that-has-been-orphaned-to-date>. [11 March 2016]
14. PeerCoin is a peer-to-peer cryptocurrency inspired by Bitcoin and which uses much of the same sources code. It can be found at <peercoin.net>. [11 March 2016]
15. Ripple is a real-time gross settlement system, currency exchange and remittance network. It can be found at <ripple.com>.
16. Brunner, G. 13 May 2013, The Bitcoin network outperforms the top 500 supercomputers combined, ExtremeTech. Available at <www.extremetech.com/extreme/155636-the-bitcoin-network-outperforms-the-top-500-supercomputers-combined> [11 March 2016]
17. Quora, By saying, 'The blockchain is controlled by Chinese miners...'? (Mike Hearn 2016) Is that to say that there are insufficient miners outside of China?, Available from <www.quora.com/By-saying-The-blockchain-is-controlled-by-Chinese-miners-Mike-Hearn-2016-Is-that-to-say-that-there-are-insufficient-miners-outside-of-China> [11 March 2016]
18. A private currency is a currency issued by a private organisation.

19. Free banking refers to an arrangement where banks are free to issue their own paper money, and are not subject to any special regulations beyond those applicable to most enterprises.
20. The Bitcoin Volatility Index. Available at <btcvol.info>. [11 March 2016]
21. Foreign Exchange Rates for Feb 29, 2016, Australia spot exchange rate US$/AU$ & Euro area spot exchange rate. Available at <www.federalreserve.gov>. [11 March 2016]
22. Crypto-Currency Market Capitalizations. Available at <https://coinmarketcap.com>. [11 March 2016]
23. Evans-Greenwood, P.; Harper, I.; Hillard, R.; & Williams, P. January 2016, The Future of Exchanging Value: Cryptocurrencies and the Trust Economy, Deloitte Australia.
24. ZeroCoin <zerocoin.org> is an extension to Bitcoin that would add true cryptographic anonymity to transactions. [11 March 2016]
25. AUSTRAC 2012, AUSTRAC typologies and case studies report. Available at <www.austrac.gov.au/files/typ_rprt12_full.pdf> [11 March 2016]
26. Middleton, P; Maya Chilaeva, M.; Metuku, A.; Lam, H. & Quiet, S. February 2016, How Will Blockchain Change European Market Structure?; Bank of America Merrill Lynch.
27. Namecoin <namecoin.org> provides a censorship-resistant top level domain .bit, which is functionally similar to .com or .net domains but is independent of ICANN, the main governing body for domain names. Namecoin was the first alternative cryptocurrency to be spun out of Bitcoin.
28. EverLedger <www.everledger.io> is a distributed asset ledger that records diamond certifications and transaction histories. [11 March 2016]
29. The Economist 31 October 2015, *The great chain of being sure about things*. Available at <www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable> [11 March 2016]
30. Parker, L. 8 July 2015, Everledger Uses the Blockchain, Tackling Conflict Diamonds and Insurance Fraud, BraveNewCoin. Available at <bravenewcoin.com/news/everledger-uses-the-blockchain-tackling-conflict-diamonds-and-insurance-fraud/>. [11 March 2016]
31. Prem, S., 5 February 2016, Beni Rogers and Imogen Heap: Building the Music Blockchain, Musically. Available at <musically.com/2016/02/02/benji-rogers-and-imogen-heap-talk-building-the-music-blockchain/>. [11 March 2016]
32. Howard, G., 17 July 2015, Imogen Heap's Mycelia: An Artists' Approach for a Fair Trade Music Business, Inspired by Blockchain, Forbes. Available at <www.forbes.com/sites/georgehoward/2015/07/17/imogen-heaps-mycelia-an-artists-approach-for-a-fair-trade-music-business-inspired-by-blockchain/ - 476281c35912>. [11 March 2016]
33. Witt, J., 2 October 2015, Live stream: Imogen Heap releases Tiny Human using blockchain technology, The Guardian. Available at <www.theguardian.com/membership/2015/oct/02/live-stream-imogen-heap-releases-tiny-human-using-blockchain-technology>. [11 March 2016]
34. Uno Music <ujomusic.com> is a prototype rights management and digital distributed platform built on the Ethereum ledger. [11 March 2016]
35. Gluu [GluuFederation] 4 March 2016, *Yet to see a use case for blockchain that can't be solved with an existing simpler technology* Adi Shamir #RSAC, Twitter post. Available from <twitter.com/GluuFederation/status/705125001880403968>.
36. We note Bitcoin's seminal paper, Bitcoin: A Peer-To-Peer Electronic Cash System, contains multiple references to a 'proof-of-work chain', and one reference to a 'chain of blocks', but other than that neither 'blockchain' nor 'block chain' ever make an appearance.
37. Blockchain currently supports 3-7 transactions per second across a global network with millions of CPUs and purpose-built ASICs.

About the authors

Peter Evans-Greenwood

Peter has spent his entire career working at the intersection between business and technology. During his career he has worked in Asia, Australia, Europe and the US, lived in Silicon Valley through boom and bust, and held leadership roles in global organisations as well as start-ups and research and development labs. These days he works as a consultant and advisor on the business and technology sides of the fence.

Robert Hillard

As the Managing Partner of Deloitte Consulting, Robert helps clients respond to change (technological, economic and social) through a team of more than 1,500 management consultants. Based on his more than 25 years' experience, Robert believes organisations can only achieve lasting results with a combination of transformation skills and supporting technology. Robert is the author of Information-Driven Business (Wiley 2010) and sits on the national board of the Australian Information Industry Association.

Ian Harper

Ian Harper is one of Australia's best known economists. He chaired the Federal Government's Competition Policy Review, served as inaugural Chairman of the Australian Fair Pay Commission, and was one of three panellists chosen to review Victoria's state finances. In March 2011, Ian joined Deloitte Access Economics as a Partner, following a 25-year academic career that included 16 years at the Melbourne Business School and was elected Emeritus Professor of the University of Melbourne on his departure. Ian is currently a member of the Australian Advisory Board of Bank of America Merrill Lynch.

Peter Williams

Peter Williams is an innovator and thought leader in the digital world.

Peter founded the eBusiness Consulting group in Deloitte in 1996 and was CEO of The Eclipse Group, one of Australia's largest web development companies, from 2003 to 2008. He was also the founder of Deloitte Digital, a business pioneering the delivery of professional services online.

Peter is a sought-after speaker and media commentator both locally and internationally and has worked with boards and senior executives of many companies helping them understand and adapt to the rapidly changing digital environment.

Contacts

Peter Williams
Chief Edge Officer, Centre for the Edge
+61 3 9671 7629
pewilliams@deloitte.com.au

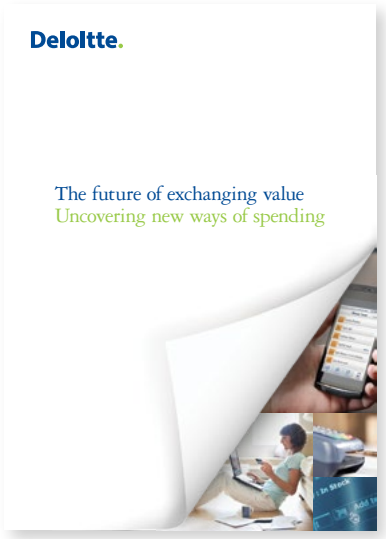
Ian Harper
Partner, Deloitte Access Economics
+61 3 9671 7536
iaharper@deloitte.com.au

Robert Hillard
Managing Partner, Consulting
+61 3 9671 7971
rhillard@deloitte.com.au

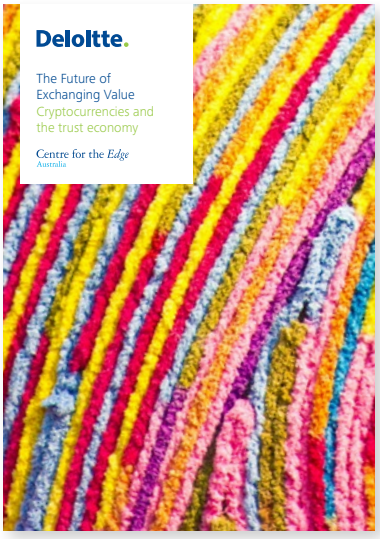
Richard Miller
Director, Payments Advisory
+61 3 9671 7903
rimiller@deloitte.com.au

Jonathan Persinson
Partner, Assurance & Advisory
Banking & Payments
+61 2 9322 3705
jonperkinson@deloitte.com.au

Further reading



The Future of Exchanging Value
Uncovering New Ways of Spending



The Future of Exchanging Value
Cryptocurrencies and the Trust Economy

Deloitte.

Centre for the Edge, Deloitte
550 Bourke Street
Melbourne
Victoria 3000