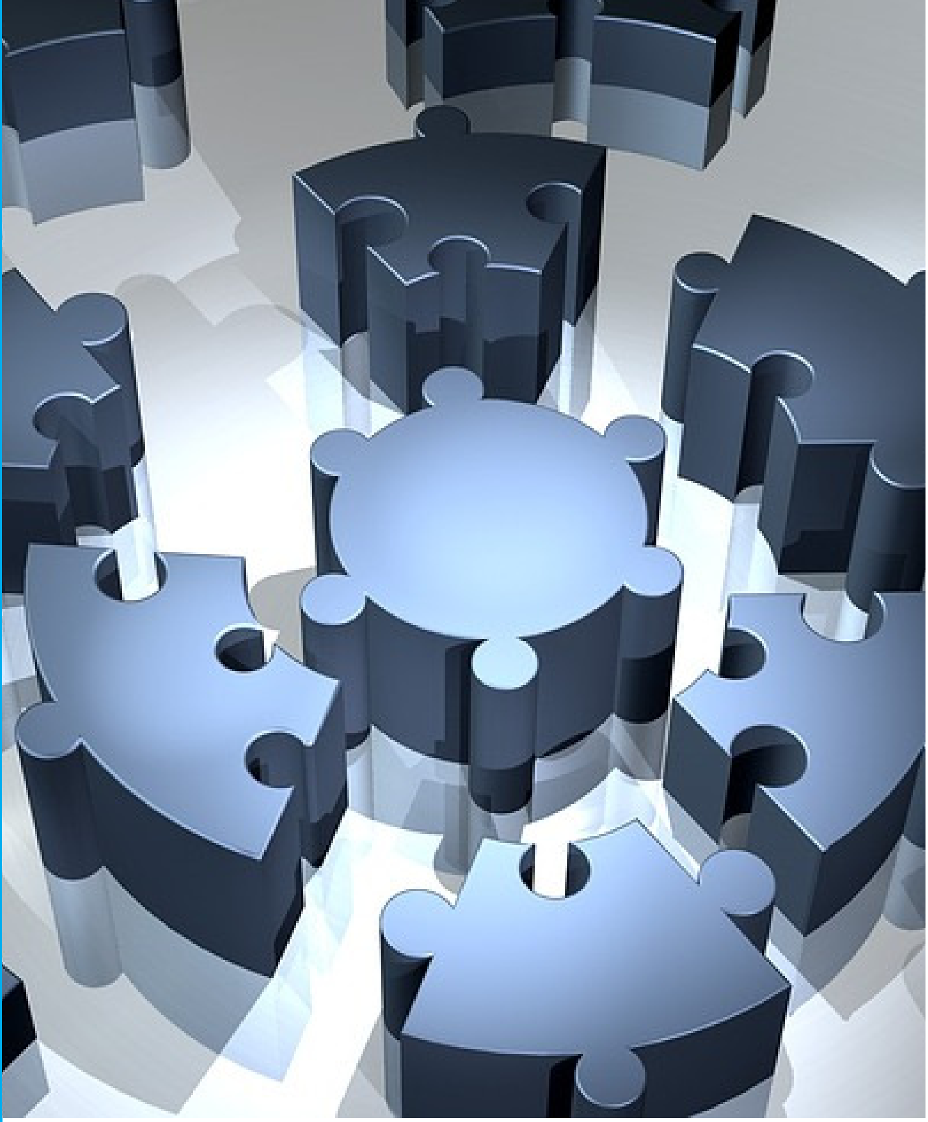


•TECHNOLOGY•RESEARCH HIGHLIGHTS•VISIONS•SCIENCE

330

Blockchain review

BOND project (Blockchains Boosting Finnish Industry) report

Jere Backman | Kristiina Valtanen | Arto Laikari |
Visa Vallivaara | Juuso Ilomäki

VTT TECHNOLOGY 330

Blockchain review

BOND project (Blockchains Boosting Finnish Industry) report

Jere Backman, Kristiina Valtanen, Arto Laikari, Visa Vallivaara

VTT Technical Research Centre of Finland Ltd

Juuso Ilomäki

Aalto University

ISBN 978-951-38-8649-3 (URL: http://www.vttresearch.com/impact/publications)

VTT Technology 330

ISSN-L 2242-1211
ISSN 2242-122X (Online)
http://urn.fi/URN:ISBN:978-951-38-8649-3

JULKAISIJA – UTGIVARE – PUBLISHER

Teknologian tutkimuskeskus VTT Oy
PL 1000 (Tekniikantie 4 A, Espoo)
02044 VTT
Puh. 020 722 111, faksi 020 722 7001

Teknologiska forskningscentralen VTT Ab
PB 1000 (Teknikvägen 4 A, Esbo)
FI-02044 VTT
Tfn +358 20 722 111, telefax +358 20 722 7001

VTT Technical Research Centre of Finland Ltd
P.O. Box 1000 (Tekniikantie 4 A, Espoo)
FI-02044 VTT, Finland
Tel. +358 20 722 111, fax +358 20 722 7001

Cover image: www.pixabay.com

Preface

BOND project (Blockchains Boosting Finnish Industry) started to research Blockchain technology usage for non-cryptocurrency Use Cases in Q4/2016. One part of the project was to create in the beginning of the project an overview of existing Blockchain platforms and tools to support the project work. This report, Blockchain review, was finalised in Q1/2017. During the writing of this report, it was already visible that the Blockchain and Distributed Ledger technologies were gaining momentum rapidly. It is evident that at the end of our project, Blockchain world will look very different, comparing to the time at the start of the project.

Acknowledgements

The authors sincerely thank all the funding partners of the joint research project BOND, Blockchains Boosting Finnish Industry, who have supported us and made it possible to research Blockchain and distributed ledger technologies and produce this report.

Public funding agency

Tekes – the Finnish Funding Agency for Technology and Innovation

Research institutes

VTT Technical Research Centre of Finland Ltd.

Aalto University

Research Institute of the Finnish Economy, ETLA

Companies

3Step IT Group Oy

Boogie Software Oy

Euroclear Finland Oy

Fortum Oyj

Keskinäinen Työeläkevakuutusyhtiö Elo

Kouvola Innovation Oy

Nokia Solutions and Networks Oy

Telia Finland Oyj

Tietomitta Oy

Contents

Preface 1

Acknowledgements 2

1. Introduction 4

2. The Nakamoto Consensus Mechanism 6

2.1 Consensus as an Emergent Phenomenon 6
2.2 Digital Signatures 7
2.3 Stamping Transactions on a Timeline 7
2.4 Peer-2-peer Network 8
2.5 Other Consensus Mechanisms 9

3. Blockchain Platforms 11

3.1 Bitcoin Based Meta-data Platforms 12
3.2 Blockchain Platforms for Financial Applications 13
3.3 Smart Contract Platforms 14
3.4 Consortium/Enterprise Platforms 15
3.5 Sidechain/Anchored Chain Platforms 16
3.6 Multipurpose Platforms and Services 17

4. Widely Adopted Blockchain Platforms and Services 18

4.1 Hyperledger 18
4.2 Microsoft Azure BaaS (Blockchain-as-a-Service) 24
4.3 Comparison of Bitcoin and Ethereum 32

5. Feasibility of Blockchain Technologies 33

5.1 Scalability of the Public Blockchain Systems 33
5.2 Private and Consortium Blockchain Systems 33
5.3 Six Requirements for Blockchain Use Case 38

6. Blockchain Use Cases 40

6.1 Financial Use Cases 41
6.2 Non-Financial Use Cases 43

7. Summary 50

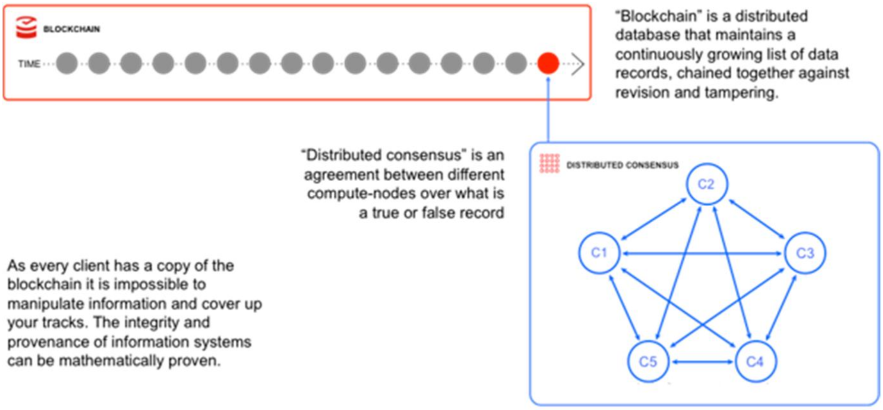
References 52

1. Introduction

Blockchain is a decentralized transaction and data management technology developed first for Bitcoin cryptocurrency (Yli-Huumo et al., 2016). Satoshi Nakamoto is the name used by the unknown person (or persons) who designed bitcoin, created Bitcoin Core (original reference implementation) and devised the first Blockchain database. The Blockchain technology enables maintenance of a shared distributed ledger, Blockchain, which can be simultaneously read and modified by all involved parties but is not owned by any party. This can be implemented with no trust, as in the case of Bitcoin. Another possibility for implementation is limited amount of trust as in the case of consortium Blockchains. The possibilities of the Blockchain technology has inspired and fueled an entire ecosystem around it, focused on fully unleashing its potential. This area has had exponential growth in the past couple of years, leading to a number of platforms, applications, startups, projects and research around this new invention. (Baliga, 2016)

In practice Blockchain is a distributed database solution maintaining a continuously growing list of data records that are confirmed by the nodes participating in it. The data is recorded in a public ledger, including information of every transaction completed. This kind of decentralized solution does not require any third party organization in the middle. The information about every transaction completed is shared and available to all nodes. This makes the system more transparent than centralized solutions. The nodes in Blockchain are also anonymous, which makes it more secure for other nodes to confirm the transactions. (Yli-Huumo et.al, 2016)

Following figure presents Blockchain fundamentals in high level (Guardtime, 2017).



"Blockchain" is a distributed database that maintains a continuously growing list of data records, chained together against revision and tampering.

"Distributed consensus" is an agreement between different compute-nodes over what is a true or false record

As every client has a copy of the blockchain it is impossible to manipulate information and cover up your tracks. The integrity and provenance of information systems can be mathematically proven.

Figure 1. The Blockchain Fundamentals (Gault, 2016).

International electronic financial exchanges have begun to explore the adoption and utilization possibilities of Blockchain technology in their trade processing and reporting for execution and clearing (Peters & Vishnia, 2016). Interest has also arisen in industry domain towards Blockchain's possibilities together with Internet-of-Things (IoT) or Industrial Internet. There haven't been a lot of IoT applications that use the technology efficiently, although the biggest opportunities could be found there. The Blockchain technology offers a disruptive solution to the problem of security and privacy in the Internet of Things environment, providing a new computational layer where data can be safely processed and analyzed, remaining private. (Atzori, 2016)

The rapid development of the Blockchain technology and its various applications has risen need for the guidelines for adopting it. Wang et al. (2016) have researched and presented Blockchain maturity model and its adoption process. The study can be seen as a systematical guide for institutions to adopt Blockchain. Even more important than easiness of technology adoption are the valid and value creating use cases in which the technology will be used as enabler. Greenspan (2015) has presented some guidelines to ensure that a Blockchain use case is valid and the way to avoid pointless Blockchain projects.

This Blockchain review presents technology basics, Blockchain platform review and deep dive to the most popular Blockchain platforms. The feasibility of public, private and consortium Blockchain technology is discussed, and requirements for feasible Blockchain use cases presented. In addition to this, the review of promising use cases, that Blockchain technology has enabled or can enable in the future, has been collected from public sources and materials.

2. The Nakamoto Consensus Mechanism

In following chapters basis for Blockchain technology is presented. The basis includes Nakamoto consensus mechanism, digital signatures, stamping transactions on a time line, Peer-2-Peer network and other consensus mechanisms.

2.1 Consensus as an Emergent Phenomenon

The main invention of pseudonymous creator of Bitcoin, Satoshi Nakamoto, is a decentralized consensus mechanism, which allows pseudonymous participants to agree on the contents of the distributed database: Blockchain. Nakamoto discovered novel ways to use a number of existing technologies which together would form a system with emergent properties, which were previously considered impossible to implement (Fischer et al, 1985).

Following figure illustrates the decentralized consensus between participants (dinbits, 2016)

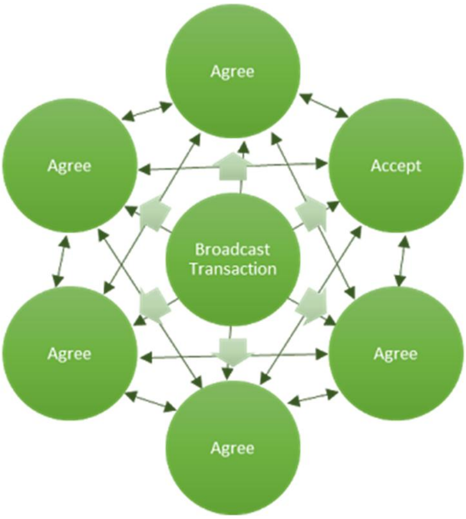


Figure 2. Decentralised consensus between participants (dinbits, 2017).

Nakamoto's system would use internal currency based on public key cryptography to create incentives for mining nodes, who are the ledger's upkeepers stamping transactions on a timeline. Adam Back's proof-of-work scheme (Back, 2002) is used in a novel way to decide who gets to add information on the Blockchain next. Pending transactions waiting to be written on Blockchain are propagated in p2p network.

2.2 Digital Signatures

Public key cryptography is a framework where a key pair is generated and then used to control the access to information. Public key, as the name states, can be publicly available to anyone, whereas private key must be kept secret by the owner. The owner of the private key can use the key to sign any message after which anybody who knows the public key can verify that the signature attached to the message is valid. It is therefore possible to verify that the messages with digital signature have been written by a person who knows the matching private key. Following figure presents the fundamentals of public key cryptography utilization in digital signatures (Driscoll, 2013).

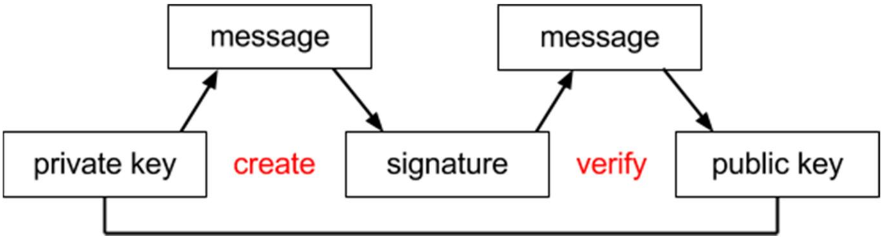


Figure 3. Public key cryptography in digital signatures (Driscoll, 2013).

Bitcoin uses the public key cryptography in a novel way: Bitcoin address is essentially a public key and anybody knowing the matching private key can unlock any funds associated to it. Bitcoin public key can be associated to a bank account and the matching private key to its password, albeit many long term cypherpunks shun this comparison as it’s not 100% accurate.

2.3 Stamping Transactions on a Timeline

Digital signatures can be used to verify that the person trying to spend the money indeed controls the private key, but how can we be sure that she has not spent the money before? It would be entirely possible to sign two separate transactions and send them to two different receivers. Who would then control that the money can only be spent once?

Traditionally there has been a central authority to control that the money can only be spent once, but Satoshi Nakamoto on his paper describes a decentralized framework to tackle the double spend problem. The solution is a distributed time stamp server where a number of transactions are collected into blocks which are then chained together in a temporal order. For a block to be valid, all transactions in it must not be double-spends. Following figure presents an example about chained blocks in timeline (BitGo, 2015).

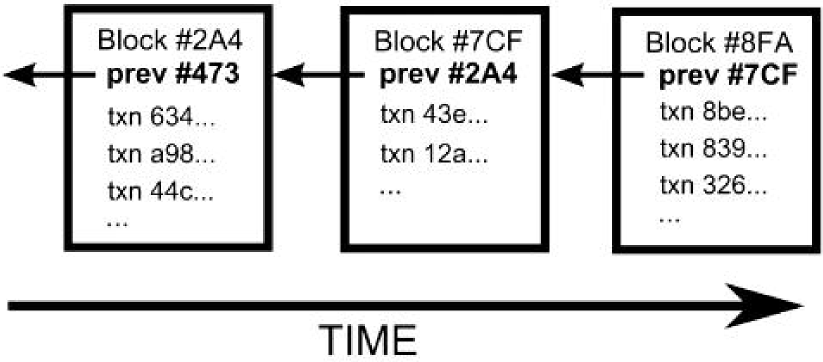


Figure 4. Chained blocks in timeline (BitGo, 2015).

2.4 Peer-2-peer Network

The Bitcoin Network is Peer-2-Peer (P2P) network. Figure 2 presented also the topology of P2P network. The Bitcoin Network is run by nodes which collectively validate the information submitted by other nodes. The process is as follows (Nakamoto, 2008):

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Following figure illustrates the process as practical money transfer example (Financial Times, 2015).

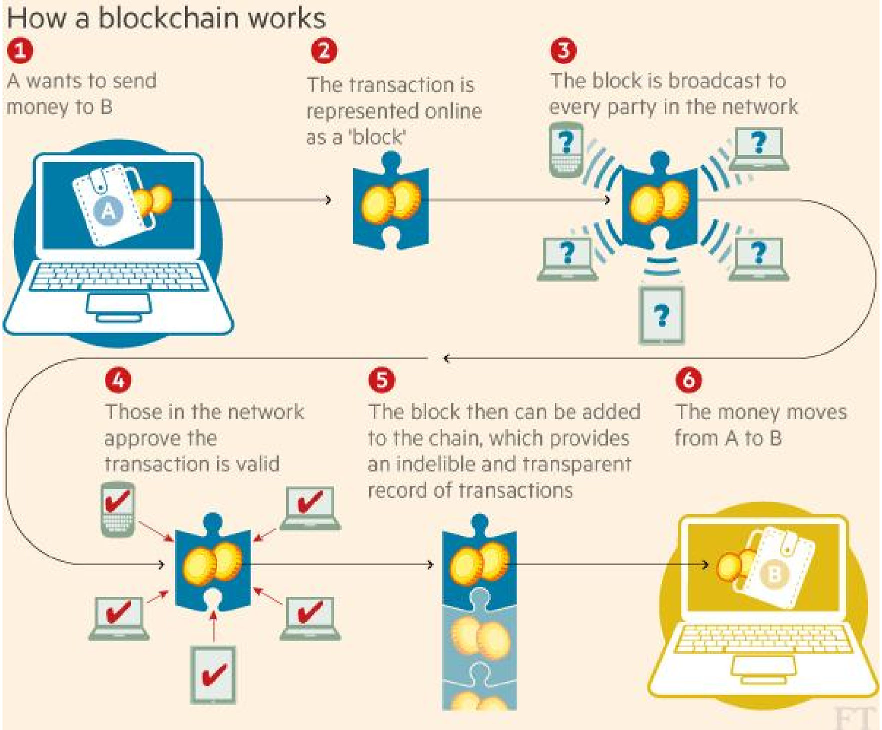

How a blockchain works
1
A wants to send money to B
A
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
?
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
B
FT

Figure 5. Example how a Blockchain works (Financial Times, 2015).

2.5 Other Consensus Mechanisms

A wide variety of consensus mechanisms has appeared, each having its own way of deciding the next valid block. We have identified the following five high-level categories: Computational power based, stake based, disk space based, time based, and user based consensus mechanisms. Bitcoin's proof of work (PoW) and it's variants are well known examples of computational power based mechanisms. (Vallivaara et al. 2017)

Compared to computational power based consensus mechanisms that make use of an external resource, stake based voting requires a cryptocurrency's internal resource, namely coins. The main idea is that, in contrast to PoW, selecting a random node does not require a large amount of resources. The basic idea is that the participant with the most coins has the largest chance to vote for the next block. Peercoin uses Proof of Stake and also Ethreum platform has decided to switch from PoW to staked based Casper. (Sameeh 2017)

The main idea in the disk space voting is to use memory in the computer as resource for consensus voting. The main benefits for this is to tackle the PoW's energy consumption issues. Time based voting doesn't consume so much resources as the previously introduced consensus mechanisms. It achieves the consensus by randomizing who can choose the next block by using the time as deciding factor. In the user based consensus system, the users decide who of the them is the next validator of the block.

3. Blockchain Platforms

Several companies and public organizations/foundations develop Blockchain platforms that are mostly open sourced. The platforms enable fast prototyping, development and deployment of new Blockchain applications. The platforms can be categorized to following categories (Baliga, 2016):

- Bitcoin based meta-data platforms
- Blockchain platforms for financial applications - FinTech
- Smart contract platforms
- Consortium/Enterprise platforms
- Sidechain/Anchored platforms.

In addition to these available are some multipurpose platforms providing for example Blockchain as a service. There are also new kind of platforms under development all the time, including Industrial Internet of Things based on the Blockchain technology. For example, BPIIoT by Bahga & Madisetti (2016). The BPIIoT platform claims to enable peers in a decentralized, trustless, peer-to-peer network to interact with each other without the need for a trusted intermediary in Cloud-Based Manufacturing domain. (Bahga & Madisetti, 2016)

One of the distributed ledger based new or coming platforms in IoT domain is IOTA. In IOTA Tangle ledger is able to settle transactions with zero fees. It enables devices to trade exact amounts of resources on-demand, as well as store data from sensors and data loggers securely and verified on the ledger. The Tangle is blockless distributed ledger which is scalable, light and enables to transfer value without fees. This means that even nano payments can be made through the platform. Consensus is not decoupled but instead an intrinsic part of the system, leading to decentralized and self-regulating peer-to-peer network. IOTA is currently in Beta phase (14.12.2016). (IOTA, 2016) (Popov, 2016)

3.1 Bitcoin Based Meta-data Platforms

Bitcoin based meta-data platforms are designed to utilize already adopted Bitcoin Blockchain in sharing and transferring of custom assets. The goal is to use Bitcoin Blockchain itself for new kinds of applications. Meta-data will be added into transactions on the Bitcoin blocks and the meta-data has application specific meaning. Following table presents some of the available bitcoin based meta-data platforms including comparison relating to main features:

Table 1. Bitcoin based meta-data platforms.

Platform	Domain	Source Code	Native Token	Wallet Support	API Support	Website
ColoredCoins	Smart property, coupons, assets, etc.	Open	Bitcoin	Yes	Yes	http://coloredcoins.org
Coinprism	Stocks, currencies, smart property	Open	Bitcoin	Yes	Yes	https://www.coinprism.com
CoinSpark	Asset transfer	Partially Open	Bitcoin	Yes	Yes	http://coinspark.org
ChromaWay	Custom asset transfer	Partially Open	Bitcoin	Yes	Yes	http://chromaway.com
Omni Layer	Asset transfer, property, financial	Open	Mastercoin	Yes	Yes	http://www.omnilayer.org
Stratis Platform	Financial and other (as a service)	Closed?, nBitcoin based	Bitcoin	Yes	Yes	https://stratisplatform.com
Lykke	Financial (ColoredCoin based)	Open	Bitcoin	Yes	Yes	https://www.lykke.com

3.2 Blockchain Platforms for Financial Applications

Blockchain platforms for financial applications are also known as FinTech Blockchain platforms. These platforms aim for application in financial domain. Following table presents some of the available Blockchain platforms for financial applications including comparison relating to main features:

Table 2. Blockchain platforms for financial applications.

Platform	Domain	Source Code	Native Token	Wallet Support	API Support	Website
Ripple	Financial	Partially Open	XRP	Yes	Yes	https://ripple.com
HyperLedger	Financial	Open	None	Yes	Not yet	https://www.hyperledger.org
Counterparty	Financial	Open	XCP	Yes	Yes	https://counterparty.io
Stellar	Financial	Open	Lumen	Yes	Yes	https://www.stellar.org
Bitshares	Financial	Open	BTS	Yes	Yes	https://bitshares.org
Nxt	Financial	Open	NXT	Yes	Yes	https://nxt.org
Interledger	Financial Blockchain protocol	Open	None	Yes	Yes	https://interledger.org

3.3 Smart Contract Platforms

Smart contract platforms enable building and enforcing smart contracts on top of the Blockchain. Smart contracts are software programs that can enforce the contract in a way that the contract itself and its effects on the inputs are verifiable. In these platforms complex logic beyond simple cryptocurrency transfers are expressed utilizing a programming language. Smart contracts have lots of applications in different domains. Smart contracts can enable decentralized applications, like voting, auctions, lottery, escrow systems, crowd funding and micropayments etc. Following table presents some of the available smart contract platforms including comparison relating to main features:

Table 3. Smart contract platforms.

Platform	Domain	Source Code	Native Token	Wallet Support	API Support	Website
Ethereum	Contracts in various domains	Open	Ether	Yes	Yes	https://www.ethereum.org
Rootstock (RSK)	Financials and smart contracts	Closed?	Rootcoin	Yes	Yes	http://www.rsk.co
Codius	Financial	Open	None	Yes	No	https://www.codius.org
Etherparty	Smart contracts platform as a Service	The service is closed but the implementation is based on Ethereum	See Ethereum	See Ethereum	See Ethereum	http://etherparty.io
Monax Eris	Smart contract applications	Closed	?	Yes	Yes	https://monax.io
Waves Platform	Custom token exchange	Closed?	Custom tokens	Yes	Yes	https://wavesplatform.com
Enigma (MIT)	Smart contracts (Ethereum based)	Partially Open/Closed?	See Ethereum	See Ethereum	See Ethereum	http://www.enigma.co

3.4 Consortium/Enterprise Platforms

Consortium platforms enable consortiums, organizations and enterprises to maintain a Blockchain, read, update and share the data in a trustworthy manner. These platforms are not using Proof-of-Work computations. Instead, the trust is enforced by other means, such as legal contracts with the enterprises. The platforms also enable enterprises to define their own rules and block structure. Every enterprise or entity maintains a mining node that will participate in the consensus process and consensus is achieved by a majority of the peers within the group. Following table presents some of the available consortium/enterprise platforms including comparison relating to main features:

Table 4. Consortium/Enterprise platforms.

Platform	Domain	Source Code	Native Token	Wallet Support	API Support	Website
MultiChain	Data sharing/management in and between organizations	Open	None	Yes	Yes	http://www.multichain.com
OpenChain	Issue and manage digital assets in organizations	Open	None	Yes	Yes	https://www.openchain.org
BlockStack	Internal assets transfer between enterprise users	Open	None	Yes	Yes	https://blockstack.org
Chain	Enterprise financial services	Partially Open	None	?	Yes	https://chain.com
HydraChain	Extension of the Ethereum platform for private chain or consortium chain setups	Open	Ether	Yes	Yes	https://github.com/HydraChain

3.5 Sidechain/Anchored Chain Platforms

Sidechains can be seen as completely different Blockchains. Sidechains have two-way connection to Bitcoin Blockchain. The platforms can convert Bitcoins to its native currency or work using Bitcoins. Bitcoins can be transferred back and forth between the sidechain and the main Bitcoin Blockchain. Sidechains enable new applications independent of the Bitcoin network but allow also users with Bitcoins to start using the sidechains with their Bitcoin address.

Anchored chain platforms enable users to create their own Blockchains suited for their application. In Blockchain anchoring permissioned Blockchains periodically submit hashes of their block headers into a permissionless chain. Anchoring enables permissioned chain to verify the hashes that are validated and included by miners in the permissionless chain. Following table presents some of the available sidechain/anchored chain platforms including comparison relating to main features:

Table 5. Sidechain/Anchored Chain Platforms.

Platform	Domain	Source Code	Native Token	Wallet Support	API Support	Website
SideChain Elements	Sidechain applications	Open	Bitcoin	Yes	No	https://elementsproject.org
Factom	Anchored chain applications	Open	Bitcoin	Yes	Yes	https://www.factom.com
Chainpoint	Anchored chain protocol	Open	-	-	-	http://www.chainpoint.org

3.6 Multipurpose Platforms and Services

In addition to actual Blockchain platforms there are available some multipurpose platforms providing for example Blockchain as a service. There are also new kind of platforms under development all the time, including Industrial Internet of Things based on the Blockchain technology. Following table presents some of the available multipurpose platforms and/or services including comparison relating to main features:

Table 6. Multipurpose Platforms and Services.

Platform	Domain	Source Code	Native Token	Wallet Support	API Support	Website
Microsoft Azure BAAS (Blockchain as a Service)	For example Ethereum as a service in MS Azure	Azure is commercial, but Blockchain platforms running on top of it are open	See Ethereum	See Ethereum	See Ethereum	https://azure.microsoft.com/en-us/solutions/Blockchain
IBM Blockchain on Bluemix	Hyperledger as a service on Bluemix	See HyperLedger	See HyperLedger	See HyperLedger	See HyperLedger	http://www.ibm.com/Blockchain
IOTA	IoT	Open	IOTA	Coming	Yes	https://iotatoken.com/

4. Widely Adopted Blockchain Platforms and Services

In the following chapters, we will present two common Blockchain platforms that provide different solutions to enterprise Blockchain development, Microsoft Azure BaaS and Linux Foundation’s Hyperledger, and comparison of two most adopted public Blockchains, Bitcoin and Ethereum.

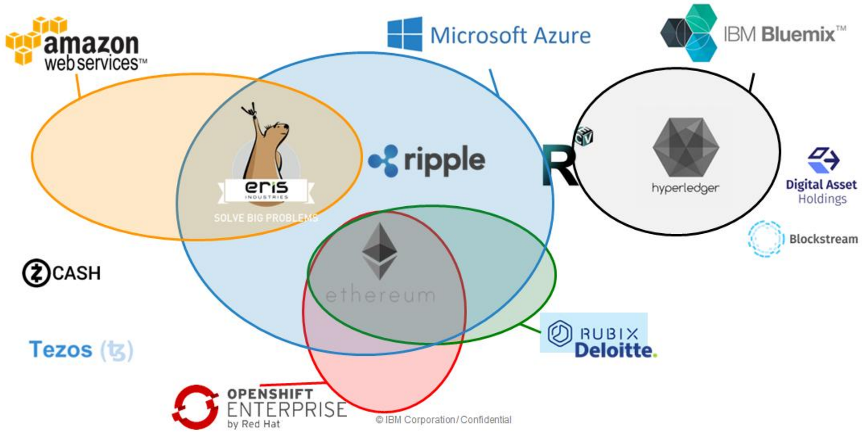


Figure 6. Blockchain as a Service (BaaS) competitors. (Fuentes 2016)

4.1 Hyperledger

The Hyperledger Project is Linux Foundation’s collaborative effort to create an enterprise-grade, open-source distributed ledger framework and code base. It aims to advance Blockchain technology by identifying and realizing a **c**ross-industry open standard platform for distributed ledgers, which can transform the way business transactions are conducted globally. (Cachin 2016) Also, Hyperledger is considered as an effort to bring Blockchain technology to mass markets as a business-ready Blockchain fabric (Hyperledger Whitepaper, 2016).

Note! The name Hyperledger has previously (before November 2015) been actively used for financial technology platform from company Hyper (later DigitalAssetHoldings). As DAH joined the Linux Foundation's Blockchain project as one of the founding members in December 2015, the brand name "Hyperledger" was also donated to the project with their codebase. Today, the name Hyperledger thus represents completely different architectural design and codebase compared to the original financial permissioned distributed ledger because in addition to DAH's contribution, Linux Foundation's Hyperledger has got many other codebase donations e.g. from IBM. (Swanson, 2016)

In February 2017, Hyperledger Project has 100 members (partly depicted in **Figure 7**). Among them there are tech giants like IBM and Intel but also financial parties like messaging service company SWIFT and international bank consortium R3CEV. In fact, R3CEV has also open-sourced their distributed ledger Corda and handed it over to Hyperledger project. (Gautham, 2016)

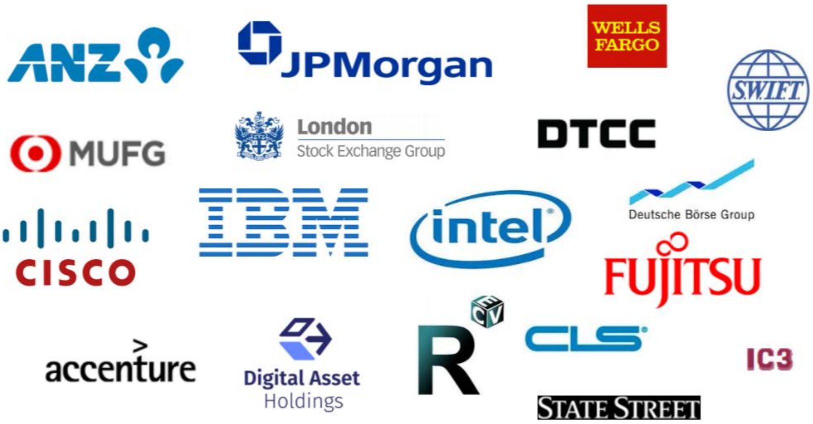


Figure 7. Hyperledger partners (Manoj 2016).

At the moment, Hyperledger Project has several projects in the incubation (Table 7. Hyperledger Incubation Projects).

Table 7. Hyperledger Incubation Projects (https://www.hyperledger.org/community/projects).

Project name	Focus
Fabric	· An implementation of Blockchain technology that is intended as a foundation for developing Blockchain applications or solutions. It offers a modular architecture allowing components, such as consensus and membership services, to be plug-and-play. It leverages container technology to host smart contracts called "chaincode" that comprise the application logic of the system.
Sawtooth Lake	· Intel's modular Blockchain package.

	· Provides Intel's own proof-of-elapsed-time (PoET) algorithm as a one option for a consensus mechanism. PoET offers some benefits over Practical Byzantine Fault Tolerance (PBFT), e.g., it scales to a larger number of nodes and is more reliable since it works when larger numbers of nodes are not available. However, PoET is notably designed to be used on a certain type of computer manufactured by the Intel. (Hertig 2016)
Iroha	· A Japanese Blockchain project with following features o simple construction o modern, domain-driven C++ design o emphasis on mobile application development o new, chain-based Byzantine fault tolerant consensus algorithm, called Sumeragi
Blockchain explorer	· A project for building a user-friendly web application for Hyperledger to view/query blocks, transactions and associated data, network information (name, status, list of nodes), chain codes/transaction families (view/invoke/deploy/query) and any other relevant information stored in the ledger.

As a starting point for its effort, Hyperledger has identified challenges of existing Blockchain implementations:

- Limited throughput
- Slow transaction confirmations
- Designed for cryptocurrency
- Poor governance
- No privacy
- No settlement finality
- Anonymous Processors.

These challenges combined with varying industrial requirements for Blockchains across different use-cases make it impossible to find one solution that fits all. Therefore, Hyperledger has been designed to be modular with pluggable options to suit different needs. (Hyperledger Project, 2016) By providing a modular framework that supports different components for different uses, it brings together a number of independent efforts to develop open protocols and standards. Consequently, this approach will enable a variety of Blockchains with their own consensus and storage models, and services for identity, access control and contracts. (Hyperledger-Wikipedia, 2016)

Structure

IBM has gathered key concepts and benefits of Blockchain for business (Figure 8). They have also explored further each of these four concepts (Shared ledger, Permissions, Smart contract and Consensus) and these details are listed in Figure 9.

To achieve these goals, several R&D efforts have been donated to Hyperledger project: IBM's codebase and intellectual property from its ADEPT project on

Ethereum as well as other research. Digital Asset Holdings' Hyperledger brand and related code and developer resources. R3's framework for transactions, designed with its consortium partners to meet the requirements of its global banks and other financial institutions. These set the scene for Hyperledger; a focus on enterprise-specific applications, robustness, security and business support. (Michalik, 2016)

"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, the chief engineer at New York-based fintech firm about R3CEV's Corda joining Hyperledger (Gautham, 2016)

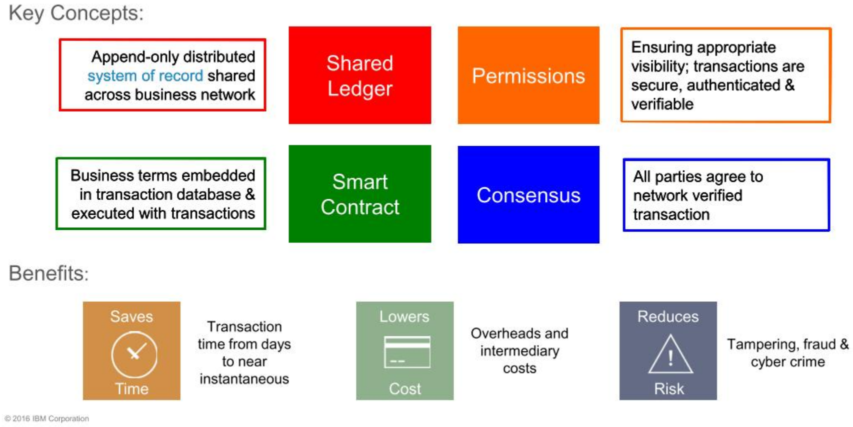

Key Concepts:
Append-only distributed system of record shared across business network
Shared Ledger
Permissions
Ensuring appropriate visibility; transactions are secure, authenticated & verifiable
Business terms embedded in transaction database & executed with transactions
Smart Contract
Consensus
All parties agree to network verified transaction
Benefits:
Saves Time
Transaction time from days to near instantaneous
Lowers Cost
Overheads and intermediary costs
Reduces Risk
Tampering, fraud & cyber crime
© 2016 IBM Corporation

Figure 8. Key concepts and benefits of Blockchain for business. (O 'dowd, 2016)

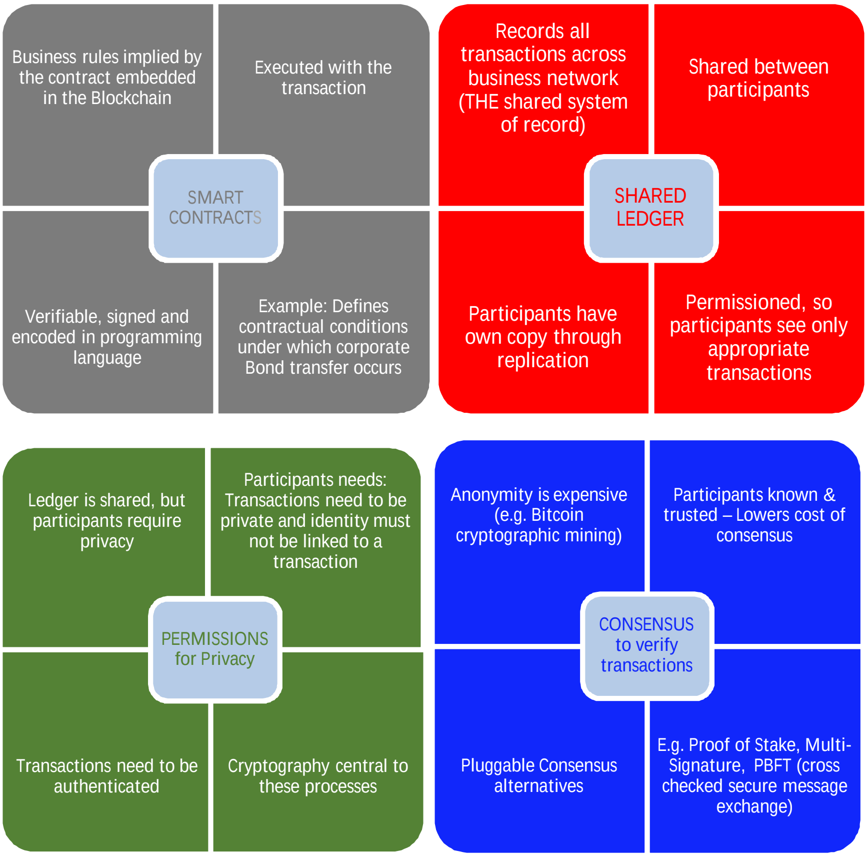

Business rules implied by the contract embedded in the Blockchain
Executed with the transaction
SMART CONTRACTS
Verifiable, signed and encoded in programming language
Example: Defines contractual conditions under which corporate Bond transfer occurs
Records all transactions across business network (THE shared system of record)
Shared between participants
SHARED LEDGER
Participants have own copy through replication
Permissioned, so participants see only appropriate transactions
Ledger is shared, but participants require privacy
Participants needs: Transactions need to be private and identity must not be linked to a transaction
PERMISSIONS for Privacy
Transactions need to be authenticated
Cryptography central to these processes
Anonymity is expensive (e.g. Bitcoin cryptographic mining)
Participants known & trusted – Lowers cost of consensus
CONSENSUS to verify transactions
Pluggable Consensus alternatives
E.g. Proof of Stake, Multi-Signature, PBFT (cross checked secure message exchange)

Figure 9. Detailed key concepts of Blockchain for business. (O ’dowd, 2016)

Hyperledger has defined its project scope so that its focus is on the shared ledger and its internal structures. Therefore, the application layer as well as value added systems are out of the project’s scope (Figure 10).

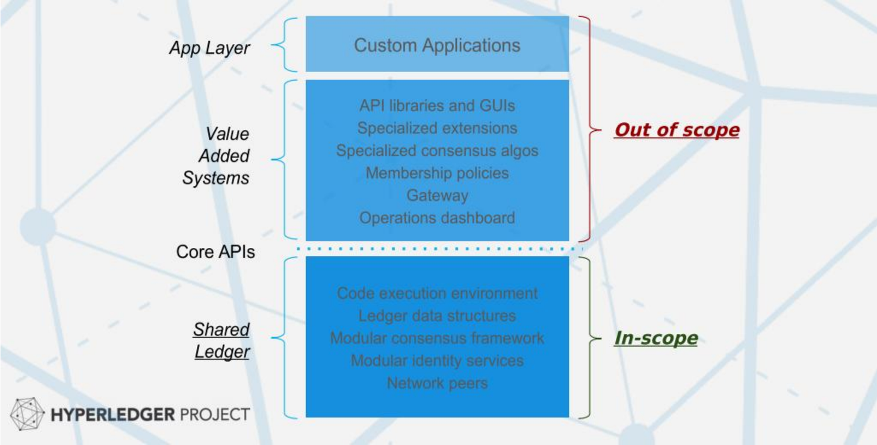


Figure 10. Hyperledger Project Scope (Hyperledger Project 2016).

Thus, the focus of the project is in designing "an evolving Blockchain fabric that permits for compliance with regulations, while supporting the varied requirements that arise when competing businesses work together on the same network. The central elements of this specification are smart contracts called "chaincode", digital assets, record repositories, a decentralized consensus-based network, and cryptographic security." (Lombardo, 2016)

As a result, reference architecture for this kind of Blockchain fabric is presented (Figure 11).

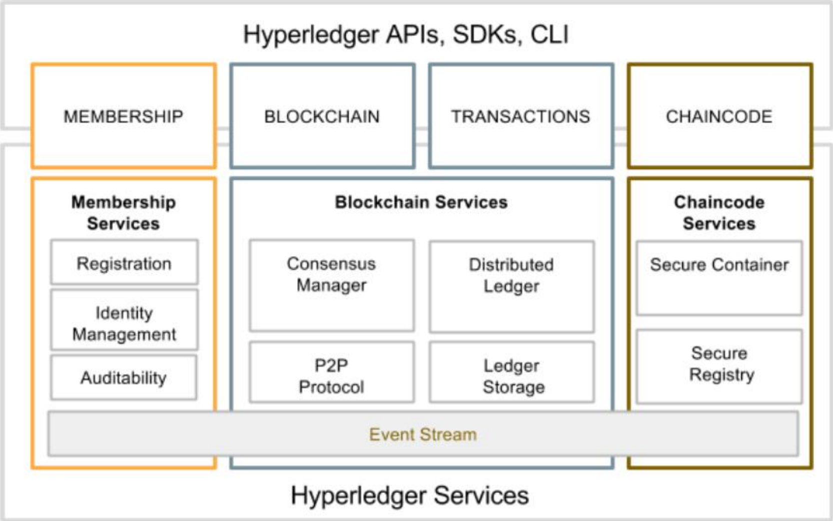


Figure 11. Hyperledger reference architecture.

Some key features of the current fabric release are: (Cachin, 2016)

- A permissioned Blockchain with immediate finality
- Runs arbitrary smart contracts (called chaincode) implemented in Go:
  - User-defined chaincode is encapsulated in a Docker container
  - System chaincode runs in the same process as the peer;
- Consensus protocol is pluggable, currently an implementation of Byzantine fault-tolerant consensus using the PBFT protocol is supported, a prototype of SIEVE to address non-deterministic chaincode is available, and a protocol stub (named NOOPS) serves for development on a single node
- Security support through certificate authorities (CAs) for TLS certificates, enrolment certificates, and transaction certificates
- Persistent state using a key-value store interface, backed by RocksDB (rocksdb.org)
- An event framework that supports pre-defined and custom events
- A client SDK (Node.js) to interface with the fabric
- Support for basic REST APIs and CLIs.

4.2 Microsoft Azure BaaS (Blockchain-as-a-Service)

In November 2015, Microsoft announced with ConsenSys (the collective of Ethereum coders) to start offering Ethereum Blockchain as a Service (EBaaS) on the Azure platform so that enterprise clients and developers can have a single click cloud based Blockchain developer environment. (Allison 2015) In the later phase, as more and more partners have joined in the Azure ecosystem, Marley Gray, Principal Program Manager of Azure Blockchain Engineering comments that

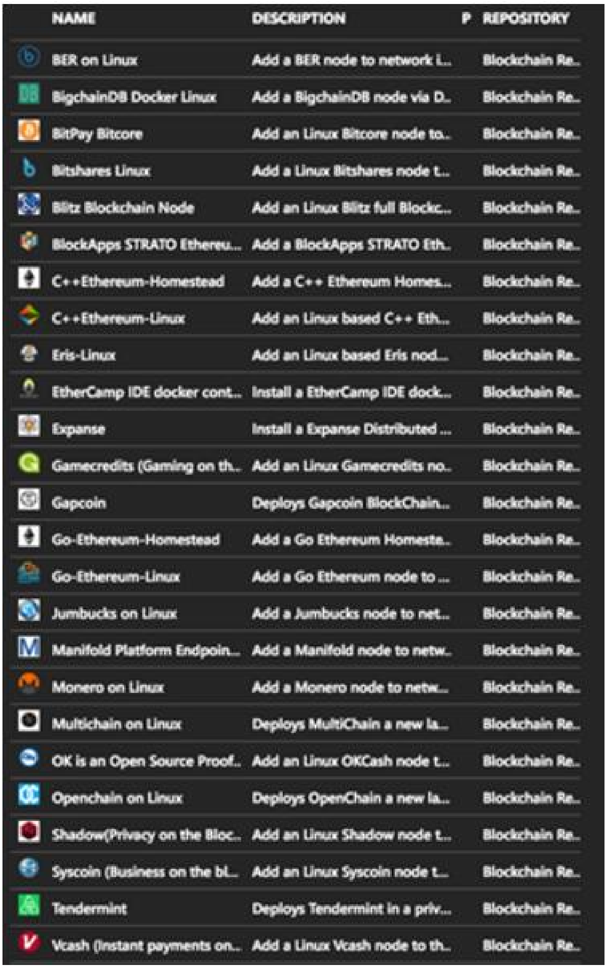
“It’s getting hard to keep saying Blockchain for everything in this space, so I'll just start referring to it as the distributed ledger ecosystem”.

Thus, Blockchain as a Service is NOT a Blockchain, but a Dev/test platform for all different types of Blockchains or in other words, a place for partners to put new platforms, frameworks, tools and services for customers to discover and experiment with. Among others, innovation firm R3 with its financial institution partners have simulated financial transactions using Azure BaaS.

The financial services are not the only beneficiaries of distributed ledgers. Public sector and industries (e.g. retail, manufacturing) as well as healthcare are also strong potentials for this technology. Within the Azure platform, these user sectors may find it useful to combine the existing Azure IoT and predictive analysis tools with their Blockchain solutions, e.g. in healthcare the data from medical devices and wearables.

Pieces of Azure Blockchain-as-a-Service offering

The initial EBaas offering contained two tools that allowed for rapid development of smart contracts based applications: Ether.Camp (An integrated developer environment) and BlockApps (a scalable Ethereum compliant platform for rapid development, deployment and management of enterprise Blockchain applications). Since, many other members have joined to Azure ecosystem, see Figure 12. See also detailed list in Table 8. Thus, developers have multiple alternative templates for experimenting, comparing and selecting the best building blocks for their implementations which may be solutions for very varying needs.



NAME	DESCRIPTION	P	REPOSITORY
BER on Linux	Add a BER node to network l...		Blockchain Re...
BigchainDB Docker Linux	Add a BigchainDB node via D...		Blockchain Re...
BitPay Bitcore	Add an Linux Bitcore node to...		Blockchain Re...
Bitshares Linux	Add a Linux Bitshares node t...		Blockchain Re...
Blitz Blockchain Node	Add an Linux Blitz full Blockc...		Blockchain Re...
BlockApps STRATO Ethereu...	Add a BlockApps STRATO Eth...		Blockchain Re...
C++Ethereum-Homestead	Add a C++ Ethereum Homes...		Blockchain Re...
C++Ethereum-Linux	Add an Linux based C++ Eth...		Blockchain Re...
Eris-Linux	Add an Linux based Eris nod...		Blockchain Re...
EtherCamp IDE docker cont...	Install a EtherCamp IDE dock...		Blockchain Re...
Expanse	Install a Expanse Distributed ...		Blockchain Re...
Gamecredits (Gaming on th...	Add an Linux Gamecredits no...		Blockchain Re...
Gapcoin	Deploys Gapcoin BlockChain...		Blockchain Re...
Go-Ethereum-Homestead	Add a Go Ethereum Homeste...		Blockchain Re...
Go-Ethereum-Linux	Add a Go Ethereum node to ...		Blockchain Re...
Jumbucks on Linux	Add a Jumbucks node to net...		Blockchain Re...
Manifold Platform Endpoin...	Add a Manifold node to netw...		Blockchain Re...
Monero on Linux	Add a Monero node to netw...		Blockchain Re...
Multichain on Linux	Deploys MultiChain a new la...		Blockchain Re...
OK is an Open Source Proof...	Add an Linux OKCash node t...		Blockchain Re...
Openchain on Linux	Deploys OpenChain a new la...		Blockchain Re...
Shadow(Privacy on the Bloc...	Add an Linux Shadow node t...		Blockchain Re...
Syscoin (Business on the bl...	Add an Linux Syscoin node t...		Blockchain Re...
Tendermint	Deploys Tendermint in a priv...		Blockchain Re...
Vcash (Instant payments on...	Add a Linux Vcash node to th...		Blockchain Re...

Figure 12. Azure open source stacks and third party offerings. See also detailed list in **Table 8**. Azure BaaS offerings.

Table 8. Azure BaaS offerings.

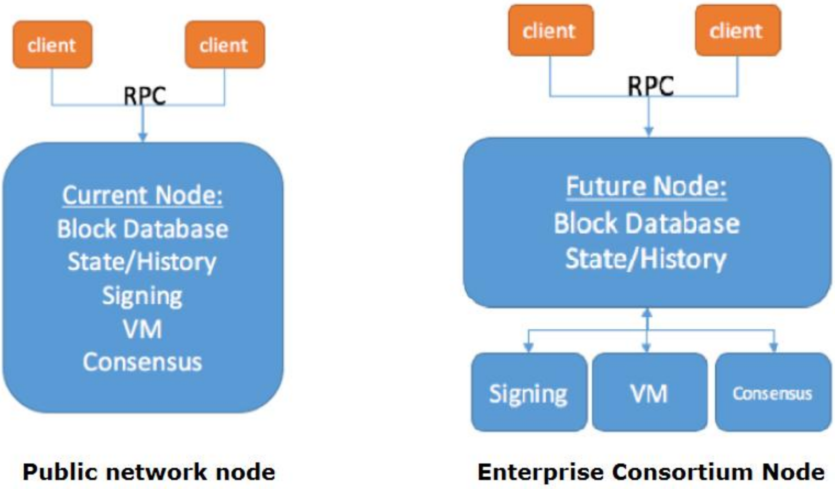
Member/tool/package	Offering
ConsenSys	the collective of Ethereum coders, a consulting venture production studio
Ether.Camp	**Ethereum Studio**: an **IDE** and Blockchain explorer
BlockApps	A toolkit for building Ethereum applications. The **STRATO** is a single-node Blockchain instance, which acts as a developer sandbox for testing Ethereum Blockchain applications and offers the STRATO RESTful API for connecting applications to private, semi-private (consortium) and public Ethereum Blockchains.
Ripple	Ripple provides **global financial settlement solutions**. Ripple's Interledger Protocol available for exploration, also a validating Ripple node operating in Azure
Eris Industries	A leading platform for industrial applications of **smart contract** technology
CoinPrism/OpenChain	An open source distributed ledger technology for organizations wishing to issue and manage digital assets in a robust, secure and scalable way. OpenChain instance can be configured as a pegged sidechain.
Factom	Simplify **records** management, record business processes, and address security and compliance issues
BitPay	The world's **leader in Bitcoin payments**, providing Bitcoin payment processing and local currency payouts to over 65,000 businesses worldwide
Manifold Technology	Manifold's Rewards application is built on the patent-pending Manifold Liquidity Platform (MLP). MLP is a powerful, private Blockchain, capable of **unprecedented transaction speed and throughput**
LibraTax	LibraTax is the reporting, accounting, audit, and integration layer for Blockchain technology and digital assets that is built for the future of digitized ownership and trading
Emercoin	A leading digital currency and Blockchain platform that focuses on innovative, scalable enterprise services.
MultiChain	Rapidly design, deploy and operate distributed ledgers
Netki	Designs enterprise-grade solutions promoting scalability, security and ease of use for Blockchain-based products. The Netki **Wallet Name Service** is an open standard that makes it easy to send digital currency between users or services, interconnecting the entire ecosystem.
AlphaPoint	The platform powers digital asset exchanges and provides institutions Blockchain-enabled solutions to store, track, and trade digital assets. The company's future offerings on the Azure Marketplace will allow

	users to test and build Blockchain applications leveraging a **.NET stack**.
IOTA	The world's first **Directed Acyclic Graph**/Tangle based distributed ledger. IOTA came up with this model to solve the scalability issues of the Blockchains, which become very apparent in the world of **Internet of Things**.
Augur	A **decentralized prediction market** platform built on the Ethereum Blockchain. While a company may not want their markets public or may not want to deal with the compliance costs of running a public market, Augur will offer a turn-key solution for enterprises interested in running an internal version of the platform.
Lisk	The Lisk platform allows developers worldwide to easily deploy their own custom Blockchains, and program **decentralized applications (e.g. IoT)** on top of them **using JavaScript**.
BitShares	A Financial Services platform for **SmartCoins** (a price-stable digital asset pegged to the value of various currencies, commodities, stocks and other financial instruments) coupled with a decentralized asset exchange
SysCoin	Provide merchants the ability to buy and sell goods and services, encrypted messaging, escrow, digital asset storage, reselling and more. Also, provides a replacement for typical Blockchain addresses, known as aliases; providing ease-of-use.
Slock.it	Slock.it aims to address **security, identity, coordination and privacy over billions of devices**. Integration with Microsoft Azure will make it very easy for developers to build apps for Slock.it first product, the **Ethereum Computer**.
Algorythmix	Decentralized **KYC and Credit Rating** services
Expanse	A community-based, decentralized information, application, and smart contract platform
Influx	A X11 algorithm based **coin with no pre-mine** using a PoW+PoS Hybrid backend and designed specifically for CPU/GPU setups
Monero	A cryptocurrency which transactions are cryptographically **untraceable and unlinkable**
Radium	A Proof-Of-Stake cryptocurrency that serves as the base Blockchain for the Radium SmartChain
Tendermint	Byzantine fault-tolerant replicated state machines in any programming language
Chain	Chain Core is enterprise-grade Blockchain infrastructure that enables organizations to build better financial services from the ground up
Storj	Distributed, open-source, encrypted cloud storage
Also Jumbucks, Bitswift, Vcash, Shadow, Blocknet, Blitz, Gamecredits, Okcash	

Project Bletchley

“Bletchley is Microsoft’s architectural approach to building an Enterprise Consortium Blockchain Ecosystem. To be clear, this is not a new Blockchain stack. It is Microsoft’s approach to bring distributed ledger (Blockchain) platforms into the enterprise to build real solutions addressing real business problems while keeping the platform open.”

Azure will remain open to all protocols, consensus algorithms, databases and virtual machines. However, Bletchley will introduce a modular framework allowing for you to choose what combination of technologies best fits the business domain you are trying to address. Because each Blockchain/distributed ledger will have all nodes on that network agree, there will by default be many ledgers. (Gray, 2016a)



Public network node

Enterprise Consortium Node

Figure 13. Azure Enterprise Blockchain has a modular framework (Gray, 2016a).

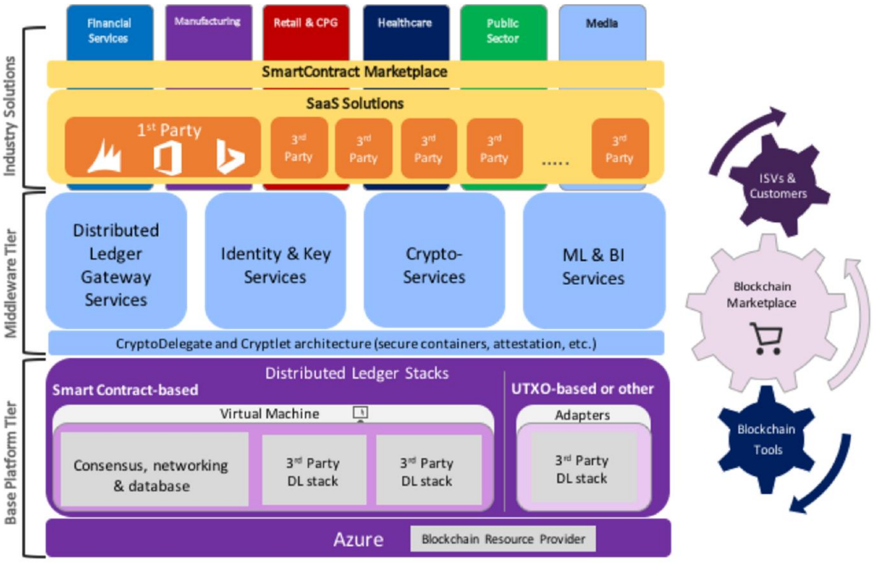


Figure 14. Bletchley is Microsoft’s architectural approach to building Enterprise Blockchain Ecosystem (Gray, 2016a).

In Figure 14 is depicted the architecture of Bletchley. The leading idea of the Base Platform located down is that it may comprise any pluggable distributed ledger implementation and the implementation can also be swapped if needed. Further, there is a Middleware Layer (blue one, also called Fabric) that offers many important services for consortium Blockchains: Identity and certificate services, Encryption and Cryptlet (more on this below) services, Blockchain gateway and Data services as well as Management and Operations. These services may ease the development of distributed applications remarkably. Additionally, the user may find useful parts for one’s applications in the Marketplace. In there, e.g. base platform components, additional distributed Fabric services, Cryptlets as well as full SmartContract libraries are provided and also new ones can be created to get paid for them.

Cryptlets

Previously mentioned cryptlet services are a special feature of Azure BaaS. By being like “improved” version of the concept of oracles (See Figure 15), cryptlets provide *“much needed functionality like integration, secure execution, privacy, interoperability, management and a rich set of data services… [And thus give] opportunities to address some of the most concerning limitations of today’s Blockchain platforms like performance, scale and security.”* (Gray, 2016b)

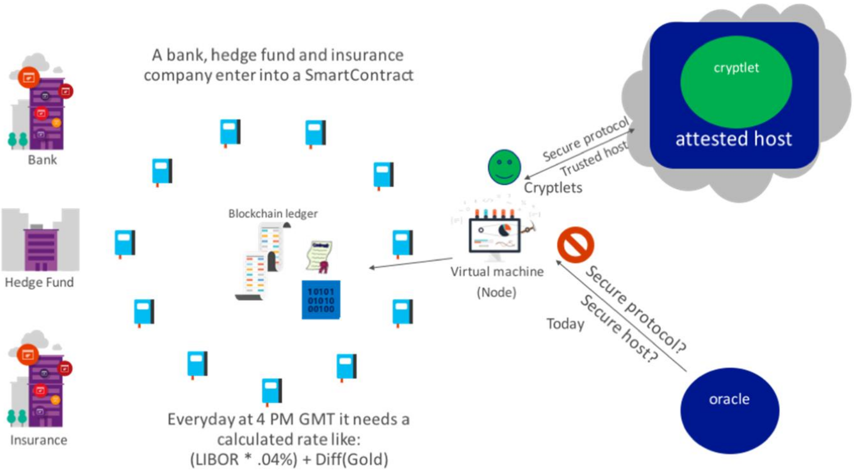


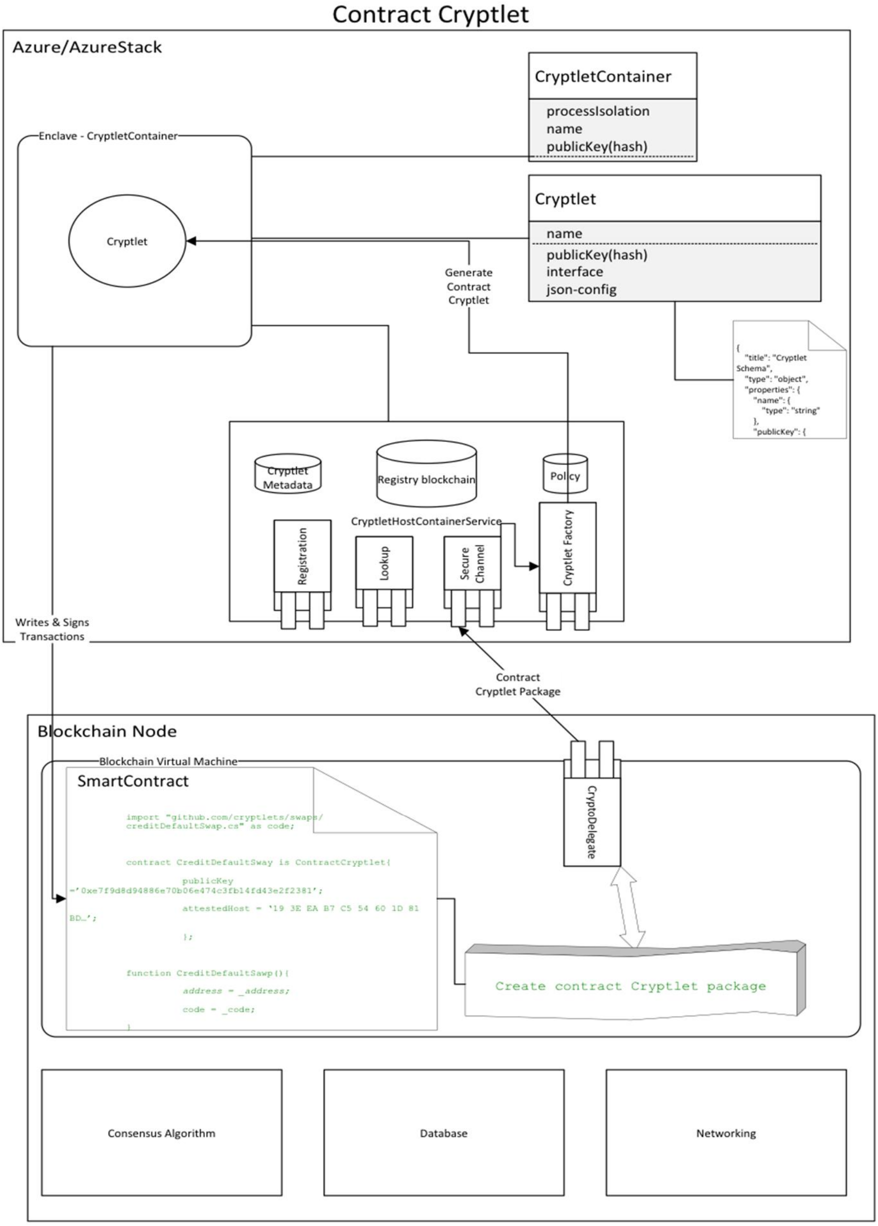
Figure 15. Using external data with Blockchain. (Gray, 2016a)

As mentioned (Gray, 2016a), calling code or data outside a Blockchain or a smart contract may be ”breaking the trust barrier threatening the authenticity of the dependent transactions.” This means that we need a means to interact with external events and data preserving the integrity of Blockchain and that is where cryptlets come in.

Cryptlets are off-chain code components that are written in any language, execute within a secure, trusted container and communicate with using secure channels. (Gray, 2016a) They reside in the cloud (Azure, AWS, Google and Private) and are consumed as library services. There are two kinds of cryptlets:

- Utility cryptlets
  - For encryption, time based event publication and access to external data. Utility Cryptlets have attested IDs that are made available via a registration process.
- Contract cryptlets
  - Always created and bound to a specific SmartContract instance, can host logic not fully suited to run in the EVM for performance or privacy scale purposes (e.g. can perform the entire operation of a SmartContract in parallel with other Contracts without tying up EVM).

For their operation, cryptlets need some services around them: e.g. trust validation and secure isolated containers (usually hardware-based enclaves). These services are provided by particular cryptlet fabric components like CryptletContainers or CryptletRegisters and they are initialized within a cryptlet registration process. As an example of the structure of Contract Cryptlet environment, see Figure 16. For Utility Cryptlets the environment is a little simpler because no Cryptlet Factory is needed for cryptlet instance creation.



```
{
   "title": "Cryptlet
Schema",
   "type": "object",
   "properties": {
      "name": {
         "type": "string"
      },
      "publicKey": {
```

```
        import "github.com/cryptlets/swaps/
        creditDefaultSwap.cs" as code;


        contract CreditDefaultSway is ContractCryptlet{

                publicKey
='0xe7f9d8d94886e70b06e474c3fb14fd43e2f2381';

                attestedHost = '19 3E EA B7 C5 54 60 1D 81
BD…';

                };


        function CreditDefaultSawp(){

                address = _address;

                code = _code;

        }
```

Figure 16. Contract Cryptlet (Gray, 2016b).

4.3 Comparison of Bitcoin and Ethereum

The two most popular public Blockchains are Bitcoin and Ethereum. Both serve their own specific purpose with some trade-offs made in their design. Ethereum is a decentralized computing platform that uses consensus mechanism similar to Bitcoin, but allows more flexibility in transactions which in Ethereum's case are often referred to as contracts. Bitcoin is more established and more rigid system aimed primarily for financial transactions. Table 9 compares the main differences of Bitcoin and Ethereum Blockchain systems.

Table 9. Comparison of Bitcoin and Ethereum.

	Bitcoin	Ethereum
Key Purpose	Decentralized book keeping system for financial transactions	Decentralized computation engine
Primitive Data Structure	Transactions based on scripting language	Contracts based on Turing-complete programming language
Role of Nodes	Nodes validate transactions	Nodes run program code
Block Time	On average 10 min	On average 15s
Hashing Algorithm	SHA256	ethash
Competitive Advantages	Network effect More “rigid”	Second mover advantage More “flexible”

5. Feasibility of Blockchain Technologies

Following chapters presents feasibility aspects of Blockchain technologies: The scalability of the public Blockchain systems, private & consortium Blockchain systems and six requirements for Blockchain use cases.

5.1 Scalability of the Public Blockchain Systems

The rules of public Blockchain systems are, by design, very difficult to change once they are in use. The systems have no owner and no official governance process. Instead, the control over the system is decentralized to a number of independent participants: users, developers, miners and non-mining nodes. Mattila & Seppälä call this equilateral governance (Mattila and Seppälä, 2017).

Ultimately it's the miners who decide what gets written on the Blockchain, but miners follow the economic incentives set up by the users. Miners are usually also dependent on the coordinative work of developers as to make sure that everybody follows the same consensus rules. As there are neither official governing bodies nor governance processes, it is burdensome to estimate support for changes.

5.2 Private and Consortium Blockchain Systems

Public Blockchains like Bitcoin and Ethereum let anyone with internet connection to participate the network activities without registration or provision of identification. Participants only need to generate an anonymous address for themselves through a trivial process and after that, they are able to make transactions within the limits of their balances. By having a decent hardware and loading a full Blockchain history data, anyone can join the mining process of public Blockchains. In addition, public Blockchains are developed open-source and therefore they provide an open platform for further service creation.

The ultimate openness of public Blockchains is enabler for innovation but it also brings along certain features that some Blockchain adopters want to avoid. For example, in the public Blockchain every transaction is publicly visible (although it may be encrypted) and with enhanced data mining algorithms some sensitive business data may be collected by outsiders. Therefore, while especially enterprise consortia do see the potential of immutable ledgers they at the same time worry issues like privacy and regulation. For addressing these issues, there is forming the concept of consortium Blockchains and even giant IT companies like IBM and Microsoft are involved in this evolution.

Microsoft describes the need of consortium Blockchains in the advent of their Blockchain approach (Project Bletchley) with the following arguments (Gray 2016a):

"…Distributed Ledger, is more of a catalyst to inspire change in the way disparate organizations work together in highly competitive markets. Existing inter-company transactions carry enormous costs in process, procedure and crosschecking of records to come to settlement…"

“..Smart Contracts offer a lot of promise to create intelligent systems with self-enforcing contracts to allow business processes to operate independently…”

Depending on a source, the naming practices of different kinds of private Blockchains are varying. In some cases, the terms “private” and “permissioned” are used equivalently but usually these terms have special, divergent meanings. As shown in Figure 17, private/public Blockchains differ in terms of who has the right to view the data in the Blockchain and in turn, permissioned/unpermissioned have contrasting rights of transaction validation.

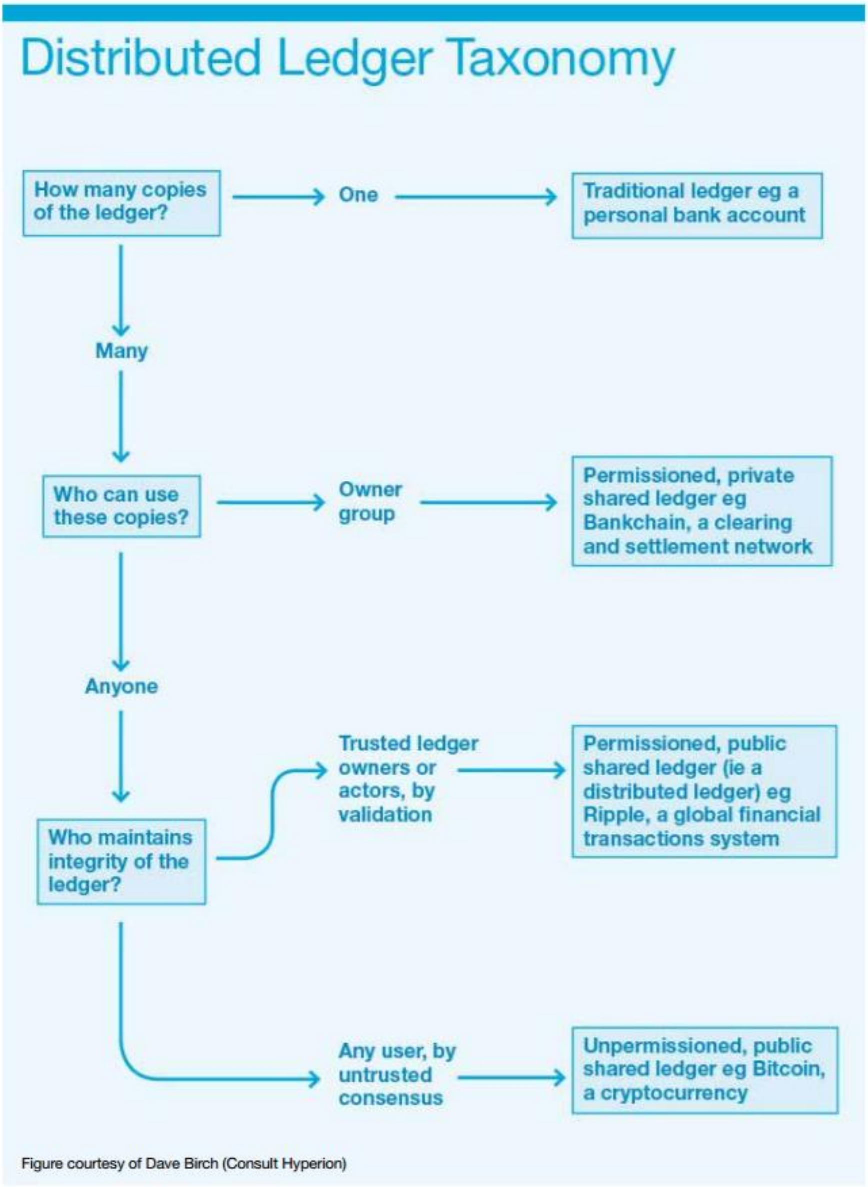

Distributed Ledger Taxonomy
How many copies of the ledger?
One
Traditional ledger eg a personal bank account
Many
Who can use these copies?
Owner group
Permissioned, private shared ledger eg Bankchain, a clearing and settlement network
Anyone
Who maintains integrity of the ledger?
Trusted ledger owners or actors, by validation
Permissioned, public shared ledger (ie a distributed ledger) eg Ripple, a global financial transactions system
Any user, by untrusted consensus
Unpermissioned, public shared ledger eg Bitcoin, a cryptocurrency

Figure courtesy of Dave Birch (Consult Hyperion)

Figure 17. Distributed Ledger Taxonomy (Walport, 2016).

What are the pros and cons of consortium Blockchains?

As mentioned, “consortium Blockchain” is a collective term for diverse private / permissioned Blockchains. These consortium Blockchains have many similarities with their public counterparts, for example peer-to-peer architecture, public key cryptography and Byzantine Fault Tolerance (i.e. network coordination can be guaranteed despite faulty nodes). However, the public Blockchains have some weaknesses that make them less attractive for many industrial uses, see **Table 10**. Thus, in more detail:

- Slow transaction processing
- Lack of settlement finality
- The risks of anonymous miners
- An inability to limit network participation to known entitie
- The size of one bloating ledger
- Privacy and reputational concerns
- Troubles to predict the public Blockchain's core development process make the use of public Blockchains in enterprises complicated. These issues have led enterprises to look for alternative solutions.

Table 10. Strengths and weaknesses of public Blockchains (Hileman, 2016).

Strengths	Weaknesses
Immutable ledger	Irreversible transactions
Comparatively fast settlement (e.g. 10 minutes or less)	Slow transaction clearing (e.g. 3–7 transactions/second)
Reduce security risks associated with centralization-trusted third party	More vulnerable to attacks i.e. 51% spam, DDoS
Easy to audit	Reduced privacy
Reduced need to trust	Energy consumption

Consortium Blockchains with known validators and modifiable distributed consensus protocols can be an answer to above issues and they have many desirable features and advantages over public Blockchains (Buterin, 2015):

- The consortium can change the rules of a Blockchain, revert transactions and adjust balances, if needed

- Known validators and identity verifications eliminate the risk of impersonation attacks (but the validator collusion is still a risk, of course)

- Cheaper transactions and energy efficiency

- Much shorter block times, greater transaction throughput and better scalability

- Greater level of privacy.

These differences are further depicted in **Table 11** in which we also notice that consortium Blockchains allow more freely the creation of the token representing a real-world asset directly. In public Blockchains, we need to use the "colored coin" scheme or otherwise add the real-world asset as metadata to already existing native assets, which may hinder the development of an optimal Blockchain solution.

Table 11. Public vs. Private Blockchains: Generalized Features Comparison (Hileman 2016).

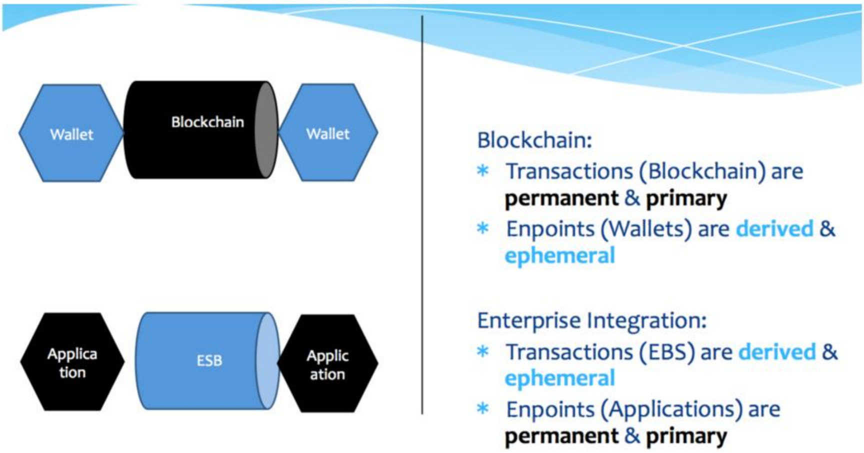
	Public	Private
Access	Open read/write access to database	Permissioned read and/or write access to database
Speed	Slower	Faster
Security	Proof-of-Work/Proof-of-Stake	Pre-approved participants
Identity	Anonymous/Pseudonymous	Known identities
Asset	Native assets	Any assets

Additionally, Gray (Gray, 2016a) highlights that consortium Blockchains differ from public Blockchains because the architecture of consortium Blockchain implementations varies depending on the case while in the public Blockchain it is more stable:

"Public Blockchains like Bitcoin, Ethereum and others will define their protocol stacks, however consortium □new way to refer to member/private/permissioned Blockchains□ distributed ledgers will define their networks based on the business they are addressing."

Thus, in enterprise Blockchains, the implementation may be more tailored and the Blockchain is used more as a tool instead of as an ideology.

What would then be the killer use case for enterprise Blockchains? Herudek (Herudek, 2015) states that integration could be the one. As he states, despite ESB (Enterprise Service Bus) and MDM (Master Data Management) solutions there is still endless "integration battle" going on with most of IT projects dealing with some kind of data migration from one format to another, usually without any additional business value. In Figure 18, he presents how Blockchain based system changes the approach to data integration in whole. As shown, the relation between endpoints and integration layer turns upside down. In the traditional ESB system, applications are primary and permanent endpoints and ESB's messages are temporary and derived based on these endpoints. In contrast, in Blockchain based integration system the Blockchain forms permanent and primary message layer to which temporary wallet (application) endpoints need to conform. This makes fundamental difference by not only providing the single source of truth (as MDM does centrally) in a distributed manner but also by controlling the language used to communicate between endpoints i.e. wallets cannot introduce their own data models. Consequently, when new systems are added to the Blockchain there is no need for data migration and this makes integration a lot easier. These features alone may justify the introduction of enterprise Blockchain as an efficient integration medium. Further, the Blockchain as an immutable transaction log can enhance the traceability of transactions, outsourcing services and even protect companies from e.g. their compromised employees. Naturally, in addition to these features, completely different collection of advantages appears if a consortium can further create / combine their existing business with other promising Blockchain use cases like e.g. finance, energy or logistics.



Blockchain:
- Transactions (Blockchain) are **permanent** & **primary**
- Enpoints (Wallets) are **derived** & **ephemeral**

Enterprise Integration:
- Transactions (EBS) are **derived** & **ephemeral**
- Enpoints (Applications) are **permanent** & **primary**

Figure 18. Blockchain vs. ESB integration (Herudek, 2015).

Finally, it has to be remembered that public Blockchains, despite their some questionable features described above, also have some inherent advantages for enterprise use also. Shortly according to (Buterin 2015), public Blockchains:

- have ultimate censorship resistance: even the creator of an application may be unable to change the application code running in the public Blockchain
- are widely used, include a wide range of assets (which could be combined innovatively) and therefore can gain some network effects.

Thus, Buterin (Buterin 2015) concludes that some kind of combination of public and private Blockchain is often the most optimal solution for enterprises:

“..By creating privately administered smart contracts on public Blockchains, or cross-chain exchange layers between public and private Blockchains, one can achieve many kinds of hybrid combinations of these properties.”

5.3 Six Requirements for Blockchain Use Case

More important than easiness of technology adoption are the valid and value creating use cases in which the technology will be used as enabler. Greenspan (2015) has presented some guidelines to ensure that a Blockchain use case is valid and the way avoiding pointless Blockchain projects. The guidelines emphasize eight conditions that a use case should fulfill in order to be potential use case implemented using Blockchain technology. The conditions (Greenspan, 2015) relate to:

1. Shared databases
2. Multiple writers
3. Absence of trust

4. Disintermediation
5. Interaction between the transactions
6. Rules restricting the transactions performed
7. Validators
8. Assets

Etla (Mattila J. et. al., 2016) has developed a tentative use case for autonomous machine-to-machine transactions of electricity in a housing society environment through an iterative process with stakeholders in the energy industry. The use case, outlined concept and technical specifications have been evaluated against six criteria for a sensible Blockchain use case. These six criteria have been derived from Greenspan's (2015) eight conditions and those are (Mattila J. et. al., 2016):

1. A database shared by multiple parties
2. Enabling multiple concurrent writers
3. Maintaining consensus regarding the content of the database
4. Interacting modifications
5. The absence of trust
6. The undesirability of intermediation

The first of these six criteria (for the sensibility of a potential Blockchain use case) is that use case requires a database to be shared between many parties. The Blockchain has no applicability in a centralized database. The second criteria is that there must be a need for many parties to be able to make potentially overlapping modifications into the database at the same time. If such a need is not present, some more conventional database structures will be sufficient for the purpose. The third criteria relates to consensus regarding to the content of database. For any system that involves maintaining a distributed consensus architecture, it is important that all participants agree on the content of the shared database. As fourth criteria, the modifications written into the shared database by all the concurrent writers must somehow interact together. This means that even if the modifications do not directly overlap or contradict each other, they are still somehow interconnected. The fifth criteria concerns about the absence of trust. The key disruptive element in Blockchain technology is its ability to maintain consensus on the content of a shared database between equipotent, equally privileged nodes that are unknown to each other. Therefore, it is well suited for situations where the parties that have a need for a shared database do not trust each other in some level. The last criteria about the undesirability of intermediation means that using a trusted third party is undesirable for one reason or another. (Mattila J. et. al., 2016)

6. Blockchain Use Cases

According to the Moody's, Blockchain technology has the potential to improve the efficiency and security of transactions and record keeping across a variety of mainstream processes and regulated industries. Companies and enterprises are assessing how Blockchain technology could affect their businesses and Over 120 ongoing projects have been identified in addition to huge amount of investments and partnerships with start-ups to internal projects and industry collaborations. The technology seems to have application potential in domains and sectors from capital markets and trade finance, healthcare and energy, to government taxation. (Moody's, 2016)

BlockchainTechnologies.com (free resource to help entrepreneurs, investors, and consumers learn about the rapidly emerging field of Blockchain technologies) divides the Blockchain use cases into four categories: (BlochchainTechnologies.com, 2017)

- Finance
  - Trade and settle securities at a fraction of the time and cost.
- Property
  - Permanently record and access real-time property rights.
- Contracts
  - Self-enforcing contracts based on predefined conditions.
- Identity
  - Eliminate invasive identity practices via digital identities.

Let's Talk Payments (LTP. News, insights & data-driven research in emerging financial services and payments), presents the Blockchain use cases in two domains: Financial and non-financial use cases. Both use case domains include vast amount of application specific use cases where the Blockchain technology can be seen as enabler or has already been utilized. (LTP, 2017)

There are not so many scientific publications available relating to potential or researched Blockchain use cases. Most of the realized use cases of the Blockchain relate to the financial sector. Focus in over 80% of the papers is on Bitcoin system and less than 20% deals with other Blockchain applications including e.g. smart contracts and licensing (Yli-Huumo et.al, 2016). Despite these facts, in practice there is many non-financial use case ideas risen that might realize in the future.

Following chapters presents a review of promising use cases that Blockchain technology has enabled or can enable in the future. The cases are divided into Financial and non-financial use cases.

6.1 Financial Use Cases

Table 12. Financial use cases.

Use case/Application Domain	Description/Utilization Idea	Real life solution examples
Currency	Cryptocurrency and payment.	Bitcoin and several other similar currencies/solutions.
Digital security trading	Ownership and transfer. Trade and settle securities at a fraction of the time and cost. Post Trade Processing, Settlement, Clearing.	Royal Mint hopes to start accepting trades from the middle of 2017 on its Royal Mint Gold platform, which will log each transaction using Blockchain. A bank consortium consisting of Bank of America Merrill Lynch, HSBC and the Infocomm Development Authority (IDA) of Singapore successfully applied distributed ledger technology to replace paper-based letters of credit (LCs) in trade finance transactions and streamline global trade.
Escrow/custodian service	Escrow or custodian service.	RAISTONE is a Blockchain-based digital asset transfer and distributed escrow system.
Securities	Smart Securities via Smart Contracts.	
Loans	Loan Origination and Servicing.	Synaps Loans: A proof-of-concept (PoC) which will run through the end of this year. Through Synaps, loan investors have direct access to an authoritative system of records for syndicated loan data. By connecting a network of agent banks through Blockchain, faster and more certain settlements in the syndicated loans market can be achieved.
Exchange	Foreign Exchange Markets.	Fidor Bank bank has partnered with Kraken to

Use case/Application Domain	Description/Utilization Idea	Real life solution examples
		provide a digital currency exchange in EU, and with Bitcoin.de, a P2P BTC trading platform in Germany. Fidor has also partnered with Ripple Labs to provide money transfer services.
Payments and transactions	Cross border payments and transactions.	The first ever cross-border Blockchain transaction has taken place, between the Commonwealth Bank of Australia and California-based Wells Fargo, for a shipment of cotton sent from the United States to China. The Ripple network has announced that seven banks including Santander, CIBC, UniCredit, UBS, ReiseBank, National Bank of Abu Dhabi and ATB Financial of Edmonton "had made a breakthrough by being among the first financial institutions in the world to move real money across borders using Blockchain-based distributed ledger technology provided by Ripple" Santander has piloted Ripple for cross border payments.
Crowdfunding	Enabling secure and transparent crowdfunding	
RegTech	Regulatory Technology: For example automatic customs services.	
Invoicing	Distributed invoicing.	Standard Chartered, the Development Bank of Singapore (DBS) and the Infocomm Development Authority of Singapore (IDA), the government's

Use case/Application Domain	Description/Utilization Idea	Real life solution examples
		IT and communications arm developed a Blockchain-based invoice trading platform (TradeSafe) that uses the distributed ledger technology developed by Ripple.

6.2 Non-Financial Use Cases

Table 13. Non-financial use cases.

Use case/Application Domain	Description/Utilization Idea	Real life solution examples
Application development	Proof of ownership of modules in application development.	
Digital content	Proof of ownership for digital content storage and delivery.	See the Music use case.
Ride-sharing	Points-based value transfer for ride-sharing.	Ridesharing startup Arcade City has launched its mobile application. The platform uses Blockchain technology (Ethereum based) “to issue crypto-equity” to drivers
Digitization of documents and contracts	Digitization of documents and/or contracts and proof of ownership for transfers.	See the Real estate use case.
Decentralized storage	Decentralized storage using a network of computers on Blockchain.	
Company incorporations	Digitizing company incorporations, transfer of equity, ownership and governance.	
Decentralized Internet and computing resources	Decentralized Internet and computing resources to cover homes and/or business.	
Home automation	Platform to link the home network and electrical devices to the cloud.	Increasing number of companies are starting to offer Blockchain-based home automation systems. For example Edgelogic.
Digital identity	Digital identity that protects consumer privacy.	ShoCard is one of the block chain based identity verification systems for

Use case/Application Domain	Description/Utilization Idea	Real life solution examples
	Eliminate invasive identity practices via digital identities. Digital Identities like passports, E-Residency, Birth Certificates, Wedding Certificates, IDs, Online Account Logins, etc.	security, privacy, and fraud protection.
IT portal	A smart contract IT portal executing order fulfillment in e-commerce or manufacturing.	See the Market place use case.
Digitizing assets	Improving anti-counterfeit measures.	
Reputation management	Helps users engage, share reputation and collect feedback.	White Paper: Feedback Based Reputation on Top of the Blockchain by Davide Carboni.
Prediction platform	Decentralized prediction platform for the share markets, elections, etc.	Augur is a decentralized prediction market platform that runs on Ethereum.
Authenticity of a review and endorsements	Enabling authenticity of a review through trustworthy endorsements for peer reviews.	
Authentication and authorization	Authentication and authorization based on digital identity	See the Digital Identity use case.
Market place	Digital trusted and secure market place.	See the Energy use case.
Smart contracts	Self-enforcing contracts based on predefined conditions.	
Real estate	Mostly paper-record based industry, when Blockchain allows for a significant gain in efficiency in how records are stored and recorded.	Atlantic Sotheby's International Realty has tested real property ownership transfer with Blockchain based real estate platform Ubitquity.
IoT and Smart property	Smart, Autonomous Property allows ownership of both physical and non-physical property to be verified, programmable and tradeable on the Blockchain. Physical examples of smart property include vehicles, phones and houses that can be activated, deactivated, tracked and maintained.	

Use case/Application Domain	Description/Utilization Idea	Real life solution examples
	Blockchain technology can be seen as missing link to settle scalability, privacy, and reliability concerns in the Internet-of-Things. Connected Vehicles, wearables, Smart Appliances, Supply Chain Sensors, etc.	
Energy	Energy market place. New peer-to-peer models of power production and distribution.	RWE/BlockCharge: Working prototype for Electric Vehicle Charging on the Ethereum Blockchain. Australia's first Blockchain powered residential electricity trading market has been launched in Perth based on Power Ledger's trading platform.
Property	Permanently record and access real-time property rights.	
Music	Streamline ownership rights, provide fair payment for musician's work, and bring transparency to all.	MUSE is a Blockchain specifically tailored for the music industry. It serves as a global database for copyrights, a means of payment for all music related transactions (including royalties) as well as a tool to simplify licensing of musical works.
Smart Corporations	Decentralized autonomous corporations or organizations.	
Health	Universal EMR, Health data banks, QS Data Commons, Big health data stream analytics, Digital health wallet, HealthToken, Personal development contracts, patient records, etc.	
Supply chain management, logistics and stock optimization	Routing and tracking. Improving logistical process and transparency of supply chains.	Kouvola Innovation's Smart logistics. The goal is smart containers that partly arrange themselves their transport.
Public services	GBI - Guaranteed Basic Income	Switzerland freicoin

Use case/Application Domain	Description/Utilization Idea	Real life solution examples
Manufacturing	Enabling newly formed distributed manufacturing models, like 3-D printing.	innogy and EOS GmbH Electro Optical Systems will develop a prototype of a Blockchain-powered shared 3-D printing factory.
Gaming	Games that integrate cryptocurrencies in their own economy.	Spells of Genesis is a game developed by the Swiss-based company EverdreamSoft that integrates the bitcoin Blockchain technology in both its game economy and its storyline.
Elections and voting	By casting votes as transactions, created Blockchain keeps track of the tallies of the votes. Enables ensuring that no votes are changed or removed, and no illegitimate votes are added.	Online voting technology: https://followmyvote.com The Abu Dhabi Securities Exchange (ADX) has launched the service enables stakeholders to both participate in and observe votes held during annual general meetings (AGMs).
Insurances	Peer-to-peer insurance: P2P insurance empowers policyholders to a greater portion of the premiums rather than the individual private wealth managers working to produce returns for insurance companies.	Dynamis is a peer-to-peer supplemental unemployment insurance protocol that uses the policy holders' social capital to replace underwriters: http://dynamisapp.com/
	Parametric insurance: Instead of indemnifying the pure loss, insurers would agree to pay a certain amount upon the occurrence of triggers within preset smart contracts.	Rainvow's Ethereum platform facilitates automatically compensating unforeseen transportation costs on rainy days: http://www.rainvow.org/
	Micro insurance: Enable trust between peers to increase transparency for populations living in remote regions of the world. The virtual nature of the transactions could side-step governmental bureaucracy to make geographic limitations irrelevant within its context.	Platform-creating startups like Factom facilitate highly specific insurance policies: https://www.factom.com/ Helperbit uses the Blockchain protocol to enable philanthropists to donate digital currencies to underfunded, hard to

Use case/Application Domain	Description/Utilization Idea	Real life solution examples
		reach nonprofits in remote regions of the world. Their risk assessment platform allows pooling money while limiting fraud exposure: https://www.helperbit.com/
Smart buildings	Integrated building and communications services.	
Land titles	Handling land titles.	Honduras is planning to use Blockchain to handle land titles
Taxation	Blockchain could have significant implications for helping reduce tax frauds. It provides numerous solutions for tax reporting.	UK Government Explores The Use Of Blockchain To Track Tax Revenue.
Notary service and document registry	Registering notary services and documents.	The Isle of Man has begun testing the technology with a registry of companies on the island.
Agricultural & drone networks	Smart farms, food tracking, weather forecasts and weather data, minimizing unfair pricing, etc.	Provenance is a Blockchain-based system that tracks goods such as food and makes the information public, secure and all-inclusive.
Mobile networks	Blockchain solutions can help telecommunication operators cut costs and make their digital services more competitive. Block chain can be applied to for example internal processes, roaming, connectivity provisioning, digital asset transactions, M2M, smart cities, mobile money and identity management.	
Integrated smart city	Enabling urban area where applied integrated technology such as smart grids and smart meters for enhancing infrastructure for electricity, water supply, waste management, and other basic needs.	The city of Rotterdam will use a Blockchain to record lease agreements for the Cambridge Innovation Center (CIC)
Self-driving car	Self-driving cars could leverage Blockchain	

Use case/Application Domain	Description/Utilization Idea	Real life solution examples
	technology for example in automated car sharing.	
Car leasing/buying	Process of leasing or buying a car by automating all the steps into secure electronic environment	DocuSign proof-of-concept app (developed by Visa) for car-based commerce.
Digital assistants/chatbots	A record of all digital assistant/chatbot activity.	Bank of America announced the launch of “Erica,” its new digital assistant that will be available inside the bank’s mobile app. Erica will help customers to handle money better by providing investment advice and account analysis.
Science	Community supercomputing, Crowd analysis, P2P resource nets.	
Household appliances	Household appliance operations. Appliances/devices operating autonomously looking after themselves	IBM’s ADEPT-project in which the operation of washing machine is based on the Blockchain technology.
S2aaS	Sensing-as-a-Service: physical goods that help to create data initiate multi-sided markets for sensor data in which one or more customer groups (the markets buying side) subscribe to and pay for data that is provided by one more data creator (selling side).	For example, weather stations.
Circular Economy	Products carry and possibly communicate information about their materials and status. The products automatically negotiate the most profitable way of recycling based on the offers in the network. The transportation of materials could respectively be planned and negotiated through the Blockchain-based system.	
Forestry	Enhancing the forestry business and timber market utilizing Blockchain and smart contracts.	

Use case/Application Domain	Description/Utilization Idea	Real life solution examples
Employment service	Decentralized employment company.	Colony: Decentralized employment company helps employers with freelancers.
Vehicle inspection	During inspection, vehicle data and mileage could be stored in Blockchain. This leads to the fact that the possibility of fraud could be reduced.	Ethlance: Decentralized zero-fee jobs marketplace.

7. Summary

Blockchain is a decentralized transaction and data management technology developed first for Bitcoin cryptocurrency. The Blockchain technology enables maintenance of a shared distributed ledger, Blockchain, which can be simultaneously read and modified by all involved parties but is not owned by any party.

The possibilities of the Blockchain technology has inspired and fueled an entire ecosystem around it, focused on fully unleashing its potential. This area has had exponential growth in the past couple of years, leading to a number of platforms, applications, startups, projects and research around this new invention. International electronic financial exchanges have begun to explore the adoption and utilization possibilities of Blockchain technology in their trade processing and reporting for execution and clearing. Interest has also arisen in industry domain towards Blockchain's possibilities together with Internet-of-Things (IoT) or Industrial Internet.

Several companies and public organizations/foundations develop Blockchain platforms that are mostly open sourced. The platforms enable fast prototyping, development and deployment of new Blockchain applications. There are also new kind of platforms under development all the time, including Industrial Internet of Things based on the Blockchain technology.

Even more important than easiness of technology adoption are the valid and value creating use cases in which the technology will be used as enabler. The feasibility of Blockchain technology depends on the use case where it will be applied. The use case should have clear needs for database shared by multiple parties and multiple writers, consensus, interacting modifications, trust and undesirability for intermediation.

Blockchain technology has the potential to improve the efficiency and security of transactions and record keeping across a variety of mainstream processes and regulated industries. Companies and enterprises are assessing how Blockchain technology could affect their businesses. Most of the realized use cases of the Blockchain relate to the financial sector, but there are many non-financial use case ideas that might realize in the future.

References

Allison, I. (2015). “ConsenSys Announces Microsoft Partnership to Deliver ‘Ethereum Blockchain-as-a-Service.’” http://www.ibtimes.co.uk/ethereum-spin-off-consensys-announces-microsoft-partnership-deliver-Blockchain-service-1526090 (December 13, 2016).

Atzori, M. (2016). Blockchain-based Architectures for the Internet of Things: A Survey.

Back, A. (2002). Hashcash-a denial of service counter-measure.

Bahga, A. and Madisetti, V.K. (2016). Blockchain Platform for Industrial Internet of Things. Journal of Software Engineering and Applications, 9, 533–546.

BitGo. (2015). “The Challenges of Block Chain Indexing”. URL: https://blog-archive.bitgo.com/the-challenges-of-block-chain-indexing/

BlockchainTechnologies.com. (2017). URL: http://www.Blockchaintechnologies.com/

Buterin, V. (2013). Ethereum white paper.

Buterin, V. (2015). “On Public and Private Blockchains - Ethereum Blog.” https://blog.ethereum.org/2015/08/07/on-public-and-private-Blockchains/ (January 4, 2017).

Cachin, C. (2016). “Architecture of the Hyperledger Blockchain Fabric *.” https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf (November 14, 2016).

Crosby, M., Nachiappan, P., Verma, S. & Kalyanaraman, V. (2016). Technical Report. Sutardja Center for Entrepreneurship & Technology, University of California Berkeley.

dinbits. (2016). “The Blockchain Verses Blockchains Verses Block-chains”. URL: http://news.dinbits.com/2016/11/the-Blockchain-verses-Blockchains.html

Driscoll, S. (2013). “How Bitcoin Works Under the Hood”. URL: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Financial Times. (2015). “How will Blockchain technology transform financial services?”. URL: https://www.weforum.org/agenda/2015/11/how-will-Blockchain-technology-transform-financial-services/

Fischer, M. J., Lynch, N. A., & Paterson, M. S. (1985). Impossibility of distributed consensus with one faulty process. Journal of the ACM (JACM), 32(2), 374–382.

Fuentes, B. (2016). “Blockchain with Hyperledger.” 65(April): 821–22. http://www.slideshare.net/benjaminfuentes1/Blockchain-with-hyperledger-public-version (November 30, 2016).

Gault, M. (2016). “Increasing Healthcare Security with Blockchain Technology”. Guardtime. URL: https://guardtime.com/blog/increasing-healthcare-security-with-Blockchain-technology

Gautham, N. (2016). “R3’s Corda Becomes Open Source, Joins Hyperledger - NEWSBTC.” http://www.newsbtc.com/2016/10/22/r3-corda-hyperledger-open-source/ (November 29, 2016).

Gray, M. (2016a). Introducing Project “Bletchley.” https://github.com/Azure/azure-Blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md#bletchley.

Gray, M. (2016b.) Project Bletchley - The Cryptlet Fabric Cryptlets in Depth. https://github.com/Azure/azure-Blockchain-projects/blob/master/bletchley/CryptletsDeepDive.md (December 19, 2016).

Greenspan, G. (2015). Avoiding the pointless Blockchain project. URL: http://www.multichain.com/blog/2015/11/avoiding-pointless-Blockchain-project/

Greenspan, G. (2016). Four genuine Blockchain use cases. URL: http://www.multichain.com/blog/2016/05/four-genuine-Blockchain-use-cases/

Hertig, A. (2016). “Intel Is Winning Over Blockchain Critics By Reimagining Bitcoin’s DNA - CoinDesk.” http://www.coindesk.com/intel-winning-Blockchain-critics-reimagining-bitcoins-dna/ (December 28, 2016).

Herudek, B. (2015). “Integration – The Blockchain ‘Killer Usecase’ – Part I.” http://www.servicetechmag.com/I93/1215-1 (January 4, 2017).

Hileman, G. (2016). “State of Blockchain Q1 2016: Blockchain Funding Overtakes Bitcoin - CoinDesk.” http://www.coindesk.com/state-of-Blockchain-q1-2016/ (February 1, 2017).

“Hyperledger-Wikipedia”. (2016). (December 2015). https://en.wikipedia.org/wiki/Hyperledger.

Hyperledger Project. (2016). “Overview of Hyperledger Introduction to the Linux Foundation’s Hyperledger Project.” http://www.redwoodmednet.org/projects/events/20160718/docs/rwmn_20160718_behlendorf.pdf (November 21, 2016).

“Hyperledger Whitepaper”. (2016). https://docs.google.com/document/d/1Z4M_qwILLRehPbVRUsJ3OF8Iir-gqS-ZYe7W-LE9gnE/edit#heading=h.m6iml6hqrnm2 (November 21, 2016).

IOTA. (2016). URL: https://iota.readme.io/ URL: https://www.iotatoken.com/

Lombardo, H. (2016). “Hyperledger’s Evolving Blockchain Fabric, Merging Blockstream, DAH, IBM Code | Chain-Finance.com.” http://Blockchain-finance.com/2016/03/28/hyperledgers-evolving-Blockchain-fabric-merging-blockstream-dah-ibm-code/ (November 30, 2016).

LTP - Let’s Talk Payments. (2016). URL: https://letstalkpayments.com/an-overview-of-Blockchain-technology/

Manoj, S. (2016). “Hyperledger & Smart Contracts.” https://www-01.ibm.com/events/wwe/grp/grp307.nsf/vLookupPDFs/2-3. Introduction to Hyper-ledger Fabric & Exploring Blockchain Application & Docker Containers/$file/2-3. Introduction to Hyper-ledger Fabric & Exploring Blockchain Application & Docker Contain (November 29, 2016).

Mattila, J., Seppälä, T., Naucler, C., Stahl, R., Tikkanen, M., Bådenlid, A. & Seppälä, J. (2016). Industrial Blockchain Platforms: An Exercise in Use Case Development in the Energy Industry.

Mattila J. and Seppälä T. (2017). ‘Equilateral governance in Multi-sided Platforms’, presented at the ISA 2017.

Michalik, V. (2016). “Digital Transformation : Hyperledger: Giants Respond to Blockchain Challenge.” http://digitaltransformation.frost.com/expert-insights/viewpoints/hyperledger-giants-respond-Blockchain-challenge/ (November 22, 2016).

Moody’s. (2016). URL: https://www.moodys.com/research/Moodys-Blockchain-can-bring-benefits-to-the-financial-industry-and--PR_352414

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

O ’dowd, A. (2016). “IBM’s Open Blockchain Making Blockchain Real for Enterprises.”

Peters, G.W. & Vishnia, G.R. (2016). Overview of Emerging Blockchain Architectures and Platforms for Electronic Trading Exchanges.

Poelstra, A. (2014). “A treatise on altcoins”.

Popov, S. (2016). The Tangle. IOTA White Paper. Jinn Labs. V 0.6

Sameeh, T. (2017). "CASPER – Proof of Stake (PoS) Consensus Protocol For Implementation On Ethereum" https://www.deepdotweb.com/2017/01/15/casper-proof-stake-pos-consensus-protocol-implementation-ethereum/ (January 22, 2017)

Swanson, T. (2016). “What Is the Difference between Hyperledger and Hyperledger? | Great Wall of Numbers.” http://www.ofnumbers.com/2016/03/05/what-is-the-difference-between-hyperledger-and-hyperledger/ (November 21, 2016).

Tschorsch, F., & Scheuermann, B. (2015). Bitcoin and beyond: A technical survey on decentralized digital currencies.

Vallivaara, V. Koens T, Hoepman J-H., (2017).)" Consensus Mechanisms in Blockchain Technologies: A Survey"

Valtanen, K. & Vallivaara, V. (2016). Blockchain – new possibilities for Industrial IoT. ECIIIOT report.

Walport, M. (2016). Tech. Rep UK Government Office for Science Distributed Ledger Technology: Beyond Block Chain.

Wang, H., Chen, K. & Xu, D. (2016). A Maturity Model for Blockchain Adoption.

Yli-Huumo, J., Ko, D., Choi, S., Park, S. & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?–A Systematic Review.

Series title and number

VTT Technology 330

Title	**Blockchain review** BOND project (Blockchains Boosting Finnish Industry) report
Author(s)	Jere Backman, Kristiina Valtanen, Arto Laikari, Visa Vallivaara, Juuso Ilomäki
Abstract	Blockchain is a decentralized transaction and data management technology developed first for Bitcoin cryptocurrency. The possibilities of the blockchain technology has inspired and fueled an entire ecosystem around it, focused on fully unleashing its potential. The area has had exponential growth in the past couple of years, leading to a number of platforms, applications, startups, projects and research around this new invention. Several companies and public organizations/foundations develop blockchain platforms that are mostly open sourced. The platforms enable fast prototyping, development and deployment of new blockchain applications. There are also new kind of platforms under development all the time, including Industrial Internet of Things based on the blockchain technology. The feasibility of blockchain technology depends on the use case where it will be applied. The use case should have clear needs for database shared by multiple parties and multiple writers, consensus, interacting modifications, trust and undesirability for intermediation. Blockchain technology has the potential to improve the efficiency and security of transactions and record keeping across a variety of mainstream processes and regulated industries. Most of the realized use cases of the blockchain relate to the financial sector, but there are many non-financial use case ideas that might realize in the future.
ISBN, ISSN, URN	ISBN 978-951-38-8649-3 (URL: http://www.vttresearch.com/impact/publications) ISSN-L 2242-1211 ISSN 2242-122X (Online) http://urn.fi/URN:ISBN:978-951-38-8649-3
Date	03 2017
Language	English, Finnish abstract
Pages	55 p.
Name of the project	BOND - Blockchains Boosting Finnish Industry
Commissioned by	Tekes – the Finnish Funding Agency for Innovation, Research institutes: VTT Technical Research Centre of Finland Ltd., Aalto University, Research Institute of the Finnish Economy, ETLA, Companies: 3Step IT Group Oy, Boogie Software Oy, Euroclear Finland Oy, Fortum Oyj, Keskinäinen Työeläkevakuutusyhtiö Elo, Kouvola Innovation Oy, Nokia Solutions and Networks Oy, Telia Finland Oyj and Tietomitta Oy
Keywords	blockchain, blockhain platform, distributed ledger, consensus, blockchain use case
Publisher	VTT Technical Research Centre of Finland Ltd P.O. Box 1000, FI-02044 VTT, Finland, Tel. 020 722 111

Julkaisun sarja ja numero

VTT Technology 330

Nimeke	**Blockchain review** BOND-projektin (Blockchains Boosting Finnish Industry) raportti
Tekijä(t)	Jere Backman, Kristiina Valtanen, Arto Laikari, Visa Vallivaara, Juuso Ilomäki
Tiivistelmä	Lohkoketju on hajautettu tapahtumien ja datan hallintateknologia, jonka ensimmäinen laajasti tunnettu toteutus on Bitcoin-kryptovaluutta. Lohkoketjuteknologian mahdollisuudet ovat inspiroineet kokonaisia ekosysteemejä ympärilleen, joiden tarkoituksena on päästää valloilleen sen lupaukset. Tämän teknologian alueella on muutaman viimeisen vuoden aikana tapahtunut eksponentiaalista kasvua, joka on johtanut lukuisten toteutusalustojen, applikaatioiden, start-up:ien, projektien ja tutkimuksen kehittämiseen lohkoketjujen saralla. Lukuisat yritykset ja organisaatiot kehittävät lohkoketjualustoja avoimen lähdekoodin toteutuksina. Alustat mahdollistavat nopean prototypoinnin ja sovelluskehityksen lohkoketjutoteutuksille. Uudenlaisia lohkoketjualustoja kehitetään koko ajan, myös teollisen esineiden Internetiin perustuvilla teknologioilla. Lohkoketjuteknologian soveltuvuus erilaisiin sovelluksiin riippuu vahvasti käyttötapauksesta. Käyttötapauksen pitää tarvita usean toimijan jakamaa hajautettua tietokantaa, yhtäaikaisia tapahtuman tuottajia, kaikkien toimijoiden konsensusta, vuorovaikutteisia tapahtumia sekä keskinäistä luottamusta ilman kolmansia osapuolia. Lohkoketjuteknologian lupauksena on parantaa tapahtumien kirjanpidon tehokkuutta ja turvallisuutta sekä monissa valtavirran prosesseissa, että säänneltyjen teollisuuksien aloilla. Useimmat toteutetut lohkoketjukäyttötapaukset ovat finanssisektorilta, mutta tulevaisuudessa tultaneen näkemään myös monia muiden toimialojen käyttötapauksien toteutuksia.
ISBN, ISSN, URN	ISBN 978-951-38-8649-3 (URL: http://www.vtt.fi/julkaisut) ISSN-L 2242-1211 ISSN 2242-122X (Verkkojulkaisu) http://urn.fi/URN:ISBN:978-951-38-8649-3
Julkaisuaika	03 2017
Kieli	Englanti, suomenkielinen tiivistelmä
Sivumäärä	55 s.
Projektin nimi	BOND - Blockchains Boosting Finnish Industry
Rahoittajat	Tekes, Tutkimuslaitokset: Teknologian tutkimuskeskus VTT Oy, Aalto yliopisto, Elinkeinoelämän tutkimuslaitos ETLA, yritykset: 3Step IT Group Oy, Boogie Software Oy, Euroclear Finland Oy, Fortum Oyj, Keskinäinen Työeläkevakuutusyhtiö Elo, Kouvola Innovation Oy, Nokia Solutions and Networks Oy, Telia Finland Oyj ja Tietomitta Oy
Avainsanat	lohkoketju, lohkoketjualusta, hajautettu tilikirja, konsensus, lohkoketjukäyttötapaus
Julkaisija	Teknologian tutkimuskeskus VTT Oy PL 1000, 02044 VTT, puh. 020 722 111

Blockchain review

BOND project (Blockchains Boosting Finnish Industry) report

BOND project (Blockchains Boosting Finnish Industry) has been researching Blockchain technology usage for non-cryptocurrency Use Cases. We started our project in Q4/2016. As the Blockchain landscape is developing with increasing speed, we collected this snapshot view of existing Blockchain platforms and Use Cases to support our work in the beginning of our project.

This project, Tekes Dnro: 2421/31/2016, has been funded by Tekes – the Finnish Funding Agency for Innovation, research organizations: VTT Technical Research Centre of Finland Ltd, Aalto University, Research Institute of the Finnish Economy, ETLA and participating companies: 3Step IT Group Oy, Boogie Software Oy, Euroclear Finland Oy, Fortum Oyj, Keskinäinen Työeläkevakuutusyhtiö Elo, Kouvola Innovation Oy, Nokia Solutions and Networks Oy, Telia Finland Oyj and Tietomitta Oy.

ISBN 978-951-38-8649-3 (URL: http://www.vttresearch.com/impact/publications)
ISSN-L 2242-1211
ISSN 2242-122X (Online)
http://urn.fi/URN:ISBN:978-951-38-8649-3