

BLOCKCHAIN AND SHARED LEDGERS

THE NEW AGE OF THE CONSORTIUM

9 NOVEMBER 2016

INTRODUCTION

Shared ledger technologies promise to create a new age of the consortium. There is significant potential to reduce transaction and record-keeping costs, streamline business operations and enable new business models by using shared ledger technologies.

However, early investigations and attempts at adapting the public blockchain to these types of commercial relationships have identified a number of limitations. In particular, the transparent, decentralised model of public blockchain significantly compromises the commercial confidentiality required.

Commercial consortia are better suited to modified or reconstructed versions of blockchain technology – which we refer to in this paper as “private shared ledgers”. These allow consortia to capture the advantages of shared ledgers without the complexity or distributed transparency of public blockchain. A number of private shared ledger platforms are emerging, many of which are providing open source software to enable further development around niche requirements.

Developing a successful business consortium is more than simply selecting the right technology platform. It requires a careful design of the consortium’s governance framework and operational rules, some of which can be embedded in the technology and others must be dealt with in ‘real world’ agreements. The consortium participants must also carefully address the regulatory requirements, in particular those relating to competition law.

This paper discusses the differences between private shared ledgers and public blockchain to support commercial consortia. It then identifies the critical choices to be taken in forming a consortium, including the necessary components of a governance and operational framework.

CONTENTS

PART A – THE OPPORTUNITY

1	THE CONSORTIUM PROMISE	4
2	THE SHARED LEDGER POTENTIAL	6

PART B – THE NEED FOR PRIVATE SHARED LEDGERS

3	LIMITATIONS OF PUBLIC BLOCKCHAIN	10
4	HOW DO PRIVATE SHARED LEDGERS WORK?	14
5	WHERE ARE THE NEW CONSORTIA EMERGING?	22

PART C – LIFTING THE COVERS ON THE SHARED LEDGER CONSORTIUM

6	CRITICAL CHOICES FOR BUSINESS CONSORTIA ON PRIVATE SHARED LEDGERS	27
---	---	----

	CONCLUSION	42
--	------------	----

PART A THE OPPORTUNITY

1 THE CONSORTIUM PROMISE

The industry participant-led consortium is back. Powered by blockchain and shared ledger technologies, these new consortia can revolutionise the way that companies transact with each other.

Blockchain and shared ledger technologies provide opportunities for collaboration across multiple organisations and across broad industry groups. They create a new kind of trust, enabling organisations to deal with each other directly – peer-to-peer – without intermediaries.

- + This is redefining the relationships between consortium members – enabling them to go back to the more traditional style of consortium-based market participation, but within today's digital environment.
- + Consortium members can collaborate and share information in ways that have not previously been viable – sharing information with each other (and with regulators) where appropriate, while at the same time restricting the permissions for access to confidential information. This is enabling new approaches to corporate innovation – providing a platform for corporations to work together and innovate in a collaborative and agile way, driven by the goal of disrupting before they are disrupted.

All of this has the potential to create more efficient markets and reduce transaction, processing and reporting costs.

- + Industry consortia have been the key to establishing efficiency gains in markets and transactions throughout history. Consider the emergence of stock exchanges in the 19th century, the Visa and MasterCard payment platforms in the 1960s, and the procurement consortia in the early days of the internet.
- + In more recent times we have seen these consortia evolve into independent entities that need to be trusted, and paid a fee for that role, eg: stock exchanges themselves becoming substantial listed companies; and Visa and MasterCard demutualising from their member banks into independent, global companies. This has meant that the participants have to trust “someone else”, ie: a third party intermediary.

IN THE NEW AGE OF THE CONSORTIUM,
SHARED LEDGER TECHNOLOGIES PROVIDE
A NEW MEANS OF ESTABLISHING THE SOURCE
OF TRUTH – STEEPED IN THE TECHNOLOGIES
OF THE 21ST CENTURY.

Blockchain and shared ledgers herald the promise of a new age of the consortium. They are creating a new type of trust in commercial transactions that is distributed, and does not rely on the institutional trust of intermediaries (see Figure 1). This will enable corporations to transact directly with each other in ways that are far more efficient and reliable than under current practices.

Today, shared ledger technologies create the potential for new consortia to emerge and thrive for specific niche business purposes – including consortia that would have been unworkable or cost prohibitive in the “clunky” world of legacy systems and shared services.

However, the technology can’t do it all. The fundamentals still apply. Participants in a consortium need to have a strategy and a framework for managing their dealings with each other and daily decision-making – even though some of that decision-making may subsequently be converted into code. This requires the participants to construct a framework of business processes, operating rules, governance, smart contracts and contractual agreements

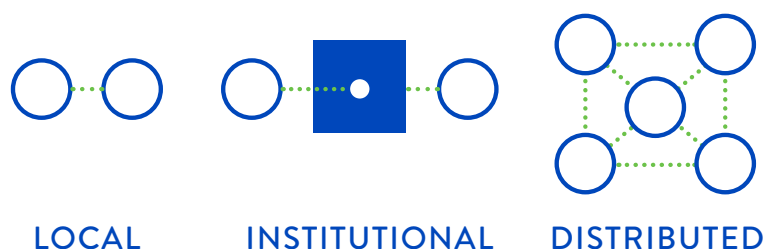
that are fit for purpose and work together consistently in the shared ledger environment – and also ensure compliance with regulatory requirements and competition laws.

This new framework will be a critical success factor for these new consortia, just as the early consortia needed to set out the rules many years ago.

While the efficiencies and other benefits that will flow from the consortium arrangements may be obvious, the extent to which they can be taken into account under current competition laws is limited. Unless or until the laws are updated to allow for these benefits to be considered, consortium members will need to understand when collaboration and information sharing may give rise to competition risks. Appropriate safeguards can strike the right balance by addressing the competition risks, but not at the expense of the efficiencies and other benefits that the consortium will bring.

Many corporates are exploring opportunities for shared ledger technologies – including for transactions processing and settlement, record-keeping and reporting, and supply chains. This paper explores some of the important choices to be made in the new era of the consortium – including those critical technology, governance and operational choices to be made in the early stages of establishment.

FIGURE 1 - EVOLUTION OF TRUST



“Blockchain” has become the catch-all term to describe a wide range of innovations around blockchain and shared ledgers – including the hybrid models for private shared ledgers.

2 THE SHARED LEDGER POTENTIAL

Shared ledger innovations provide real opportunities for corporates to simplify and improve the complex and messy world of information technology and traditional clearing house models where:

- + details about transactions and assets are recorded across multiple databases, spread across multiple institutions (each of which maintains its own records in its own unique format) – often with a lack of consistency and confidence about the true position;
- + enormous resources are deployed to reconcile data and records and ascertain the true position (time, money, technology and people – including regulatory resources), while the risks of errors and inconsistencies still remain; and
- + manual reconciliation processes and fact checking are costly, timely and subject to many errors between the corporations, counterparties or departments involved in them.

This is the 21st century's “paperwork crisis”:¹

“... the tens of billions of dollars spent annually maintaining and managing the duplicated records that each firm maintain about the same deals. The same information about a deal is recorded multiple times across these parties and in situations where a centralised solution can't be deployed, which is in lots of places, small armies are required to ensure that these disparate records agree with each other, get updated correctly and in synchrony – and deal with the issues when they don't.”

Richard Gendal Brown, Chief Technology Officer, R3

WHY NOW?

There are obvious imperatives for seizing the moment and leveraging the innovation opportunities of shared ledgers:

- + Many organisations are facing looming deadlines for system upgrades as their on-premises legacy systems and licensing arrangements reach end of life. In some organisations, this will be their first major systems upgrade since Y2K, and the costs of change are very high.
- + Blockchain and distributed ledger technologies provide real opportunities for industries like financial services, which are suffering from a host of challenges.
 - The global financial crisis led to the introduction of new regulation: imposing increased capital, liquidity and funding requirements on financial institutions. Those regulations have not been implemented consistently on a global basis, and the resultant volume of regulation creates a significant burden – leading to increases in compliance and operational costs.
 - At the same time, banks are operating in a low growth environment with low interest rates. They are facing potential disruption from fintech operators, with the emergence of new business models that are challenging traditional banking models.

In this challenging environment, it makes sense to do away with manual processes and manual reconciliation exercises forever – and to seize the innovation opportunities of private shared ledgers (see Box 1).

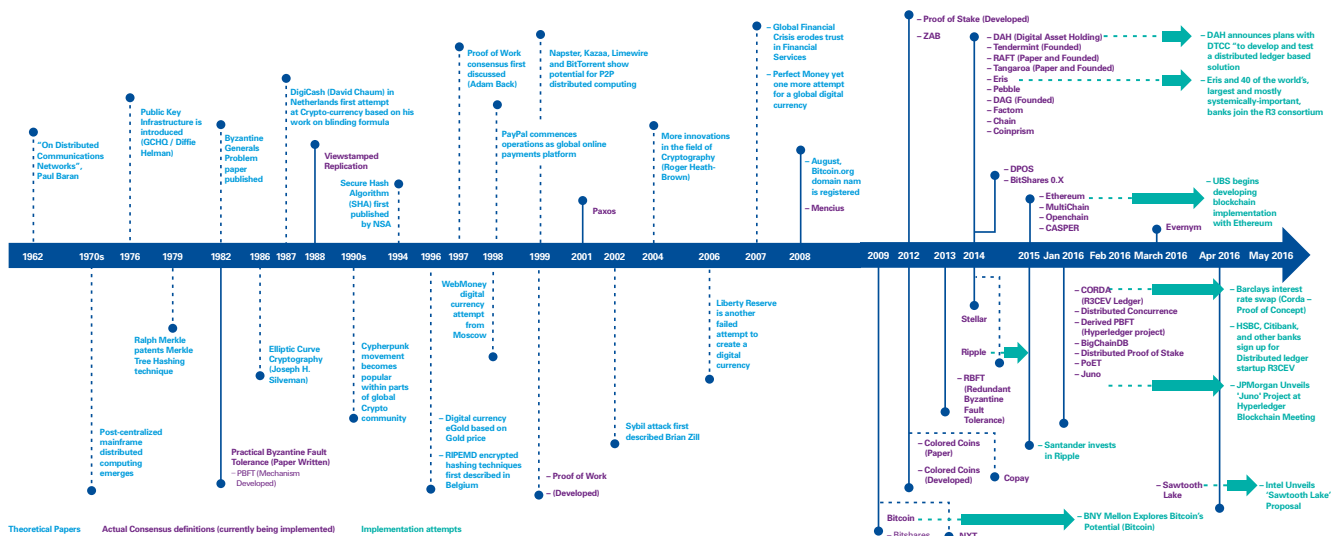
¹ Richard Gendal Brown, ‘R3 Corda: What makes it different’ on Richard Gendal Brown, *Thoughts on the future of finance* (25 October 2016) <<https://gendal.me/2016/10/25/r3-corda-what-makes-it-different/>>.

WHAT TOOK US SO LONG?

The components of shared ledgers have been around for many years (see Figure 2):

1. **Decentralisation:** byzantine fault tolerance has been around since the 1980s (as introduced by Leslie Lamport), with the first practical algorithms emerging around 1999;²
2. **Immutability:** has been around for decades, with ReThinkDB using this feature commercially for a number of years;³ and
3. **Asset transfers:** the concept of assets on a blockchain can be traced back to the transactional databases (which have been used for decades) – while the storing of assets on a database (as part of double entry accounting) has been used by financial institutions for a number of years.⁴

FIGURE 2 - CONSENSUS TIMELINE⁵



2 Leslie Lamport, Robert Shostak and Marshall Pease, 'The Byzantine Generals Problem' (1982) 4(3), ACM Transactions on Programming Languages and Systems 382 <<http://dl.acm.org/citation.cfm?doid=357172.357176>>; Miguel Castro and Barbara Liskov, 'Practical byzantine fault tolerance' (1999) OSDI '99 Proceedings of the Third Symposium on Operating Systems Design and Implementation <<http://dl.acm.org/citation.cfm?doid=296806.296824>>.

3 RethinkDB, The open source database for the realtime web <<https://www.rethinkdb.com/>>.

4 Ibid.

5 Sigrid Seibold and George Samman, 'Consensus: Immutable Agreement for the Internet of Value' (KPMG, 20 June 2016) <<https://home.kpmg.com/us/en/home/insights/2016/06/consensus-opportunities-blockchain-and-beyond.html>>.

BOX 1

WHAT IS THE INNOVATION BEHIND BLOCKCHAIN?

The key innovation driving the original public blockchain model is the combination of cryptographic signatures with a distributed byzantine fault-tolerant database so as to create open, permissionless systems on a shared ledger where:

- + all nodes on a blockchain platform can read and append information to that shared ledger;
- + each of the nodes (acting individually and autonomously) validates new information via the cryptographic processes before that information is added to the ledger;
- + validation by all miners on the blockchain platform leads to “consensus” (using “proof of work” processes or other hash algorithms), following which:
 - all copies of the information to the shared ledger are automatically reconciled – so that the same data is stored locally in every node (replication), and each node maintains an identical copy of the shared ledger; and
 - the information then takes on unique status as a “source of truth”:
 - the updated record is allocated a hashing algorithm, ie: a unique number generated from a string of text and a key; and
 - the data itself is stored by the local node.

Because everyone always has the same information, they can rely on that shared ledger as the single source of truth:

- + the records on the shared ledger are tamper-proof – they cannot be “undone” or “reversed” (except through updates using the same validation / consensus process); and
 - + there is no need to go back and check everyone's records against one another, or to reconcile multiple databases.
-



PART B

THE NEED FOR PRIVATE SHARED LEDGERS

3 LIMITATIONS OF PUBLIC BLOCKCHAIN

Early developments in public blockchain involved a leap of faith – moving away from traditional centralised systems with a trusted intermediary to a **fully decentralised** public blockchain model (see Box 2).

These initiatives were centred around building new applications and commercial operations on public blockchain.

The original blockchain – bitcoin – was designed for a cryptocurrency. The design choices lead to the creation of a transparency machine – utilising an open shared ledger and validated by broad consensus. This enabled people who did not know or trust each other to exchange cryptocurrency in relative confidence, without the need for any other type of relationship – whether participation rules or contractual framework.

However, while the original blockchain model worked for that use case, it was not designed for others. Since financial services began exploring the opportunities of blockchain in 2014, corporates have recognised that there are weaknesses in the original public blockchain model that make it problematic for many commercial transactions.

For example:

- + Public blockchain is highly distributed and highly transparent. While it offers pseudonymity, it does not guarantee anonymity or confidentiality.

- + In theory, anyone can be a validator and anyone can write to or read from the blockchain. While clients and validators can be anonymous, all of the data gets stored locally on every node (replication). This makes all transaction data public, for example:
 - Even if pseudonymous addresses are used, it is still possible to find out whose addresses they are through various techniques.
 - Even if the identities of the parties are masked, it is still possible to see and derive commercially sensitive information, such as the volume of transactions passing between particular nodes.

There are many challenges around creating a totally confidential environment on a public blockchain platform. Complex work-arounds are required to achieve scalability and confidentiality. In many cases, confidentiality can only be achieved by allowing transactions to happen “off-chain” (via “state channels” or “side chains”) – so that only the final state is recorded on the blockchain.⁶ These challenges have led to some complex new cryptographic solutions such as:

- + Confidential Transactions⁷
- + Mumblewimble⁸
- + Zero Knowledge Proofs, in particular zk-SNARKS, including Zerocash, Zcash and Baby ZoE⁹
- + Hawk¹⁰

6 Jeff Coleman, ‘State Channels’ on *Jeff Coleman Blog* (6 November 2015) <<http://www.jeffcoleman.ca/state-channels/>>; Vitalik Buterin, ‘Privacy on the Blockchain’ on *Ethereum Blog* (15 January 2016) <<https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/>>; Vitalik Buterin, ‘Ethereum: Platform Review. Opportunities and Challenges for Private and Consortium Blockchains’ (R3CEV, 1 June 2016) <<https://www.scribd.com/doc/314477721/Ethereum-Platform-Review-Opportunities-and-Challenges-for-Private-and-Consortium-Blockchains>>; High Speed Asset Transfer for Ethereum, Raiden Network <<http://raiden.network/>>.

7 Adam Back, ‘Bitcoins with Homomorphic Value (Validatable but Encrypted)’, Simple Machines Forum, Bitcoin Forum (1 October 2013) <<https://bitcointalk.org/index.php?topic=305791.0>>; Gregory Maxwell, ‘Confidential Transactions’, The Elements Project <<https://www.elementproject.org/elements/confidential-transactions/>>.

8 Tom Elvis Jedusor, ‘Mumblewimble’ (19 July 2016) <<https://download.wpsoftware.net/bitcoin/wizardry/mumblewimble.txt>>

9 Eli Ben-Sasson et al, ‘SNARKS for C: Verifying Program Executions Succinctly and in Zero Knowledge’ (2013) <<https://eprint.iacr.org/2013/507.pdf>>; George Danezis et al, ‘Pinocchio Coin: building Zerocoin from a succinct pairing-based proof system’ (2013) In Proceedings of the 2013 Workshop on Language Support for Privacy Enhancing Technologies <<http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/DanezisFournetKohlweissParno13.pdf>>; Eli Ben-Sasson et al, ‘Zerocash: Decentralized Anonymous Payments from Bitcoin’ (18 May 2014) <<http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf>>; Daira Hopwood et al, ‘Zcash Protocol Specification’ (4 October 2016) <<https://github.com/zcash/zips/blob/master/protocol/protocol.pdf>>; Sean Bowe, ‘zkSNARKS in Ethereum’ *Zcash* (28 July 2016) <<https://z.cash/blog/zksnarks-in-ethereum.html>>.

10 Ahmed Kosba et al, ‘Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts’ (2015) <<https://eprint.iacr.org/2015/675.pdf>>.

BOX 2

WHAT DOES IT MEAN IN PRACTICE TO BE FULLY DECENTRALISED?

The original public blockchain opened up new possibilities: creating a single record that is a “source of truth”, reconciled in near real time and accessible by multiple participants and institutions on a transparent basis.

The computers are distributed and no single entity controls the network – control is entirely decentralised (amongst all the nodes/participants in the network).

This decentralisation can be viewed as part of a spectrum from fully centralised control of a network through to fully decentralised control.

	Fully Centralised	Server Based Decentralised	Server Free Fully Decentralised
Control of Network	Single Entity	No Single Entity	No Single Entity
Distributed	Computing power can be distributed; but a single entity still controls the network	Yes	Yes
Consensus Algorithm	Need only handle crash faults, because nodes are altruistic	Crash and Byzantine Faults	Crash and Byzantine Faults plus Sybil Attacks
Anonymity of Clients	No	Can be	Can be
Anonymity of Validators	No	No	Can be
Read/Write Functions		Anyone	Anyone
Examples	Google, Facebook	Federation Super P2P: Bigchain DB, Multichain etc	Bitcoin, Ethereum, Zcash

For confidential transactions, blockchain is not the right solution: they need to leverage the benefits of blockchain technology to create a reliable record or “source of truth”, but without the transparency.

The principle of a shared “source of truth” **does** work. But sharing that truth too broadly is a problem.

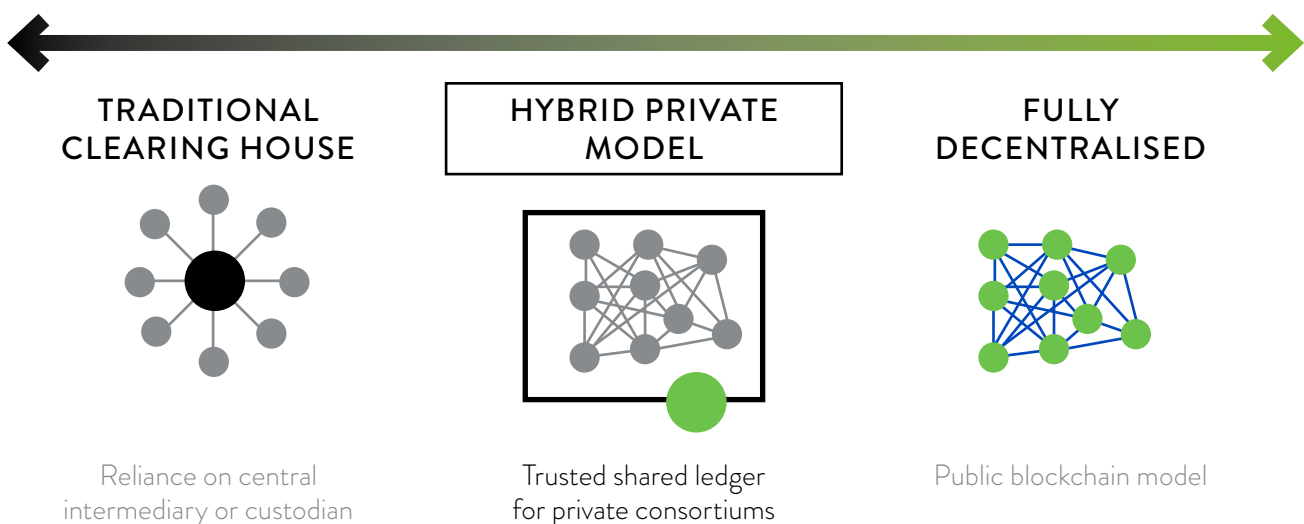
This requires a middle ground hybrid model (see Figure 3)

– sometimes referred to as “**controlled transparency**”¹¹ – where:

- + everyone can maintain their own private records on the shared ledger; and
- + participants can selectively share information on a need-to-know basis, eg: limited to the counterparties to a transaction and the regulator as required.

This hybrid model for private shared ledgers is the key focus of this paper.

FIGURE3 - THE SHIFT TOWARDS A HYBRID PRIVATE MODEL



¹¹ Danny Bradbury, 'Blockchain seeks to squeeze out the lawyers', *E&T Magazine*, 11 October 2016, quoting Tim Swanson, Director of Market Research, r3cev <<https://eandt.theiet.org/content/articles/2016/10/blockchain-seeks-to-squeeze-out-the-lawyers/>>.

```

    mod = modifier_ob.modifiers.new("mirror")
    mirror_object = mirror_ob
    mirror_mod.mirror_object = mirror_ob

    operation == "MIRROR_X":
        mirror_mod.use_x = True
        mirror_mod.use_y = False
        mirror_mod.use_z = False
    operation == "MIRROR_Y":
        mirror_mod.use_x = False
        mirror_mod.use_y = True
        mirror_mod.use_z = False
    operation == "MIRROR_Z":
        mirror_mod.use_x = False
        mirror_mod.use_y = False
        mirror_mod.use_z = True

    #selection at the end -add back the deselected
    mirror_ob.select= 1
    modifier_ob.select=1
    context.scene.objects.active = modifier_ob
    print("selected" + str(modifier_ob)) # modifier
    mirror_ob.select = 0
    one = bpy.context.selected_objects[0]
    one.data.objects[one.name].select = 1

    print("please select exactly two objects,")

```

OPERATOR CLASSES -----

```

    bpy.types.Operator):
    @classmethod
    def mirror_to_the_selected_object(cls, context):
        mirror_x = context.mirror_mirror_x
        mirror_y = context.mirror_mirror_y
        mirror_z = context.mirror_mirror_z

```

```

    context):
    if context.active_object is not None

```


4 HOW DO PRIVATE SHARED LEDGERS WORK?

Private shared ledgers are still distributed ledgers, but they no longer fit the classic blockchain model.

A private shared ledger is still “**distributed**”, in that:

- + each participant still holds a (distributed) node on the blockchain platform; and
- + each participant can have their node located on a server co-located anywhere in the world,

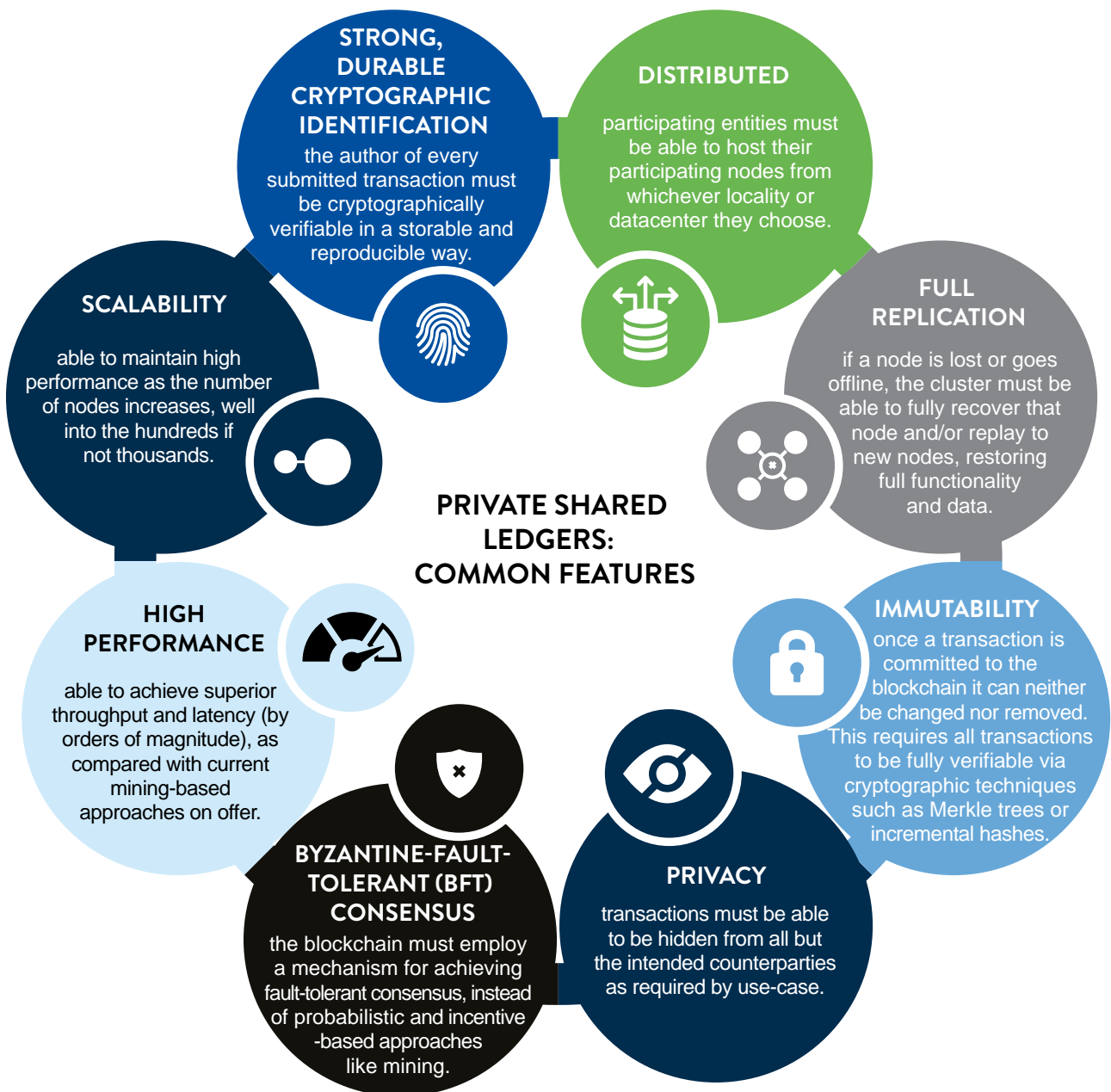
but the shared ledger is not fully decentralised (where anyone can be a validator) and there is no longer full replication of data across **all** nodes. This generally means that full synchronisation is no longer necessary.

Decentralisation of network control (see Box 2) becomes less important on private shared ledger platforms, since all the nodes are operated by known parties. Because the consortium members and consortium operator are known to each other, they are able to satisfy certain regulatory and compliance requirements without relying on complex software protocols that the full blockchain solution offers (even between parties who do not necessarily trust each other). They can instead look to “real world” solutions for legal recourse.

Figure 4 highlights some of the common features of private shared ledger technologies.

This means that the focus can shift to privacy and confidentiality (while still achieving speed, scalability and network stability) – preserving the blockchain features around scalability and consistency, but with some trade-offs in relation to decentralisation.

FIGURE 4 - COMMON FEATURE OF PRIVATE SHARED LEDGERS



PRIVATE SHARED LEDGERS – A SIMPLER APPROACH

Private shared ledgers have been developed with different design choices – modified in various ways to achieve confidentiality and scalability, and to address the specific requirements of particular industry consortia (see Box 3):

- + They enable transparency and privacy to co-exist – so that consortium participants can share information with each other (and with regulators) where it makes sense, while at the same time restricting the “permissions” for access to confidential information.
- + Since they are deployed in a closed system, they require **less** decentralisation – as the participants are a closed group of users who are known to each other and who have accepted the rules of participation or operating rules.
- + Private shared ledgers are changing the way that “permissions” are designed on the shared ledger: who can see, who can write, who reads, who validates – and they are also questioning how consensus is done, and if it is even necessary.

The private shared ledger is still “distributed”, but it is not fully decentralised – some aspects of the operating rules are implemented in a more centralised manner.

You could say that the technology service provider is replacing the traditional third party intermediary on a private shared ledger – in the way that they are maintaining and operating the shared ledger technology systems which, in turn, automate the processing on the private shared ledger.

This is leading to much simpler technology solutions for private shared ledgers – as compared with public blockchain. There is no need to worry about the complexities of mining, and consensus (including “proof of work”) becomes simpler and less important.

The impact of this, however, is that a fundamental change in approach to governance is required.

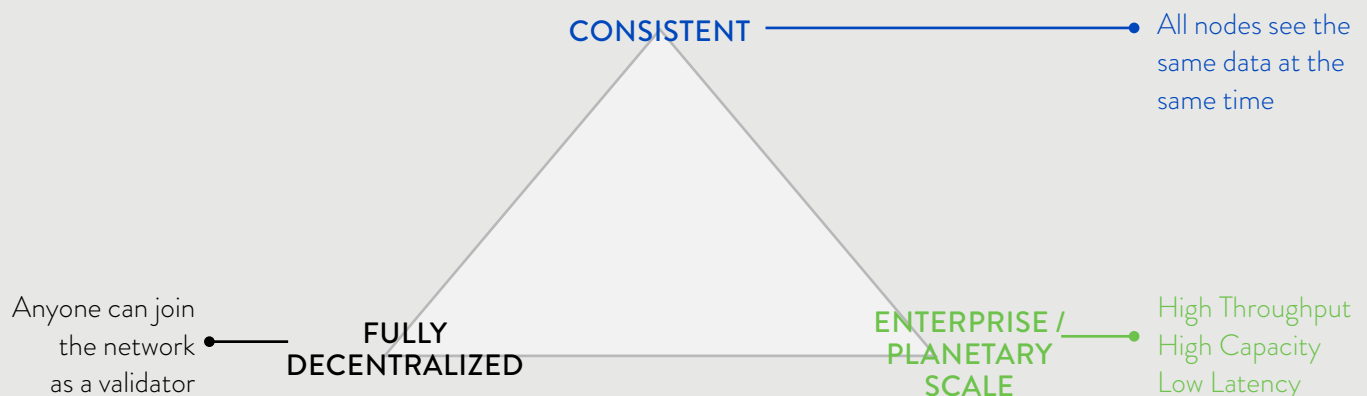
BOX 3

WHAT TRADE-OFFS ARE REQUIRED TO ACHIEVE CONFIDENTIALITY?

You cannot have all of the features of blockchain PLUS confidentiality, it is not (yet) technically feasible. Trade-offs and design decisions are required.

This requires a trade-off exercise in relation to the design of private shared ledgers. The “DCS (**D**ecentralised-**C**onsistent-**S**cale) Triangle”¹² (see Figure 5) illustrates this trade-off exercise, ie: it is only possible to have two out of three sides of the triangle, due to the technological limitations that exist today. Recognising that privacy and confidentiality are business requirements for corporations and start-ups wanting to build “fit for purpose” solutions that can work technologically today, and are consistent and highly scalable, this means that they can give up decentralisation – it is not needed for the use cases that are being explored for private shared ledgers.

FIGURE 5 - THE DCS TRIANGLE



12 Trent McConaghy, 'The DCS Triangle', *Medium*, 10 July 2016 <<https://blog.bigchaindb.com/the-dcs-triangle-5ce0e9e0f1dc#.52d1lmgmj>>.

SHIFTING MINDSETS ON HOW VALIDATION AND CONSENSUS ARE ACHIEVED

With private shared ledgers, there will be varying degrees of “centralised” network control (in terms of processing on the shared ledger) – depending partly on:

- + the design and architecture of the particular platform; and
- + how a consortium chooses to design and implement their particular technology solution and governance arrangements on the private shared ledger.

For example, the design and architecture of the platform will determine the options for how validation and consensus can be performed – and this is one area where shared ledger platforms vary significantly from one to the other.

- + For public blockchain, all updates to the shared ledger are broadcast to all of the nodes, and each node holder validates the update – leading to consensus and updating of the shared ledger in a transparent way.
- + By comparison, that validation process can be performed on private shared ledgers in a multitude of different ways – often involving a more centralised approach (see Figure 6).

The participants on private shared ledgers are effectively “getting out of the way” so that more efficient and confidential processes can be implemented for validation (rather than each of the participants performing the validation role themselves).

BOX 4

NEW APPROACHES TO VALIDATION AND CONSENSUS

Example 1: Delegating validation and consensus to a single node: Consortium participants can delegate the process of validation (via operating rules that are automated and can't be tampered with). This ensures that blockchain/consortium participants have no visibility of details relating to confidential transactions on the shared ledger (except for those transactions which they are a party to):

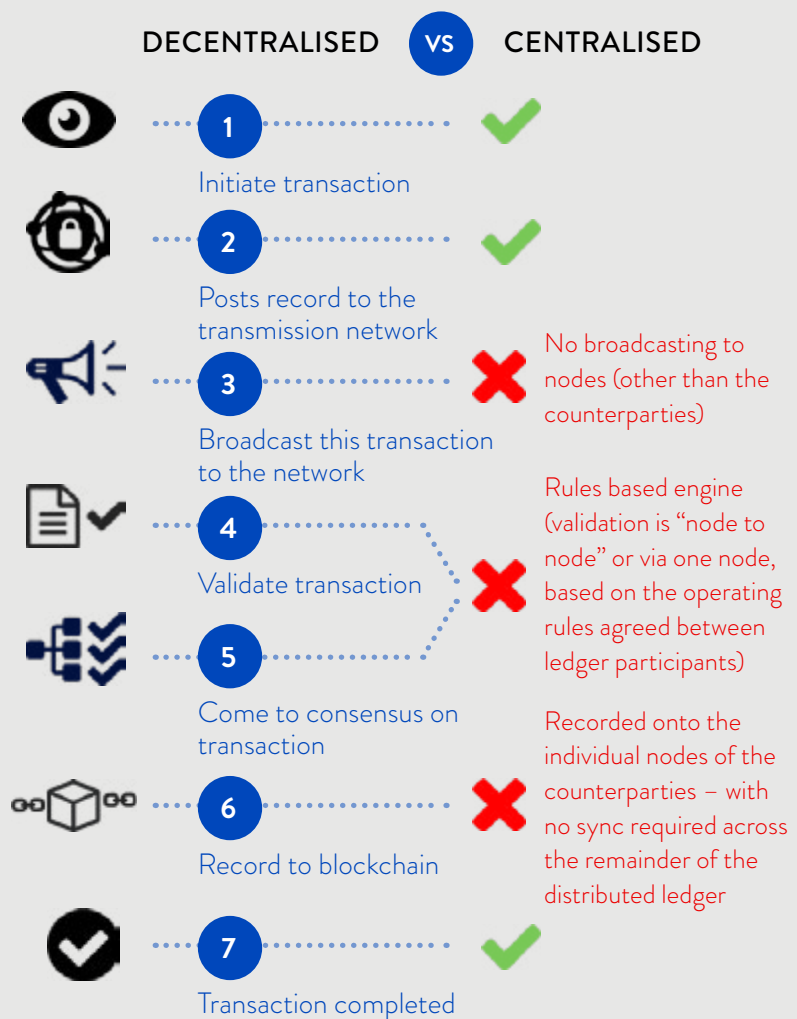
- + the participants still retain control over how validation is done, by agreeing to a set of operating rules up-front which govern how validation will be performed; and
- + this means that the operating rules become critical to the integrity of a private shared ledger platform.

Technically, validation is achieved through the use of a designated block generator to collect and validate proposed transactions, periodically batching them together into a new-block proposal:

- + consensus is provided by a generator that applies rules (validates) agreed to by the nodes (chain cores) to the block and designated block signers; and
- + the participants can still co-locate their nodes (storing their own confidential data) wherever they want (regardless of where the master node or generator node is located).¹³

Example 2: Node to node transactions: An alternative approach is to use encrypted node to node (n2n) transactions, where only the two parties involved in the transaction receive data – with opt-ins for third party nodes (regulators) to be a part of the transaction.¹⁴

FIGURE 6 – PRIVATE SHARED DISTRIBUTED LEDGERS - NEW APPROACHES TO VALIDATION AND CONSENSUS



¹³ See, eg, Chain Protocol Whitepaper, Chain <<https://chain.com/docs/protocol/papers/whitepaper>>.

¹⁴ See, eg, Richard Gendal Brown et al, 'Corda: An Introduction' August 2016 <<http://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57bda319ebbd1acc9c030abd/1472045850269/corda-introductory-whitepaper-final.pdf>>

WHAT ARE WE TRYING TO VALIDATE?

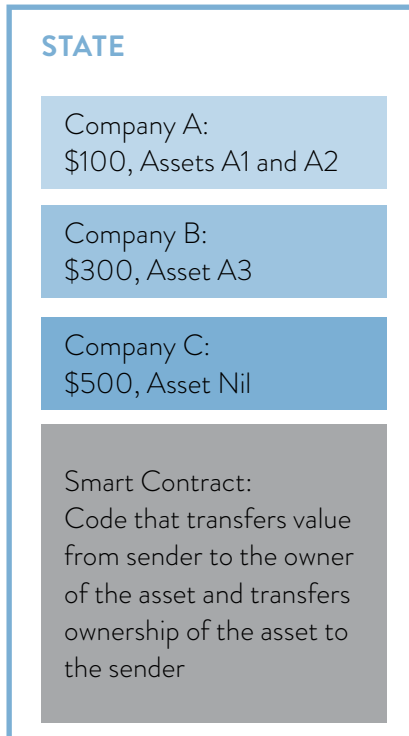
When talking about validation and consensus on private shared ledgers, the main priority is about validation in relation to a “change of state” on the ledger – and not sharing details of the information behind that (see Figure 7).

The challenge: how to automatically verify that there has been a change of information on the shared ledger (a “change of state”), without revealing the information itself?

FIGURE 7 – CHANGE OF STATE

BEFORE:

Three companies A, B and C, each with different balances of money and assets.



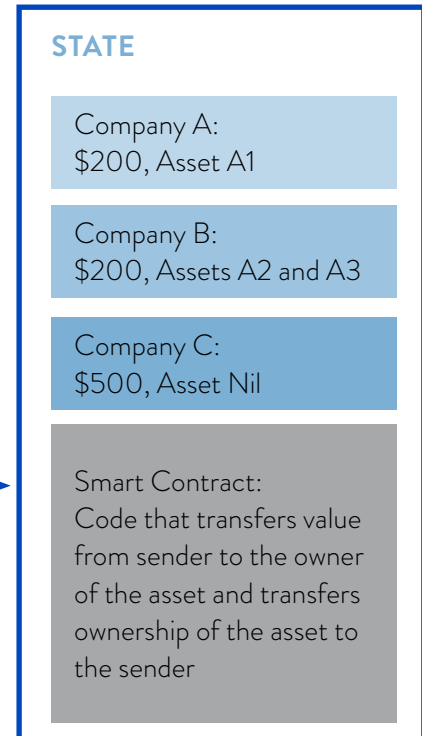
TRANSACTION:

Company A transfers asset A2 to Company B for \$100

From:
Company A
To:
Company B
Value:
\$100
Asset:
A2

AFTER:

Company A has more money,
Company B has less money and Asset A2 is now owned by Company B



CRYPTOGRAPHIC SECURITY ON PRIVATE SHARED LEDGERS

With private shared ledgers being designed for confidentiality, data encryption is a key design feature in transactions between counterparties on the ledger.

Advanced cryptographic techniques are being deployed which:

- + provide strong mathematically provable guarantees for the confidentiality of data and transactions; and
- + allow for confidentiality of the data/transaction to be preserved, and for computations to be performed without revealing the underlying data/transaction – so that only those with decrypt keys can access the underlying data/transaction.

Private shared ledgers make it possible to ensure that only the parties to a particular transaction hold the encryption keys for that transaction – and so limit the potential points of failure.

Whoever holds the cryptographic keys controls the data – they are critical to confidentiality and security on the shared ledger, and there are various options available such as:

- + deploying a master key held by the lead / master node (as a trusted operator);
- + generating unique public keys for each control program; or
- + generating multiple private keys from the master key.

Private keys can be stored in hardware security modules (HSM), making key compromise much more difficult. It is possible to independently generate public and private keys from the common master key pair – making it possible to create unique public keys without access to the master private key.

FUNDAMENTAL CHANGES IN APPROACH TO GOVERNANCE

The original blockchain platforms embedded all the rules of the game in software protocols designed to be exhaustive. Participants could transact without any other type of formal contractual or legal relationship and without any “real world” governance.

However, in the world of private shared ledgers, consortia members do not want or need the technology to completely control all interactions. In fact, the technology is unable to do this because of technical limitations.

The potential centralisation of validation control to the “new” intermediaries (eg: technology operator) also requires new layers of governance and control by the consortium.

Different use cases and different design choices will lead to different features and trade-offs, and require new control and governance requirements.

This means that the consortium framework and operating rules cannot be developed independently of the platform. The two heavily interact and depend on each other for different elements.

As a result, consortia operating on private shared ledgers are heavily dependent on a rigorous framework of governance, operating rules, smart contracts and contractual agreements – designed to work together consistently in the shared ledger environment and achieve the business goals of the new consortium.

This framework can inevitably leverage some of the elements of traditional participation and market rules (such as regulatory regimes) – but it often needs to be supplemented or overlayed by operating rules for the new shared ledger environment.

Finally, it is also important to recognize that the technology decisions (including upgrades) and design choices themselves need to be appropriately governed by the consortium.

5 WHERE ARE THE NEW CONSORTIA EMERGING?

Private shared ledgers provide new opportunities for collaboration across multiple organisations and across broad industry groups.

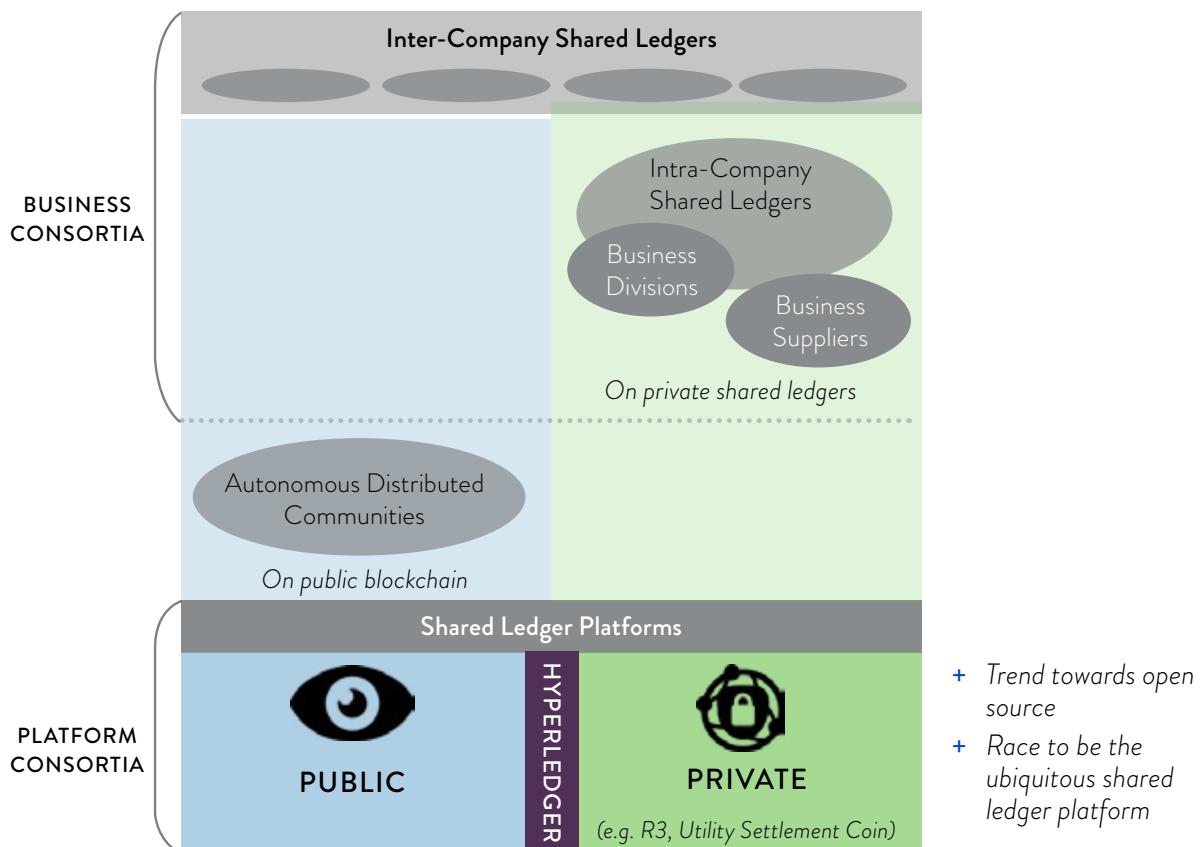
Consortia in the shared ledger ecosystem are emerging at two levels (see Figure 8):

- (i) platform consortia building the underlying technologies; and
- (ii) business consortia building commercial operations on these platforms.

Microsoft Azure's CTO Mark Russinovich envisions a world where **every industry is involved in a blockchain consortium**:

“... If they're going to get disrupted, they want to do it to themselves and then take advantage of the disruption.”¹⁵

FIGURE 8 - TYPES OF CONSORTIA



¹⁵ Michael del Castillo, 'Microsoft Azure's CTO Wants Blockchain to Connect Every Industry', *CoinDesk*, 6 September 2016 <<http://www.coindesk.com/microsoft-azure-cto-wants-to-connect-every-industry-with-a-blockchain/>>.

PLATFORM CONSORTIA

Platform consortia are building the underlying shared ledger platforms – both public blockchain platforms, and private shared ledger platforms such as: R3 (for financial services); ASIS (in Taiwan, focused on telecoms); and Utility Settlement Coin (for digital cash, operated by Clearmatics). The Linux Foundation's Hyperledger Project is establishing a collection of both public and private platforms – there is no exclusivity in the Hyperledger Project.

In addition, there are technology developers working independently to establish their own private shared ledger platforms (eg: Chain Open Standard and Digital Asset Holdings, which both have significant investment from corporate shareholders).

As mentioned above, private shared ledger platforms are by no means standard. The particular features and functionality of each private shared ledger platform are an outcome of the particular architecture and design decisions made along the way to achieve specific industry requirements around confidentiality and scalability – and there are many options here (see Section 4: How do private shared ledgers work?).

For this reason, platform consortia rely heavily on industry input and engagement. There is often blurring between, and merging of, platform and business consortia. This can lead to issues down the track, particularly if interests between “business” members and “technology” members diverge. In this context, establishing appropriate governance and decision rights early is vital.

The positive news is that many of these consortia are making their basic software available for anyone to develop on the private shared ledger platform:

- + Access to these private shared ledger platforms is often paid for via venture capital funding and consortium membership fees (which may vary across consortium members, depending on their class of membership).
- + However, there has been a flurry of announcements over

the past few weeks from platform consortia proposing to “open source” their basic software,¹⁶ making it available so that it can be scrutinised and adapted by anyone, enabling accelerated community-driven innovation.

- + Going forward, paid-up consortium members will continue to have access to higher levels of functionality (that are developed by the platform consortium, but not initially incorporated in the open source software). However, those paid-up consortium members will also derive significant benefits from the open source strategy. It means they will not be limited to the functionality offered by the platform consortium – they can also build out their own ecosystem of developers, and create their own niche functionality on the private shared ledger. This will inevitably lead to faster and cheaper innovation for corporates.
- + For the platform consortia, these “open source” commitments are part of their strategy in the race to become the platform of choice. There are many private shared ledger platforms emerging at the moment, but it is likely that consolidation will occur further down the track as the “winners” emerge.
- + For example, on 20 October 2016 R3 announced plans to open-source their software from 30 November 2016 and stated that they hoped their platform would become the industry standard – with multiple firms building products on top of it.¹⁷

“We want other banks and other parties to innovate with products that sit on top of the platform, but we don't want everyone to create their own platform ... because we'll end up with lots of islands that can't talk to each other.”

James Carlyle, Chief Engineer, R3

- + Chain announced plans to open-source their shared ledger platform, Chain Protocol, on 24 October 2016 so that it will be freely available to developers worldwide to download and install.¹⁸

“I don't want to be a gatekeeper. I want people to go from PowerPoint to pilot.”

Adam Ludwin, CEO, Chain

16 See, eg, Chain Protocol Whitepaper, Chain <<https://chain.com/docs/protocol/papers/whitepaper>>.

17 Richard Gendal Brown, ‘Introducing R3 Corda™: A Distributed Ledger Designed for Financial Services’ on *The R3 Report* (5 April 2016) <<https://r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services>>; Jemima Kelly, ‘Blockchain platform developed by banks to be open-source’, *Reuters*, 20 October 2016 <<http://www.reuters.com/article/us-banks-blockchain-r3-exclusive-idUSKCN12K17E>>.

18 Chain, ‘Chain Launches Open Source Developer Platform’ (Press Release, 24 October 2016) <<https://chain.com/press-releases/chain-launches-open-source-developer-platform/>>; Robert Hackett, ‘Visa's Blockchain Bet Opens Up to Developers’, *Fortune*, 24 October 2016 <<http://fortune.com/2016/10/24/visas-blockchain-chain-open-source/>>.

BUSINESS CONSORTIA

The biggest growth phase is yet to come and will be in the area of new business consortia, which are the key focus of the remainder of this paper.

These business consortia will generally not be developing their own shared ledger platforms. Instead, they will develop technology solutions to meet their own niche business requirements – built on the existing private shared ledger platforms. Business consortia may also be stakeholder or pilot participants for platform consortia who are developing platforms for particular industry or business groups.

Special-purpose niche business consortia are emerging – both “inter-company” and “intra-company”:

- + At the inter-company layer, special-purpose consortia are being designed to facilitate transactions and the transfer of value between participants across multiple organisations. These may involve:
 - organisations that are **already dealing with each other**, and can derive new efficiencies by migrating to a private shared ledger; or
 - organisations that have **never worked together** – but where new kinds of consortia are becoming viable on private shared ledgers.
- + At the intra-company layer, organisations are establishing their own shared ledgers to facilitate end-to-end processing and records for corporate operations – across their corporate divisions, and encompassing the supply chains of their suppliers.¹⁹

The success of these business consortia will be critical to delivering on the promise of shared ledger technologies.

AUTONOMOUS DISTRIBUTED COMMUNITIES

There is another category of consortia emerging between smaller businesses with the potential to “disrupt the disruptors”. Using shared ledgers, they can create new business models which no longer need central companies to act as the middle-person (see Box 5). They have the potential to disrupt the “Ubers” of the world, and create their own business communities.²⁰ These communities will generally operate on public blockchain platforms.

19 R Tyler Smith PhD, ‘Awaking the sleeping giant: the natural resource industry and the blockchain’ (Presentation at 2nd Global Blockchain Summit, Shanghai, 23 September 2016); Peter Rizzo, ‘World’s Largest Mining Company to Use Blockchain for Supply Chain’, *CoinDesk*, 23 September 2016 <<http://www.coindesk.com/bhp-billiton-blockchain-mining-company-supply-chain/>>.

20 Fred Ehrsam, ‘How the Blockchain Could change Corporate Structure’, *Wall Street Journal* (online), 19 October 2016. <<http://www.wsj.com/articles/how-the-blockchain-could-change-corporate-structure-1476887998>>.

21 Fred Ehrsam, ‘App Coins and the dawn of the Decentralized Business Model’ *Medium* 2 August 2016. <<https://medium.com/the-coinbase-blog/app-coins-and-the-dawn-of-the-decentralized-business-model-8b8c951e734f#8nrjp7af>>.

BOX 5

AUTONOMOUS DISTRIBUTED COMMUNITIES²²

- + Up until now, a centralised company has been the best way to establish and manage special-purpose networks, eg: Uber connects riders with drivers; banks connect savers with borrowers; and Twitter connects content writers with content consumers.
 - + However, new consortia will no longer need central companies to act as the middle-person. This means that they have the potential to disrupt the “Ubers” of the world, and create their own communities on either public blockchain networks or private shared ledgers.
-

“ These projects are raising money by creating and then selling their own “App Coins” through crowdfunding on a blockchain. At first glance this just looks like a new way to raise money, much like how a normal company issues and sells stock to raise capital. At second glance it goes far beyond that... It is projects creating their own economic ecosystems to make the entire thing tick. More precisely, it is about an entirely new business model that is being created and tried for the first time: a decentralised business model. In this model there is no central controlling company, and has shared contributions and ownership by all involved. This business model is uniquely enabled by the combination of the internet and cryptocurrency... You’ll notice one other thing about these “projects” or “apps”: they are really decentralised software protocols²¹ ”

Fred Ehrsam, Co-founder, Coinbase

²² Ehrsam, above n20.

The background of the page is an abstract composition. It features a dark, textured surface with a grid of small, light-colored dots. A prominent blue diagonal band, also composed of dots, runs from the bottom left towards the top right. The text is overlaid on this blue band.

PART C

LIFTING THE COVERS ON THE SHARED LEDGER CONSORTIUM

6 CRITICAL CHOICES FOR BUSINESS CONSORTIA ON PRIVATE SHARED LEDGERS

WHY USE A CONSORTIUM?

The success of blockchain and shared ledger technologies requires significant levels of market participation, collaboration and investment. A strong and stable framework is required to provide the confidence and certainty necessary for this to be achieved. The reality is that the commercial interests of participants on a private shared ledger don't need to be perfectly "aligned". The participants on a shared ledger just need to have similar requirements in terms of:

- + the mix of confidentiality and transparency (as captured in the design choices and operating rules for the shared ledger platform);
 - + functionality and processes;
 - + the approach to governance; and
 - + a shared view of regulation and compliance
- and they need to commit to complying with the operating rules of the consortium.

The consortium is less about a technology solution or a particular business model, and more about a way for companies to come together and collaborate.

Where the participants are known to each other, they can leverage the efficiencies of working on a private shared ledger:

- + to deal with other participants directly, without the need for a third party intermediary; and
- + to innovate in a cost effective manner – and collaborate with other consortium members where it makes sense.

CONSORTIUM FAILURES OF THE PAST

Consortiums and shared services are difficult to do well, and there have been many dismal failures in the past. The take-up of shared services has been limited (despite the potential efficiencies and savings that can be achieved within industry groups). Corporations have preferred to establish their own separate IT infrastructure and systems due to:

- + a lack of trust between industry members – and concerns around ensuring the security of data and systems;
- + the complex and clunky nature of traditional technologies for delivering shared services to multiple organisations;
- + the additional costs of third party intermediaries required to operate those shared services;
- + the challenges of balancing a consortium's common goals with the self-interests of particular members' goals – which may prove fatal to the consortium's common platform, particularly if a consortium member chooses to invest in any competing ventures;
- + intellectual property disputes in relation to ideas generated via consortium activities;
- + challenges in relation to governance and control (politics and personalities) – and the development of separate alliances within consortiums;
- + the challenges of achieving the optimal size of the consortium – building scale, but not to the point that the consortium is so large that it can't operate effectively; and
- + the sustainability of the consortium – and the risks of building a "white elephant" or a "Frankenstein".

WHAT ARE THE CRITICAL CHOICES THAT NEED TO BE MADE AT THE OUTSET FOR BUSINESS CONSORTIA OPERATING ON PRIVATE SHARED LEDGERS?

- 1 SETTING THE CONSORTIUM STRATEGY
- 2 CHOOSING THE RIGHT SHARED LEDGER PLATFORM
- 3 CHOOSING THE SOLUTION DESIGN
- 4 PLANNING TO MITIGATE POTENTIAL PITFALLS
- 5 ESTABLISHING THE CONSORTIUM FRAMEWORK

The salutary lessons of past consortia failures highlight the importance of those critical choices to be made at the outset:

1 SETTING THE CONSORTIUM STRATEGY

Setting a consortium strategy at the outset is critical to the long-term success of the business consortium:

- + Identifying new revenue opportunities, which may not have been viable outside of the shared ledger environment;
- + Identifying possibilities for working with new organisations which may not have been practical in the past – and which could deliver new opportunities for collaboration, innovation and efficiencies;
- + Identifying the target consortium members – as well as those who may not be permitted to join;
- + Strategically consider who should control the consortium?
- + What are the competitive threats and long-term strategies for the sustainability of the consortium?

2 CHOOSING THE RIGHT SHARED LEDGER PLATFORM

Selection of a shared ledger platform is not like any other technology project – status quo processes won't work. Before evaluating potential options and selecting a “fit for purpose” platform, critical preparatory steps need to be taken to establish the basis for evaluation:

- + identifying all of the business processes and operational requirements (including regulation) that will need to be performed on an end-to-end basis; and
- + identifying how those business processes will be reconstructed on the shared ledger platform.

Private shared ledger platforms are by no means standard or uniform. Each platform provides different options for:

- + how confidentiality is achieved and how the “permissions” are designed: who can see, who can write, who reads, who validates;
- + how scalability is achieved;
- + how consensus is done (although some platform developers are questioning if consensus is even necessary);
- + how encryption and security are implemented and managed;
- + how smart contracts are linked with “real world” contracts (including hashing options), and how validation is carried out to ensure consistency between them;
- + capabilities for interfacing with information feeds (or “oracles”); and
- + capabilities for interoperability with other shared ledger platforms and legacy systems.

It is critical to choose a “fit for purpose” shared ledger platform from the outset. If the platform design doesn't readily lend itself to delivering the consortium's strategy, there is no assurance that workarounds will achieve the required result. Even if workarounds are possible, they may prove to be just too complex in practice. Failure to choose a “fit for purpose” platform from the outset may leave the consortium with little choice but to start all over again.

3 CHOOSING THE SOLUTION DESIGN

Once the shared ledger platform is chosen, that is not the end of the matter. A technical solution design is still required, determining how the consortium's specific strategy and operational requirements will be delivered on the shared ledger platform. This requires decision-making around:

- + the overall architecture of the solution – including how security and safeguards will be built into the technology and the processes, and how real-world governance and decision-making will be integrated with the technical solution;
- + the design of the “rules engine” and the “smart contracts system” for automated processing on the consortium (including automation of the consortium's operating rules where practicable);
- + how to create trust and security on the shared ledger? How will the public / private encryption keys be managed? Who will hold those keys? Where will the keys be held?
- + the specific protocols to be adopted in relation to “permissions” on the shared ledger: who can see, who can write, who reads, who validates – and how consensus will be performed, if required;
- + how the technical design will prevent (as far as possible) any breach of the consortium's operating rules – whether by the technical operator or by participants on the shared ledger?
- + the required information feeds or “oracles” to be incorporated into the design; and
- + how to achieve compliance with applicable regulatory requirements – and in financial services, this may include considerations around redundancy and other technology matters which could impact on the stability of the relevant financial markets.

4 PLANNING TO MITIGATE POTENTIAL PITFALLS

While there are clear efficiency benefits and cost savings that shared ledgers can provide through collaboration and more effective information sharing, this doesn't mean that competition / antitrust risks will disappear. There is no reason why consortium activity on a private shared ledger would be exempt from these laws. Under current Australian laws, consortium activity can constitute cartel conduct if the structure fails to incorporate appropriate compliance and enforcement measures. Upcoming changes to Australia's competition laws will see the introduction of a “concerted practice” prohibition which sets a lower threshold for illegal coordinated activity than the existing cartel laws.

It is arguable that current competition laws do not take appropriate account of developments in the digital economy – at least in Australia. While this may change in the future, efficiencies and cost savings do not currently constitute any defence to cartel conduct – unless the consortium members pre-emptively seek “authorisation” from the Australian Competition and Consumer Commission. This is a public process that could take six months to complete. By comparison, if the consortium can establish well-designed operating rules and governance for the consortium, then it may be possible to rely on that framework to clearly establish the efficiency benefits – without the need to go through the public authorisation process.

5 ESTABLISHING THE CONSORTIUM FRAMEWORK

Detailed planning is required in relation to the overall structure and governance of the consortium, as outlined below.

CONSORTIUM FRAMEWORK

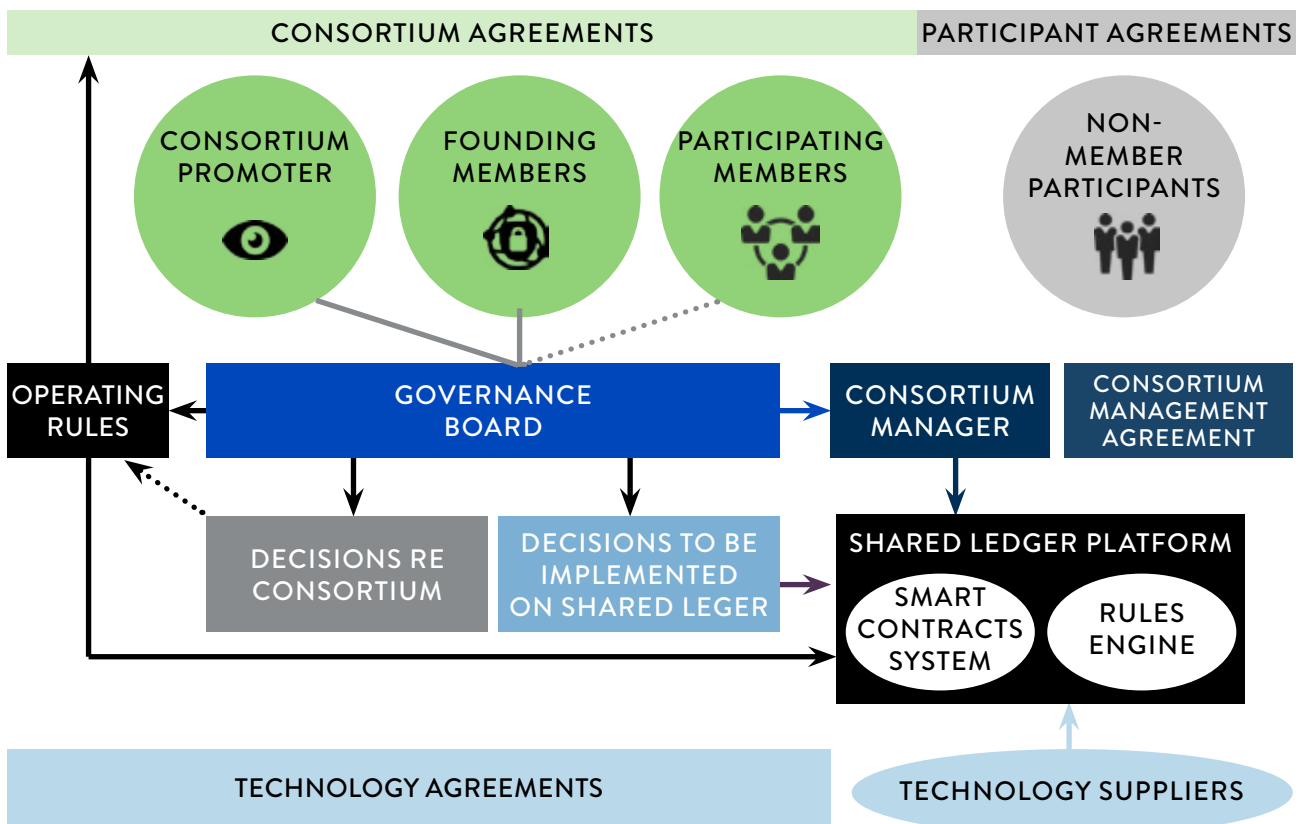
The right consortium framework will be a critical success factor for the sustainability of business consortia on private shared ledgers.

Sustainable delivery of the value promised from these business consortia requires design and execution of the entire consortium framework – the business processes, operating rules, governance, smart contracts and contractual agreements. The business processes need to be entirely reconstructed so as to work in the shared ledger environment.

The technology makes the consortium rules easier, but participants still need a strategy and a framework for managing day-to-day decision making and dealings with each other.

Figure 9 sets out the key components of a framework for a business consortium. Of course this framework would need to be adapted to specific circumstances, but it provides a starting point for thinking about the important issues.

FIGURE 9 - CONSORTIUM FRAMEWORK



WHO CONTROLS THE CONSORTIUM?

The consortium promotor could be a technology vendor or a start-up. It could also be a current participant in the market, or a group of consortium members operating through a joint venture or separate corporate entity.

Whatever the structure or make-up, the consortium promoter will naturally hold sway on decision rights relating to the shared ledger platform and the consortium market place, unless those decision rights are expressly moved elsewhere.

From the perspective of other consortium members, however there may be a desire to ensure that certain decision rights are not centralised in one party – whose interests could drift over time in conflict with those of the consortium members. This could result in a scenario where the consortium members have no real control over the platform, the way it operates, or the fees for participation.

When this happens, there is the risk of an irretrievable scenario – the investment by consortium members is too great and the transition costs are too high to shift away. The parties end up dissatisfied and the consortium may fail.

The initial governance choices that are made in establishing the consortium framework will therefore be critical to long-term incentives and the sustainability of business consortia on private shared ledgers.

KEY COMPONENTS OF A CONSORTIUM FRAMEWORK

CONSORTIUM AGREEMENTS

Establishing consortium agreements with consortium members – with detailed consideration around the matters referred to in Box 6.

The rights around appointments to the governance board may be critical (depending on the level of power allocated to the governance board).

PARTICIPATION AGREEMENT

Establishing participation agreements with corporates who are entitled to use the private shared ledger (on a fee-paying basis) but without having consortium membership, eg: suppliers to the consortium who need to be on the shared ledger.

GOVERNANCE BOARDS

Establishing consortium governance for the shared ledger environment:

- + A degree of centralised governance is required for ongoing decision-making, enforcement of the operating rules and managing regulatory obligations (eg: via a governance board).
- + What decisions will need to be made along the way (ie: what decisions can't be pre-determined and automated)? (see Box 6).
- + What decisions will be centralised via the governance board, and what decisions will be decentralised and determined by consortium members?
- + What is the process for ensuring that decisions are implemented via the rules engine and the smart contracts?
- + How to manage risk and accountability – particularly when things go wrong?

OPERATING RULES

Establishing the operating rules for the consortium (which will be binding on all participants).

- + The operating rules will need to ensure compliance with all applicable regulatory requirements.
- + In many cases, consortium members will essentially be setting up a private market place. In some instances, there will already be rules of a public marketplace which will need to be translated and supplemented to apply on the private shared ledger. In other instances, the consortium will be starting afresh.
- + Significant components of the operating rules will need to be embedded in and enforced by the automated rules engine on the private shared ledger. Other parts will need to be implemented and enforced via traditional legal constructs.
- + Multi-party participation rules are generally the most efficient option for implementation – and they become binding on members and participants via consortium agreements and participation agreements.

TECHNOLOGY AGREEMENT

Establishing contractual arrangements with the various technology service providers, including:

- + for the licensing and maintenance of shared ledger software;
- + for a solution design;
- + for the development of niche functionality to meet the specific requirements of consortium members and participants; and
- + for the operation of the private shared ledger on a daily basis, including performance requirements and support obligations.

This requires considerations around how best to manage technology, security and stability risks.

CONSORTIUM MANAGEMENT AGREEMENT

Establishing contractual arrangements with a consortium manager (if required).

SMART CONTRACTS / “REAL WORLD” CONTRACTUAL AGREEMENTS

Establishing the optimal mix of automated smart contracts and “real world” contractual agreements to govern operations and processing on the private shared ledger (See overleaf).

BOX 6

WHAT TYPES OF MATTERS NEED TO BE ADDRESSED IN THESE CONTRACTUAL AGREEMENTS?

Matters which can't easily be pre-determined and automated, and which need to be addressed in contractual agreements, include:

- + managing dispute resolution inside the consortium and among participants and service providers;
- + managing ongoing updates and changes to the operating rules;
- + how new participants will be added – what eligibility criteria apply and what competition aspects are relevant?
- + how consortium members can be removed;
- + how relationships with the regulator(s) will be managed – and how to respond to regulatory changes;
- + contractual obligations on participants in respect of confidentiality, privacy and data control/ownership;
- + decision-making in relation to intellectual property rights arising from ideas shared between members or created in the course of collaborating together;
- + how fees will be established and amended;
- + how relationships with technology service providers will be managed, including appointment and termination;
- + platform security and integrity and service standards, and ongoing decision-making in relation to the technology solution, eg: issues relating to technology performance and technology upgrades; and
- + how risk and accountability will be managed – particularly for when things go wrong (eg: how to clarify the intentions of the parties in the event of coding errors in the smart contract, addressing the problems that rose with The DAO – see Box 8).

WHAT IS THE RIGHT MIX OF AUTOMATED SMART CONTRACTS AND “REAL WORLD” CONTRACTS?

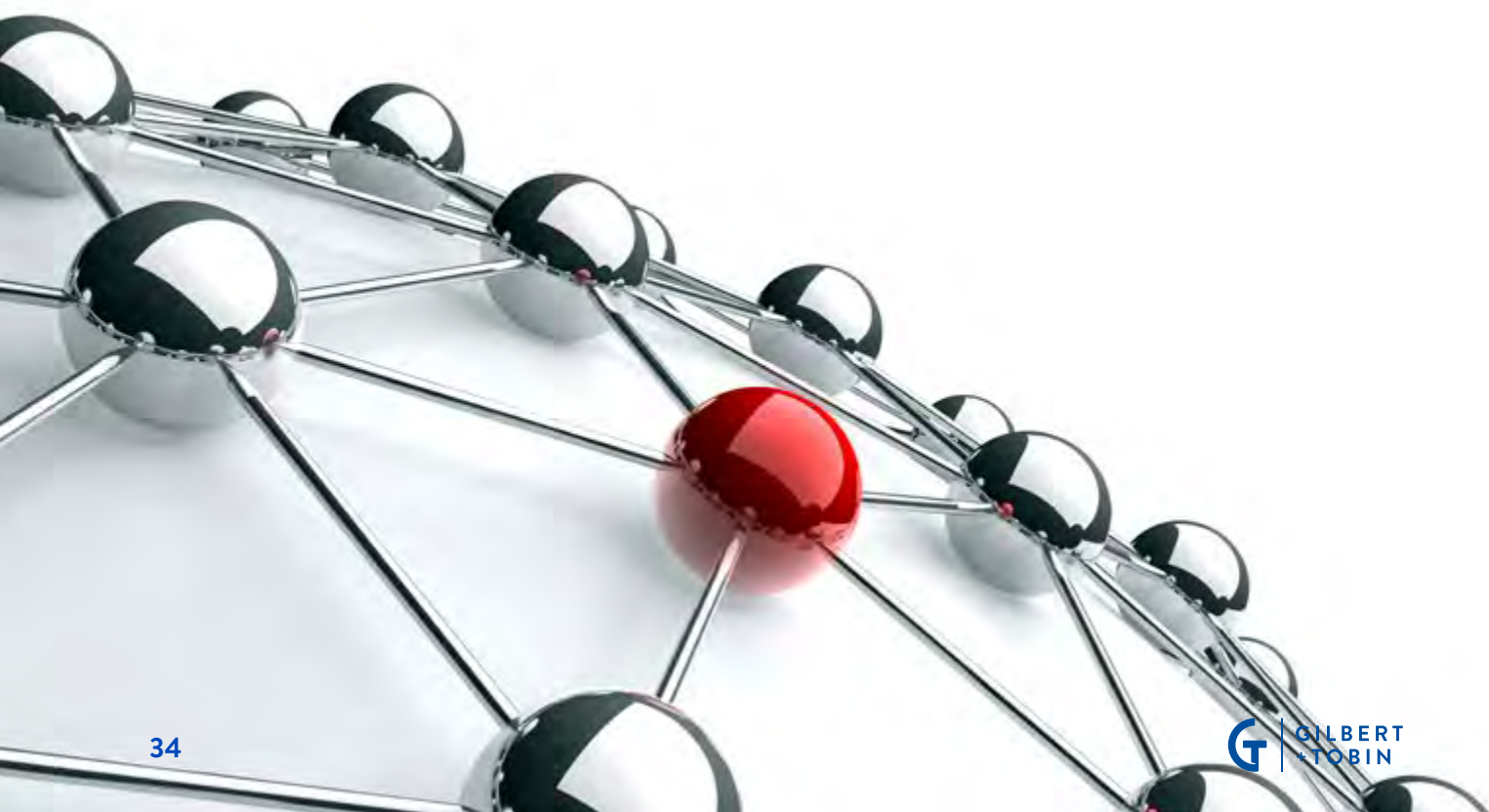
Without a smart contract, we couldn't exploit the full potential of blockchain and shared ledgers. However, smart contracts do not replace contractual agreements.

Doing business in a shared ledger environment is not simply a matter of replacing traditional contracts with automated smart contracts. Smart contracts can only work for those arrangements that are suited to automated processing – they are really no more than “smart transactions” (see Box 7). By comparison, a contractual agreement is about the intentions of the parties which:

- + can be far broader in scope than just automated processing; and
- + can be manifest in many different ways: in writing, verbally, by conduct, by smart contract coding on the blockchain ledger – or by any combination of these.

“Real world” contractual agreements are still required to set out the intentions of the participants and provide a framework for responding to unforeseen circumstances, enabling the parties to:

- + enforce their legal rights – whether via alternative dispute resolution mechanism or via the courts; and
- + achieve an outcome, based on the actual events transpiring – taking into account all relevant information that is available at the time when the event occurs.



BOX 7

WHAT ARE SMART CONTRACTS?

Smart contracts provide the logic on the shared ledger – with opportunities for far greater automation than we have ever seen before. They are computer programs which:

- + execute processes to effect changes on the shared ledger; and
- + are capable of automatically enforcing themselves upon the occurrence of pre-defined conditions.

Smart contracts perform a role rather like that of a trusted third party:

- + they will faithfully perform whatever tasks they are programmed to do in the blockchain environment – they are “self-executing” and “self-enforcing”; and
- + participants can trust the results of this automated processing – which could never happen in a traditional environment, without a central gatekeeper or intermediary to manage the database.

HISTORY OF THE SMART CONTRACT

The term “smart contract” was arguably first used by Nick Szabo in 1994.²³ It was then implemented in Bitcoin and subsequently Ethereum.²⁴ In parallel Ian Grigg developed the concept of Ricardian Contracts to leverage the combined benefits of automated processing and traditional legal agreements.²⁵ This concept has been adopted, in whole or part, in a number of solutions including Open-Transactions, Monax and Barclays’ Smart Contracts Templates.²⁶

23 Nick Szabo, ‘Smart Contracts’, Virtual School (1994) <<http://www.virtualschool.edu/mon/Economics/SmartContracts.html>>; Nick Szabo, ‘Formalizing and Securing Relationships on Public Networks’ (1997) 2(9) <<http://dx.doi.org/10.5210/fm.v2i9.548>>.

24 Ethereum: A Next Generation Smart Contract and Decentralized Application Platform <<https://github.com/ethereum/wiki/wiki/White-Paper>>; see also Stuart Popejoy ‘The Pact Smart-Contract Language’ (October 2016) <<http://kadena.io/docs/Kadena-PactWhitepaper-Oct2016.pdf>> and ‘Introducing the Digital Asset Modeling Language: A Powerful Alternative to Smart Contracts for Financial Institutions’, Digital Asset Holdings (2016) <<https://digitalasset.com/press/introducing-daml.html>>.

25 Ian Grigg, ‘The Ricardian Contract’ (2004) Proceedings of the First IEEE International Workshop on Electronic Contracting <http://iang.org/papers/ricardian_contract.html>; Ian Grigg, ‘On the Intersection of Ricardian and Smart Contracts’ (2015) <http://iang.org/papers/intersection_ricardian_smart.html>.

26. Chris Odom ‘Open-Transactions: Secure Contracts between Untrusted Parties’ (2015) <<http://www.opentransactions.org/open-transactions.pdf>>; Monax <<http://monax.io>>; Christopher Clack, Vikram Bakshi and Lee Braine ‘Smart Contract Templates: foundations, design landscape and research directions’ (3 August 2016) <<http://www0.cs.ucl.ac.uk/staff/C.Clack/SCT2016.pdf>>.

FAILED BUSINESS CONSORTIUM EXPERIMENTS ON SHARED LEDGER PLATFORMS

Business consortia on shared ledgers have experimented with abandoning the real-world framework of governance and contractual agreements – and replacing all of that with coding and automation on the shared ledger. However, those extreme approaches have proved to be unsuccessful in practice (see Box 8).

Certain events and their consequences are just not predictable, and can't be automated into a smart contract.

There is no smart contract code for dispute resolution. Most transactions in the real world are managed by a framework of governance and contractual agreements. Therefore, it makes sense to design a shared ledger solution that provides a way to tie the processes and smart contract functionality on the shared ledger to that real-world framework.

This approach reflects the practical realities of managing disputes. In the event of a default, smart contracts need to go into a halt position because these take considerable time to resolve. Once a halt position is implemented, it becomes very difficult to return to the automation state. Disputes can take months or years to resolve, and the smart contract may or may not be functional at the end of that period.

BOX 8

THE DAO

Recently, smart contracts on public blockchain have been in the headlines, and not for positive reasons. While the future of the technology looks bright, some hard lessons have needed to be learned. The DAO²⁷ illustrates the risks of throwing out the real-world framework and moving to a totally code-based environment.

A “DAO” is a Decentralised Autonomous Organisation. Its goal is to codify the rules and decision-making of an organisation, eliminating the need for documents and people in governance, and creating a structure with decentralised control. A DAO is not owned by anyone – its just software running on the a blockchain network. The premise behind a DAO is that smart contracts are their own arbiters, and nothing outside the code can “change the rules” of the transaction.

The DAO refers to a particular DAO, established on the Ethereum network by the team behind German start-up Slock.it. The DAO launched on 30 April 2016, raising over US\$150m – only to have a third of it siphoned away by an unknown attacker, due to coding errors in The DAO’s smart contract.

There were two key problems here – the obvious technical problems, and also the lack of governance. The technical problems centred around:

- + coding errors – reflecting the lack of tools to assist with de-bugging for this kind of software; and
- + the sheer complexity of what they were trying to achieve – combining too many functions in risky ways that were not optimal.

From a governance perspective it wasn't clear what the contract was ultimately the code on the blockchain was changed arbitrarily (via a hard fork). This led to a splitting of the Ethereum blockchain into two distinct blockchains. It was done arbitrarily, based on real-world decision-makers reacting to the situation.

This response could **not** have been managed via smart contract code, nor linked to the contract running on the Ethereum blockchain. It would have been impossible to automate a response to this attack. It is impossible to foresee all possible events that could go wrong – or to pre-determine what the appropriate response would be to each and every one of those circumstances.

²⁷ Christoph Jentzsch, ‘The History of the DAO and Lessons Learned’, on *Slock.it* (25 August 2016) <<https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5#.m5hvi0rfm>>.

HOW TO ENSURE CONSISTENCY BETWEEN SMART CONTRACTS AND “REAL WORLD” CONTRACTS?

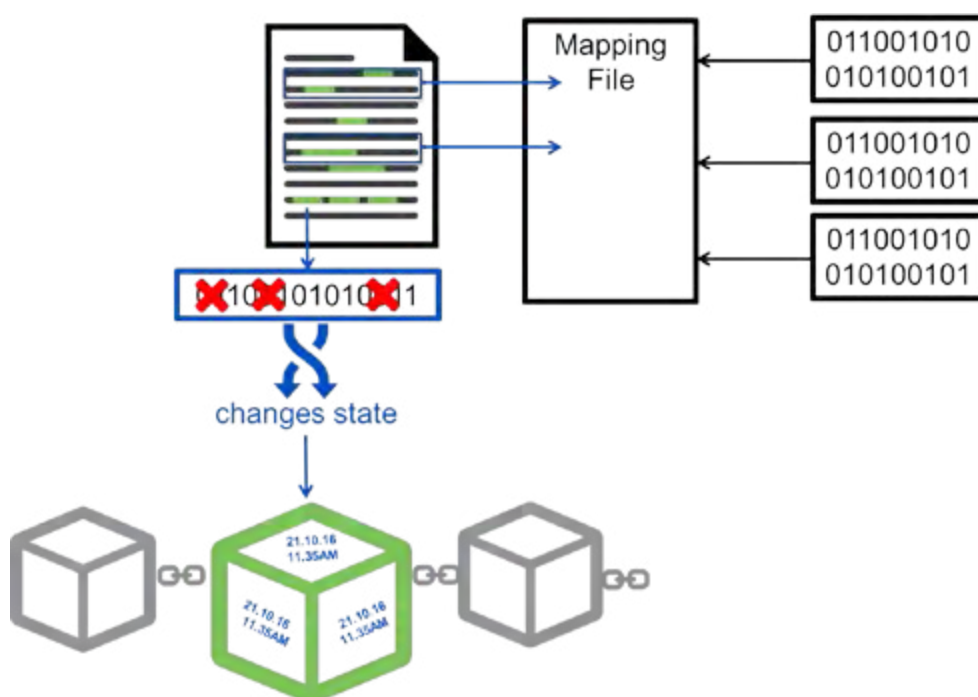
There are risks of inconsistencies between the smart contract and the intentions of the parties (as per their contractual agreement).

One of the most pragmatic initiatives to solve this challenge has been developed by the R3 consortium with their shared ledger platform, Corda.²⁸

Corda solves the problem by tying real world legal contracts to smart contracts through hashing (see Figure 10):

- + Coders write smart contracts for automated processing on the shared ledger – which are “hashed” (ensuring that the automated processing can’t be tampered with).
- + As the same time, traditional legal agreements are written to address those issues which can’t be converted into code – and they are also hashed.
- + As a result of this hashing process, the smart contract and the “real world contract” are both lodged and linked on the shared ledger. The technology becomes so much simpler to execute in a private consortium, where all of the participants are known and invited.

FIGURE 10 - ENSURING CONSISTENCY BETWEEN SMART CONTRACTS AND “REAL WORLD CONTRACTS”



²⁸ Richard Gendal Brown, above n 14.

“ Corda is a distributed ledger platform designed and built from the ground up for the recording and automation of legal agreements between identifiable parties. It is heavily influenced by the requirements of the financial industry but we believe the community will find the underlying architecture will lend itself to a broad range of applications.²⁹ ”

Richard Gendal Brown, Chief Technology Officer, R3

The Corda solution achieves consensus in two ways:

1. **Transaction validity:** The parties need to check that the contract code matches the real-world contract, ie: ensure that they are consistent, and that there are no coding errors. The parties agree on transaction validity through a process which involves each of them independently running the same contract code and validation logic.
2. **Transaction uniqueness – no double spend:** The parties need to ensure that the inputs are valid, and that there is no duplication or double-spend. This role is generally performed by an independent third party.

The Corda solution makes this possible because transactions are “node to node” only, between the two counterparties (and with an opt in for a third party validator).

²⁹ Richard Gendal Brown, above n 1.

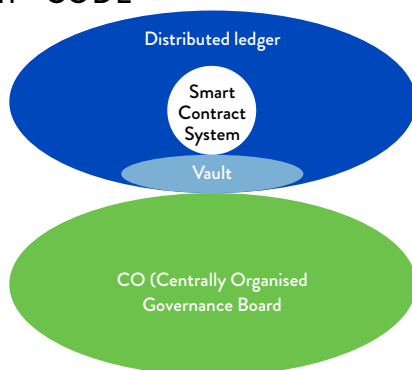
NEW GOVERNANCE FRAMEWORKS ON SHARED LEDGERS

Even on public blockchain, there is now recognition that real world contractual agreements and dispute resolution processes are going to remain relevant in a digital world. Decision-making can't just be made in code – in fact, it must not be.

The CODE (**C**entrally **O**rganized **D**istributed **E**ntity)³⁰ is a recent innovation on public blockchain that provides an excellent example of a “bottom up” approach to establishing a new governance framework, designed specifically for the shared ledger environment. In essence, it creates a centralised decision-making process for the decentralised shared ledger.

CODE is premised on a simplified governance structure – where a real-world governance board manages real-world activities, in parallel with automated processing (via smart contracts on the public blockchain) (see Figure 11).

FIGURE 11 - CODE



The governance structure removes many of the security flaws of the DAO model – with its decentralised voting and poorly coded “splitting functions” (which ultimately led to the DAO being exploited). At the same time, the CODE functions enable project funding and revenue sharing, similar to a DAO.

As an additional layer of protection, tokens are placed in a “**Vault**”³¹ – a special account in which the keys can be “disarmed” if they fall into the hands of an attacker. It locks the funds away for minimum period to prevent the siphoning of funds, and to stop malicious actors from stealing private keys.

The combination of the Centrally Organised component (the “CO”) and the Distributed Entity (“DE”) builds the bridge required to create a centralised decision-making process for the decentralised shared ledger:

- + **“Governance Board”:** The CO (Centrally Organized component) contains real world decision makers; comprised of a Board (pseudo-directors) who unilaterally decide what is best for the project-based on their specialised expertise and knowledge of the industries in which the CODE is investing. The CO also manages day-to-day consortium issues. The CO can be implemented via a number of different corporate structures in various jurisdictions around the world.
- + **“Shared ledger platform”:** The DE (Distributed Entity) is the component existing on Ethereum’s blockchain.
- + **Security:** The CODE establishes an extra security layer called “**the Guard**” to protect against hacks and code failures, such as those which occurred in the DAO. The Guard performs a two tier auditing process with stress tests for both human and code fail-safe functions.
- + **Implementation of decision-making:** Decisions are first made by the CO, and then implemented via code on smart contracts – and placed on the Ethereum public blockchain via a Smart Contract System (SCS).
- + **Smart Contract System (SCS):** The SCS creates smart contracts for the purpose of funding, building, maintaining and growing real world projects and lodging them on the blockchain.

30 Zach LeBeau, ‘Anatomy of SingularDTV’s CODE (Centrally Organised Distributed Entity): A Decentralization Generator for the Tokenized Ecosystem,’ Anatomy of the Code (9 August 2016) <<https://medium.com/@SingularDTV/anatomy-of-singulardvs-code-centrally-organized-distributed-entity-cd7285d63549#fq2leog7g>>.

31 Vaults were first proposed in the Bitcoin Covenants White Paper. See, Malte Möser, Ittay Eyal and Emin Gün Sirer, ‘Bitcoin Covenants’ (2016) <<http://fc16.ifca.ai/bitcoin/papers/MES16.pdf>>; See also, Malte Möser, Ittay Eyal, and Emin Gün Sirer, ‘How to Implement Secure Bitcoin Vaults’ on *Hacking Distributed* (26 February 2016) <<http://hackingdistributed.com/2016/02/26/how-to-implement-secure-bitcoin-vaults/>>.

CONCLUSION

CONCLUSION

Institutional trust wasn't designed for the digital age. The emergence of shared ledger technologies – empowered by consortia – is a game changer for a major trust shift, which will empower new business models and relationships between corporations and consumers. If shared ledger technologies realise their full potential, then the consortium model should thrive and be sustainable in the way that hasn't been possible in the past.

Successful private shared ledger solutions will be designed with a mix of automation and real world governance:

- + There has been a stark realisation from the entire industry that “real world” contractual agreements, governance, dispute resolution mechanisms and legal enforcement through traditional legal institutions are going to remain relevant in a digital world.
- + As the technology continues to improve, more of the governance will be automated – but there will always be a need for real-world solutions to resolve disputes and other issues which were not foreseen by code.

Corporate success in this new world of private shared ledgers requires a creative approach to the consortium framework. This also requires a paradigm shift on the part of incumbents who have traditionally worked in isolation and often failed to collaborate or innovate, and are now facing the challenges of disruption.

Just as we have seen in past eras of the consortium, we can expect to see many of these business consortia fail – because they were not set up to succeed. Critical success factors lie in the up-front choices – and it is not just about the technology. Choices as to governance, consortium structure, operational rules and contractual arrangements are also critical to defining future success of the new business consortia on private shared ledgers.

LEAD AUTHORS



BERNADETTE JEW

Partner, Technology
Media + Telecommunications
Sydney

T +612 9263 4032

E bjew@gtlaw.com.au

 [@bernadette_jew](https://twitter.com/bernadette_jew)



GEORGE SAMMAN

E george.samman@gmail.com

W www.sammantics.com

 [@sammantic](https://twitter.com/sammantic)

CONTRIBUTING AUTHORS



CHARLES COOREY

Partner,
Competition + Regulation
Sydney

T +612 9263 4019

E ccoorey@gtlaw.com.au

 [@cooreycharles](https://twitter.com/cooreycharles)



PETER REEVES

Special Counsel,
Corporate Advisory
Sydney

T +612 9263 4290

E preeves@gtlaw.com.au

 [@peter_reeves](https://twitter.com/peter_reeves)



SIMON BURNS

Partner, Technology, Media +
Telecommunications
Sydney

T +612 9263 4776

E sburns@gtlaw.com.au




SIMON GILCHRIST

Manager Innovation R&D
Sydney

T +612 9263 4099

E sgilchrist@gtlaw.com.au

 [@sgilchrist](https://twitter.com/sgilchrist)



SYDNEY

Level 35, Tower Two
International Towers Sydney
200 Barangaroo Avenue
Barangaroo NSW 2000
T+61 2 9263 4000
F +61 2 9263 4111

MELBOURNE

Level 22
101 Collins Street
Melbourne VIC 3000
T+61 3 8656 3300
F +61 3 8656 3400

PERTH

1202 Hay Street
West Perth WA 6005

T+61 8 9413 8400
F +61 8 9413 8444

WWW.GTLAW.COM.AU

This document is prepared by Gilbert + Tobin for information only. Whilst reasonable care has been exercised in preparing this document, it is subject to change. Gilbert + Tobin cannot be held responsible for any liability whatsoever or for any loss howsoever arising from or in reliance upon the whole or any part of the contents of this document. ©Gilbert + Tobin 2016