impleum

blockchain solutions

Technical White Paper v1.0

20 November 2018

www.impleum.com

Contents

Common information

Technical whitepaper

Impleum technical whitepaper is Software Architecture Document. This is a living document that is updated as implementation is completed, and as the architecture and implementation changes.

Abstract

Impleum is a powerful and scalable path to develop decentralized applications (DApps). DApps use the decentralised capabilities of blockchain technology and a layer of powerful service nodes to route information. Integration of the blockchain is the deployment of the network node and setting up its connection with the DApp through a documented API. The core of Impleum platform is an object-oriented programming language C# with a huge developer community.

Disclaimer

This Impleum Technical White Paper is for discussion and information purposes only. The information contained herein is subject to change. No part of this draft document is legally binding or enforceable. Impleum Core Contributors and Impleum developers does not guarantee the accuracy of or the conclusions reached in this white paper, and this white paper is provided “as is”. Core Contributors and Impleum developers does not make and expressly disclaims all representations and warranties, express, implied, statutory or otherwise, whatsoever, including, but not limited to: (i) warranties of merchantability, fitness for a particular purpose, suitability, usage, title or noninfringement; (ii) that the contents of this white paper are free from error; and (iii) that such contents will not infringe third-party rights. Impleum Core Contributors and Impleum developers and its affiliates shall have no liability for damages of any kind arising out of the use, reference to, or reliance on this white paper or any of the content contained herein, even if advised of the possibility of such damages. In no event will Impleum Core Contributors and Impleum developers or its affiliates be liable to any person or entity for any damages, losses, liabilities, costs or expenses of any kind, whether direct or indirect, consequential, compensatory, incidental, actual, exemplary, punitive or special for the use of, reference to, or reliance on this white paper or any of the content contained herein, including, without limitation, any loss of business, revenues, profits, data, use, goodwill or other intangible losses.

Summary

A **blockchain** is a growing list of records, called *blocks*, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a merkle tree root hash).

By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer

network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.

Blockchain was invented by Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin.The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications, and blockchains which are readable by the public are widely used by cryptocurrencies. Private blockchains have been proposed for business use.

Bitcoin ultimately made its first appearance in 2009, bringing together the classic idea of the mutual distributed ledger, the blockchain, with an entirely digital currency that wasn't controlled by any one individual or organization. Developed by the still anonymous "Satoshi Nakamoto," the cryptocurrency allowed for a method of conducting transactions while protecting them from interference by the use of the blockchain.

Blockchain can be used for a much broader range of assets than just cryptocurrency: tangible assets such as cars, real estate and food products, as well as intangible assets such as bonds, private equity and securities. DApps based on Impleum platform can use blockchain to track the provenance of goods to minimize fraud, document tampering and double financing and etc.

The advantages in terms of costs, transparency, immutability, security and confidence that are characteristic of blockchain solutions mean that financial businesses, government departments and other organisations are exploring applications of all kinds with a view to delivering services more profitably and efficiently. However, reliable deployment of a new blockchain fit for purpose entails extensive overheads in terms of network infrastructure, development, security and ongoing maintenance. Moreover, use of an existing blockchain (such as Bitcoin) comes with numerous problems for a mainstream business, not least because users have no control over blockchain features or future development.

An attractive model for blockchain service provision exists in cloud computing. Cloud services may be tailored according to the needs of the organisation and infrastructure, platforms and software provided as services via web interfaces - without businesses having to take on the maintenance of these themselves.

Impleum will take a similar approach to blockchain deployment, enabling organisations to provision their own private blockchains, tailored to their precise needs but secured on the parent Impleum chain. This approach means there are few unnecessary overheads whilst allowing businesses to secure the benefits of a blockchain-based solution, developing services via powerful APIs and lite web-based clients.

Blockchain: a distributed ledger

Blockchain technology is commonly associated with Bitcoin and other cryptocurrencies, but that's only the tip of the iceberg. Some people think blockchain could end up transforming a number of important industries, from health care to politics.

Blockchain technology is commonly associated with Bitcoin and other cryptocurrencies, but that's only the tip of the iceberg. Some people think blockchain could end up transforming a number of important industries, from health care to politics.

While blockchain technology isn't simple when you dig into the nitty-gritty, the basic idea isn't too hard to follow. It's effectively a database that's validated by a wider community, rather than a central authority. It's a collection of records that a crowd oversees and maintains, rather than relying on a single entity, like a bank or government, which most likely hosts data on a particular server. Of course, a physical database kept on paper could never be managed by tens of thousands of peers. That's where computers, and the internet, come in.

Each "block" represents a number of transactional records, and the "chain" component links them all together with a hash function. As records are created, they are confirmed by a distributed network of computers and paired up with the previous entry in the chain, thereby creating a chain of blocks, or a blockchain.

The entire blockchain is retained on this large network of computers, meaning that no one person has control over its history. That's an important component, because it certifies everything that has happened in the chain prior, and it means that no one person can go back and change things. It makes the blockchain a public ledger that cannot be easily tampered with, giving it a built-in layer of protection that isn't possible with a standard, centralized database of information.
While traditionally we have needed these central authorities to trust one another, and fulfil the needs of contracts, the blockchain makes it possible to have our peers guarantee that in an automated, secure fashion.

That's the innovation of blockchain, and it's why you may hear it used to reference things other than Bitcoin and other cryptocurrencies. Though generally not used for it yet, blockchain could be used to maintain a variety of information. An organization called Follow My Vote is attempting to use it for an electronic voting system that's more secure than modern versions, and healthcare providers might one day use it to handle patient records.

Where did blockchain come from?

Although blockchain technology has only been effectively employed in the past decade, its roots can be traced back far further. A 1976 paper on New Directions in Cryptography discussed the idea of a mutual distributed ledger, which is what the blockchain effectively acts as. That was later built upon in the 1990s with a paper entitled How to Time-Stamp a Digital Document. It would take another few decades and the combination of powerful modern computers, with the clever implementation with a cryptocurrency to make these ideas viable.

Data security is failing and there has to be a better system. Blockchain creates a secure, unalterable public record and is poised to dramatically improve the world around you, from voting systems to rental contracts.

In order to validate the blocks in the same manner as a traditional private ledger, the blockchain employs complicated calculations. That, in turn, requires powerful computers, which are expensive to own, operate, and keep cool. That's part of the reason that bitcoin acted as such a great starting point for the introduction of blockchain technology, because it could reward those taking part in the process with something of financial value.

How do cryptocurrencies use the blockchain?

Although bitcoin, and alternative currencies, all utilize blockchain technology, they do so in differing manners. Since bitcoin was first invented it has undergone a few changes at the behest of its core developers and the wider community, and other altcoins have been created to improve upon bitcoin, operating in slightly different ways.

In the case of bitcoin, a new block in its blockchain is created roughly every ten minutes. That block verifies and records, or "certifies" new transactions that have taken place. In order for that to happen, "miners" utilize powerful computing hardware to provide a proof-of-work — a calculation that effectively creates a number which verifies the block and the transactions it contains. Several of those confirmations must be received before a bitcoin transaction can be considered effectively complete, even if technically the actual bitcoin is transferred near-instantaneously.

This is where bitcoin has run into problems in recent years. As the number of bitcoin transactions increases, the relatively-hard 10-minute block creation time means that it can take longer to confirm all of the transactions and backlogs can occur. This has lead to the creation of certain "off chain" solutions like the Lightning Network, which validate transactions less frequently, to provide faster transactions without slowing the rate of confirmations.

Certain alt-coins, geared towards faster transactions, don't have such a problem with scaling. With Litecoin it's more like two and a half minutes, while with Ethereum the block time is just 10-20 seconds, so confirmations tend to happen far faster. There are obvious benefits of such a change, though by having blocks generate at a faster rate there is a greater chance of errors occurring. If 51 percent of computers working on the blockchain record an error, it becomes near-permanent, and generating faster blocks means fewer systems working on them.

How does blockchain technology work?

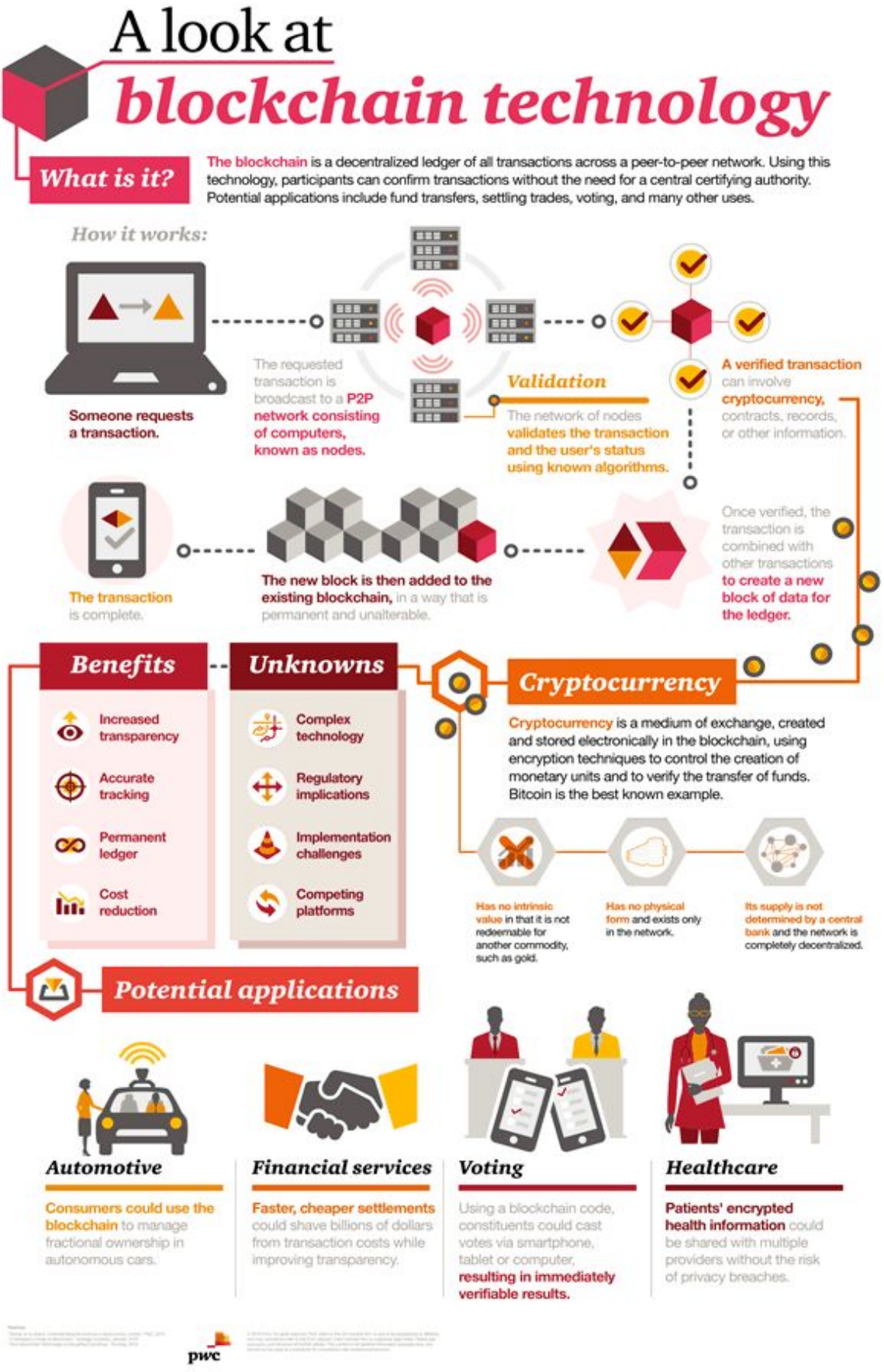
Each stage of a transaction is generating a set of data which are called blocks. As the transaction progresses, more blocks get added, forming a chain, hence the name.

Just as in cryptocurrencies like Bitcoin and others, which are based on blockchain technology, encryption software guarantees no one can ever delete or change blocks.

Several computers across a network have the blockchain software installed. Each transaction is shared to these nodes in the network and they compete (in Bitcoin jargon 'mining') to verify the transaction. The first one that verifies it also adds the block of data to the chain and gets an incentive for being first. The other nodes next check the transaction, agree that it's correct and replicate the record. All the computers then keep an updated copy of the ledger, and this acts as a form of proof that the transaction occurred.

As said, blockchain relies on peer-to-peer agreement as opposed to a central authority to validate a transaction. Until now, if you wanted to make a transaction, you informed a central authority who checked the details with everyone involved and holds a central record such as a bank, a notary or any other central certifying authority. In the blockchain model there is no such central authority. Transacting parties rely on an open register, the ledger, to validate the transaction. Authority comes from the fact that numerous computers, 'miners', have looked at the broadcast data, checked it and found it correct. Trust comes not from a notary's stamp, but the presumption that those computers can't all be wrong. You can imagine that there is quite some discussion here as well.

In the earlier mentioned press release regarding its series of IDC FutureScape 2018 webcasts and report, IDC described blockchain as follows: "At the core of blockchain is distributed ledger technology (DLT) that offers the potential to support digital trust at scale by providing one version of the truth (secure information), transfer of value (secure ownership records), faster settlements, and smart contracts (automated buying and selling)".


A look at
blockchain technology
What is it?
The blockchain is a decentralized ledger of all transactions across a peer-to-peer network. Using this technology, participants can confirm transactions without the need for a central certifying authority. Potential applications include fund transfers, settling trades, voting, and many other uses.
How it works:
Someone requests a transaction.
The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
The transaction is complete.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
Benefits
Increased transparency
Accurate tracking
Permanent ledger
Cost reduction
Unknowns
Complex technology
Regulatory implications
Implementation challenges
Competing platforms
Cryptocurrency
Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.
Has no intrinsic value in that it is not redeemable for another commodity, such as gold.
Has no physical form and exists only in the network.
Its supply is not determined by a central bank and the network is completely decentralized.
Potential applications
Automotive
Consumers could use the blockchain to manage fractional ownership in autonomous cars.
Financial services
Faster, cheaper settlements could shave billions of dollars from transaction costs while improving transparency.
Voting
Using a blockchain code, constituents could cast votes via smartphone, tablet or computer, resulting in immediately verifiable results.
Healthcare
Patients' encrypted health information could be shared with multiple providers without the risk of privacy breaches.
pwc

Some benefits of blockchain technology

In the blockchain model transacting parties rely on an open register to validate the transaction. This has some consequences for transactions of all kinds.

Speed
The absence of a central authority in theory makes blockchain faster. If you're relying on a central certifier, you depend on limited resources. Clearing and settling stock trades, for instance, can take days and usually involves some human intervention. With blockchain you have lots of computers competing to process your transaction as quickly as possible. Today they can do it in a matter of minutes. In the future it may only take seconds.

Cost
Blockchain is also cheaper. All the computers holding the blockchain are paid for by the participants in the hope that they will earn the incentive for being the first to validate the transaction.

Transparency
Blockchain is more transparent. It can give regulators and compliance officers clearer insight into the provenance of financial transactions, helping them to combat money laundering and manage risk.

Tracking
As nothing can be changed and the ledger is present across multiple nodes, blockchain is easier to track. It won't come as a surprise that blockchain is often used for asset tracking as a consequence *(more below)*.

What's the catch?

Blockchain technology has a lot of exciting potential, but there are some serious considerations that need to be addressed before we can say it's the technology of the future.

Remember all that computing power required to verify transactions? Those computers need electricity. Bitcoin is a poster child of the problematic escalation in power demanded from a large blockchain network. Although exact statistics on the power requirements of Bitcoin is difficult, it's regularly compared to small countries in its current state. That's not appealing given today's concerns about climate change, the availability of power in developing countries, and reliability of power in developed nations.

Bitcoin, blockchain 2.0 and the growth of distributed ledger technology

Blockchain 2.0 is in effect a mechanism allowing programmable transactions (transactions modified by a condition or a set of conditions). Sound simple enough, but in Ethereum network, for example, the language used to write such scripts is aTuring complete one that is, allowing to

implement any computable function. This enables a number of interesting concepts, which are adding value to the platform and causing a stir across the IT community.

Blockchain uses are not limited to transactions: they enable plenty of brand new economic opportunities previously unavailable on the world web. These include:

- *Microtransactions;*
- *Decentralized exchange;*
- *Creating and transferring digital assets;*
- *Smart contracts*

Smart contracts are scripts executed in blockchain environment; their codes are accessible to all and anyone can verify the correctness of code execution. The verification is carried out by miners in the blockchain environment. This ensures honest execution of the "contract."

Thus, an ecosystem of international decentralized, but trusted, links based on the blockchain technology is created. Which makes it possible for economic aspects to be built into all sorts of different things:

- Decentralized computer networks with built-in economic links;
- IoT (Internet of Things, if you happen to forget the meaning of this acronym); individual devices will engage in economic interplay (picture it: the refrigerator itself decides what is wanted, places orders and effects payments J);
- Smart cars, smart homes, smart cities. Let us not write these off: they are a part of not so remote a future, at some places they already make the present.

In all these cases blockchain allows transferring money or value. All the while being an effective and trusted information exchange tool for efficient distribution of resources.

Main concepts

Blockchain 2.0 being at the height of its development, there are quite a few different terms and concept, often overlapping ones. Let us cover the main ones in brief.

Microtransactions

This appears to be the simplest concept among those I am to describe, but it is certainly worth mentioning.

The Visa/Mastercard backbone technologies had been originally designed as centralized structures, and their bases make attractive targets for attackers, as we see from the many "hacker" movies and real life cases. Plus they are unable of effecting really small (micro)transactions. By small I means the minute transactions not supported by the traditional payment systems. Blockchain enables transactions worth portions of a cent. Small as they may be, this opens up a whole new horizon of opportunities.

Let me give you a simple example. Let's suppose in a city there are several companies operating cargo drones.Blockchain will make the drones able of economic team play — not only with the drones of the same fleet of but with third-party drones, too. For example,Drone 1 has to deliver cargo from A to B. It is free to calculate whether or not it is more economical for it to deliver its

payload to point C and put out a tender for it to be delivered from there to B by third-party drones; if feasible for both parties, it may strike a deal or complete the delivery by itself. This will improve the overall performance of the drone network.

There is another example I have seen quoted in the literature: your car is caught in dense traffic but you badly need to get along really quickly: let's suppose your wife is in labor. You are ready to pay the other road users a certain amount of money to make them move aside and give you the right of way. Those who let you pass (drivers who are not in a hurry to make their destinations) will each get a microtransaction for their help. Blockchain with its microtransaction feature set is exactly the engine to enable this. In a centralized system such transactions would be too costly to be considered.

Smart contract

Those of you who had never heard the term before are probably now asking themselves what a smart contract is. And yet, indirectly, we deal with this concept every day. This is a contract from our life, but one written using a programming language and automatically executed as soon as certain triggers are pulled.

The classic example of such a contract is the vending machine, always automatically operating according to a fixed set of rules: you pay the money, your make your choice — the machine releases your purchase. In the smart contract context, code becomes law; it cannot be contested and it will always be executed to a letter as soon as the conditions are met. At least, until recently I had never heard of any means of challenging such a contract. But every rule has its exceptions (I am going to tell you about one such interesting case later). The most important nuance here is that the contract must be executed without fail.

Smart property

Smart property is a new concept we are not used to at all yet. In this case property rights (for a car, apartment, etc.) are cryptographically fixed in the code.The asset (property) will only operate if recognizing legitimate user rights for the use of that property. This makes the transfer of property as simple as any transaction.

Of course, the smart property concept is based on widespread use and adaptation of decentralized trusted blockchain, which as of now appears to be quite a distant future. Yet I wouldn't be overly pessimistic — there are already blockchain startups used to register diamonds and watches.

By way of adding to the idea: using the information about the current balance of supply and demand supplied to it from the internet, the smart property item can potentially be engaged in economic activities of its own. Thus, a taxicab without a driver — a self-owned one — will be marketing its services or taking orders all by itself, balancing out its tariff based on time of day, current supply and demand.

DApps (Decentralized Applications)

These are apps executed in blockchain. Bitcoin, being a transaction-focused peer-to-peer network, happened to be the first ever decentralized application. The opportunity to make smart contracts and write executable code within blockchain has given birth to all sorts of decentralized applications. Besides, DAps can be quite independent from any particular blockchain, operating as entirely stand-alone applications. Example: MadeSafe, a distributed data storage application. In short, it operates like this: you make your disk space and up-time available to the network users and collect your premium for that; alternately, you can upload your data to the network in exchange for your service. There had been similar projects in the past (for example, Wuala), but now, for the first time ever, they are founded on economic principles: you simply offer your space and get paid. So far there is no certainty whether the project will survive.

Internet sources give a list of criteria an application must satisfy to be called a DApp:

- A Dapp must be fully open-code, it must operate as a stand-alone application and no organization may be able to claim possession of the greater part of its tokens. A Dapp may adapt its protocol in response to suggested improvements and market feedback, but all changes must be adopted by consensus of all its users.
- A DApp's data and operating reports must be encrypted and stored in a public domain, the so called decentralized blockchain, to avoid any potential network outage.
- A DApp must require a cryptographic token (bitcoin or original app token) for access to it. Every bit of input contributed by miners must be rewarded in DApp's tokens.

DAOs (Decentralized Autonomous Organizations)

One of the most impressive blockchain-based concepts is that of a decentralized autonomous organization. The traditional organizations we know of are all based onsets of contracts and agreements enforced by external agencies (laws, courts of justice, authorized bodies, etc.). This certainly increases the operating cost of such an organization and impairs the reliability of its rules and procedures. DAO, too, is based on a set of contracts, but these are not paper contracts but smart contracts executed in blockchain environment. This puts DAO ahead of the previous concepts and turns it into a sort of a company's robotized manager. DAO can collect and store the money received by way of investment, it can spend that money based on a known set of rules agreed upon by DAO members, and so forth.

Examples of decentralized autonomous organizations:

- An automated marketplace for trading resources or other valuables. A distributed independent marketplace with equal conditions for all participants. Some of the closer examples: stock markets or RTB-based advertising markets.
- The communities involved in organizing p2p interplay, such as you do or profi.ru, can well be based on decentralized principles.

In addition to DAO, there are such concepts as DACs (decentralized autonomous corporations) and DASs (decentralized autonomous societies).These appear a bit redundant to me, as they are in effect integral to the DAO concept and are not much different from DAO in terms of operating a decentralized organization. The different terms in this case seem only to mimic the familiar forms of centralized organizations, as we know them.

Summary: the DAO concept may greatly alleviate (or completely do away with) the company's operating costs by automating its operations, in full or in part.

This broader application was developed by a number of '2.0' platforms including Nxt and BitShares, amongst others. To date, however, all of these have been relatively limited in one way or another, and lack suitability in their current forms for adoption by real-world financial businesses.

The rise of Bitcoin and similar protocols was accompanied by a rapid re-evaluation by governments, regulators and the financial services industry of the existing paradigms. Due to Bitcoin's position outside of the control of state and financial authorities and its potential for misuse as a tool of fraud, money laundering and other illegal activity, as well as other concerns such as its volatility and the unregulated nature of the exchanges on which it traded, the first reactions tended to be scepticism and concern. However, an increasing number of actors have also recognised the potential of blockchain technology and the broad range of use cases to which the distributed ledger lends itself.

Blockchain technology: digital trust and distributed ledger technology (DLT) in business

Distributed ledger technology (DLT, also known as blockchain technology) revolves around an encoded and distributed database serving as a ledger (hence distributed ledger technology) whereby records regarding transactions are stored. At the core DLT is an innovative database approach with a data model whereby cryptography (encryption) is utilized in each transaction update and verification become possible across the specific blockchain network, depending on its goal and stakeholders.

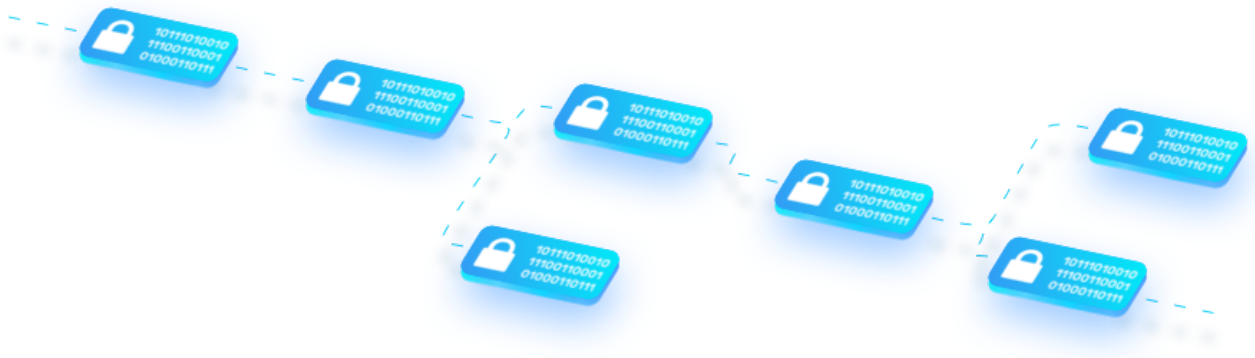
Distributed ledger technology in practice and beyond cryptocurrencies – how blockchains and DLT work, industries, applications, evolutions, networks and the business reality.
Is there still something that blockchain, a Distributed Ledger Technology *(DLT),* and known as the technology that powers cryptocurrency Bitcoin, doesn't promise to change in digital business and transaction processing and digital services requiring trust in one shape or another? Or perhaps better: is there still some challenge, organizational or other, whereby blockchain isn't hyped as the ultimate solution?

Although indeed being hyped in this stage *(and for most applications being in the early stages of hype cycles)* blockchain technology is part of the arsenal of software and solutions which are highly relevant in the scope of, among others, digital transformation. It certainly isn't the solution for everything *(well on the contrary)* as one might believe when seeing the hype but it is highly valuable in specific circumstances where its use is relevant.
Do note that today many opinions on what blockchain could mearn for "xyz" *(whereby blockchain really means DLT)* as you can see them in popular media and vendor talk are indeed just about that "what it could mean". Terms such as 'potential' and even 'revolutions' are very frequently used when the possibilities, rather than the realities of DLT are covered. As you know, between potential and reality there is a big gap – and there seem to be quite some revolutions

these days: the Industry 4.0 revolution, the artificial intelligence revolution *(really an umbrella term)*, you name it.

Blockchains *(indeed, plural)* are tested and deployed across several use cases of digital trust and exchanges in all industries, in and beyond cryptocurrencies, and as a contractual backbone of trust in a digital age. DLT is poised to be one of the fastest growing digital technologies and evolutions for several years to come and has a key role in ample relevant use cases in the digital transformation of several processes and industries.

Blockchain technology hype also leads to big difference between what a technology could possible do and what it really can do, or even better, does. However, there is no doubt about it: distributed ledger technology is becoming big business and big in business, some business that is.



Pic. 1 Blockchain technology

57% of organizations with over 20,000 employees is “actively considering” or in the process of deploying blockchain technology (Jupiter research, Summer 2017)

There are several reasons why DLT adoption is poised to be grow across use cases and industries of all kinds faster than expected while in many others it will not meet expectations or simply will not be needed. And even if it is still relatively early days for DLT for most companies, all signs are clear *(as are the roadmaps of some of our partners, de facto implementations and industry initiatives)*: distributed ledger technology is among the top evolutions, albeit with adoption, testing and effective usage at different speeds, depending on context, industry, use case and maturity of the organizations as tends to be the case with all technologies.
Table of Contents

The growth of DLT business initiatives

In 2017 and 2018 literally hundreds of companies, including leading global companies and leaders within their respective countries or regions across various sectors have joined important blockchain and DLT initiatives.

If you only look at the partners of a few more or less recent initiatives which we mention below such as IBM's cross-border payment blockchain initiative which mainly has companies from the Asia Pacific region on board as that's where it starts and which was announced in October 2017 you already have close to 100 companies. Yet, at the same time many of these initiatives *(will)* fail to meet their objectives while others are becoming more important.

However, before we start looking more in depth at some use cases and projects *(or, at least, link to them)* we need to give a small overview of DLT for business. For many distributed ledger technology is still relatively new, certainly outside of its Bitcoin and cryptocurrency scope *(and that's the scope OUTSIDE of which most business initiatives want to leverage DLT, leading to discussions about which terms we should really use)*. And since we only tackled blockchain technology from the financial services industry perspective in the past *(because that is where the attention outside the cryptocurrency context started and loads of transactions are involved)* and the IoT perspective *(because that is our second digital trend in our list to really watch in case you don't yet and involves even more transactions)*, we also want to look at what blockchain technology is and how it gets adopted in more applications and sectors than the mentioned ones *(from government to legal and supply chains)*. Use the table of contents above to jump to the section that interests you most.

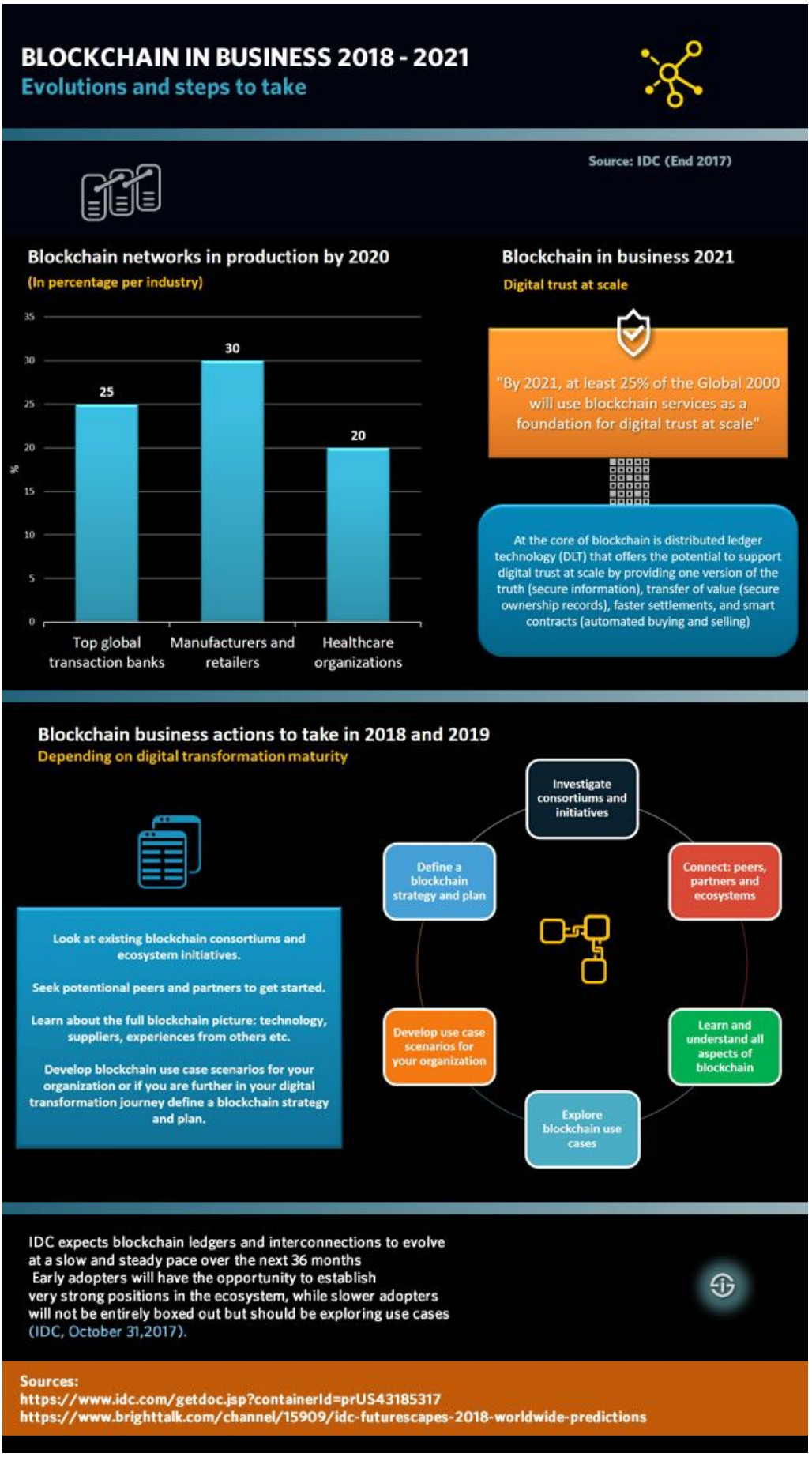
The scale and transformation of transactions in a decentralized digital age

As technologies and business approaches get distributed in virtually all digitalized areas, so do transactions. Moreover, new digital services pop up where there is a need for integrity, trust and security and existing services can be transformed using those same essential principles in a digital transaction context.

From transactions in the de facto distributed reality of the Internet of Things (IoT) to an increasing distributed transaction processing in business processes: the scale, speed, volumes and data involved are on the rise as we speak, with transactions in some applications and use cases being more than just on the rise.

The question is how do you deal with ever more and faster transactions as the core of digital business in a reliable way that doesn't slow down transactions in any way but, on the contrary, offers the speed they need in a trustworthy and cost-efficient way? Using a distributed technology and a different data model is the answer for many. Enter blockchain technology.

Blockchain 2018 – 2021 the future of blockchain and distributed ledger in business according to IDC's IDC FutureScapes: 2018 Worldwide Predictions



Blockchain technology: an encoded and decentralized database

As mentioned, blockchain revolves around an encoded and decentralized or distributed database (the 'distributed' part of distributed ledger technology) which serves as a ledger whereby records regarding transactions are stored and cryptography is used for each update in transactions.

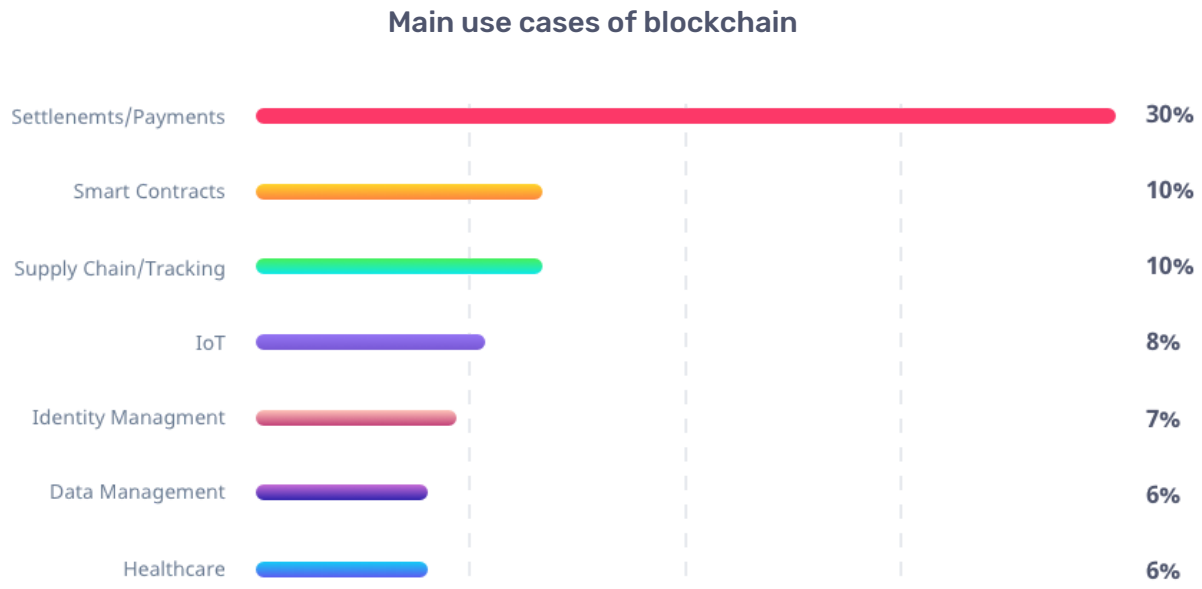
As mentioned in the introduction blockchain technology is rooted in the world of cryptocurrencies, more specifically Bitcoin. That connotation will disappear and we will not speak about the blockchain but about blockchains *(note the letter 's'),* blockchain technology or distributed ledger technology. Although today decentralization and the absence of a predefined central authority are often mentioned now in times where cryptocurrencies still have most attention, they aren't the strict essence *(moreover, even in Bitcoin there are central authorities so to speak, the Bitcoin miners, but that's a different story)*.

Blockchain technology is being tested and implemented across a broad range of applications, industries and use cases for endless applications. Examples, on top of the Internet of Things and financial services *(banking, insurance and reinsurance, capital markets)* include Industry 4.0, fraud management, digital identities, information management and far more areas and industries where it fits in a context of transactions, payments, contracts (smart contracts), proof, trust and so forth in the decentralizing nature of digital transformation technologies.

These records can't be changed as the model is distributed: there isn't a central authority but there also isn't any involved party *(those doing transactions)* that can change information. Blockchain relies on peer-to-peer network principles whereby each encrypted block in the chain is linked to the next. Why the peer-to-peer network and absence of a central authority? Because blockchain was precisely 'invented' to solve the challenge of the lack of a central authority in cryptocurrency Bitcoin.

However, this doesn't mean that blockchain is only used for very decentralized applications. Blockchain is used by organizations and/or groups of organizations for specific services where trust from other parties is needed or to build a blockchain network with other parties without traditional intermediaries. It's also important to differentiate between public and private blockchains and between blockchain networks from the perspective of the relevance of the goal and context in which they are used, which organizations and/or groups of organizations use them and what those exact services are.

The attention for blockchain from a security and secure transaction perspective is, among others, related to the fact that blockchain is a cryptographic ledger whereby the chain consists of encrypted blocks and after the validation of the transaction *(peer-to-peer and across the network)* it is added as a block to the chain as a permanent and unchangeable record of transaction in digital ecosystems with heavy transaction processing whereby transactions, data and speed increase and meet the need for a layer of trust.



Main use cases of blockchain as found by Juniper Research in the Summer of 2017 – more details below – source Venturebeat

Where blockchain technology is used – application areas

Below are some examples of where blockchain or distributed ledger technology is tested and implemented with some details per mentioned industry or area of application.

Blockchain in banking, insurance and finance services

Especially since 2015-2016, many initiatives were taken by large financial service providers and institutions, as well as FinTechs, regarding blockchain for finance.

Distributed ledger technology is among others used and/or tested for insurance applications such as claims management and for banking applications where digital identity and smart contracts are just a few use cases that fit in myriad financial operations. The transfer of funds and financial transactions are other areas which are also closer to the roots of blockchain.
A token of the rapid evolutions in banking is the earlier mentioned IBM blockchain-based cross-border payment solution which the company announced on October 16th, 2017. The solution aims to solve cross-border payment challenges and offers real-time clearing and settlement.

Over a dozen banks and institutions were involved in the development and deployment process. Cross-border payments are undoubtedly a key use case as in 2017 also SWIFT, Mastercard and the R3 consortium took initatives, the latter two and IBM did so in October 2017.

Digital identity is one of many applications that can be very useful in specific banking applications and even totally change the way we onboard customers, solving the identity problem and enabling full mobile onboarding as we explained at the occassion of the launch of Alastria, the first nation-wide and multi-sector blockchain ecosystem ever which was announced in Spain in October 2017 and where digital ID is an initial priority.

The Internet of Things and blockchain technology

The combination of blockchain and IoT is looked at and effectively leveraged for myriad reasons, ranging from smart contracts and IoT data monetization models across complex chains of connectivity where trust is crucial.

There are already blockchain applications in the context of the Internet of Things and some vendors have specific solutions to enable the use of blockchain for IoT to, among others increase trust, save costs and speed up transactions. IBM is a frontrunner here, although several vendor and industry initiatives have been launched with new solutions and actual deployments. IoT is all about transactions, contracts and trust in a distributed environment. Blockchain is, among others, the missing link to settle privacy and reliability concerns in IoT as the IEEE's Ahmed Banafa writes. Do note that IoT and blockchain convergence also touches upon the various other technologies (e.g. AI), industries (e.g. insurance and telematics) and activities (e.g. supply chain management, security) we mention on this page. In other words: IoT and blockchain needs to be seen in context and isn't just a matter of how blockchain can boost IoT and help solve challenges we see in IoT.

Blockchain and IoT

Supply chain management, logistics and blockchain

There is a very long road between manufacturing or even the design of a product and buying it in a retail store or online.

By keeping track of all transactions, again endless applications arise, for example with regards to where the product was made. There are several existing projects with regards to the usage of blockchain in supply chain management, logistics, transportation and so forth.
If there is one major part of global business where there is a high volume of transactions, an ecosystem with many players *(certainly in cross-border trade)* and still a high dependence on paper in a fast evolving and highly inter-connected ecosystem it's everything related to end-to-end supply chains.

So, it's not really a surprise that, after the financial sector, blockchain spending is poised to be largest in the distribution and services sector on a global level according to IDC's blockchain spending forecasts.

With blockchain, logistics and the various stakeholders in trade we are really in pretty much all areas of the by definition connected supply chain ecosystem where speed and accuracy matter more than ever. From outbound logistics and all the way *(with several forms of transportation)* to distribution or export with even more intermediaries, forms of transportation, freight forwarders, container shipping, import and inbound logistics, depending on the supply chain.
In order to really function we should have blockchains encompassing all these stakeholders and the many others we left out of this simplified ecosystem picture, or at the very least and certainly in a global supply chain context interoperability would be key as stakeholders such as customs, to name just one also have their systems.

In the past few years we've seen blockchain supply chain, logistics and transportation efforts and consortiums pop up, sometimes with a more global cross-border shipping focus and sometimes with a more specific focus such as container release and cargo flows in ports or dispute resolution in logistics.

Gradually these efforts are coming to fruition and existing initiatives announce new members. These also include e-commerce giants. In February 2018, for instance, Chinese retailer JD.com which is preparing to compete with Amazon in Europe and opened offices in Australia in 2018, all part of a major international push, joined BiTA, the Blockchain in Transport Alliance that has been announcing new members since the beginning of 2018 at an astonishing rate.
A major announcement in the context of global trade and supply chain digitization leveraging blockchain concerned the start of a joint venture between container shipping giant Maersk and IBM end January 2018.

IBM and Maersk have been working on blockchain possibilities for quite some time now and started their collaboration in the Summer of 2016. Several companies, ports and authorities already conducted pilots with the platform and several more are planning to join.
Yet, blockchain initiatives are also realize on a perhaps what less encompassing scale but with an ambition of growth that does beyond the initial goals which solve specific real challenges and then lead to more applications and blockchain use cases in a specific logistics context. A good example is this blockchain smart port case in the port of Antwerp where real challenges in the scope of maritime logistics and especially container release are tackled.

Industry 4.0 and blockchain

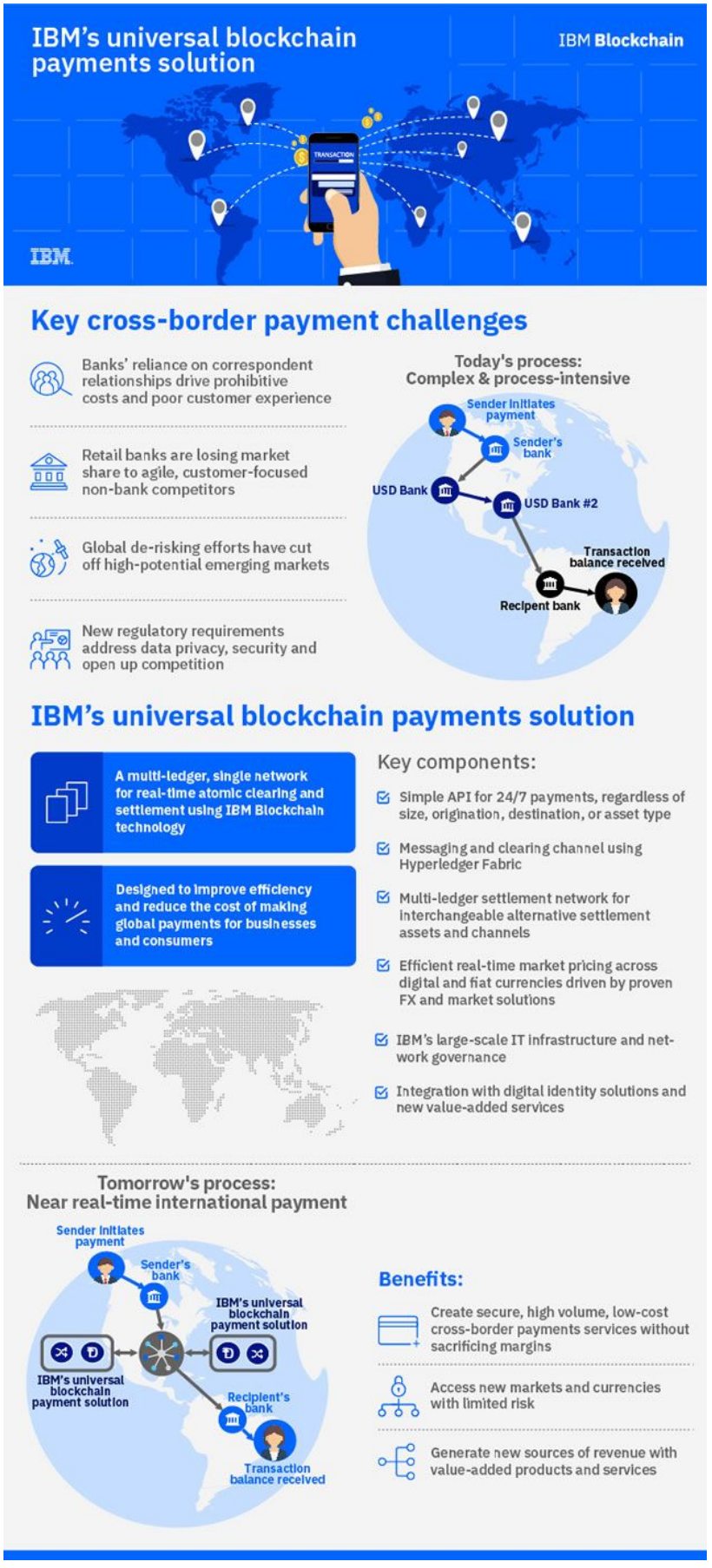
This is partially related to the previous area. If you thoroughly study the key aspects of Industry 4.0 and its Reference Architecture Model you no doubt will see how data-intensive and transaction-intensive it is.

The life cycle and value stream dimension of the architecture starts with early data collection and provisioning and maps data acquisition of production objects across the entire lifecycle. Blockchain technology is already used in Industry 4.0 applications and not just for industrial data. It is also a building block of intelligent ERP.

Other blockchain technology application areas

Some other application areas with a focus on transactions and security (the potential of blockchain also stretches to cybersecurity as such) include the use of blockchain in the public sector and government *(even including voting)* and myriad industries and use cases where rights management, trust and reliability, data protection and contracts are concerned in the increasingly digitized environments of sectors going through digital transformation: from the music and media industry to healthcare, the legal sector and more.
This list is far from exhaustive. In the next sections you can find some predictions (end 2017) with regards to the adoption of blockchain services and networks among large companies and a few of the major industries.

IBM universal blockchain payments solution – one of several blockchain cross-border payment initiatives launched in 2017 – read more about the IBM solution as depicted in this infographic



Blockchain in business

Looking back at 2017

As mentioned in the introduction, several large *(and less large)* firms, research bodies, start-ups, universities and so forth have launched or joined industry initiatives, blockchain research groups and alliances with roadmaps and standardization projects in 2017.

This happened in an increasing variety of areas, ranging from a secure and blockchain-based IoT project and vendor-led supply chain initiatives to a trucker association blockchain consortium, the mentioned cross-border payments blockchain initiative and Spain's national blockchain project – to name a few. After the Summer of 2017 the number of pilots, projects and initiatives grew fast, not just in number but also in business scope. This isn't going to stop in 2018 of course, well on the contrary. In the end, on top of new initiatives, existing ones enter in stages with solutions. That's when it really becomes interesting.

The sheer list of companies testing blockchain or having implemented it in 2017 is huge. From giants such as Maersk, dozens of insurance companies, the Port of Rotterdam, Lufthansa that recently announced a project to customers of a growing list of blockchain technology providers and hundreds of companies which you find in one or several of the associations, alliances and vertical/topical research groups.

The big blockchain technology leaders

Earlier we said that IBM is a frontrunner in the IoT and blockchain space but IBM also has the strongest credentials of all players in the blockchain sector and is quite ahead of its closest competitors.

That's at least what Juniper Research found in a survey. The results were announced in September 2017 *(and in several other releases throughout the Summer)* and it seems that over 40 percent of respondents cited IBM as being ranked first by enterprises that either consider or are in the process of deploying blockchain technology. According to Juniper's Blockchain Enterprise Survey, IBM is followed by Microsoft *(20 percent of respondents)* and Accenture.

Among the reasons for IBM's leadership position:

- High-profile R&D engagement with initiatives such as Hyperledger.
- A big list of actual blockchain clients across several verticals and use cases such as banking, asset tracking and the music industry.

Blockchain business adoption, investments and practices

The announcement of the Blockchain Enterprise Survey wasn't just about which technology players are recognized most when it boils down to blockchain, nor was the survey by Juniper (more findings in the infographic below).

There are some interesting numbers on the market and success factors, based upon the answers of some of the approximately 400 responding executives and IT leaders.

- Among the respondents prepared to share their investments in blockchain, 67 percent said already having invested over $100,000 by the end of 2016.
- Of those respondents, a whopping 91 percent said to at least spend the same amount in 2017.

The reason why spending continues or grows is related with the fact that the first results of the first investments were convincing/positive enough to conduct more extensive tests or integrate on a more extensive level. If this is a trend, then it's another token that in 2018 we'll see more spending and initiatives as the predictions of IDC clearly indicate.

A final takeaway: Juniper Research urges companies to focus on private blockchains for commercial deployments instead of public ones.

Where is blockchain a potentially good business fit?

End July 2017, Juniper Research released some other findings from the report showing that (as you can also check in the infographic below) 57 percent of organizations with over 20,000 employees is either 'actively considering' or in the process of deploying blockchain technology.

34 percent doesn't know and 9 percent is not actively considering or deploying. That picture completely changes when looking at all companies, including those with over 200,000 employees where we see that the majority of respondents is still saying 'yes' but instead of 57 percent that number considerably drops to 39 percent *(play with the interactive infographic below)*.

That brings us to the question for which kind of companies, industries and use cases blockchain is a good fit. And that's also what Juniper Research wanted to know. The result is a white paper with the apt name 'Which Industries are the Best Fit for Blockchain?'.
From the press release we remember a few things. According to the research, companies which would benefit most from blockchain include those with:

- a need for transparency and clarity in transactions
- a current dependence on paper-based legacy storage systems
- and/or a high volume of transmitted information.

So, indeed transactions, trust, transparency and a lot of data with the need for speed in a decentralizing technology landscape. With regards to the paper aspect don't think that tomorrow we'll live in a paperless society with blockchain, trust us. On the other hand, in various applications blockchain can indeed speed up a higher independence from paper-based legacy storage systems *(especially when powered by a consortium and a private blockchain that is de facto changing the game in areas where those who want to remain relevant simply have no choice)*.

Disruption and underestimation of the blockchain challenge as risks
When we talk about changing the game there are also the human, cultural and other contextual transformation parameters. And here Juniper research really hits the nail when saying that, despite growing awareness of (the benefits of) blockchain and more initiatives, it

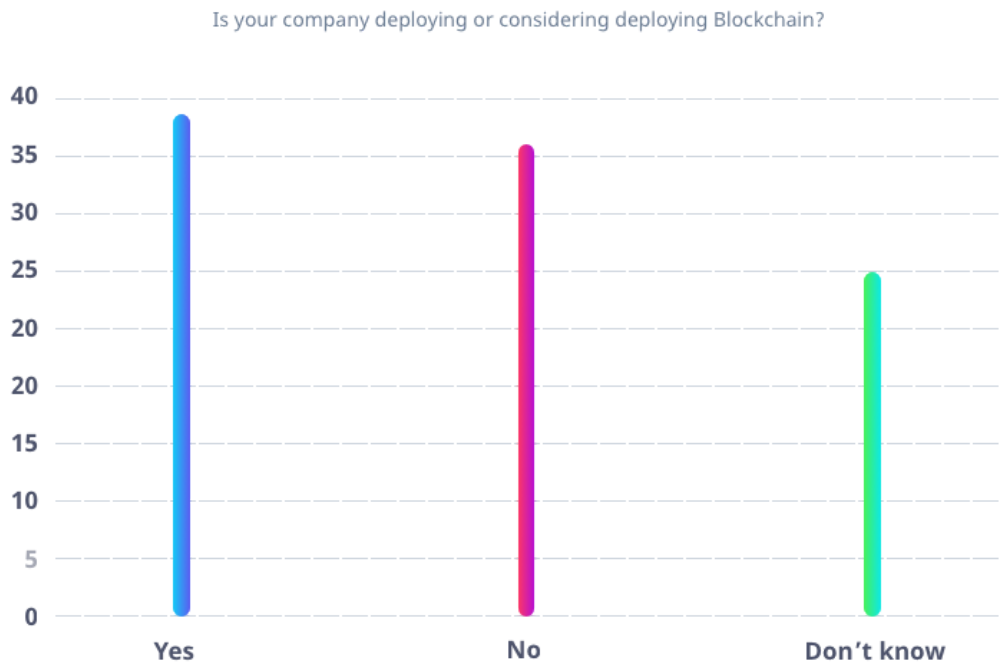
might be dangerous to leverage blockchain without first looking at other options as there is an element of disruption as the survey shows.

And that might also slow down the current enthusiasm a bit as, quoting the press release "the research found that companies may have underestimated the scale of the blockchain challenge". Without interoperability, clients and partner ecosystems wanting to collaborate and so forth you might indeed get in trouble and underestimating the scale and complexity of internal and external disruption through the adoption of blockchain might be your blockchain party pooper. That is the very reason why big names put their shoulders under blockchain and blockchain associations across various use cases and industries and why you'll see more and more client cases coming, ideally within an ecosystem context. If you have a feeling of déjà-vu: indeed, it feels a lot like the early days of IoT and so many other technologies. But this time it seems that the stakeholders are moving way faster. After all, history has a tendency to repeat itself but companies like the leading ones above now and then also learn from history.

Additional resources on blockchain in business

Blockchain enterprise survey

Below is a screenshot of the interactive infographic from the blockchain enterprise survey of Juniper Research, presented in the Summer of 2017 and tackled in this blockchain overview.



Jupiter Blockchain survey: Blockchain Awareness and Usefulness

	**15%**
	Proportion of survey respondents who knew “very little” about blockchain
	**76%**
	Proportion of respondents believing that blockchain could be “very useful” or “quite useful” for their company

Jupiter Blockchain survey: Enterprise Disruption

	**35%**
	Proportion of companies considering or actively deploying blockchain that feel it will cause “significant” internal disruption.
	**51%**
	Proportion of companies considering or actively deploying blockchain that feel it will cause “significant” disruption to their partners/customers.

Blockchain technology report for IT managers
End January 2018 the US National Institute of Standards and Technology published a draft report regarding blockchain technology as covered in our NIST blockchain technology report article.

The report gives a great overview of blockchain technologies and more. Although it aims to target IT managers who want to take decisions with regards to blockchain in business applications it does offer a great introduction to blockchain in a somewhat more technical context but also with ample use cases and more.

Blockchain Global Benchmarking Study
Last but not least, below is the previously mentioned SlideShare of the Global Blockchain Benchmarking Study by the University of Cambridge Judge Business School (Cambridge Centre for Alternative Finance).

2018-2021: data and action plans for the near future

Analysts across the globe see an important future for blockchain in myriad organizations and use cases. On top of Juniper Research, which we mentioned earlier and several others, also IDC states that blockchain services are poised to become the foundation for digital trust at scale IDC stated end 2017. You could already see that much in the infographic above of course.

According to IDC's 2018 IT industry forecasts, fully entitled "IDC FutureScape: Worldwide IT Industry 2018 Predictions", revealed in a webcast with a press release on October 31st, 2017, by 2021 at least 25 percent of the G2000 would use blockchain services with exactly that purpose. When looking at some industries and the data from IDC mainly global transaction banks, the manufacturing industry, retailers and healthcare organizations would be along the earliest movers to have blockchain networks in production (so no tests or proof of concept).

Blockchain networks in production by 2020: main industries
Below are the forecasts for the mentioned industries *(note that IDC looks at 2020 here and not at 2021 as in the earlier mentioned prediction)*.

- Top global transactions banks: 25 percent with a blockchain network in production.
- Manufacturers and retailers together: a blockchain network in production by 2020 for close to 30 percent.
- Healthcare organizations: 20 percent of healthcare organizations with a blockchain network in production by 2020.

Another interesting finding, this time from IDC's "FutureScape: Worldwide IoT 2018 Predictions" concerns blockchain and the Internet of Things, a topic we covered earlier.

Most of us look at blockchain as one of the ways to solve multiple IT data exchange and IoT monetization challenges, among others through using smart contracts. Well, IDC predicts that by 2020 up to 10 percent of pilot and production blockchain distributed ledgers will incorporate IoT sensors as you can read here or hear when you listen to the appropriate webcast in the IDC FutureScape 2018 series.

What does a business have to do in 2018 order to get ready for blockchain?
Although being a first mover doesn't always mean being in the best position, with regards to the adoption of blockchain in business things could be different.

According to the research firm early adopters can establish very strong positions while organizations that are not participating in blockchains and the industry ecosystems they require, will encounter significant disadvantages with regards to, among others, speed and costs.

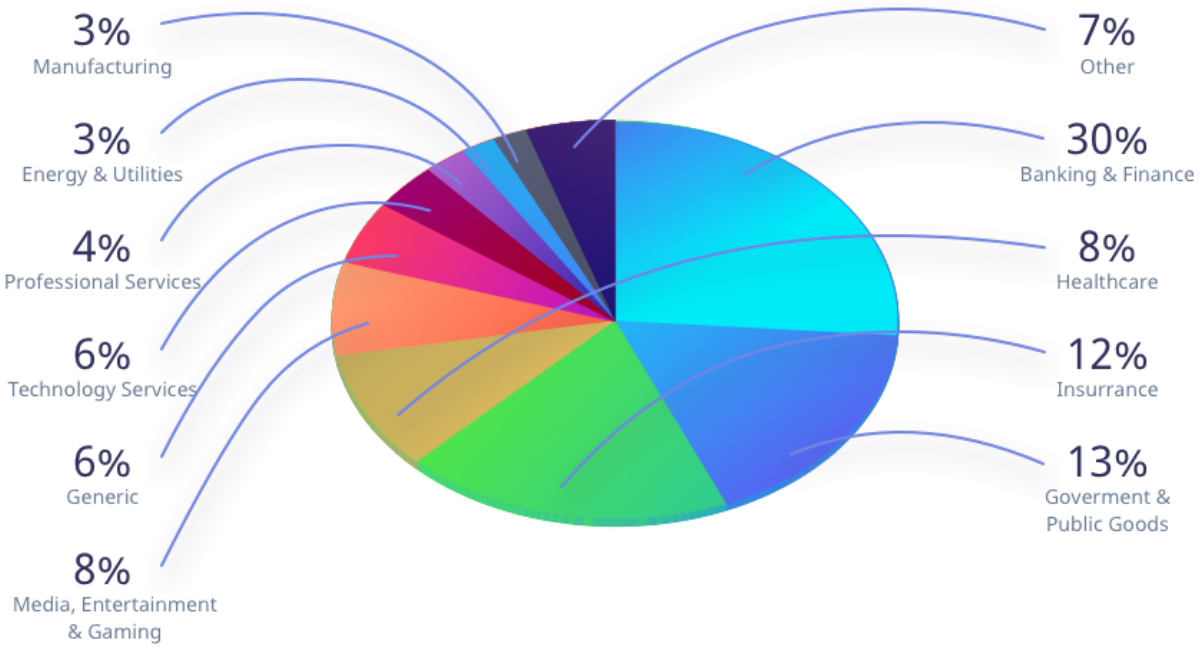
- *Start by looking at all the blockchain consortiums and initiatives out there and see which could bring the benefits of blockchain within their specific industries, use cases and ecosystems.*
- *In the case there isn't such an ecosystem and there is a case and benefit to do so, investigate the opportunity, which by definition obviously also means finding the right peers and partners that can help start one (or, less ambitious, join or start a blockchain network or a pilot).*
- *Companies that are slower in their digital transformation efforts, which really is the majority of organizations today, have to do their homework, start learning, experience the potential, talk with their peers and so forth in 2018. More importantly they need to develop use case scenarios for blockchain that make most sense for them. Those who are ahead in their digital transformation journey should put a blockchain strategy and plan and place in 2018 IDC states.*

Blockchain 2018: forecasts and industries

In our article on blockchain in the EU and Western Europe we mentioned some data regarding the adoption of blockchain across several industries as per the Cambridge Centre for Alternative Finance (research end 2017, see SlideShare at the bottom of this page).

The results as depicted below are part of the EU blockchain factsheet which was presented at the occasion of the EU Blockchain Observatory and Forum, covered in the article. However, the 2017 Global Blockchain Benchmarking Study of the Cambridge Centre for Alternative Finance.

Sectors currently using blockchain



Sectors currently using DLTs according to the EU blockchain factsheet based upon Cambridge Centre for Alternative Finance data. However, the authors came to this result by looking at the largest number of identified DLT use cases, whereby "132 blockchain use cases were grouped into industry segments that have been frequently mentioned in public discussions, reports and press releases".

In the meantime IDC announced its inaugural Worldwide Semiannual Blockchain Spending Guide (January 24th, 2018) and a version for Western Europe as also mentioned in that same article which looks more into detail from the spending rather than identified DLT use case perspective.

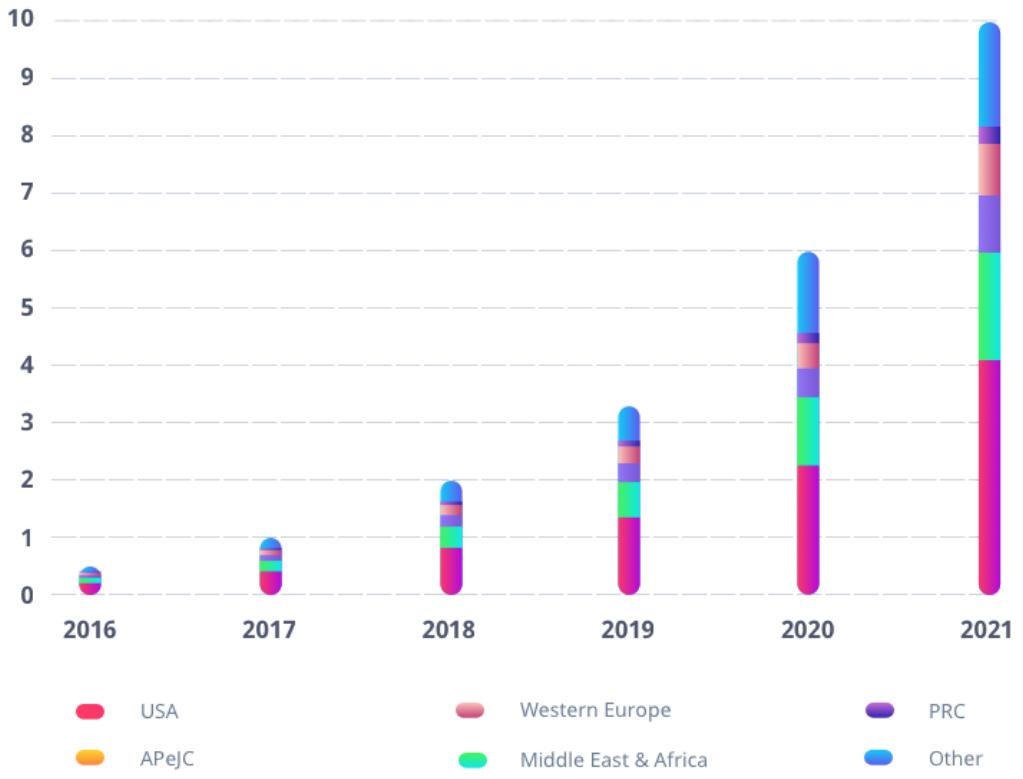
According to IDC, global blockchain spending is expected to reach $2.1 billion in 2018 and total spending of $9.2 billion in 2021. In the scope of this section of industries and blockchain use cases, it's interesting to note that, according to IDC, spending per industry for 2018 shows the following picture:

- *The financial sector leads with blockchain spending of $754 million in 2018. Mainly the fast adoption in the banking industry is key here.*
- *The distribution and services sector ranks second with $510 million in 2018, with retail and professional services showing strong blockchain investment.*

- *The manufacturing and resources sector ranks third with $510 million in 2018. Here most blockchain investments in 2018 will happen in the discrete and process manufacturing industries.*

As per usual there are geographical differences though. Looking at the different regions from a blockchain spending perspective the chart below shows the split and evolutions until 2021: the US leads, followed by Western Europe.

Top region based on spend, 2017 (Value (Constant Annual), USD, B)
Source: IDC Worldwide Semiannual Blockchain Spending Guide, 2017H1



Blockchain spending per region according to IDC's Worldwide Semiannual Blockchain Spending Guide (January 2018)

However, while in the US the distribution and services sector will account for most blockchain investment in Western Europe the financial services sector is the main driver. The latter is also the case in China *(PRC)* and the APeCJ region *(Asia Pacific, excluding Japan)*.
The fastest growers in blockchain spending globally are, respectively, professional services *(85.8% CAGR)*, discrete manufacturing *(84.3% CAGR)*, and the resource industries *(83.9% CAGR)*.

The limitless applications of blockchain – revisiting transactions in the digital age

Time to move beyond the better known potential and current applications of blockchain and get the broader picture by revisiting transactions in this digital age – and look at more areas

where a new system of contracts, keeping track and ultimately recording and being able to control or prove in complex digital ecosystems is needed.

Let's use the definition of Merriam-Webster of a transaction to make it clear: "an exchange or transfer of goods, services, or funds". Now, let's elaborate on that and look at two key aspects.

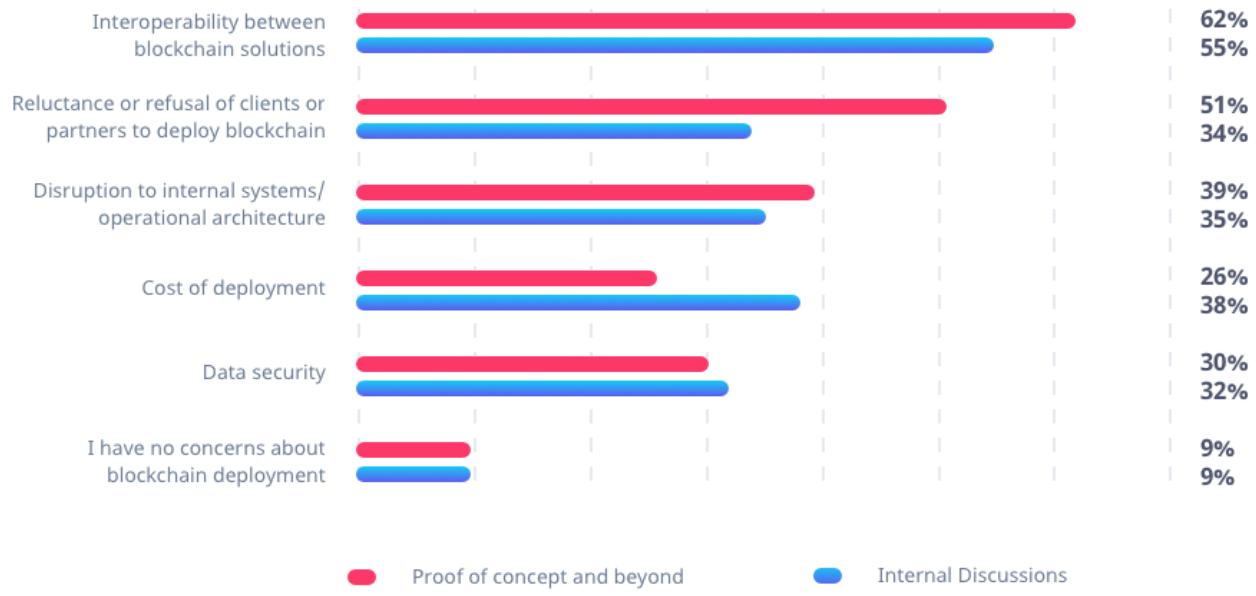
Goods and services mean many things
As you know we live in a data-intensive age of information where data has become a key business asset.

Think about how important data sharing and monetization has become, for instance IoT data monetization. Or think about how data is turned into actionable intelligence or business process outcomes, how important it is to have an audit trail and how automated processes which are moving data across the value chain and across ecosystems really are transactions. In order to leverage, let alone 'exchange' data it is key to have mechanisms in place, for instance to make sure that pieces of crucial data have not been tampered with and are reliable and trustworthy original versions which can be leveraged for whatever purpose. We can go on, even on this level of data alone.
Now start thinking about the goods and services in this day and age in the broadest sense and the number of transactions that happen regarding them as well as the need to record those, for instance from a regulatory perspective in the transfer and exchange of personal and sensitive data or how essential information is as it gets shared and used for critical medical purposes or for actions, decisions and transactions for myriad digital services. And we haven't even really started exploring the services in this as-a-service economy yet. You see the vastness and it's far from done yet.

Transactions don't just happen between people
There are far more transactions between systems, between devices and between devices and systems in an increasingly hyper-connected reality.

Devices communicate with each other, intelligent building components take decisions based on data exchanges or changes/triggers of any sensor-measured external state, information gets automatically sent from one system to another in the scope of a business process or a "case" in the sense of case management, a trigger caused by a change in a system leads to a result, the list goes on.
If you entirely remove the human element and several changes in status and transactions between systems and devices lead to ever more autonomous – and decentralized – decision making as they increasingly do in industrial automation, building automation, IoT, advanced analytics with AI-driven actions and much more you really start seeing why blockchain is seen as key to the digital transformation economy by so many.

Concerns with regards to blockchain for organizations as found by Juniper Research in the Summer of 2017 and reported on Venturebeat



What is cloud computing?

Everyone is talking about "the cloud." But what does it mean?

More and more, we are seeing technology moving to the cloud. It's not just a fad — the shift from traditional software models to the internet has steadily gained momentum over the last 10 years. Looking ahead, the next decade of cloud computing promises new ways to collaborate everywhere, through mobile devices.

So what is cloud computing? Essentially, cloud computing is a kind of outsourcing of computer programs. Using cloud computing, users are able to access software and applications from wherever they are; the computer programs are being hosted by an outside party and reside in the cloud. This means that users do not have to worry about things such as storage and power, they can simply enjoy the end result.

Life before cloud computing

Traditional business applications have always been very complicated and expensive. The amount and variety of hardware and software required to run them are daunting. You need a whole team of experts to install, configure, test, run, secure, and update them.

When you multiply this effort across dozens or hundreds of apps, it's easy to see why the biggest companies with the best IT departments aren't getting the apps they need. Small and midsize businesses don't stand a chance.

Cloud computing: a better way

With cloud computing, you eliminate those headaches that come with storing your own data, because you're not managing hardware and software — that becomes the responsibility of an experienced vendor like Salesforce. The shared infrastructure means it works like a utility: You only pay for what you need, upgrades are automatic, and scaling up or down is easy.

Cloud-based apps can be up and running in days or weeks, and they cost less. With a cloud app, you just open a browser, log in, customize the app, and start using it.
Businesses are running all kinds of apps in the cloud, like customer relationship management (CRM), HR, accounting, and much more. Some of the world's largest companies moved their applications to the cloud with Salesforce after rigorously testing the security and reliability of our infrastructure.

As cloud computing grows in popularity, thousands of companies are simply rebranding their non-cloud products and services as "cloud computing." Always dig deeper when evaluating cloud offerings and keep in mind that if you have to buy and manage hardware and software, what you're looking at isn't really cloud computing but a false cloud.

The three types of cloud computing

Infrastructure as a Service (IaaS)
A third party hosts elements of infrastructure, such as hardware, software, servers, and storage, also providing backup, security, and maintenance.

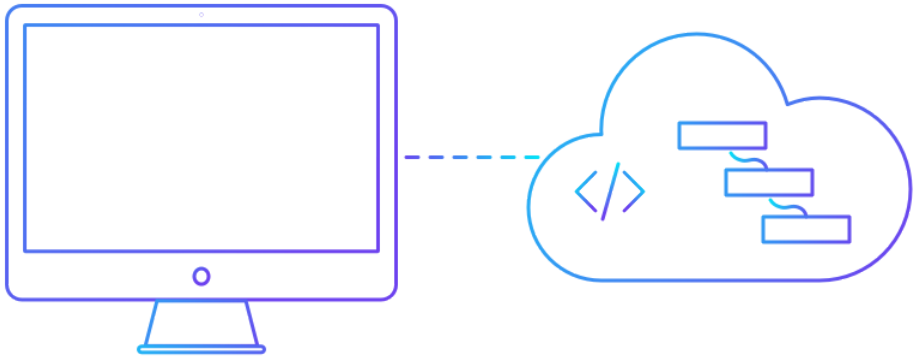
Software as a Service (SaaS)
Using the cloud, software such as an internet browser or application is able to become a usable tool.

Platform as a Service (PaaS)
The branch of cloud computing that allows users to develop, run, and manage applications without having to get caught up in code, storage, infrastructure and so on.

There are several types of PaaS. Every PaaS option is either public, private, or a hybrid mix of the two. Public PaaS is hosted in the cloud, and its infrastructure is managed by the provider. Private PaaS, on the other hand, is housed in onsite servers or private networks, and is maintained by the user. Hybrid PaaS uses elements from both public and private, and is capable of executing applications from multiple cloud infrastructures.

Platform as a Service (PaaS)

The branch of cloud computing that allows users to develop, run, and manage applications without having to get caught up in code, storage, infrastructure, and so on.

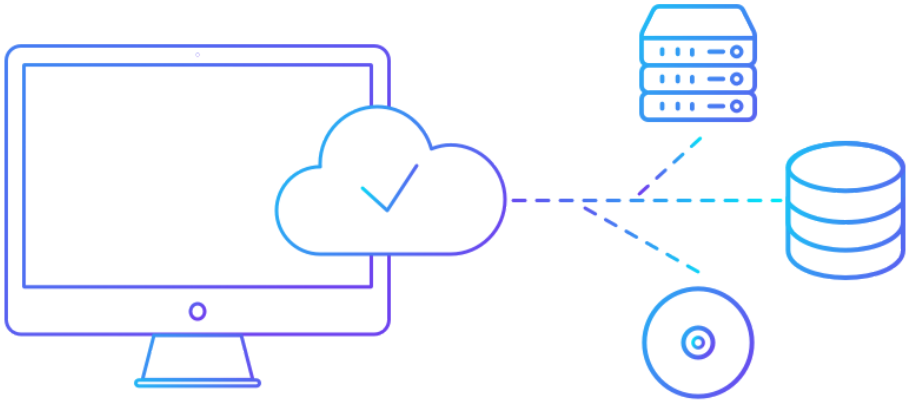


PaaS can be further categorized depending on whether it is open or closed source, whether it is mobile compatible (mPaaS), and what business types it caters to.

When choosing a PaaS solution, the most important considerations beyond how it is hosted are how well it integrates with existing information systems, which programming languages it supports, what application-building tools it offers, how customizable or configurable it is, and how effectively it is supported by the provider.

As digital technologies grow ever more powerful and available, apps and cloud-based platforms are becoming almost universally widespread. Businesses are taking advantage of new PaaS capabilities to further outsource tasks that would have otherwise relied on local solutions. This is all made possible through advances in cloud computing.

Using cloud computing, users are able to access software and applications from wherever they need, while it is being hosted by an outside party – in "the cloud".



Traditional business applications have always been very complicated and expensive. The amount and variety of hardware and software required to run them are daunting. You need a whole team of experts to install, configure, test, run, secure, and update them.

When you multiply this effort across dozens or hundreds of apps, it's easy to see why the biggest companies with the best IT departments aren't getting the apps they need. Small and mid-sized businesses don't stand a chance. The affordability of cloud-hosted data makes it an essential tool for these types of situations. Here are some other benefits of cloud computing.

Adaptable
Cloud computing allows for adaptable programs and applications that are customizable, while allowing owners control over the core code.

Multitenant
Cloud software provides the opportunity to provide personalized applications and portals to a number of customers or tenants.

Reliable
Because it is hosted by a third party, businesses and other users have greater assurance of reliability, and when there are problems, easy access to customer support.

Scalable
With the Internet of Things, it is essential that software functions across every device and integrates with other applications. Cloud applications can provide this.

Secure
Cloud computing can also guarantee a more secure environment, thanks to increased resources for security and centralization of data.

What is a Blockchain as a Service?

In order to offer the benefits of blockchain to the wider business community, companies such as Microsoft decided to offer blockchain technology through the cloud As Service business model. Most people are aware of IaaS, PaaS and SaaS, given that most of us in some way use cloud-based applications or storage.

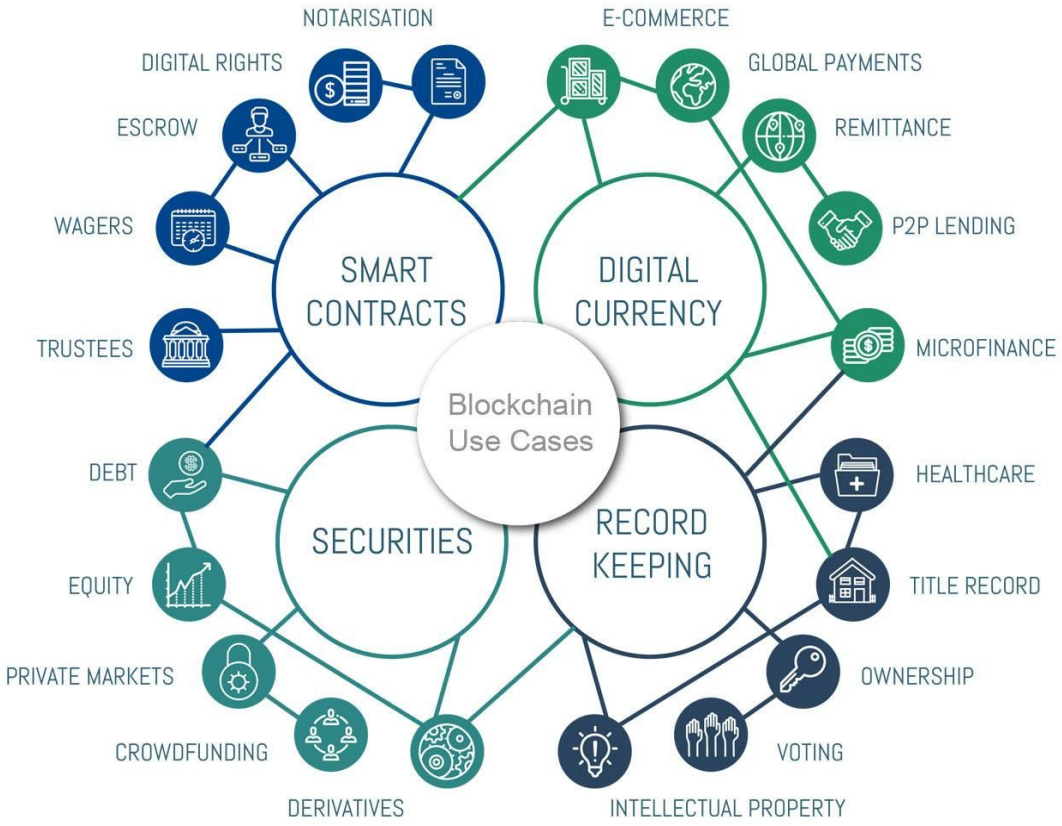
The BaaS model acts in very much the same way, allowing businesses of all shapes and sizes to access blockchain based technology without having to invest in developing it in-house first. Therefore, the BaaS model would allow companies to access a blockchain provider's services where they can then access/develop blockchain based applications.

The only downside to the BaaS model is that it demands a certain amount of centralization as transactions would need to be funneled through the host platform's blockchain services. Since decentralization is one of the key features that makes blockchain so useful, companies will need to think long and hard as to whether this is the right solution to their problem.

Advantages of the As Service model:

- Low-cost access to technology
- Offers companies massive scalability
- Increased data security
- Compatibility
- Anywhere access
- Better software

What kinds of things can Blockchain as a Service be used for?



Anyone from startups to huge multinational corporations will eventually be able to use Blockchain-as-a-service for tasks ranging from improving stocktaking, securing confidential customer records, recording property ownership, to helping to launch their own ICO. Blockchain can provide at least a partial solution to the problems underlying the vast number of transactions and processes that underwrite the entire global economy today.

Blockchain in the healthcare industry, for example, will eventually be used to allow fully electronic medical records, order and record drug stock levels, help improve the development of new drugs, and streamline claims adjudication.

Blockchain in the insurance industry is set to create accurate real-time risk assessments of customers which will allow for the first ever 'smart insurance plans' that could facilitate the world's first pay-as-you-need insurance policies. This technology will also help to streamline internal processes, reduce fraud, and even improve customer service too.

Other industries that are set to benefit from blockchain:

- Advertising
- Entertainment industry
- Retail
- Cloud
- Rideshare
- Energy
- Finance Industry
- Government

Check out this article for a more comprehensive list of the industries that are set to be disrupted by blockchain.

Blockchain as a Service Amazon AWS

Amazon has been the world's largest cloud provider for a number of years now. It made over $6 billion from its Amazon Web Services in 2017. It is the leading provider of IaaS, SaaS, and PaaS services that recently combined forces with the investment firm Digital Currency Group (DCG) to create a BaaS environment that it now offers through its AWS platform.

The aim of this BaaS environment is to allow DCG affiliated blockchain providers to work with its clients in a secure blockchain environment to aid development. Access to financial institutions, enterprise technology companies, and insurance companies will help developers on the project to ascertain what the real business needs are for blockchain allowing them to push BaaS development in that direction.

This is the same cleaver feedback loop based business model that Amazon used to develop such great IaaS applications in the past. As a result, few insiders doubt that AWS's strategy won't succeed in really advancing BaaS and ensuring its quick implementation.

Blockchain as a Service Azure

Microsoft's Azure is the second-biggest provider of cloud-based services in the world today. While Microsoft was caught napping by AWS, it quickly used its expertise and heavyweight resources to create its own cloud platform, which is called Azure.

In recent years, they have made up a lot of the ground on AWS, particularity after they migrated their highly successful Office software to the cloud. While their flagship Windows operating system continues to lose market share, Azure is quickly becoming a huge cash cow for the company.

Microsoft has followed AWS lead by recently adding BaaS modules to their existing cloud platform. However, Microsoft has chosen to focus its BaaS development around the open source Ethereum blockchain. For those of you who are unaware of the Ethereum Project, it is probably the most exciting company to have come out of the blockchain revolution so far. It focuses on the use of 'smart contracts' to facilitate a huge range of agreements that include the exchange of products and services between parties.

Microsoft Azure's BaaS service aims to provide fast and affordable access to blockchain technology. It offers a good development environment for developers and businesses in order to facilitate the innovation of new processes and techniques using blockchain. Like Amazon, Microsoft plans to allow new systems to be developed in this space which will eventually be rolled out to the wider business market.

By combining blockchain developer's skills with their vast platform, Microsoft is offering the scalability that should hasten the development of the kind of solutions that are in so much demand. So intent on winning this race are Microsoft that they have even thrown the weight of their AI services being the project to facilitate more powerful and efficient data analysis and management.

Blockchain as a Service IBM

Just outside of the 'big three' cloud providers is IBM. It is the world's fourth-largest cloud provider and focuses most of its efforts on providing services to businesses. It was also caught napping by AWS in the early days of cloud development but has worked hard to catch up in the proceeding years.

IBM has developed its own BaaS service that is based on the Hyperledger BaaS system. Their system also provides an environment for developers and businesses to create blockchain solutions. Its primary aim is to digitize transaction workflow through a shared ledger and to create secure blockchain networks.

Like Amazon and Microsoft, IBM hopes that this strategy will help to develop blockchain technology to the point where it can replace many of the existing solutions in use today. Since IBM's core business is already focused on the buisness sector, it stands to gain enormously if it is able to help develop secure, reliable, and adaptable blockchain technologies before the competition.

How big can the BaaS model become?

Right now no one really knows how big BaaS is going to be. It's a little like asking how long is a piece of string? Since the blockchain revolution is still only just beginning it is still struggling to keep up with all the different ideas and directions that developers are trying to explore.

Undoubtedly, this reasoning is behind the larger cloud company's decision to open up their resources for companies and developers to use. After all, they must have learned a lesson from when they were caught napping as Amazon took the lead in initial cloud platform development. Gartner also noted that searches on blockchain increased 400% in the 12 months before February 2017. Since the surge in the price of the cryptocurrency market, it is likely that this figure will have risen massively yet again.

The real question that is going to limit the rise of BaaS is not whether or not there is the demand, or even whether companies actually need blockchain technology, but rather can BaaS development overcome the limitations that current blockchain technology suffers from?
The industry will need to find solutions to such problems as blockchain bloat and the massive energy requirements of blockchain processing. As blockchains grow in size they inevitably contain more and more information. This must be sent and received during every single

blockchain transaction, resulting in vast amounts of network capacity being needed to process them.

The same goes for the amount of electricity needed to process each blockchain transaction. A recent estimate is that it now takes about 1 barrel of oil's worth of energy to process a single bitcoin transaction. Already, daily Bitcoin transactions account for more energy than is used by some small countries.

Facilitating widespread use of blockchain solutions, including those provided by BaaS will require massive amounts of energy. Recently the Quebec region in Canada, which has a surplus of electricity, refused the request of various cryptocurrency mining companies permission to relocate there on the grounds energy consumption.

It is hoped that the industry will be able to use solutions such as the use of child chains to overcome these problems and make blockchain a completely viable alternative to existing solutions. Once this happens, we are certain to see a rapid rise in their implementation that will truly unleash the power of the blockchain revolution.

Specifically, BaaS allows developers to test and deploy their bespoke blockchain-based applications in the cloud, without having to maintain the network or full clients themselves. The implementation of the blockchain can be tailored to their needs and accessed via lite clients or APIs.

Impleum Blockchain platform overview

The Impleum blockchain platform

Impleum is a powerful and versatile way to create decentralized applications [dApps]. The ‘dApps’ utilize the ability of decentralization of the blockchain innovation technology and are accompanied by a layer of ground-breaking nodes to route data. Integration of the blockchain is the deployment of the network node and setting up its connection with the

DApp through a documented API
DApps based on the Impleum blockchain platform are interrelated and constitute an open ecosystem.

Impleum is a widely dispersed system, which is why it is indestructible. The cryptographic encryption of the system keeps the user’s information encrypted and safe. By leveraging Impleum’s masternodes, developers can easily create DApps that are highly secure and scalable. The core of Impleum platform is an object-oriented programming language C# backed by a huge developer community.

Impleum’s coin [IMPL]

Impleum has not only introduced a dApp building platform but also has launched its own coin named IMPL. The coin stands as the shorter name of ‘Impleum’. IMPL has its own set of unique technical parameters. The coin is a hybrid as it is a combination of PoW and PoS.
IMPL coin Donation

Cross-platform Wallets

Impleum highlights the usage of its accessible wallets through GUIs [Graphical User Interfaces]. This is available across all major operating systems such as Windows, macOS, and Linux. A wallet set-up is finished in no time, while the encryption of funds is maintained with high scale security. The wallets are advanced enough to let the user stake IMPL coins for greater rewards over time. For technical clients, a more specialized CLI [Charge Line Interface] wallets are offered.

Integration of Blockchain

Impleum main chain as of now has the IMPL currency which has the potential to be the future hub for all side chains. Impleum enables organizations to effectively deploy their own particular altered blockchains without the overheads inheritance running their own particular blockchain arranged framework. Side chains will store all the data of the created DApp, scaling effortlessly in tandem with the new developing venture.

Mining opportunities

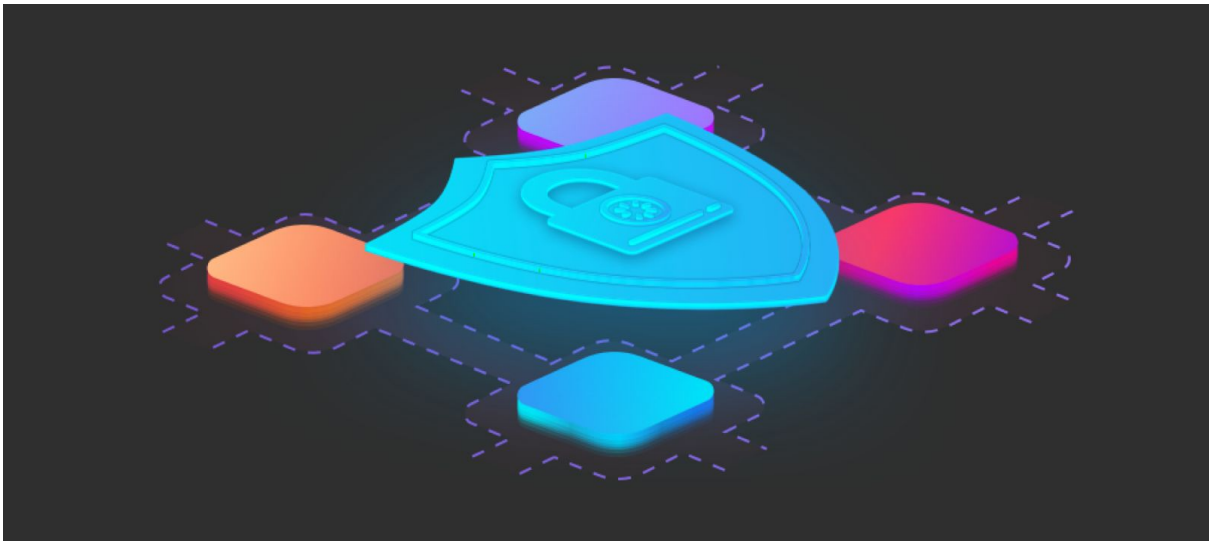
Impleum is a hybrid coin, which based on a proof-of-stake [PoS] and proof-of-work [PoW]. Proof-of-Stake is a mechanism that allows the network to affirm transactions and prevent fraud or counteract extortion. However, it does not require any asset-intensive calculations or figurings to be carried. The only thing required is IMPL coins in the user's account balance, while the IMPL Wallet is associated with the network and the system. Intermittently, the balance will experience an increment as new coins are granted to the user as loyalty.

Impleum's Proof-of-Work mining is the process of making computer hardware such as CPU and GPU carry out mathematical calculations for the Impleum network. This is required in order to affirm transactions and trigger increment of security. Mining algorithm is x13.

As a reward for their administrations, Impleum miners can collect transaction fees for the transactions they affirm, along with newly created IMPL. PoW block reward directly decreases the reward of PoW block from 48 IMP to 0.48 IMPL. Mining is a specific and aggressive market where the prizes are separated up as per how much calculation is accomplished. On the block 100 000, the last PoW block was found. From block 100 001 Impleum becomes pure Pos coin.

Impleum Masternodes

Impleum Masternodes are PCs that are continually associated with the Impleum Network and play out specific assignments enabling Impleum to accomplish faster and more private transactions. To run the Impleum Masternode one is required to have a specific measure of IMP in their balance, as security, and satisfy different prerequisites implied by the protocol. As it is intended to create a circulating coin supply for mass-market adoption, a user can provide price stability as needed. This gesture of support will be rewarded by more revenue.



Architecture and development

The Impleum platform is based on C# Impleum Bitcoin Fullnode developed over the NBitcoin library, almost complete Bitcoin Core port written in C# and .NET. Given that the basis of NBitcoin is pure C# code and the .NET platform, the development and support of the system is easier compared to the traditional C++ Bitcoin Core source code.
Other projects was developed specifically for the cryptocurrency. But blockchain technology could be adapted for use in other areas.
Blockchain can be used for a much broader range of assets than just cryptocurrency: tangible assets such as cars, real estate and food products, as well as intangible assets such as bonds, private equity and securities. DApps based on Impleum platform can use blockchain to track the provenance of goods to minimize fraud, document tampering and double financing and etc.

Stages in Impleum development will include:

- Development of the Impleum Bitcoin Full Node
- Fork the Impleum Bitcoin Full Node for NImpleum
- Implement the required changes to NImpleum and port Elements sidechains to C#.

What keeps Impleum highly resistant to external attacks?

On the source code level of this project conceived the interest (for staking coins in the user's wallet) that is involved in calculating the reward for finding a block – Proof of Stake (PoS). Staking your Impleum not only secures and stabilizes the network. It also rewards you with an annual interest rate based on the current block reward. This key difference puts the earning power in your hands and not powerful mining cartels.

What are the advantages Impleum smart contracts over other platforms?

Impleum has smart contracts built in native C# on the .NET framework, the most popular enterprise programming language on the most widely-used enterprise framework. This makes it easier to integrate into existing enterprise architectures than other platforms.

What Impleum has to offer:

- Instant. Impleum transactions are simple and efficient.
- Private. All financial information, history and balance is confidential.
- Secure. Transactions are backed up across hundreds of servers.
- Staking. Forget power-hungry mining rigs – stake and earn interest.
- Masternodes. Service nodes that allows Impleum DApps to scale off-chain.
- Low fees. Impleum improves your savings with .001 transaction fees.
- Sidechains. This means that IMPL can be passed to and from the sidechain and the gateway through which they pass is controlled by a federation.

Seamless integration of blockchain solutions on the software.
Impleum main chain currently hosts the IMPL currency will be future hub for all sidechains. Impleum side chains allow businesses to easily deploy their own customised blockchains without the overheads inherent in running their own blockchain network infrastructure. Side chains will house all the data of your DApp, scaling effortlessly in tandem with your evolving project. Join the open ecosystem based on Impleum blockchain platform now.

There are several advantages to building Impleum on the NBitcoin platform

It was developed in pure C# and it utilizes the Microsoft .NET framework, which is easier to maintain and develop further than the traditional C++ Bitcoin Core source code.

C# is one of the dominant languages in business application development and it offers several advantages over C++.

NBitcoin is currently the only cross-platform alternative Bitcoin implementation available. Impleum will upgrade the code base to .NET Core, Microsoft's latest version of .NET that can run natively across even more devices.

Architecture of the Impleum Bitcoin Full Node

A full node is an application whose goal is to keep track of valid blocks in the blockchain.
It is essentially composed of several layers:

Network Layer - this deals with which messages are exchanged between full nodes, and how.
Consensus Layer - this sets the (blockchain-wide) rules for what is considered a valid block.
Node Policy Layer - this adds more restrictive rules than the Consensus Layer to prevent DDoS (node-wide rule).
Infrastructure Layer - governs how to store and verify blocks and transactions efficiently.
Interface Layer - API for developers to query the state of the node, and/or user interface.

While Bitcoin Core deals with all these layers in the same source code, Impleum Bitcoin Full Node will only have to deal with the Node Policy Layer, Infrastructure Layer and Interface Layer.

The Consensus Layer is an integral component in the Full Node architecture that should ideally not be modified without industry-wide consensus, since a bug in this layer could cause a fork in the Blockchain and result in loss of funds. As a result of this risk Consensus Layer should be as close to Bitcoin Core as possible.

Bitcoin Core provides part of the consensus code in a library called LibConsensus. NBitcoin will be used to fill in any gaps. To simplify the transition to the Impleum Bitcoin Full Node, all of the RPC API endpoints available in Bitcoin Core will be provided, so users and businesses will not have to rewrite their software to utilise the Impleum Bitcoin Full Node. Impleum Bitcoin Full Node in C# and Microsoft's .NET Framework

Impleum Bitcoin Full Node

Bitcoin was originally developed by Satoshi Nakamoto as a piece of software that bundled together several different functionalities. What users called 'Bitcoin' was at the same time the protocol, the wallet, the key storage, the mining software, the infrastructure for other apps, and the full node.

As with all maturing technology, the Bitcoin industry became more and more specialised, and the functionality once provided only by Bitcoin Core has now been diffused among different players in the industry. An all-purpose piece of software has now been replaced and complemented by multiple specialised parties and applications.

The most basic layer of Bitcoin on which everybody depends is a full node. Changing the code of a full node is a controversial matter, as the consequences impact virtually every company in the ecosystem. On the other hand, if consensus about an improvement to Bitcoin is reached and a new feature is successfully implemented in the full node, then the benefits ripple out across the

whole industry. A typical example is the new OP_CSV and Segregated Witness improvement that will allow the development of off-chain payments, which will permit Bitcoin to scale as a currency.

At present, the most popular Bitcoin node is called Bitcoin Core and is developed in C++. The Bitcoin Core team is a group of highly skilled developers who generally adopt a very conservative approach to accepting improvements. One of the reasons for this is that a full node is such a critical component for Bitcoin that any new features require extensive reviews and testing. Contributors to Bitcoin Core generally work on it for free, and their review time is valuable but limited.

We believe that one way to allow improvements to be implemented faster is to develop a full node in C# instead of C++. Highly skilled C++ engineers are in short supply in the corporate world, which tends to prefer higher-level languages like C# or Java. Higher-level languages are also easier to review and learn, and it is harder to make coding mistakes.

As such, we propose that the Impleum Bitcoin Full Node will be based on the NBitcoin framework, which is the most complete and portable library for developing blockchain applications and platforms in C# and Microsofts .NET.

Security Analysis of Proof-of-Stake Protocol v3.0

Proof of Stake's security has proven itself over years of testing. Advances in this technology in *Impleum's Proof-of-Stake 3.0* have solved the issues faced with Coin-Age, *Block Reward* and *Blockchain Pre-computation* The protocol is robust and keeps nodes connected to the *network*. It disincentives inactive nodes. In this *paper* we will highlight and outline the advantages and perform a security analysis of the system. We also outline ideas here in *Impleum* to potentially increase security further.

I. Introduction

Cryptography has managed to change the way finance and money is defined. Recently the advent of Bitcoin has showed how a peer-to-peer network can prevent forgery by solving the *"Byzantine Generals Problem"*. Since then many different coins have been created based on Bitcoin's open source code. There are two major methods for generating new funds on the network. The first is *"Proof of Work"* and the second being *"Proof of Stake"*. The theory behind Proof of Work is to hold a mathematical competition. The first computer to solve the puzzle receives the coins. This makes distribution of coins a completely fair process.

However, this also creates a problem of wasted energy. Computers in order to compete, create and arms race of hardware. Thus, money and energy is wasted to generate new coins. *Proof of Stake* is a competition between shareholders, where based on connectivity to the network and random chance, you can receive new coins. Interest is generated based on how much you hold. This solves the energy waste problem in Bitcoin and introduces new challenges in network security. Here at Impleum, we would like to write a technical analysis of the advantages in this protocol and to honor our predecessors, discuss potential improvements and pitfalls. *Proof of Stake* was first implemented in *"Peercoin"*. Later, major breakthroughs in *Proof of Stake* were

made in Impleum namely, *"Proof of Stake 2.0"* and *"Proof of Stake 3.0"*. We have implemented the *Proof of Stake 3.0* system because we believe it to be the worlds most secure and efficient method of coin generation. We will outline and highlight the great security of this system and the technical problem it solved.

II. Security, Coinage and Attacks

The whole purpose of holding competitions for coins is to avoid *attacks*. Confirmation of transactions is an honor given to the winner of a block. However, if this system can be gamed, then it is flawed. In ***Proof of Stake***, you first prove you have access to coins and from that point you can compete to win blocks randomly. The more people competing the more secure the block. Coin age is the idea that the longer you hold coins the higher the probability you can win a block. It's original intention was to incentive dormant holders of coins.

However, this does not encourage a node to stay connected to the network in practice since they can wait for the reward to increase. Also, shareholders can disconnect from the network for long periods of time, then reconnect and win enough blocks to *risk* a ***50% attack*** on the network. The time calculation will effect payouts discouraging connectivity. Also, the fewer the nodes that are connected, the easier it is to gain a majority of the blocks forging consensus. Also, stakes can be computed in advance to make the attack more effective. Timestamps are used in *Proof of Stake* to get a general idea of time. Drift calculations are used to prevent forging erroneous timestamps. In *Proof of Work*, a difficulty increase or decrease is made depending on how quickly a block was produced. However, as a precautionary method to prevent any sort of "***Timing Attacks***" ***Proof of Stake*** *coins* use centralized checkpoints.

III. All problems have a solution

A. Coin Age

Coin Age *is calculated by the weight of unspent coin and the time they have been dormant*. The calculation is simply "***proofhash < coins • age • target***" The proof hash is the hash of an obfuscation sum that depends on a stake modifier, the unspent output, and the current time. The attack of saving up ***Coinage*** was previously outlined as *improbable*. The reasoning behind this is because it is very difficult to perform consecutive double spending since ***Coin-Age*** would reset after the first expense. However, this is not entirely clear because an input can be split into ***1000s*** of outputs. This may give the possibility for consecutive double spend attacks. However, this is still a *difficult problem* because the attacker would need a significant amount of funds to hold weight greater than the network. In theory, this makes sense. However, if we look at the amount of forks of Impleum and other popular ***POS systems***, we can see the amount of nodes are fairly low and this gives much greater weight to a smaller handful of nodes. A holder of many coins may not want to perform this attack since they run the potential of losing value of their share if detected. However rational this may seem, it is probably a fallacy because it is still an attack vector and a very real one indeed. More importantly, with so many coins being published daily, keeping as many nodes connected as possible is imperative to security. Solution from ***Proof of Stake 2.0:*** *Remove Coinage from the equation – "proofhash < coins • target".*

B. Blockchain Precomputation

The block timestamp is key to the ***Proof of Stake*** *system*. It is possible in theory to fork a coin by changing previous timestamps. The stake modifier does not obfuscate the hash of sufficiently to prevent knowing future proofs. So an attacker can attempt to compute all of the blocks in

advance and run a higher probability to forge multiple consecutive *blocks*. Solution from ***Proof of Stake 2.0:*** The stake modifier is changed at every modifier interval to better obfuscate any calculations that would be made to pinpoint the time for the next proof-of-stake. The expected block time was increased from *original 60 seconds to match the granularity.*

Past limit: Time of last block Future limit: +15 seconds Granularity: 16 seconds (effectively increased from 1 second) Expected block time: 64 seconds

C. Block Reward

The Block Reward in most ***Proof of Stake*** systems is unfortunately based on ***Coin Age***. In theory, this is to distribute interest fairly by allowing nodes to receive latent payments due. It is an attempt to keep a common ***APR***. However, this system does not work because nodes can stay disconnected and with many split inputs, reconnect to the network and game the reward system. Also, it does not give nodes any incentive to stay connected. In a decentralized system, the more nodes connected the better the securitysince it shifts trust from a single entity to the network itself. Solution from ***Proof of Stake 3.0***: The block reward was made a constant ***5 coins per block.*** This was based proportional to the supply of coins maintaining interest.

IV. Multisignature/cold staking

The final noteworthy addition to the protocol was the implementation of "**Multi-signature Staking**". One drawback to many staking algorithms is they only support staking with a single key. Since the popularity and use of software such as **BlackHalo**, which uses a two party escrow system also known as ***"Double deposit escrow"*** and more secure dual key accounts, it has become important to allow these accounts to participate in securing the network. Beyond dual key accounts there is many other types of inputs that make use of *p2sh* and lock times and those must also be allowed to secure the network as well. The other problem is that in a single key account, a hacker can use key loggers to obtain your password and compromise your wallet while it is unlocked for staking. Solution from ***Proof of Stake 3.0***: We allow users to place the block signing key in the output of "*6a*" known as a burn address so they can stake by sending a standard transaction. This allows any input to be eligible for submission. This gives Impleum a huge advantage for custom staking software, voting and the legendary "***Cold Staking***". The "***Cold Staking***" technique involves multiple computers. Basically when a multisignature input is eligible for staking, the signatures are split up between many computers. This makes an account virtually impossible to hack because even if a single key was compromised, the other keys are in a completely different location either on the local area network or on multiple servers. This technology is already being implemented in the latest release of *BlackHalo*.

V. Security Analysis

The elimination of ***Block Reward*** based on time was an obvious improvement. Thus, if the amount of nodes staking drops, yearly interest would increase proportional to the disconnected nodes. For example, if only ***1/5th*** the network was *Staking,* you can expect up to 5 times the reward! Since many coins do not have enough nodes, this is a great advantage even to smaller shareholders. Although statistical data on all relevant coins would be time consuming to obtain, it is self-evident that there is usually a lot less than ***20%*** of the shareholders *staking*. We think this increase in incentive will certainly keep the nodes more competitive. The change in granularity was useful to prevent "***Stake Grinding"***. A good analysis of the probability of this attack was done in ***Neucoin***. Their claim is that even with all the hashing power of the ***Bitcoin network***, the attack

would not be possible. However, a rollback of a few minutes could cause new users to the network unsure of which chain to join. Therefore, Proof of Stake systems use "***Checkpointing***" which is basically centralized control of the main developer to choose chains that attempt to do this. Of course, this is not an ideal solution. There was a good proposal made in ***Ethereum*** for this. They proposed that a new node to the network asks other nodes "***off-band***" if they are indeed on the *correct chain*. Using our decentralized markets, it is possible we can get nodes to share this information periodically. The solution will require further investigation. The additional removal of ***Coin*** age in general is a secure decision. It is possible to perform a hybrid system of checking popular time servers as well to help calculate drift and require nodes to keep closely synchronized with a *general consensus* of time. Addition of other random factors based on the *blockchain* itself may also be a consideration.

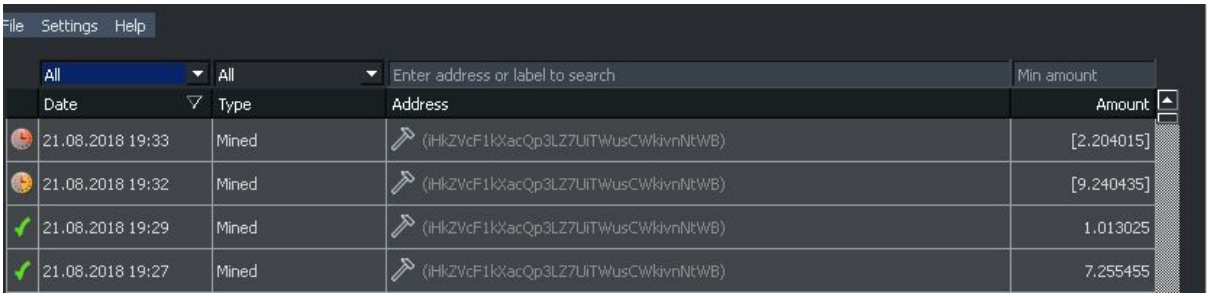
VI. Conclusion

One of the most secure ***Proof of Stake*** systems in the world is being used here at Impleum. We also have several candidate solutions and ideas for improving security further. Here at Impleum, we take your security seriously. We have done everything possible to maintain anonymity, keep as many nodes connected as possible, guarantee decentralization and mitigate all attacks. *Decentralization* was the original core ideology in ***Bitcoin***, although we feel this ideology has not been completely maintained. The entire purpose of a secure and fair financial system is to place control of it in the hands of the people. ***Proof of Stake 3.0*** has the economic advantage over *Bitcoin* because it does not waste electricity to generate new blocks, nor does it create unfair competition for new coins. And now with the incentive to stay connected, shareholders get greater benefits across the board.

Inflation rate

IMPL coins are issued at a rate of 5 coins per Block – every 60 seconds, the more an individual stakes Impleum, the more IMPL coins is giving out as a reward. An incentive for users to contribute towards making a more secure POS-based network by staking their coins
Many of you, eager to start staking your IMPL will ask yourself this;

What is the total supply / inflation of the IMP coins?
To get a better understanding based on findings, as of 2018-08-21 there are 3 287 806 IMP outstanding. A common misconception I see all the time in the Impleum community regards the Inflation rate, since many individuals claims that the inflation rate is 79%
A new block is derived via POS about every minute, and 5 IMP is generated per block. This means, on average, about 7200 new IMPL are mined each day since there are 1440 minutes in a day. That equates to 2 628 000 new IMPL in a 365 day year. 2 628 000 /3 287 806= 0,79931723



So the inflation rate as of 2018-08-21 is about 79%, and this rate decreases as the total supply grows.However, we can assume that not everyone stakes their IMPL. This is what makes it seem like the inflation rate is greater than it is. Around 2 299 045 IMPL are staked right now on May 2018-08-21. This means that the 1440 IMPL generated per day are going to the holders of that 2 299 045 IMP. This would equate to earnings from staking equal to about 114% if 2299045 IMPL were being staked the entire year (2 628 000 /2 299 045 = 1,14308332).

Year	IMPL per year	Coin Supply	Inflation rate
2018	2628000	3287806	79.93172347
2019	2628000	5915806	44.42336344
2020	2628000	8543806	30.75912538
2021	2628000	11171806	23.52350193
2022	2628000	13799806	19.04374598
2023	2628000	16427806	15.99726707
2024	2628000	19055806	13.79107239
2025	2628000	21683806	12.11964357
2026	2628000	24311806	10.80956306
2027	2628000	26939806	9.755081384
2028	2628000	29567806	8.888045329
2029	2628000	32195806	8.162553843
2030	2628000	34823806	7.546561683
2031	2628000	37451806	7.017018085
2032	2628000	40079806	6.556917965
2033	2628000	42707806	6.153441832
2034	2628000	45335806	5.796742645
2035	2628000	47963806	5.479131493
2036	2628000	50591806	5.194517073
2037	2628000	53219806	4.938011236
2038	2628000	55847806	4.705645912
2039	2628000	58475806	4.494166357
2040	2628000	61103806	4.300877755
2041	2628000	63731806	4.12352978
2042	2628000	66359806	3.960228576
2043	2628000	68987806	3.809368862
2044	2628000	71615806	3.669580986
2045	2628000	74243806	3.539689223
2046	2628000	76871806	3.418678625
2047	2628000	79499806	3.305668444
2048	2628000	82127806	3.199890668
2049	2628000	84755806	3.100672537
2050	2628000	87383806	3.007422222
2051	2628000	90011806	2.919617011
2052	2628000	92639806	2.836793505
2053	2628000	95267806	2.758539438
2054	2628000	97895806	2.68448681
2055	2628000	100000000	2.628

It seems that Inflation of the IMPL coins is a measly around 79% based on 21th August Statistics, but people can earn a higher percentage than that simply because not everyone is interested or has the means to stakes their coins

Impleum Masternode Registration Protocol

Impleum Masternodes work on *Tumblebit* technology. It is a new platform for sending and receiving Bitcoin or Impleum coins. It is a trustless, decentralized and private solution for users of Bitcoin across the globe.

1% fee from all Privacy IMPL protocol transaction
You earn 1% of all Tumblebit trade fees, which, over time as trade volume grows, will probably double the worth of your staking rewards.

Minimal transaction – 0.1 BTC or IMPL
To keep transactions anonymous, users are able to send or receive increments of *0.1 BTC* just at this time.

Limited quantity
There'll be quite a limited quantity of masternode owners, which will definitely keep your transaction earnings high.

TumbleBit

You should have *10,000 Impleum* or more, you can make staking rewards. To earn staking rewards (i.e. "free Impleum"), all you need to do is hold *10,000* or more Impleum on your QT (core) pocket, and also maintain a synchronized full node running on your PC. Even though the amount of Impleum you can stake is variable, for every *10,000 Impleum* you hold, you'll stake/earn approximately *25* Impleum per day.

Impleum has lately opened up another tier of benefits for holders of *100,000* Impleum or more masternodes. By conducting a masternode, You can make additional benefits over and beyond staking rewards of *250–300* Impleum daily.

MasterNodes

Masternode owners can supply the Impleum platform with assistance, acting as a *Bitcoin* tumbler. A *Bitcoin* tumbler lets users send or receive *Bitcoin* in a more anonymous fashion, because your trade is blended, or 'tumbled' with dozens of other transactions of the same amount/size, obscuring whose *Bitcoin* originated from where and has been sent to wherever.

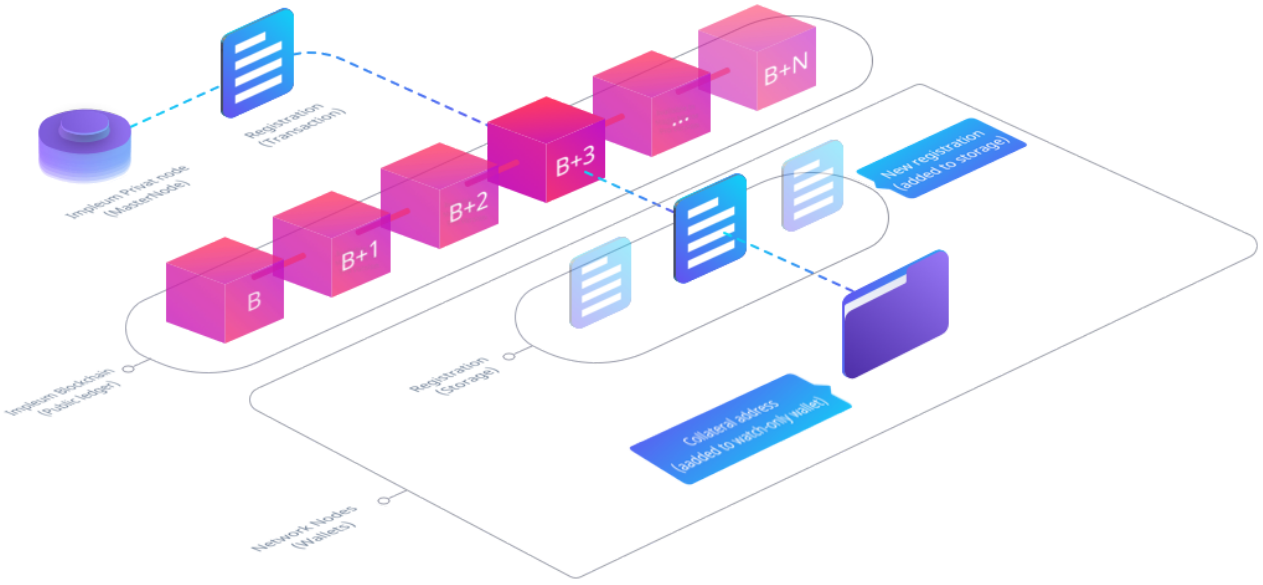
Impleum masternodes solve the problem of providing useful services to a blockchain network while keeping the list of services decentralised and tamper-proof. In the initial masternode implementation the service being provided is the Impleum Privacy Protocol, but it is anticipated that many more services can be added in future.

In order for this goal to be accomplished, each masternode must register (advertise) its existence via the Impleum blockchain. This is what is referred to as the Masternode Registration Protocol.

A masternode registration simply consists of a specially formatted Impleum transaction. This transaction contains all the pertinent information needed by a client to connect to and validate the masternode.

A registration transaction, once submitted to the network, remains valid indefinitely until invalidated by one of the consensus rules governing such registrations. These are:

- The masternode server's funding address is not funded within the initial window period.
- The collateral funds are insufficient at the conclusion of the window period (see section **Collateral Verification** for additional information regarding the collateral and the balance tracking).
- The collateral funds get moved, wholly or in part, to another address, thereby decreasing the balance below the required threshold.
- A subsequent registration is made at a greater block height than the original (e.g. to update the masternode's public parameters).
- *(Currently not enforced)* A registration expires every *N* blocks, requiring the operator to periodically refresh it.



It is the responsibility of the Privacy wallet client software to scan the Impleum blockchain for the most current masternode registrations prior to initiating contact with any server. They do this by observing each incoming block, looking for transactions that match the bitstream format. When a registration is found, it is stored in the node's local store.

The block height that the registration is received at determines the window period for the masternode funding transaction. The masternode operator has to move the required collateral into the funding address before this window elapses. If this is not done the registration will be regarded as expired and purged from the local storage of all nodes on the network.

Once a sufficient number of valid masternode registrations have been downloaded, the client can select one at random and try to connect to it to utilise its services (e.g. the Impleum Privacy

Protocol). Optionally the masternode selection can be performed once the entire blockchain is downloaded, as this is more fair to masternodes that register later in the chain.

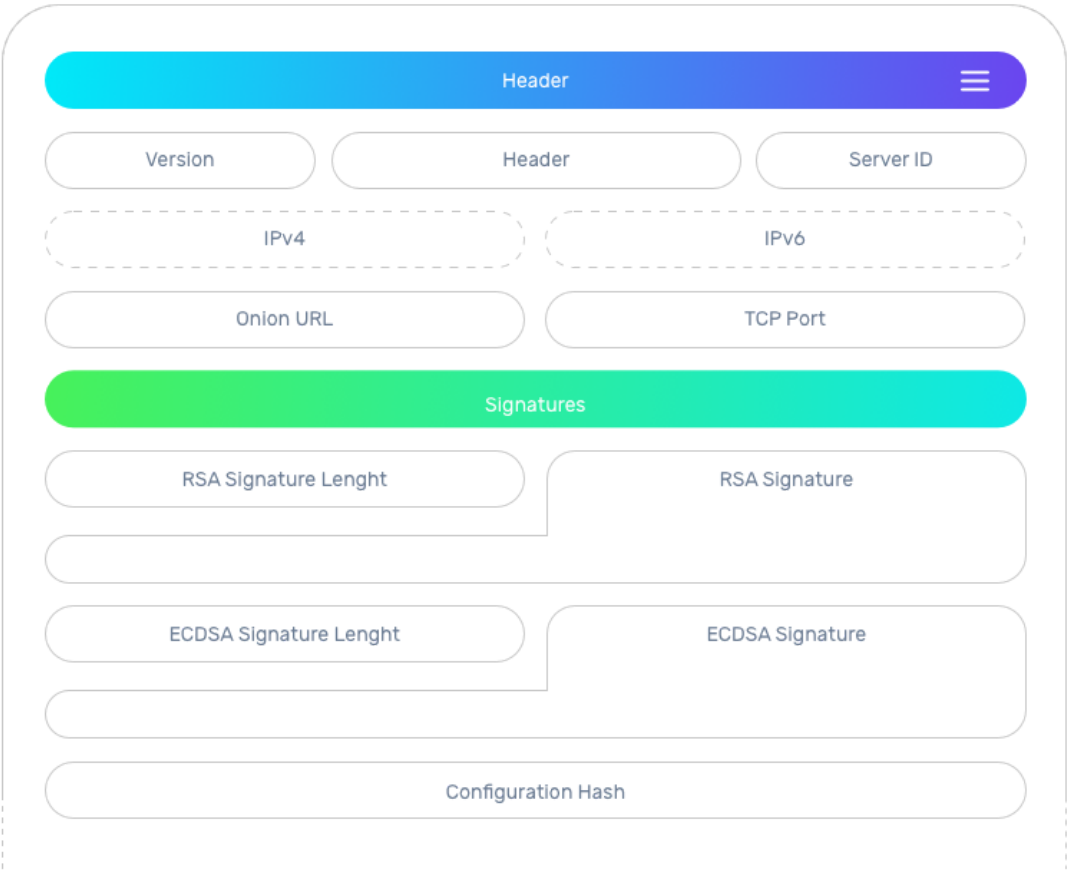
The process described above has already been implemented into the Impleum software offering.

Bitstream format for masternode registration transaction

The registration transaction consists of a single transaction broadcast on the Impleum network (either testnet for testing or mainnet for 'live' masternodes). This transaction can have any number of funding inputs, as normal.

It has precisely one nulldata (data storage) output marking the entire transaction as a masternode registration. There can be an optional change return output, which if present must be at the end of the entire output list. The remainder of the transaction outputs are of near-dust value. Each output encodes 64 bytes of data into a public key script. The contents and format of the encoded data is described below.

The presumption is that the transaction outputs are not reordered by the broadcasting masternode, as this would result in potential data corruption.



OP_RETURN transaction output

Field	Size	Description
1	26 bytes	Literal ASCII string: PRIVAT_REGISTRATION_MARKER

Encoded public key transaction output

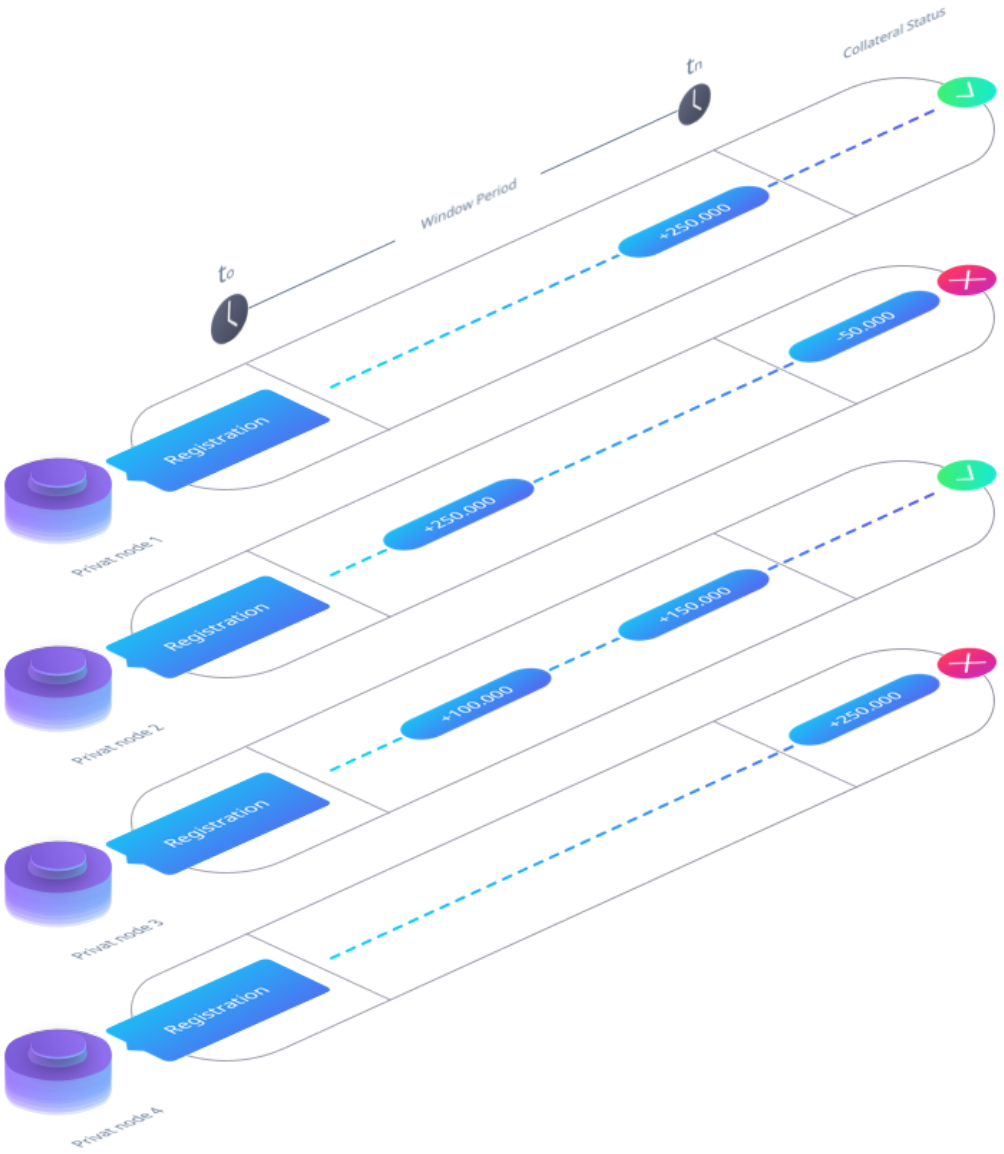
Field	Size	Description
1	1 bytes	Protocol version byte (if >200, it is a testregistration to be ignored by mainnet wallets)
2	2 bytes	Length of registration header
3	34 bytes	Server ID of masternode (base58 representationof the collateral address, right padded with spaces if it is less than 34 characters long)
4	4 bytes	IPv4 address of masternodes, one byte per octet. Use 00000000 for empty address. This field is not used for the Impleum Privacy Protocol; it is a placeholder for future functionality
5	16 bytes	IPv4 address of masternodes, one byte per octet. Use 00000000 00000000 00000000 00000000 for empty address. This field is not used for the PrIlmpleumvat Privacy Protocol; it is a placeholder for future functionality
6	16 bytes	Masternodes server URI, curreltly this an ASCII onion address hostname without any prefix or suffix. An empty address is signified by 00000000 00000000 00000000 00000000, but leaving this empty is not valid for the current Impleum Privacy Protocol Implementation
7	2 bytes	TCP port of masternodes , may be ignored by client implementation
8	2 bytes	RSA signature length in bytes
9	n bytes	RSA signature proving ownership of the Impleum Privacy Protocol server's private key
10	2 bytes	ECDSA signature length in bytes
11	n bytes	ECDSA signature made with the privaty key of address used as the server ID. This same address is where the collateral will need to be located
12	40 bytes	Hash of Impleum Privacy Protocol server's configuration file. This may be moved into the header in the next version of the protocol
...	...	The protocol format can be extended in the future to accommodate new functionality. New fields should attempt as far as possible to retain backward compatibility with the existing fields

On connection with the Impleum Privacy Protocol server by a client, the public key of the server will be verified by the client to ensure that the server is authentic and in possession of the registered keys. The Privacy Protocol is then followed as normal.

Collateral Verification

For the Impleum Privacy Protocol to function well, the creation of numerous or insufficiently powerful masternode servers must be disincentive. Therefore, consensus rules that govern the validity of a masternode need to be established and enforced by participating client nodes. A Impleum masternode requires 100 000 or 10 000 Impleum coins (IMPL) to be regarded as compliant. These coins should be kept in a single address, and should not be moved once the funding transaction is performed.

On receipt of each new block, the non-masternodes will check each transaction for those that affect a currently tracked masternode server. If funds have been moved out of the address, the calculated balance is decreased. If funds come in, the calculated balance increases. Once the balance has been computed for a masternode, its registration is automatically deleted if it falls below the 100 000 or 10 000 Impleum coins (IMPL) threshold. It is therefore not recommended that significant transactional activity be performed with the collateral funds, to avoid inadvertently invalidating registrations.



The above diagram illustrates 4 basic scenarios for a masternode's registration sequence.

- Node 1 has made a sufficient funding transaction within the window period, and as such its collateral is regarded as compliant.
- Node 2 was initially compliant after the window period, but later removed some funds from the address, and therefore no longer has sufficient collateral.
- Node 3 made two transfers that when aggregated form sufficient collateral in the target address. This is a valid, but non-standard method of performing the funding.
- Node 4 took too long for the funding transaction to be performed (it was outside the window period), and is therefore regarded as non-compliant in terms of its collateral obligation.

The collateral verification functionality has also already been implemented into the Impleum software offering.

Future improvements

Inter-node discovery protocol

A drawback of the approach outlined in this paper is that every node has to download the entire blockchain from the genesis block onwards in order to accurately determine collateral balances. It is more efficient for registrations to be accumulated by full nodes, and circulated to their peers (full or light nodes) with sufficient proof of their accuracy.

The inter-node discovery protocol has already been implemented in the Impleum node software, but is not currently used in order to keep the initial version as simple as possible. It also has an indirect requirement for the peer policing described in the **Peer policing model** section.

Improvement proposal – peer policing model

There are some differences between existing masternode implementations and the envisioned Impleum masternode approach. Briefly:

- Dash masternodes are remunerated 'passively'. This requires that they be actively pinged in a verifiable way by the remainder of the network to avoid paying a masternode that performs no work.
- Conversely, a Impleum masternode can currently only earn remuneration via active participation in the Impleum Privacy Protocol with connected clients. This removes the need to directly police the masternode in this sense.
- Due to the high cost of a top tier Impleum masternode, it is presumed that the operator will be economically incentivised to positively participate in the network. This is similar to the core tenets of the Proof Of Stake consensus mechanism.

There are also some aspects of the Dash approach that are desirable to emulate, particularly the ability to have the collateral in 'cold' storage.
The requirements for the Impleum top tier masternode may be summarised as follows:

- The node operator must be in possession of at least 10 000 or 100 000 Impleum (i.e. they possess the private key to move or spend them).
- These collateral Impleum must be present in a single address.

- Moving the Impleum collateral to a different address invalidates any proof of possession generated prior to the move.

These requirements need to be actively enforced to prevent dilution of the Privacy Protocol security model. It is proposed that the entities most suited to perform the enforcement are the masternode's peers on the Impleum network. These peers may be one of the following:

- Another masternode (essentially a full node with additional features).
- A 'full' node with a complete copy of the Impleum blockchain.
- A 'light' node that does not retain a copy of the entire chain, but does at least retain block headers.
- Other types of nodes are outside of the scope of this document.

The onus is on a particular masternode to advertise its services to the network. This means that every node can elect whether or not to regard a masternode registration as valid, depending on the information it has available to it. From a game-theoretic perspective, it is advantageous for the operators of 'rival' masternodes to immediately present proofs of non-compliance of a particular masternode to the rest of the network. It is additionally presumed that there is no advantage to be gained for an honest node to propagate registrations known to be invalid.

An example of the 'lifetime' of a registration & implementation of the 'proof of non-compliance' concept is as follows:

1. Operator configures masternode, which generates masternode registration Y on startup.
2. Node operator moves sufficient collateral into address X (the 'funding transaction'). This needs to be done within a finite window period after the registration transaction is made.
3. Registration Y is broadcast as a transaction to peer nodes for inclusion into the Impleum blockchain in block Z.
4. The registration is cached on each peer node. Nodes that join the network after block Z need not download the entire chain to receive registration Y – they can receive lists of verified historical registrations by communicating with their peers (inter-node discovery protocol). Light nodes can validate registrations for themselves by evaluating the Merkle proof of the registration against their locally downloaded block header storage.
5. All full nodes on the network can directly evaluate the balance available in address X at any time. Therefore, if it transpires that a spurious masternode registration has been broadcast (which may happen) the full nodes will not forward that registration on to new peers. Peers that attempt to send known-invalid registrations will receive a proof of non-compliance in response.
6. The status quo persists for a period of time without any changes that affect masternode registration validity.
7. The masternode operator moves a portion of the funds from address X elsewhere, i.e. they are now below the collateral requirement.
8. All nodes that download blocks will immediately be able to tell that the balance of X has changed, although a light node may not know what the actual balance is. Full nodes do know (or can calculate) what the balance is, and can construct a proof thereof showing that the masternode is no longer compliant.
9. The non-compliance proof will be broadcast between nodes. This could be done pre-emptively (i.e. broadcast proof to all known peers immediately), or it could be done passively in response to receiving an invalid registration from a peer.

At a high level, the proof of insufficient funds will consist of the following elements:

- A copy of the 'funding transaction' for the masternode. This is defined in more detail in the **Funding Transaction**
- The registration record itself (in its entirety, as the peer may not have downloaded it yet).
- At least one complete transaction with the funding transaction included as one or more of its inputs i.e. showing that collateral funds have been moved/spent.
- The net result of the movement transactions must be that the balance of the collateral address is < 100 000 IMPL (< 10 000 IMPL).
- Merkle proof(s) for the movement transaction(s) showing that they are included in a block at the same or higher height than the funding transaction.

A light node should be able to interrogate a peer node about the perceived status of one or more masternodes. If the peer being interrogated is also a light node, it will only be able to pass along proofs it already received and stored from the full nodes.

Funding transaction

The funding transaction for a masternode is the transaction that assigns the 100 000 Impleum collateral to a given address. It is recommended that only a single transaction output be used for this, to keep the size of the proofs communicated between peers to a minimum.

There is also naturally a possible gap between the block height of the funding transaction and the block height of the registration transaction, during which some fund movement may have occurred. This should not be a problem, as full nodes will evaluate the solvency of the masternode and determine whether to propagate its registration to other peers via the inter-node protocol.

Some possible attack/DoS vectors

The most vulnerable portion of the network are the light nodes. The proof mechanism therefore needs to be robust enough to allow the light nodes to participate in policing the masternode registrations without having the entire blockchain available.

The masternode operators also need to be protected from rogue full nodes attempting to stifle traffic to particular masternodes by censoring their registrations. This is mitigated by the decentralised nature of the Impleum blockchain. It is only required that a sufficient number of honest nodes participate to minimise or negate the impact of rogue nodes, as the registrations will percolate through the network via the blocks & inter-node protocol. A rogue full node cannot generate a fake proof of non-compliance, as the Merkle proofs will fail to be validated.

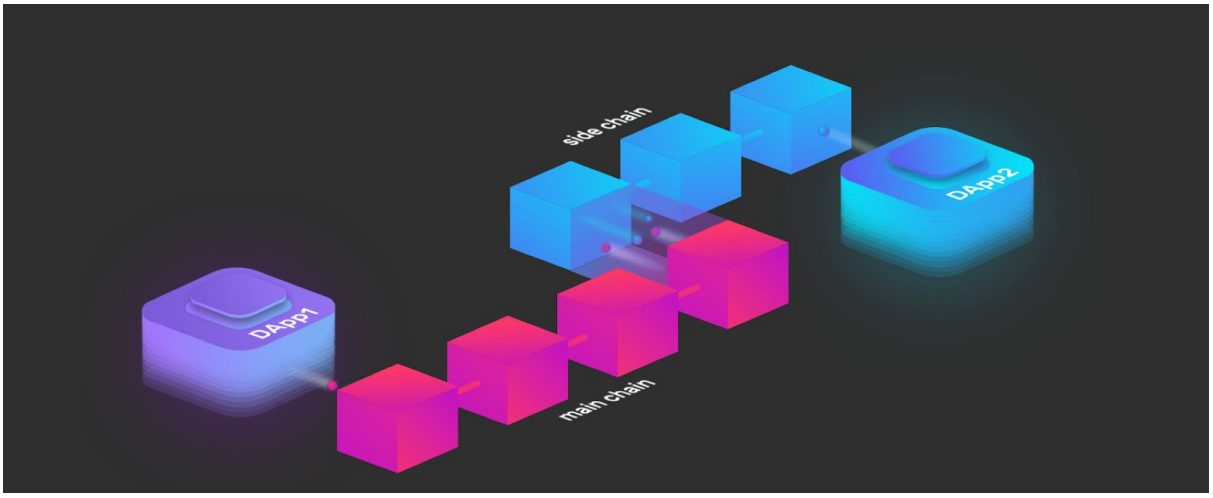
Masternode operators may generate copious registration transactions (i.e. spam) in an attempt to sway client nodes to use their server. This is mitigated by a rule that a client node will only keep the most recent valid registration for each known masternode, so spamming the network does not result in an increased likelihood that a client will select a particular masternode server.

It is important that a masternode operator avoid moving their collateral funds in such a way that they inadvertently provide an avenue for full nodes to construct a non-compliance proof. If funds need to be moved it is recommended that an entirely new address be used & a new registration performed. This will naturally cause the previous registration to be invalidated and

removed from the caches of nodes on the network. The new registration will, conversely, be cached and used going forwards.

Impleum Sidechains

The Impleum Full Node will support sidechains. This is achieved using a Two-Way Federated Peg solution. This means that IMPL can be passed to and from the sidechain and the gateway through which they pass is controlled by a federation. The federation consists of 3 or more members who have control of the sidechain.



The target audience for this document include federation members, users of the Impleum mainchain who want to send funds to the sidechain, and anyone interested in how a Two-Way Federated Peg operates.

Like the Impleum Full Node, Impleum sidechains are written in C# using the .NET Core platform. Although this material does not cover any programming tasks, a working knowledge of blockchain topics such as transactions and wallets will be very useful.

To enable users to get started, Impleum will create a sidechain running on the Impleum testnet. It has 5 federation members supporting it drawn from the Impleum Platform internal team. The sidechain has its own token called the COM. Users can deposit IMPL on the sidechain and in return they receive COM to spend on the sidechain. Impleum provides a modifed Impleum wallet and an COM wallet to help facilitate this.

One way of understanding sidechains is to think of a sidechain as a foreign country and the Impleum mainchain as the user's home country. The federation secures an amount of the foreign currency (in this case COM), which it can loan to sidechain visitors in return for depositing IMPL. When a user returns home, they can relinquish their COM and withdraw the equivalent amount in IMPL on the mainchain.

Building sidechains in C# makes it easier to integrate into existing enterprise architectures and opens the door previously blocked due to programming language barriers. Impleum sidechains in C# builds upon the established .NET framework, language and ecosystem. Therefore, it is more readily poised for wider adoption.

Impleum Sidechains solve a significant challenge facing enterprises concerned about implementing blockchain solutions due to the lack of privacy and control inherent to most existing public blockchains. An enterprise lacking the ability to influence changes in public infrastructure to suit their specific needs is a valid cause for concern.

Impleum Sidechains operate by 'locking' Impleum coins on the Ompleum mainchain as a value proxy for enterprise tokens forged on any sidechain. This overcomes the complexity of transferring digital assets between different blockchains, offering flexibility and confidence that any sidechain digital asset will always be backed by the correct amount of Impleum coins. The flexibility of a sidechain also helps to improve scalability, a long-running challenge of decentralized computing. Aside from leaving the mainchain free to exchange funds, Impleum Sidechains make it possible to specify both the block size and block interval, increasing the number of transactions in each block and/or reducing the time between each block.

The Impleum Sidechains Alpha release follows the recent news of Impleum Smart Contracts in C#, which allows a wide range of decentralized applications to be built upon the Impleum Platform.

Impleum C# Smart Contracts: smart contracts which can be deployed in C#

The value for Impleum, over all other platforms, is in using C# / .NET and being able to leverage the powerful ecosystem that already exists there:

- Using Visual Studio to develop, compile and debug the code
- Easily decompiling CIL to C# source code
- Strong testing frameworks that run natively inside Visual Studio
- C# that behaves exactly as it would inside any other .NET application and thus can be audited by countless developers
- Entire companies based around the security auditing of C# code which have produced extensive list of software tools that can scan for certain kinds of conditions in the code (essentially, Impleum could have “code scanners” which can be applied or adapted to smart contract code)
- Well established best practices and technical tools that have been developed at corporations which can be used easily with Impleum contracts, and will actually MEAN something because the code will behave the way developers expect it to

All of these (and many, many more) are only possible when running the CIL / CLR rather than a custom Virtual Machine. So far, no-one else has gone down this road with C# smart contracts. In fact, no-one has gone down this road with any smart contract offering.

NEO is perhaps the best known platform currently offering coding in C# for smart contracts. It is misleading to say “NEO has C# smart contracts” because NEO compiles the syntax of the

language into their custom instruction set to run on their custom Virtual Machine (the NeoVM). The smart contract code that executes on the Virtual Machine is not .NET, it is NEO bytecode.

Here's a handy guide on whether your code is real C#:

- Does the C# code run like it would in other environments such as .NET web, console or mobile applications?
- Hence, can C# developers audit the code knowing it's going to behave EXACTLY as they would expect?
- Can developers debug in Visual Studio natively?
- Can developers use other parts of the C# ecosystem such as decompilers?

If the answer to any of these questions is no, then you'd be hard-pressed to convince someone your code is truly C#. When the smart contract code that executes on the Virtual Machine is not .NET, it is virtually impossible to guarantee that the C# code will behave in the same way as a real .NET web or console application. This means that very few developers can effectively audit what has been written.

For Impleum, the smart contract code that executes on the VM is the same code that would execute in a web or mobile or any other C# application.

(As an aside, theoretically any language that can be translated into CIL will also be supported for Impleum. This means native C# and F#, VB, and any other language where software has been written to compile to CIL will be supported for Impleum smart contracts).

Confidence in the security of smart contracts is very important for the adoption of the technology. To this end, Impleum have ensured that auditing and testing of their contracts can be easily done by a larger group of developers than ever before. This is because their contracts can be decompiled back into the C# source code. This is SO BIG for Impleum. For every single contract, nodes can natively display the C# source for auditing, instead of just the bytecode. No-one else has this functionality yet. Even Ethereum's Solidity compilers like Porosity are very primitive.

Impleum smart contracts can be developed, compiled, debugged and unit tested all in Visual Studio without any external tools. It is just .NET code running like any other .NET application: there is no need for compilation down to a different Virtual Machine / instruction set. This means that auditing of the contracts could be done by developers from a community which is quite literally millions strong.

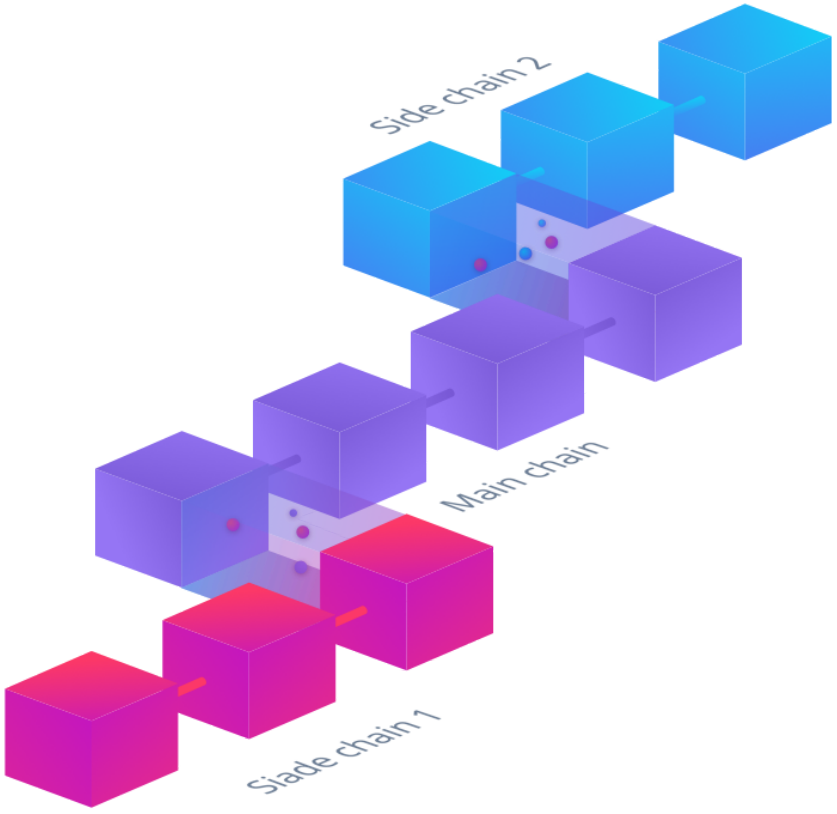
Impleum: key features

Impleum allows the creation of distinct, private blockchains, launched by third party organisations and tailored to their needs but secured on the main Impleum blockchain. They can be accessed via lite clients and simple but powerful APIs. Because these Private chains are based upon the code of the main Impleum chain and side chains are compatible and transfer between the two is straightforward.

Impleum Private chains

A secure blockchain network will typically consist of hundreds or even thousands of computers running the same protocol. Consequently, there are significant advantages to employing an established network with proven stability and security, rather than starting from scratch. Although it is possible to develop applications on top of the Bitcoin blockchain, the first and still the best-known and most secure cryptocurrency network, there are good reasons why few businesses would want to so. Bitcoin has comparatively slow 10-minute confirmation times, and periodic attacks on the network means that transactions can be delayed for hours; addressing these effectively requires a controversial hard fork and the pace of development is slow.

Businesses have no control over upgrades or other changes to the network such as the capacity of each block and the rate that transactions that may be processed. Thus Bitcoin's security advantages come at a cost of significant rigidity and unpredictability.



By contrast, Impleum private chains allow developers complete freedom to customise their implementation for their specific needs, whilst the underpinning 'parent' blockchain is established enough to give users a high degree of confidence in its security. For example, if a business requires large block sizes to accommodate a high volume of transactions; rapid block times to enable low-latency trading; controlled transactions so that only approved users can submit a request to the network; a given rate of inflation; or additional space for metadata in

each block, any or all of these can be specified at launch. The private chain can be accessed by straightforward APIs, meaning that stand-alone applications can rapidly be developed.

Impleum blockchain-as-a-service (BaaS)

The potential of Blockchain as a Service (BaaS) has already been recognized by some of the world's largest software companies. In fact, the 'big' three cloud providers, Amazon, Microsoft, and IBM have developed BaaS platforms that are already available to their cloud customers. Other companies like Google have bought up blockchain technology firms like Firebase in order to try to secure a foothold in what is shaping up to be a highly lucrative market.

A recent article in Bitcoin Magazine predicted that the Blockchain Technology Market to Reach $7.7 Billion by 2024. However, many industry insiders put their figures much higher, particularly given the phenomenal gain in popularity of blockchain based technologies resulting from 2017's meteoric rise of Bitcoin and other cryptocurrencies.

While we are all just going to have to wait and see just how big the blockchain technology market is going to become, given that it has huge potential benefits for just about every major industry in the world today, what is certain is that blockchain is set to make some pretty big waves in the years to come.

Given this fact, I want to explore in more detail exactly what this new technology is and how it can be used to help businesses of all shapes and sizes. We will examine the services that the three biggest BaaS providers are currently offering to try to get the best idea of what the potential of this technology really is.

Decentralised app hosting

As well as offering the services integrated in its own blockchain, Impleum will specialise in providing hosting and consultancy for decentralised applications (Dapps) on top of the Ethereum blockchain. This enables a complete off-the-peg approach to smart contracts. Impleum will work closely with businesses to determine their needs, before deploying nodes if required and organising hosting. This allows clients to focus solely on creating dapps without expending time and resources on infrastructure.

One-click deployment

Impleum makes it easier than ever before for organisations to deploy private blockchains, taking a cloud services approach to provisioning. A one-click process means that new chains can be launched with unprecedented speed, tailored for the needs of the organisation. A broad range of variables including block time, size and space for metadata are customisable, making it incredibly flexible. Essentially, an entire network can be bootstrapped on the back of the main chain, giving a ready-made cryptocurrency ecosystem for developers to use out of the box.

Three-tier architecture

The Impleum platform uses a three-tier architecture typical of the Microsoft® ASP.NET application style. This is a good fit as the Impleum Full Node, Impleum Blockchain API and the

Impleum SPV technology are developed in C# and run within the Microsoft .NET Framework and common language runtime.

In the client tier, Browsers, Desktops, Mobiles, and IOT (Internet of Things) devices connect to the various services in the application tier. They receive blockchain data by querying the Impleum Chain API via HTTPS.

The application tier is composed of the Impleum Chain API, Cloud Impleum Management portal, Cloud Impleum API and Secure Payment Verification (SPV). All of the components in the application tier are developed in C#. The application tier handles Blockchain requests and SPV proofs for Lite clients that do not download the full blockchain. It also provides access to the Impleum Cloud management portal and API.

The server tier consists of the Impleum Full blockchain Node, the Cloud Impleum hosting layer and the Impleum payment protocol.

Scalability

Scalability is a major issue for cryptocurrency protocols. Because every transaction is stored on the blockchain for transparency and immutability, in an unoptimised blockchain the size of the chain is a function of the number of transactions. This can cause serious issues. Bitcoin's 1 MB block sizes limit it to a low throughput of transactions per second (tps), and tensions between different stakeholders in the Bitcoin ecosystem (including miners, large holders/advocates and end-users) have meant that the problem has proven extremely difficult to fix. The result has been that there have been periods when transactions have been delayed because there is not enough space in a block. Consequently, few serious businesses would voluntarily expose themselves to the risks of using the Bitcoin blockchain for third-party applications, having no control over the future of the protocol and no influence over any improvements that might be made.

For Bitcoin, the problem of transaction volumes may yet be solved by a hard fork to enable larger blocks, but this is still a suboptimal solution. As transaction volumes grow exponentially with greater adoption (in the best case scenario), block size will also have to grow exponentially. This places greater demands on full nodes in terms of bandwidth and disk space. Despite expected advances in storage and connectivity technology, this will likely lead to an even greater centralisation of mining, in which only the best-resourced nodes can afford to maintain the network. Aside from any political and ideological concerns, this has implications for network security.

Impleum addresses these problems in several different ways. Firstly, every private blockchain is configurable, meaning that an organisation can choose how large blocks should be - reflecting their own needs and resources.

Related to this, instead of using a single ledger for every application, Impleum comprises a host chain from which financial businesses can deploy their own ledgers depending on their specific requirements, rather than directly using the same blockchain as the whole Impleum network (or the whole Bitcoin ecosystem, if the Bitcoin blockchain was employed). This offers the remarkable

versatility of an extensive 2.0 platform, combined with the full control of a private chain – secured by the host blockchain but tailored and administrated by the owning organisation.

On a separate note, Impleum employs a proof-of-stake approach to consensus which aligns the interests of end-users (businesses) and those tasked with securing the network (full nodes). This means that a business can run a full Impleum node as well as nodes for their own blockchain without the overheads associated with specialist mining hardware.

Lastly, a series of measures will be used to combat bloat on the main chain, which ultimately serves as a means to secure child chains and can therefore be kept as lightweight as possible.

Bitcoin compatibility

Because Impleum's Private chains are based on the same code as the main blockchain, the interface for private chains is 100% compatible with that of the main Impleum chain. Impleum will provide the same RPC API as Bitcoin Core initially, which means that any applications or platforms that use Bitcoin's RPC or command line can be ported quickly to Impleum's. New functionality is provided by Impleum-specific API calls.

The compatibility between main and Private chains also means that it is a simple matter to incorporate new features developed for Impleum into a private chain - and potentially vice versa, since any feature developed by a business could be released into a future update of Impleum's. However, this would only take place with the express consent of the business. Although Impleum's customers de facto have full use of every feature on the Impleum's blockchain, there is no onus on them to make privately-developed features available to others.

Conclusion

Impleum's private blockchains offer several significant advantages over the creation of a new chain from scratch, and for most organisations will provide all the required benefits without either being unnecessarily restrictive or entailing the significant overheads involved in creating and maintaining a cryptocurrency network.

The cloud provisioning approach to blockchain, or blockchain-as-a-Service (BaaS), makes deploying a new chain a process as simple as signing up for an account and selecting required parameters. These tailor-made solutions are accessible via web interfaces and APIs, although users can run full nodes for both their private chain and the host Impleum network if they wish. Compatibility with Bitcoin means that Bitcoin-based services can easily be ported to Impleum for additional functionality and convenience. As a result, Impleum is positioned strongly for an entry into the BaaS space.

Core contributors

Yurii Bulakh – blockchain developer
Yurii is a web entrepreneur, founder of Inteh-S and Avtomatizator, a business analyst with over 14 years experience in complex information systems for business management, is the technical ideologist of the project.

Pavel Lypysyvytskyi
A specialist with extensive experience in sales and maintenance of customers.
Anton Yaroshenko – blockchain developer
Anton has experience of full stack web development by using Microsoft technologies, experience in mobile app development (Xamarin). Worked on high loaded systems. He can fully implement architecture and app from scratch. Solid understanding of object-oriented design and design principles. Knowledge base: C#, .NET, Xamarin, ASP.NET, .NET Core, JavaScript, WebForms, WPF, WebAPI, android xamarin, ios xamarin, jira, tfs, redmine, JQuery,DI, IOC.

Pavel Kurianov – blockchain developer
Pavel has experience in Unity3d games/apps development, experience of full stack web development by using Microsoft technologies. Worked on high loaded systems. He can fully implement architecture and app from scratch. Knowledge base: Unity3D, C#, .NET, ASP.NET, .NET Core, JavaScript, WebForms, WebAPI, jira, tfs, redmine, JQuery, Jenkins.

Alex Hura – full stack developer
Technical Specialist with 5 year experience in front-end and 3 year experience in back. JavaScript, HTML, CSS#, ReactJS.

Vladimir Kalmyk – Linux/Unix architect
Unix / Linux IT architect with over 15 years experience.

Michael Lane Thomas – Technical Advisor
CIO at Vision Ridge Technologies
Michael has gained 20 years of enterprise IT and business development serving the frontline with prominent knowledge leaders as Microsoft, Vision Ridge Technologies. He has extensive experience in detailed technical analysis of blockchain-related business models and propositions.

Oleg Mishchenko – Product Owner Strategy
CEO and founder of ION digital
Technical Specialist with an extensive experience in development of Digital projects. Founder and CEO of «ION digital». Engaged in the development of web services and mobile applications since 2010. Participated in the development and launch of more than 10 start-ups.

References

1. Bitcoin Whitepaper https://bitcoin.org/bitcoin.pdf

2. Ethereum Whitepaper
https://github.com/ethereum/wiki/wiki/White-Paper

3. https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain

4. http://money.cnn.com/2015/11/02/technology/bitcoin-1-billion-invested/

5. http://www.ft.com/cms/s/2/eb1f8256-7b4b-11e5-a1fe-567b37f80b64.html#axzz46TUQ2D8h

6. https://research.tabbgroup.com/report/v14-009-blockchain-clearing-and-settlement-crossing-chasm

7. The most complete Bitcoin port (Part 1: Crypto),
8. http://www.codeproject.com/Articles/768412/NBitcoin-The-most-complete-Bitcoin-port-Part-Crypt

9. NBitcoin Indexer: A scalable and fault tolerant block chain indexer,
http://www.codeproject.com/Articles/819567/NBitcoin-Indexer-A-scalable-and-fault-tolerant-blo

10. See Programming The blockchain in C#,
https://www.gitbook.com/book/programmingblockchain/programmingblockchain/details

11. Blockstream Elements https://blockstream.com/sidechains.pdf

12. https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/global-blockchain/#.Wms8ZrPtypo

13. https://elementsproject.org/

14. https://stratisplatform.com/

15. https://en.wikipedia.org/wiki/Blockchain

16. https://www.i-scoop.eu/blockchain-distributed-ledger-technology/

17. https://www.jupiterresearch.com/press/%20press-releases/6-in-10large-corporations-considering-blockchain

18. https://blackcoin.org/