BLOCKCHAIN FOR HOSPITALITY

October 17, 2018

About HTNG

Hospitality Technology Next Generation (HTNG) is a non-profit association with a mission to foster, through collaboration and partnership, the development of next-generation systems and solutions that will enable hoteliers and their technology vendors to do business globally in the 21st century. HTNG is recognized as the leading voice of the global hotel community, articulating the technology requirements of hotel companies of all sizes to the vendor community. HTNG facilitates the development of technology models for hospitality that will foster innovation, improve the guest experience, increase the effectiveness and efficiency of hotels and create a healthy ecosystem of technology suppliers.

Contributors:

Douglas Rice, Hospitality Technology Network; Andrew Sanders, DataArt; Criss Chrestman, NTT Data; Marshall Knauf, CloudBeds; Klaus Kohlmayr, IdeaS; David Hochschwarzer, Modul University Vienna; Charles Ehredt, Currency Alliance; Jonathan Reynolds, Amadeus; Max Stevens-Guille, Kognitiv; Candice François, AccorHotels; Richard Sheins, Hall Booth Smith, P.C.; Balaji Krishnamurhty, Sabre.

Table of Contents

1 This Document at a Glance

In 1995, Bill Gates called the Internet the most important single development since the introduction of the IBM PC in 1981[1]. Since then, the Internet has transformed every aspect of our lives. Twenty-three years later, another disruptive technology – blockchain – rapidly gains traction.

Blockchain is still in its infancy, and a lot of confusion and misinterpretations exist about potential benefits and use cases. Available resources describe many aspects of the technology, but they fail to explain any potential relevance to the hospitality industry. Due to this, HTNG has created a white paper designed to help educate the industry on the potential of blockchain and to establish a practical knowledge framework for hospitality business leaders and the technology vendor community.

To begin, the paper provides a comprehensive overview of blockchain technology, highlighting:

- What is blockchain and why does it matter
- The difference between private and public blockchains
- How blockchain works
- Technical limitations and challenges to overcome before blockchain can be widely adopted

Next, the paper outlines potential general use cases and addresses use cases specific to the hospitality industry. In the final section, the white paper outlines a practical path to start adopting blockchain.

Subsequent to publication of this white paper, HTNG plans to provide additional relevant educational materials to help the industry stay current with rapidly evolving blockchain developments.

2 Document Information

2.1 Document History

Version	Date	Author	Comments
0.01	10 May 2018	Klaus Kohlmayr	Added Executive Summary
0.02	11 May 2018	Douglas Rice	Added 7.3; copy editing and added comments for group discussion in Sec. 2, 3, 4, and the intro to 5. Also moved some material from Sec 3 to 7.4 (cryptocurrency/gas) as a placeholder
0.03	15 May 2018	Andrew Sanders/Criss Chrestman	Inserted edited version of 14. Why Do Something
0.04	17 May 2018	Douglas Rice	Merged edits by Criss Chrestman
0.05	18 May 2018	Andrew Sanders/Douglas Rice	Some re-write and general tidy-up and editing for readability up to and including section 7.3, comments added for group resolution

[1] https://www.wired.com/2010/05/0526bill-gates-internet-memo/

0.06	20 May 2018	Criss Chrestman	Merged sections for: 8 - Challenges; 9- Technology Risks; 12.6 Identity & Data Privacy; 12.7 Governance, Regulatory, and International Issues; Resolved the main duplicate content in sections
0.07	07 June 2018	Douglas Rice	General re-write and cleanup.
0.08	12 Jun 2018	Andrew Sanders	General cleanup.
0.09	13 Jun 2018	Douglas Rice	General re-write and cleanup
0.10	10 July 2018	Douglas Rice, Criss Chrestman	Incorporated edits and/or noted comments as agreed on 3 July 2018 meeting; new Section 6-Blockchain Ecosystems from CC; updated Section 10-Use Cases from Other Industries from DR;
0.11	10 July 2018	Richard Sheinis	Replaced Sec. 8.5-Identity & Data Privacy
0.12	11 July 2018	John Bell	Replacement and rename Sec.9- Characteristics and Uses of Blockchains
0.13	11 July 2018	Douglas Rice	Incorporated edits and comments as agreed on 11 July 2018 meeting. Reorganized Sections 12-13.
0.14	16 July 2018	Criss Chrestman	Revisions to Blockchains Ecosystems section
0.15	16 July 2018	Criss Chrestman, Balaji Krishnamurthy	Added comments to appendix for group discussion. Updated jurisdiction/governing law section.
0.16	17 July 2018	Douglas Rice	Resolved comments that have been there for a while with no further issues raised; fixed some formatting.
0.17	17 July 2018	Douglas Rice	Incorporated edits and comments as agreed on 17 July 2018 workgroup call.
0.18	17 July 2018	Douglas Rice	Inclusion of comments by Chuck Ehredt received after the workgroup call of same date.
0.19	3-7 August 2018	Andrew Sanders	Various clean up, inclusion of some comments by Raimund Gross plus technical clean up (eg 14.2) in realtime with Doug Rice
0.90	8 August 2018	Douglas Rice; Criss Chrestman; Klaus Kohlmayr	Addition of Sec. 11.1.2; added R3 Corda column in appendix table (from Criss Chrestman); new section 14.3 (from Klaus Kohlmayr)
1.0	17 October 2018		Released

2.2 Document Purpose

The purpose of this document is to provide a knowledge framework for blockchain and its potential application to the hospitality industry. The aim is to educate readers and provide basic, practical knowledge on the topic. It is not intended to establish or govern standards for the hospitality industry.

Following publication of this document, HTNG's Blockchain for Hospitality Workgroup plans to develop further blockchain-related educational assets.

Blockchain is still in its infancy, so while the group attempted to highlight risks in this white paper, it is likely that there will be many unforeseen developments with the technology over time. As with any new technology, any plans and strategies for blockchain based on information in this document should be considered high-risk.

2.3 Scope

In addition to providing educational material to explain what blockchain is and, conceptually how it works, this document covers the various types of blockchains, the benefits and drawbacks of each, how organizations can get started, relevant use cases and potential value drivers for hospitality.

2.4 Audience

This white paper is aimed to help business leaders in the hospitality operator and vendor communities, or as introductory material for technical practitioners seeking to understand the basic concepts of blockchain. The greatest benefit will likely be derived by middle to senior management and executive leaders aiming to define and set strategy, rather than by purely technical teams. This document may be useful in helping leaders decide what (if anything) they should be doing, or are planning on doing, with blockchain technology, and how to get started at a high level.

3 What is Blockchain?

3.1 Blockchain is a Way to Store, Share and Securely Distribute Data

The term "blockchain" describes a method for storing data in a way that is architecturally different from the traditional transactional database management systems (ledgers) that preceded it. First, users may only append records, never delete or edit. Second, data is distributed across a community of connected peer-to-peer devices, each of which stores an identical full or partial copy of the database. As records are written to the database, several things happen to create the special characteristics of a blockchain:

1. New created records are gathered in chronological order and grouped into a specific-sized block.
2. Each new block is appended to the database record, using a unique process described in Section 7.2.
3. Each new block contains a data element that is an encrypted reference to the preceding block (thus creating a "chain").
4. When a block is appended, each server among the peer-to-peer network (other than the one that created the block) must confirm that it contains a valid set of transactions and a valid cryptographic hash. Other servers will reject (refuse to add) a block that fails the validity test. Each blockchain community has a consensus process to ensure enough participating servers approve a block before it can be viewed as a permanent part of the chain.
5. Since each block refers iteratively to the block immediately prior, the chain has chronological integrity.
6. Since data is only appended and not modified, and has proven chronological integrity, it cannot be modified retroactively and is said to be 'immutable.' However, a better term may be 'tamper-evident.' While it is possible for a bad actor to modify a historical record, the tampering is immediately evident.

7. Any attempt to add false transactions will be thwarted by the fact that all nodes monitor the real-time transaction flow and validate that new blocks are accurate. Only after enough nodes have validated, a block can be considered permanent.

The peer-to-peer nature of a blockchain community inherently means it is distributed, but a blockchain is not necessarily decentralized. Whether a blockchain is centralized or decentralized is defined by the design, nature and type of system, which is determined by the participants of that blockchain community.

The concept of blockchain (though not the term itself) was invented by Satoshi Nakamoto (a pseudonym for an unknown person or group) in 2008 as a method to record ledger transactions of the cryptocurrency, Bitcoin. The technology has evolved significantly since 2008, although all blockchains still bear resemblance to Nakamoto's design.

3.2 Why Might Blockchain Be Better?

The seven characteristics of how data is stored and shared make blockchain a suitable guaranteed method to record events and transactions in chronological sequence. Any data processing that requires the recording of transactions with such integrity and auditability may be a suitable candidate for a blockchain. Blockchains can be particularly useful when participating parties may not have trusted relationship, need a verified record of transactions, the order in which they occurred and the ability to audit them. These characteristics make blockchain very useful for currency transactions (as with Bitcoin and other cryptocurrencies) by essentially preventing digital assets from being copied or spent twice.

Proven chronological integrity and a tamper-evident design creates a trusted environment where transactions can be conducted between non-trusting parties without the need for a formal trusted authority (such as a bank). A blockchain therefore has the potential to reduce the need for certain intermediaries. The potential to eliminate intermediaries that could be overly expensive, or have other negative takeaways, is one of the key reasons for great excitement around blockchain technology.

Potential business benefits may range from lowering transaction costs through automation, to pushing application logic into the network and away from legacy systems. For companies with long supply chains or distribution channels, blockchain could enable much greater visibility into the entities involved in sourcing or distributing products, which would provide greater transparency and certainty around provenance, quality, duration and pricing. Additionally, a blockchain-based platform delivers considerable security and auditability, removing the need for a trusted third party to act on behalf of the trading parties.

4 Blockchain Design

Blockchain ecosystems all bear certain similarities, but have important differences. Three key aspects of each blockchain should be evaluated to understand its applicability to a particular situation: technology designs, governance models and consensus models.

4.1 Technology Design

The technical design of each blockchain determines what type of information can be stored on the blockchain. While all blockchains can store at least certain minimum types of data, they differ in how they support cryptocurrencies, business logic (e.g. "smart contracts" – see Section 7.7), off-chain transactions and other data structures.

4.2 Governance Model

Who is in charge? Every blockchain has a means for making decisions critical to its operation and evolution over time. A private blockchain that is run by a corporation on its own infrastructure is governed by that corporation, which can change it at will. A blockchain that is shared in a consortium model may

have a governance model where some or all consortium members can vote on changes. A public blockchain, which has no owners, typically embodies a governance model within the technology and database structure, allowing anyone who meets certain criteria to effectively vote on critical changes.

4.3 Consensus Model

How are new blocks created (or in blockchain terminology, "mined"?) Every blockchain has its own process and rules for how new blocks are approved. In a private, in-house blockchain, this may simply be a software module that is permitted to create new blocks at will. If a consortium or group of companies share a blockchain, there may be rules that say all, or some percentage, of the participants must approve new blocks before they can be added. In public blockchains, new blocks are created by miners (participants who collect transactions and try to create new blocks in order to earn cryptocurrency), using one of several approaches.

Each approach is designed to ensure it is effectively impossible for a bad-actor miner to approve new blocks. To achieve this, different blockchains rely on a mix of various factors, including:

- The need for massive computational power – more than any one miner or group can amass
- Competition among miners
- Crypto-economics – create incentives for miners to keep the blockchain healthy (i.e., not join with bad actors to corrupt it) in order to protect their investment in it

5 Types of Blockchain

Starting with Bitcoin in 2008, many different architectures have been developed to meet varying technical, business and governance design objectives. The term 'blockchain' lacks a clear conceptual definition and is used for a multitude of different developments. There are broad differences in properties of various blockchain types such as degree of decentralization, transaction capabilities, consensus mechanisms, accessibility, immutability, scalability or transparency. As a result, blockchain practitioners and the media often make generalized statements about blockchain as if they apply to all blockchains, when in fact the statements only relate to only one blockchain or a family of blockchain technologies. Also, many practitioners believe only a particular form of blockchain is "legitimate." This white paper does not make that judgment, but instead presents the different forms using popular terminology even if it is not agreed on universally.

A frequently used distinction of blockchain types is made based on the accessibility into public (i.e. permissionless) or private (i.e. permissioned). Consortium is a special type of blockchain that is offen considered a distinct type of blockchain, but also falls under the private blockchain type.

5.1 Public/Permissionless

Public blockchains, such as Bitcoin, Ethereum, and many others, offer completely open access and can be read or written by anyone, without preauthorization. Game-theoretical incentives[2] are used to promote trust between unknown nodes. Public blockchains are considered to be fully decentralized. Proponents claim that since developers of applications have no authority to adapt or modify platforms once in use,

[2] Described in https://arxiv.org/pdf/1708.04872.pdf

[3] Coin Center 2016 article "Open Matters: Why Permissionless Blockchains are Essential to the Future of the Internet".

independence and censorship resistance is assured. Based on this characteristic, advocates of public blockchains consider the technology as an enabler for openness, transparency and neutrality[3]

However, without technical or legal mechanisms to enforce compliance, public blockchains may be at risk of devolving into chaos. Public blockchains require strong security and mature governance to engender the necessary trust and confidence among those that would build long-lived commercial or sensitive applications on it.

5.2 Private/Permissioned and Consortium

Private/Permissioned blockchains have emerged as an alternative to public blockchains in order to use the technology among a set of defined, known participants. In a private (permissioned) blockchain architecture, write permissions (the ability to add a record to a database) are granted only to approved nodes. Complete or limited read permission may be made available to all nodes or to the public or entirely restricted.

Private blockchains can be attractive for some business use cases where a certain degree of privacy, auditability and governance is required. All participants within a private blockchain can be identified, but do not necessarily need to trust each other. Limited information may be visible to the public, or not. In contrast to public blockchains, any defined authority can amend the rule set for the blockchain. The consensus mechanism of private blockchains can be much simpler, with a single node or group of nodes having authority to validate new blocks.

A special type of private blockchain (often considered a distinct type) is the consortium blockchain, which can be understood as a blockchain where consensus is derived by an authorized set of nodes, such as nodes belonging to a collection of financial institutions. This type of blockchain can be described as partially decentralized, in that no one node has full control, but neither is any node allowed to join and participate at will.

6 Blockchain Ecosystems

There are multiple ecosystems of blockchain technologies that take advantage of underlying capabilities of the major platforms. Some platforms focus on a set of business capabilities, and some platforms provide technical capabilities to allow a company to build upon its own set of business capabilities. There are many hybrids; this section will attempt to outline major examples for the different types of ecosystems.

1. Bitcoin – the largest and best-known cryptocurrency has a significant ecosystem powering it. The following are Bitcoin ecosystem components and examples of companies providing the components:

    - Exchanges and Traders – There are many exchanges; Coinbase is the current largest for Bitcoin and other cryptocurrencies; bitFlyer and CoinEx are examples of other high volume digital currency exchanges.
    - Digital Wallets – can be built using the open source Bitcoin Wallet. Exchanges will have wallets, but many people prefer independent wallets. The many wallets are usually software-based with some tradeoffs between the ease of use and security. Breadwallet and Mycelium are two examples.
    - Miners – the Proof-of-Work consensus method requires miners to create new blocks. China has by far the largest market share of miners, Bitmain alone has technology which accounts for over half of all mining, both in a supporting role for other miners and its own mining company, AntPool/NEO, which is the world's largest miner.
    - Merchants – retailers such as Overstock.com and Expedia have been accepting Bitcoin as a form of payment since 2014.
    - Infrastructure components – BitGo, GoCoin, and Colu are examples of the large number of companies leveraging BitCoin API Services to provide business services for identity, payment, infrastructure and reporting.

2. Ethereum – with the second-largest cryptocurrency (Ether), Ethereum is the best-known platform for blockchain applications due to its generic flexibility, relative maturity and support for decentralized applications.

    - Ether, like Bitcoin, is bought and sold, and used by investors to buy into Initial Coin Offering opportunities (see Section 7.6). This part of the ecosystem is similar to other cryptocurrency ecosystems.
    - Extensions - Due to the open nature of the platform, some infrastructure and extension products can be considered to be a separate platform. A notable project is Quorum, an open source private blockchain network/platform developed by JP Morgan from the Ethereum code.
    - Applications – A wide variety of applications, from games to commerce to finance to gambling and other topics, has been developed. A curated list of over 1,600 apps can be found at https://www.stateofthedapps.com/.

3. Ripple – the third largest cryptocurrency, this ecosystem is focused on payment/banking services based on XRP tokens. As a result, the ecosystem includes merchant and consumer processors, gateways and integrators. Ripple references its ecosystems' solutions at https://ripple.com/solutions/.

4. R3 Corda - a capabilities platform like Ethereum but without a coin. R3 Corda started as an alliance of nine financial institutions in 2015 and has evolved to a network of over 200 financial institutions, buy-sides, insurance companies, technology companies, software firms, central banks, regulators and exchanges. R3 explains its ecosystem at https://www.r3.com/ecosystem/.

5. Hyperledger – a set of open-source blockchain projects founded by the Linux Foundation that is targeted to be the major enterprise-grade permissioned blockchain. Of note, IBM and Intel are two companies that are very active with Hyperledger, and other members can be found at https://www.hyperledger.org/members. A list of the projects can be found at https://www.hyperledger.org/projects.

6. Microsoft's recently announced Coco is an open and compatible framework with any blockchain protocol. Microsoft is integrating Ethereum into Coco and will integrate to Quorum, Hyperledger Sawtooth and Corda.

7. Other Blockchain ecosystems – There are many more significant blockchain ecosystems, including NEO (a variant of Ethereum that is popular in China), Waves, EOS, Steem and BigChainDB.

8. Distributed Ledger Technologies (DLTs) are sometimes referred to as blockchains, but they technically lack some of the characteristics of blockchains. Some practitioners refer to them as superior blockchain alternatives. Some of the better known DLTs include IOTA, Hedera Hashgraph, SDEX, Railblocks, and ArcBlock.

The blockchain ecosystems that are most commonly used for enterprise business development are those that offer capabilities such as smart contracts and simple integration. Ethereum is a relatively mature platform for smart contracts, and Ethereum-based blockchains Burrow and Quorum are popular solutions focused on the enterprise. Hyperledger projects are targeted for the enterprise. One project, Hyperledger Fabric, is intended as a foundation for developing applications or solutions with a modular architecture; it also supports smart contracts.

Similar to Hyperledger Fabric, Corda is a product designed from the ground-up for enterprise networks and is commonly used by banking institutions.

7 How Blockchain Works

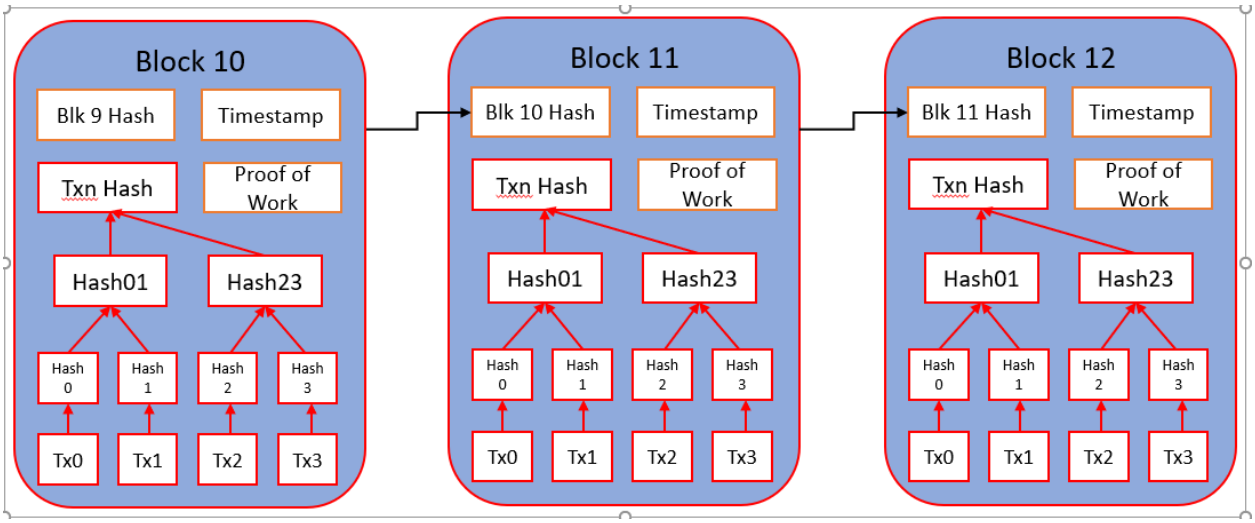
7.1 Data Structure

The data recorded in a blockchain is shared by all participants using that blockchain. These participants have access to the same information that is structured in a way that ensures no data can ever be suppressed or modified without blockchain collaborators becoming aware and likely rejecting the attemped changes.

A blockchain, as the name suggests, is a chain of blocks. Each block is made up of multiple transactions which have been grouped in order to be applied into the network together. It also comprises a string of characters to uniquely identify that block. This digital fingerprint is simply the result of a hash function, the role of which is to transform any input of data it receives into a string of seemingly random characters, such as “fhf74ed85e189gf7bgk7863jir85zdg8.” In a hash function, it is very easy to verify whether the input and output match, but impossible to determine the input from the output.

When a new block is added to the blockchain, its hash value is computed using the preceding block’s hash value as input data. Any attempt to tamper with or remove a block will automatically modify the hash value, making it obvious to all that something has changed. This is also how links between blocks get created. Discrepant records automatically identify tampering, therefore blockchains are said to be tamper-evident. The rules of each blockchain ensure that tampered records will not be propagated across the distributed ledger.

The figure below depicts the conceptual structure of blocks for a blockchain such as Bitcoin or Ethereum where blocks are added based on the “proof of work” concept. Individual transactions are at the bottom, and are hashed individually, then the hashes of adjacent transactions are hashed together, and this process repeats until there is a single hash that is unique to all of the transactions combined. The “proof of work” is a number that solves a cryptographic puzzle based on all of the other fields; it is by design difficult to solve, but simple to verify that it is a valid solution. As the name implies, it provides proof that the necessary work was done to solve the puzzle before the block was added. Each block includes a hash of the prior block to ensure the entire chain can be validated.



7.2 Role of Miners in a Public Blockchain

Certain blockchain participants, known as miners, play a key role in public blockchains by creating and adding new blocks. Depending on how blocks are added, their tasks in a private blockchain may be reduced. Miners, which are actually nodes on the network that volunteer to participate in the process, can be thought of as industrious ants whose role is to methodically add blocks to the blockchain.

The process of mining takes place in several steps:

- Whenever they are not working on a block, miners look for new transactions to process. As they find them, they group them into a block.
- Multiple miners do this at the same time, competing to add the next block. A contest takes place to do so, using the rules of the particular blockchain. When a miner creates a block that satisfies the rules (meaning they have created a block with a hash that other miners can verify),
    - The contest winner:
        - Pockets the transaction costs that senders had included in their transactions in order to incentivize miners to include them in the new block.
        - May earn a predefined amount of the blockchain's native cryptocurrency; this subsidizes the mining costs and provides an effective incentive to grow the base of miners.
        - Adds the block to its copy of the blockchain.
        - Broadcasts the new block to other nodes.
- Other nodes verify that the added block contains valid transactions, that the rules of block creation were satisfied, and that the hashing was computed correctly. If so, then they add it to their copies of the blockchain. Dependent on the rules of the blockchain, either once a majority or a certain volume of nodes have broadcasted approval, the block is considered added to the blockchain.
- Conflicts can arise if two miners are successful at creating blocks at roughly the same time; these get resolved by the consensus rules of the blockchain. Blocks that will ultimately be rejected may exist on certain nodes of the blockchain for a period of time while the other nodes are evaluating their correctness. Due to this, new blocks are generally considered permanent only when enough new blocks have been created on top of them to make it computationally impractical for modifications to be made. A common guideline is that a block's transactions can be considered confirmed when six new blocks have been added after it.

7.3 User Access

Blockchains are typically accessed via application programming interfaces (APIs) built to perform specific operations, which may range from simple ones (such as "I want to send a Bitcoin to Alan") to complex ones that may perform multiple operations and create multiple transactions. For public blockchains, APIs are maintained in open-source libraries (most commonly github). These APIs are freely accessible by anyone and can be modified by the open source community under a defined consensus model.

Most private and consortium blockchains are also accessed via APIs, but these may or may not be accessible to the general public (and if they are available, the functionality may be restricted). A public blockchain targeting a particular industry or type of transaction may, if successful, result in an active open-source community that creates APIs that become the de facto standard for transactions using that blockchain.

7.4 Cryptocurrency and Gas

Public blockchains need a cryptocurrency in order to function, and that cryptocurrency may not be core to the value proposition of the blockchain. In the case of Bitcoin, the value proposition is itself the cryptocurrency, but in many blockchains the cryptocurrency's main use may be only to provide economic incentives to miners to maintain the blockchain.

In a public blockchain, miners are incentivized to add transactions to new blocks by an amount of cryptocurrency (called "gas") that is designated within the transaction. The miner that successfully creates a block receives, as at least part of the reward, all of the gas fees designated in those transactions. Transactions may be added to the blockchain faster by designating higher amounts of gas to entice miners to select them sooner.

A typical transaction might be to transfer 100 units of a cryptocurrency from one account to another, and might specify a gas fee of one unit. In this case, when the transaction is added to the blockchain, the chain will show the sender's account having 101 units less, the receiver's account having 100 units more, and the miner's account having one unit more. In other cases, the transaction may have nothing to do with cryptocurrency (it might, for example, be making a public record of a contract), and only the gas fee changes hands.

7.5 Derivative Cryptocurrencies

Starting with Ethereum, many blockchain ecosystems provided the ability to create derivative cryptocurrencies. These may be exchangeable, under some set of rules, for the base cryptocurrency (such as Ether for Ethereum). These derivative cryptocurrencies may be used to create ecosystems to support specific applications, either as an exchange of value between participants, to compensate participants for intermediary roles or to pay the gas fees of the underlying ecosystem. For an Ethereum derivative, the transactions are still added to the Ethereum blockchain and require gas payments in Ether, but the participants in the derivative chain settle in the derivative cryptocurrency.

7.6 Blockchain Funding

It is often said that Initial Coin Offerings (ICOs) are like venture capital for blockchain-related startups. The truth is that they are more at the crossroads between an IPO (Initial Public Offering) and crowdfunding. An ICO is an issuance of cryptocoins, where an entrepreneur raises cryptocurrency funds to sustain their venture's growth. Investors can buy the newly-issued cryptocoins, whether for speculative purposes or in order to participate in a blockchain that they fund.

ICO investors typically do not own the company, but participate in any appreciation (or depreciation) in the cryptocurrency value. Additional rewards for investing can be defined by the issuers of the cryptocurrency, who can also reward themselves as the creators.

As of year-end 2017, ICOs had raised just over four billion US dollars[3] following their first appearance in 2013. In the first seven months of 2018, another $6.3 billion was raised[4].

Historically, ICOs had been unregulated, but starting around the end of 2017, numerous national governments either banned them entirely or subjected them to regulatory requirements similar to traditional securities. Many governments are still studying how best to regulate ICOs, and regulatory requirements are therefore very much in flux. For example, after the U.S. Securities and Exchange Commission announced that it would consider ICOs to be security offerings, many ICOs excluded U.S. residents from participating because there was no clear roadmap for compliance.

7.7 Smart Contracts

Smart contracts, first introduced with Ethereum in 2014 and subsequently included in most blockchain ecosystems, are self-executing code blocks deployed on the blockchain which follow decision trees, interact with other contracts, store data and transfer cryptocurrency among users as the unit of currency for payment. Like a crypto-coin, a smart contract can be examined[5] but not altered by anyone who has

[3] https://www.statista.com/statistics/863762/vc-vs-ico-funding-globally/

[4] https://www.icodata.io/stats/2018

[5] Ethereum smart contracts are written in the Solidity language and are translated into bytecode for storage on the blockchain. The bytecode is not directly human-readable but can be examined

access to the blockchain. This enables the automation of agreements between counter-parties, creating the potential for significant efficiency. Smart contracts can also be designed to execute indefinitely, thus providing all parties to the contract with a high degree of transparency and the trust that its stipulations will be carried out.

Smart contracts can enforce business logic, such as releasing funds upon fulfillment of certain requirements of a transaction. A good example would be that of an insurance company insuring farmers against droughts. The smart contract can be set up to automatically unlock the funds if and when the rainfall totals fail to reach a predetermined level.

Smart contracts can also be used as backend code, stored on decentralized servers. In this case, they are referred to as decentralized applications (or dApps). Because they are stored on the blockchain, they are transparent to all parties and immutable; and they will run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference.

7.8 Governance

Successful blockchains need to adapt and change over time. While private blockchains can be changed at will, public and consortium blockchains are each governed by a consensus model with specific rules built into the blockchain logic. Governance defines the economic incentives to participants, the rules for creation of cryptocurrency and the rules for modifying the blockchain to address evolving needs or challenges.

programmatically and, with some difficulty, reverse-engineered. In many cases, the Solidity code is stored in a public database and can be examined directly by humans.

The number of governance models is almost as large as the number of blockchain ecosystems, and new ones are born every day. While a full treatment of this topic is beyond the scope of this white paper, it is often said that governance is the single most important factor in determining whether a blockchain ecosystem can succeed. Are the economic incentives adequate to encourage all necessary participants? Can the integrity of the blockchain be guaranteed? Can the blockchain evolve and change in the future?

8 Challenges, Risks and Governance Considerations

Like any relatively new technology, blockchain has many challenges, and especially after the introduction of Ethereum in 2014, resulting innovation to address them. The biggest challenges are specific to public blockchains, or are at least easier to manage or compensate for in private and consortium blockchains. Applications that require a public blockchain are often dependent on future innovations to overcome current limitations, although they may well be supportable in private or consortium blockchains today. In some cases, the tradeoffs may be acceptable, in others, not.

The most common challenges that are cited for blockchain technology are transaction speed; block size; cost; governance, regulatory and international issues; talent and skill set; technical risks; financial risks and blockchain scams.

8.1 Transaction speed

Public blockchains do not currently support the near-instant confirmation times expected for many types of transactions. Ethereum blocks are currently written about every 15-20 seconds and transactions may be added to the next block unless the sender offers a large enough financial incentive (meaning cost). Based on its current design, Ethereum can process only about 15 transactions per second. In addition, most participants will not consider a transaction truly confirmed until as many as six additional blocks have been added after, since the likelihood of a block being rejected diminishes significantly as additional blocks are added on top of it. Enhancements to Ethereum are expected to improve its speed and/or allow more transactions to be handled off the main blockchain, but in the near term it will still handle only a small fraction of what traditional technologies can. Transaction speed is generally not an issue in private blockchains because added blocks do not require computational overhead.

8.2 Block size

Most common blockchain ecosystems have block size limitations that impact not only the transaction speed, but also the amount of data that can be stored on the blockchain. Due to this, it is recommended to minimize the amount of data stored on the chain. Some ecosystems, such as Ethereum, have integrated “side” storage capabilities such as Swarm and IPFS that maintain many key features of blockchain data storage without creating records on the main blockchain.

8.3 Cost

The current “proof-of-work” approach to validating new blocks, used by the common public blockchains including Bitcoin and Ethereum (but not by private blockchains), is computationally very expensive and requires enormous amounts of electricity. As of early 2018, Bitcoin alone required more electricity than what was used by the entire country of New Zealand. Combined with limitations on block size, this

creates scarcity and high transaction costs. For several years, Bitcoin rarely cost more than $0.25 per transaction, but in early 2018, it hit a high of $54.90 per transaction.

New validation approaches are much less computationally taxing and offer the promise of much lower costs., making them a current major focus in public blockchain innovation. The planned Ethereum Casper protocol is currently in test and uses “proof-of-stake” to validate transactions rather than “proof of work.” The NEO blockchain uses an approach called Delegated Byzantine Fault Tolerance.

8.4 Governance, Regulatory, and International Issues

8.4.1 Jurisdiction/Governing Law

Decentralization introduces some difficulties with regulatory issues. Blockchain nodes can be anywhere in the world so they can therefore cross jurisdictional boundaries. Public blockchains have no central oversight authority and rely on their programmed governance models for decision making. While public blockchains may be immune from government intervention, governments can (and increasingly do) regulate the actions of individuals interacting with them.

8.4.2 Liability and Risk Management

Given that a public blockchain is typically designed to not be controlled by anyone, the inability to control and stop its functioning can pose a risk when the blockchain is not functioning properly. Blockchains are driven by computer code, and are therefore subject to bugs and security flaws. The risk of a malfunctioning blockchain service must be thoroughly considered in regards to the risk and liability to all participants including vendors, suppliers, partners, customers and anyone else affected by the potential issues. While no public blockchains have been hacked at the time of publication of this document, cryptocurrency wallets have been compromised, and cryptocurrency balances have been made permanently inaccessible by buggy code. Private and consortium blockchains may be more prone to hacking, so contracts need to address liability and risk.

8.4.3 Data Privacy

Information stored on a blockchain is immutable and therefore has implications with respect to data privacy, particularly when the relevant data is personal data or enough data to reveal someone’s personal details. The transparency of transactions on a blockchain is also concerning; in some cases it may be incompatible with privacy standards.

To address this, technology-based solutions must be found to create privacy-protecting blockchains. This might include limiting who can join the blockchain to trusted nodes, limiting which nodes can approve transactions, encrypting the data on the blockchain or storing some data off the blockchain protects privacy.

In regard to the recent General Data Protection Regulation (GDPR), privacy by design is a requirement, along with the right to access data and the right of consumers to have their information removed from the database. A blockchain does not support the deletion of information, so the design of an application that includes personally identifiable information needs to consider methodologies that will meet the GDPR requirements, using encryption, off-chain storage or other solutions.

While some aspects of GDPR are challenging to implement in blockchain, the security of blockchains can help satisfy the GDPR requirement for “appropriate technical and organizational measures to insure a level of security appropriate to the risk.” The use of a private blockchain can also be useful to meet the requirement of data subjects being allowed to control their data.

Potential compliance problems can arise with the use of a public blockchain, which can expose personal data to individuals who should not have access to the data. However, even private blockchains can present problems with cross-border data transfer, and the rights of data subjects to rectify or erase their data. In all cases, the data privacy requirements of legal jurisdictions will be important.

8.4.4 Enforceability of Smart Contracts

With automatic execution of smart contracts in public blockchains, there is no longer any central authority (such as courts or arbitration) to resolve any ambiguities or disputes that arise, or even to enforce court or regulatory orders. To address this, customers should ensure smart contracts in public blockchains accurately implement the desired functionality because there is no recourse if they are wrong. In private or consortium blockchains, contracts can include a dispute resolution provision.

8.5 Talent & Skill Set

Blockchain is an extensive and complex discipline with a large community of talent available, but talent is not cheap[6]. A company with an urgent blockchain requirement may be well served to hire at least some of their talent, while companies more interested in just understanding and exploring may be able to build their talent internally.

The base of talent for blockchain applications and technical implementation is growing very rapidly, but as with most subject matters, the quality of the talent can widely vary. Given the probable significant impact blockchain will have on enterprises over the next 10 years, any business that anticipates deploying the technology is advised to acquire some degree of expertise through staff development or by retaining third-party experts.

The scarcity of expertise implies that finding quality talent may be expensive. Similarly, a company may need sufficient internal competence to ensure vendors can be effectively managed to deliver desired results.

Businesses should also be aware that many so-called blockchain experts may make sweeping generalizations that in reality apply only to certain blockchain platforms and not others. Heeding such generalizations without examining them closely may lead to bad decisions that harm the achievement of business objectives. To that end, a wide range of blockchain communities – both online and real-world – are available to help. Educating team members in all aspects of blockchain from trading, mining, smart contract programming, ICOs and dApp creation, will aid in understanding the overall opportunity. Some resources are listed in Appendix Section 14.3 of this document.

8.6 Technical Risks

Blockchain technology is evolving rapidly, and like many technologies, change is not always backward compatible. Risks include “hard forks,” where a blockchain changes the rules for the future but allows participants to continue on either the new rules or the old ones. Participants can choose one or the other, but if there is one participant that chooses one and everyone else chooses the other, that single participant may be left behind. There is also the risk that the blockchain ecosystem a company chooses today will fail, or even just fail to evolve as fast as others, forcing a future change.

Smart contracts are a relatively recent innovation, and as a result, are less well tested than more mature technologies. This lack of maturity may cause future issues because once embedded in a blockchain, smart contracts cannot be modified even if the smart contract is erroneous.

Blockchain technologies have the risk of hacking, corruption, bad governance models, and in some cases, improperly coded smart contracts. Public blockchains also have the coding risks inherent in any

[6] https://www.computerworld.com/article/3235972/it-careers/blockchain-jobs-continue-to-explode-offer-salary-premiums.html

open source community. All of these complications have parallels in the non-blockchain world, but require a different set of skills to diagnose, assess and prevent.

8.7 Financial Risks

Commercial enterprises will need to develop risk management strategies to prevent internal fraud since the controls embedded in the legal and financial system protect financial assets, such as bank accounts, are inappropriate for cryptocurrencies and other transactions settled on the blockchain.

8.8 Blockchain Scams

In the case of many new technologies, the first people to become experts are often criminals and fraudsters. Business executives and the general public are largely unaware of how blockchain technologies work, and will often assume protections are in place to prevent scams. These protections may be available, but may require use of the blockchain in a particular way (or even in some cases an intermediary to manage trust). If the lessons from the Internet are meaningful, bad actors will continue to invent new ways to scam money for decades to come. As each new innovation is built on top of blockchain, fraudsters will find new vulnerabilities and perpetrate new scams targeting the blockchains themselves, the systems that use them and the people that control them.

9 Characteristics and Uses of Blockchains

Primary characteristics of blockchains:

- The stored data is immutable
- The data is auditable
- They maintain a history of the data as its added
- They protect data integrity using cryptographic tools
- They maintain decentralized transactions with no need for a central authority

Immutability means it is not possible to change data once added to the chain. Data hashes and digital signatures allow data verification to ensure the data is intact. This means that blockchains are a potential solution when:

- There is limited or no trust between participants
- The information needs to be transparently shared and accessible by all participants
- Participants need the ability to audit or verify the integrity of shared data
- Records need to be captured and stored without the possibility of modification
- The amount of data per transaction is relatively small
- The data is shared, distributed between peer systems and not centrally hosted
- Steps of complex multi-party transactions need to be enforced
- Cost can be taken out of existing processes by removing inefficient and/or monopolistic intermediaries, or the administrative effort of record keeping and transaction reconciliation

These characteristics make blockchain ideal for incrementally growing data collections, such as ledgers, transaction logs and log files, when sharing the data and maintaining data integrity.

There is a cost for this integrity and auditability therefore not every technology problem can or should be addressed using blockchain. While it can be an extremely powerful technology, traditional (centralized) database technologies are better suited for many needs. In general, blockchain may not be a good choice if transaction speed and scalability are important.

10 Use Cases in Other Industries

Blockchain technologies of all varieties are in active use in many other industries. While most applications are still proposed, immature and/or under development, others have now been deployed long enough to be considered viable. While details are beyond the scope of this white paper, some highlights of systems reported to be in live production or advanced testing include:

- Supply chain management (deployed by Walmart to track product recalls, De Beers Group for diamond provenance and Chinese e-commerce site JD.com for meat quality)
- Enhancing freight, fleet and logistics management to gain real-time visibility into global transportation and shipping across all transportation modes and industries (SAP Transportation Management TradeLens)
- International bank payment clearing (Ripple blockchain in use by American Express, UniCredit, UBS, Santander and others)
- Voting and voter registration (live for voting on municipal issues in Moscow, voter registration in Switzerland shareholder voting for stock exchanges in Toronto and South Africa)
- Insurance companies such as AIG are using a smart-contract-based blockchain to save costs and increase transparency
- Academic records, allowing an individual to share their grades with universities, employers, etc. (deployed by Malta's government)
- Secure storage of real estate records such as land titles (National Agency of Public Registry in the country of Georgia); settlement of real estate transactions (in Kiev, Ukraine)
- Secure storage of data captured from security cameras (US Department of Homeland Security)
- Storage of tax records and electronic invoices (Misocai Network in China)
- Storage of inventory and maintenance data (Russian rail operator Novotrans is using for its rolling stock

11 Potential Use Cases in Hospitality

11.1 Distribution

11.1.1 Availability, Rate and Inventory (ARI) Updates

There are many disparate private databases in travel distribution that must be incrementally and endlessly synced in close to real time. Property management systems, central reservation systems and others serve as a first stop for all property-level data. These systems connect to channel managers, global distribution systems and other 'switches.' Then these further sync the same data sets with online travel agencies (OTAs), traditional travel agencies, tour operators and other customer-facing sales outlets. Differences in how these systems handle, process and send data in various formats enables an entire ecosystem of resellers and wholesalers that arbitrage these systems. The end result is the original owner of the inventory potentially paying commissions or fees to multiple third parties for a single reservation. If availability and rate information was available in a public data source such as a blockchain, suppliers would be able to quickly and easily update information. Consumer-facing sales outlets would be able to access it with full confidence in its accuracy, without the use of redundant intermediaries. Fees for technology services underpinning the travel industry would decrease, enabling more inventory online, at lower costs to hotels.

11.1.2 Descriptive Content

Hotels and their distributors are challenged to keep descriptive content up-to-date. Text descriptions, photos, videos and other content are constantly updated by hotels as they refurbish, rebrand or open new facilities. A blockchain could provide a unified location where all hotels could register and/or store their rich content. Or, as with ARI, point to a public API through which it can be accessed, enabling all distributors and other online resources (chain CRSs, GDSs, OTAs, metasearch, etc.) to keep content up-to-date without the need for many disparate connections.

11.1.3 Payments for Bookings

The idea of using blockchain for payment is very natural. Blockchain was first introduced in the financial world with Bitcoin. Other blockchains are gaining traction among banks for international currency settlement. Payments are an important aspect of travel distribution as well, and certain kinds of transactions may lend themselves to blockchain solutions.

A large portion of hotel payments are settled by credit card. These transactions can include transient bookings, group master bills, corporate accounts, payments for room-block sales to wholesalers and tour operators, and more. Credit card fees typically range up to 2.5% of the amount charged. In addition to providing financial settlement, credit cards provide additional benefits: the seller gets the funds or (with non-advance purchase consumer bookings) a guarantee of payment in advance, while the buyer typically benefits from consumer protections that are enforced by credit card companies.

Cryptocurrencies can be used to settle any or all payment obligations including deposits, advance payments, commissions and other fees. This can potentially reduce the cost associated with traditional financial settlement methods, such as payment cards and bank transfers. Participants in a transaction must be willing to acquire and use the relevant cryptocurrency, which may be a barrier (particularly for consumer-facing applications) unless and until cryptocurrencies are more widespread. Additionally, participants must be willing to forego any legal protections offered by traditional payment methods.

Smart Contracts are a way to include terms of a contract with a payment. This has several potential applications across the travel industry, for example the smart contract might be set up to release funds to a hotel according to a deposit schedule and/or a cancellation policy, or it may send them only upon check-in or completion of a stay. The automatic nature of smart contracts can save work associated with collecting payments or processing refunds, while maintaining full auditability.

Using a blockchain cryptocurrency for settlement instead of a credit card could (for the cost of a blockchain transaction) eliminate the credit card fee in cases where (a) the buyer can reasonably be expected to have, or to acquire, the cryptocurrency; and (b) where the consumer protections are not very useful. At least today, B2C applications are unlikely candidates, because most consumers will not have the required cryptocurrency, or be willing to acquire it; they also rely on the credit card companies to protect their interests in the event the hotel fails to deliver. B2B applications may make more sense. A corporate travel department, meeting planner, wholesaler or tour operator of any reasonable size would have ongoing payment needs large enough to justify acquiring the cryptocurrency. Additionally, the relationship between such bulk buyers and hotels typically includes a contract and a degree of trust that mean that the consumer protections of credit cards (if they even apply) are far less valuable.

A notable downside of using cryptocurrencies for payments is the often high volatility in the value of the cryptocurrency relative to fiat currencies, which in the current environment introduces a significant element of exchange risk to financial transactions. Additionally, accounting valuations for crypto-currencies may create challenges.

11.1.4 Coordination across Multiple Suppliers

Travelers often reserve a hotel stay, an airline flight and ground transportation in a single transaction. Smart contracts could handle payments and commissions to each, and could also enable coordination during the trip. For example, if the traveler does not check in for the flight, the hotel and rental car supplier could know that and take appropriate action, such as releasing inventory for sale to someone else.

11.1.5 Tax Compliance

One of the major headaches in distribution today is compliance with many layers of tax policy. One reservation could be subject to taxes at the city level, county level, regional level (intra country), country level, and inter-country level (European VAT). By practice or regulation, some of these may be included in the base room rate, and others may not. If the taxing authorties could post tax structures to a public blockchain, it would enable sellers of travel to always charge the appropriate tax level and reference each

fee back to the confirmed tax in the blockchain. Smart contracts could then cause remittance of taxes to occur automatically, and the paying entities would have proof of compliance.

11.1.6 Innovation Through Apps

Blockchain technology could rapidly increase the pace of innovation in travel technology, through the use of open APIs. A new application would no longer need to separately contract with dozens to hundreds of companies, each with their own private databases of availability, rates, tours, content, etc, just to assess feasibility and potential demand for the new service. By lowering the barriers to entry in this way, new services can come to market faster than today.

11.1.7 Enabling Direct Bookings

Since blockchain has the inherent capability to reduce or eliminate the need for intermediaries for rate, availabilities, confirmations and payments, it can help hotels reduce their dependence on intermediaries. This does not mean that a consumer who is currently using an online travel agent will have a reason to book direct just because of blockchain, but blockchain may offer a useful alternative for many types of bookings that use intermediaries for transactional convenience (corporate, wholesale,group bookings, etc.). Open APIs with availability and rate data can make it much easier for hoteliers to offer competitive rates to direct customers and new, lower-cost distributon channels, since the rates that third parties are using will be more transparent than they are currently. Being able to easily consume competitor's published rates could also simplify revenue strategies and improve price transparency.

11.2 API Accelerator

If public blockchains take hold in hospitality, the associated open-source application programming interfaces (APIs) could facilitate rapid innovation. Open source APIs can serve as de facto standards, incorporating changes from all quarters to maximize their ability to meet evolving industry needs. To the extent they are widely used, they become an important source of simple interoperability, ensuring that a new application developer, for example, can use the same API to get availability, rates or inventory, or to confirm a booking with any hotel.

11.3 Loyalty

While blockchain could be used by a loyalty program to manage the accounts and transactions for program members, the more interesting use cases involve using blockchain to enable connectivity with additional business partners. Some of the advantages of using blockchain in loyalty management are real-time transaction processing and reconciliation, cost, managing the logic for points exchange, managing and operationalizing contracts between loyalty players via smart contracts and providing a full audit trail.

Loyalty programs typically involve several types of transactions that could be processed on a blockchain.

- Transfers of loyalty points between accounts, including issuing points (of the operator or a partner) to an individual member; redemptions of points with the operator or a partner; and wholesale buying and selling of points between partners.
- Enabling exchange of points between loyalty programs by enabling direct connectivity among multiple cooperating loyalty programs (under rules established by each program, which can be programmed into smart contracts).
- Bundling redemption offers across multiple partners: complementary suppliers, such as airlines, hotels, rental car companies or restaurant chains often want to create packages that are attractive to customers. These could be constructed with smart contracts that enable the blockchain to manage the allocation of value across all entities participating in a transaction.

Currently, not all loyalty transactions are economically feasible on a public blockchain because the cost of the blockchain transaction can be prohibitive for low-value transactions. This may change over time; in the meantime, alternatives such as private or consortium blockchains, or mixed processing strategies, are being used. Other challenges include the current lack of blockchain-enabled partners and potential compatibility issues between multiple loyalty blockchain ecosystems.

11.4 Identity & Data Privacy

While not specific to the travel industry, blockchain initiatives around personal identity and data privacy have substantial application in travel. Hotels, as well as airlines and rental car companies, have critical needs to be able to verify the identity of customers, and in many countries to validate their right to travel and/or to report travel activities to governmental authorities.

The basic concept would be to use a blockchain to enable travelers to upload their own personal information, which would then be shared under a set of rules (presumably consistent with regulations such as GDPR) with the travel suppliers with whom they make reservations. Governmental authorities could add biometric information (such as facial recognition) that would enable airport security, immigration authorities, airlines, hotels and rental car companies to verify the identity of the person by matching the biometrics to the authenticated record on the blockchain. Governments could also add information such as passports and visas, which could then be used in place of paper documents to verify a traveler's right to enter or exit a country.

Travel reservations could also be added to the blockchain, enabling suppliers to tap into personal information without the need to store it themselves. Hotels that are required to submit reports to police or immigration authorities could simply report to the blockchain the guest's arrival or departure, so that authorities could automatically obtain the necessary reporting from the blockchain itself.

A number of governments, airlines, airports, hotel companies and other parties collaborated in describing such a future ecosystem under the auspices of the World Economic Forum. Their recommendations, released in early 2018[7] and presented to world leaders at the Forum's conference in Davos, offer a revealing glimpse at an important potential use case for travel.

12 Why Do Something Now?

New technologies are inherently risky, and blockchain is still in its early days. Early movers get the advantage of learning the new environment sooner than others, and of being in a position to better evaluate alternatives as they mature. But, early movers also face risks of using technologies that may ultimately be superseded by incompatible replacements.

Businesses with needs that blockchain appears to meet better than alternative technologies should evaluate whether they are better off starting now, or waiting until a later stage of blockchain maturity. Relevant considerations include:

- Disintermediation of the business model: If there seems to be risk of disintermediation, there probably is, and the relevant questions are how much risk and how soon. Doing something may not only address the risk of disintermediation, but also the opportunity to influence a new or modified business model. So, starting now may provide earlier insight into potential strategic threats.

[7] http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf

- Disintermediation of partner networks may cause current supply chains to change or even see a rapid demise; this may be particularly important in distribution, with its complex chain of partners. If competitors are faster at adjusting to a more efficient network, they will gain strategic advantage. Competitors may then suddenly start offering superior quality at a lower cost because they are prepared for change.

- Organizational impacts: decentralized technologies like blockchain will impact organizations at every level. The number of inquiries IT will need to field will grow as the marketplace creates new solutions for human resources, procurement, operational departments, compliance, finance, accounting and security. The future pace of change will accelerate as blockchain intersects other emerging technologies like the Internet of Things (IoT) and Artificial Intelligence (AI). There is a limit to the technical debt that your organization can reasonably tolerate, so it may be preferable to gain at least some experience with the technology early on.

- Evolving and multiple operating models: Since there are no clear blockchain 'winners' for each market sector as yet, it is possible that companies will have to develop skills not in 'blockchain' per se, but in multiple blockchain platforms. This may be needed in order to fully interoperate and conduct e-commerce with customers and suppliers, each of whom has multiple platform options from which to choose. That said, developing experience in a single blockchain will help position an enterprise so that it can more fully understand potential future effort and investment.

There may be some disadvantages to moving early:

- The organizational culture may not support an approach to taking controlled and defined risk. For example, if starting a proof of concept, consider how it is advancing organizational knowledge toward a business decision. If that cannot be defined, then it may be of no use.

- The organization may not be armed with basic decision-making criteria or equipped to exercise external forces. For example, an organization may have the desire to use a new tech solution that could advance their business model, but they may not consider hidden expenses of the new and and untested technology (fixation on the solution rather than the problem).

- An early investment in a blockchain project needs to consider the benefits of decentralized networks versus rapid changes in technology and the possibility that blockchain technology itself is not necessarily the optimal decentralized database. The number of options will be growing faster than the market can prune them out.

13 How to Get Started

Having read about the "what" and "why" of blockchain, you may now be eager to get started, whether to tackle a specific project or simply to begin building competencies for the future. What are the first steps?

1. Profile yourself and your organization using Section 12 ("Why Do Something Now?").
2. Determine whether there are particular type(s) of blockchain that you most need to understand (e.g. public vs. private, or a particular ecosystem). Which types are addressing the kinds of challenges your organization may face? This may influence your choice of proof-of-concept or the toolsets you may want to use.
3. Identify a candidate for a blockchain proof of concept whose challenges align with one or more of the scenarios in Section 9 ("Characteristics and Uses of Blockchains").
4. As with any good proof of concept, limit the scope and define success.

5. After identifying the challenges that blockchain can help overcome, make sure the use case is something that adds real value as opposed to something that could be achieved just as well using existing technology. IBM suggests to us that we apply these four "acid tests:"[8]
    a. **Consensus** – is the use case benefiting from agreement across the business network that each transaction is valid?
    b. **Provenance** – is the maintenance of a complete audit trail important in the use case?
    c. **Immutability** – is it important that the train of transactions are tamper proof?
    d. **Finality** – is there a need for an agreed "system of record" across the business network?
6. Choose a blockchain provider or ecosystem based on the best fit for your industry and business needs; this will shape the tools and approach to the project. Table 14.2 in the appendix is an example of current leading blockchain ecosystems. The left-hand column of attributes is a good framework for driving your initial choice.
7. After you choose your platform, you will then need to design, develop, test and if all goes well, deploy to that platform. Initial testing sometimes provides good reasons to consider migrating to a different blockchain ecosystem.

This white paper's scope cannot tell you how to proceed to the point of developing code, but can recommend getting involved in an online community that is focused on your platform.

Some resources that may be useful are listed in the Appendices, Section 14.3.

14 Appendices

14.1 Glossary of Terms

Blockchain terminology has evolved in the past few years. Because of the variations among ecosystems and blockchain communities, it would be difficult to create a definitive list of terms that would not provoke arguments and/or fail to stand the test of time. The authors consider the resources listed below to be reasonable sources for blockchain definitions.

- https://allthingscrypto.tech/blockchain-glossary/ (has significant detail and some additional links, including crypto investing terms)
- https://www.upfolio.com/glossary
- https://blockgeeks.com/guides/blockchain-glossary-fom-a-z/
- https://blockchainhub.net/blockchain-glossary/
- https://hackernoon.com/blockchain-dictionary-f4d098c9f89,

14.2 Some Blockchain Ecosystems and their Attributes

	Bitcoin	**Ethereum**	**R3 Corda**	**Hyperledger**
Mode of operation	Public	Public or private	Permissioned	Permissioned

[8] https://www.ibm.com/blogs/insights-on-business/government/making-blockchain-real-design-thinking/

Description of platform	First generation crypto-currency	Second generation blockchain platform upon which many crypto-currencies are based	Corda is an open source blockchain project, designed for business from the start; allows building interoperable blockchain networks that transact in strict privacy	Modular (extensible) platform
Differentiation	First generation; slow and inefficient	Introduced second generation blockchain technology; the foundation of many other currencies and tokens; relatively slow and inefficient	Blockchain-inspired technology for private networks; strong security and privacy components built-in	Distributed ledger platform for a private industry where partners trust one another
Governance	None	Ethereum developers	R3	Private consortiums
Performance	7 transactions per second	~15 tps	~1000 tps	~3500 tps
Smart Contracts	No	Smart contracts code (Solidity)	Smart contract (Kotlin, JVM)	Smart contracts code (Go, NodeJS)
Consensus	Mining based on proof-of-work	Mining based on proof-of-work, migrating to proof-of-stake Ledger level	Multiple approaches Transaction level	Multiple approaches Transaction level
Currency	Bitcoin	Ether Tokens via smart contract	None Currency and tokens via smart contract	None Currency and tokens via smart contract

Based in part on the paper by Martin Valenta, Philipp Sandner, Franfurt School Blockchain Center. Working Paper: Comparison of Ethereum, Hyperledger Fabric and R3 Corda

14.3 Resources for Blockchain

Some resources that may be useful to those wanting to learn more about blockchain follow.

- Andreessen Horowitz published a list of useful resources at https://a16z.com/2018/02/10/crypto-readings-resources/ and also a second version at https://a16z.com/category/blockchain-cryptocurrencies/
- A McKinsey article discusses the strategic business value of blockchain https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value
- Blockchain at Berkeley Research and Development (https://blockchainatberkeley.blog) provided this link to a number of blockchain related "Deep Dives": https://docs.google.com/document/d/12w7rAEQUSFd6NbLr6dUxJcLbF70YHcnzhG6mHZQjYCA/edit?usp=sharing
- Blockchain Research Institute (https://www.blockchainresearchinstitute.org/)
- Coursera has a free online course by Princeton University about Bitcoin and Cryptocurrencies: https://www.coursera.org/learn/cryptocurrency#
- Goldman Sachs primer on blockchain: http://www.goldmansachs.com/our-thinking/pages/blockchain/
- BlockGeeks community: courses in blockchain development (7 day free trial), free newsletters and articles can be found a https://blockgeeks.com