LegalThings One

Visionary paper

Version 1 - July 2018

Authors:
Rick Schmitz
Arnold Daniels
Martijn Migchelsen
Sven Stam
Martijn Broersma
and the team of LegalThings One

LegalThings One

Content

Introduction

Whereas blockchain devotees have been passionate about the technology for a longer period of time, the peak of the hype cycle has slowly been reached this year. As with any other emerging technology, the debate centred on the opportunities of blockchain has both proponents and opponents. Given the extraordinary amount of attention blockchain has received, it is no secret that some think it could give an answer to anything. On the other hand, the question, mostly posed by incumbent banks and organizations, arises whether or not the immaturity of blockchain will ever wear off and if it will be able to eventually evolve into a grown-up technology.

The problem, however, is that most of the noise about blockchain (but also crypto) is generated by the community talking to itself instead of sharing ideas with the outside world. In the so-called 'echo chamber', people seem to have little or no eye for lasting business value. So "what are the business opportunities for us?", sceptics, mostly incumbent banks and companies, ask themselves.

It is therefore time to leave this echo chamber and reach out to these organizations in doubt by offering a helping hand. This paper sets forth our vision on the current state of blockchain technology and elaborates on ways in which it could add value to businesses. We come up with several methods to apply blockchain technology to certain processes. Perceiving the implementation process, we help to iron out the wrinkles it still holds for some. We shall demonstrate how to create strategic business value with the technology, as we take a closer look at how organizational adoption can be achieved, using a baby step-by-step approach instead of giant leaps.

"The strength of trust is as weak as its weakest link"

The story of LegalThings starts in 2014. Our document engine MVP progressed into a workflow engine. As time progressed our clients got bigger and the processes more important. Manipulating data we stored could potentially influence lives.

As facilitators, we became the trusted third party. We realized that we shouldn't rely on trust alone. Adding layers of bureaucracy certainly might help, but it would kill productivity.

Clearly, we should do better. By employing blockchain technology we could and would. This is how the LegalThings One platform came into existence.

2. How business and blockchain interact

2.1. Shaking up the echo-chamber

After being the mysterious domain of insiders for almost a decade, multinationals and governments are gradually entering the blockchain arena. The spike of interest has created an atmosphere where the willingness to use blockchain technology is very high. Despite an abundance of tasks forces and working groups, organizations are struggling to figure out where the actual strategic business value lies.

Although cryptocurrencies are growing over hundreds of billions USD in market cap, blockchain barely shows any significant real-world applications which are actively used. In contrary to other emerging technologies, like artificial intelligence or the internet of things, it is unlikely you use a product powered by blockchain.

Naysayers argue that blockchain lacks strategic value to deliver real-world use cases, and is mainly a tool for swindlers and hustlers, relying on the greater fool theory. If organizations continue to fail in finding strategic applications for the blockchain, this skepticism can evaporate the current optimistic atmosphere, as blockchain technology itself may become the scapegoat for failed pilots and projects.

Meanwhile, as a blockchain community we have to check all boxes of a classic echo chamber. Visions and beliefs of a fully decentralized world without trusted or authoritative third parties are amplified. The reach of influencers often do not reach outside our community to industry leaders. An endless amount of conferences and meetups are both presented and visited by a select group of people that reinforce ideas. Through the echoing of this community chamber, it may seem for some people that a completely decentralized internet is something we are fairly close to, yet reality does not confine with this assumption at all.

Even though various organizations initiate blockchain teams within their structure, there is usually a yawning gap between these techies and top managers, characterized by vague ideas, pipe dreams and mutual misunderstandings. As a result, these teams soon find themselves inside the blockchain echo chamber, floating away from their peers to form lonely islands with little to no infiltration within the organization.

Eventually, it is up to pioneering blockchain companies to collaborate with these blockchain teams and respond to the skepticism from higher-up, by delivering a clear outline of the steps that need to be taken towards integrations and the real value in their proposals is evident.

2.2 Catching flies with vinegar

Blockchain has often been portrayed as the next big disruptor. The technology indeed shows remarkable similarities to internet as many argue. From its inception, blockchain has been viewed as disruptive technology, with the power to get rid of old customs and obsolete jobs, such as intermediaries and other third parties. Within our community, many believe that the blockchain will break down ivory towers, like banks, lawyers and civil services, causing a higher and different distribution of power.

A significant shift in power is only possible upon an economic crisis, political instability and ideological confusion in the ruling class, Karl Marx once stated. At the inception of bitcoin in 2008, we were very near such an economic and governmental crisis. However, in the current economic boom, the general public is less inclined to risk their prosperity for vague ideologies.

Even so, it is questionable whether blockchain could make any good on the promise of distributing power. History has shown that a void in power is quickly filled by a new establishment. The inherently distributed

nature of the internet could not prevent so and even created a sphere in which Facebook and Google have become the 21st century corporate power houses. When looking at cryptocurrencies, you see that a few large centralized exchanges are already highly influential within this sphere.

Instead of a disruptive force, the blockchain could also be applied to support current business processes, in which the short term value predominantly lays in reducing costs and increasing efficiency for incumbent organizations. It is important that we take the needs of this sector seriously as they play a key role in technological adoption. In the end, you catch more flies with honey than you do with vinegar.

Over a certain period of time, the value of blockchain will shift from driving costs reduction towards entirely new and disruptive business models, creating diverse revenue streams. This ongoing process, nonetheless, is very time consuming. Transformative use cases such as a distributed and secure global digital identity still have a long way to go before being massively adopted. This transformation will not happen overnight.

2.3 Baby steps instead of giant leaps

The promise of making jobs and even whole sectors unnecessary using blockchain technology echoes loudly throughout our community. This view does not resonate well with what is thought outside of this group. As many people fear change, blockchain could pose a serious threat to the societal structure, without knowing which benefits it brings along for them.

Let us look at artificial Intelligence (AI), that is quickly reaching maturity. It powers many of the tools the modern audience adopts on a daily basis. While we could argue that a decade ago the influence of AI was still minimal, it is hard to pick a moment when the widespread adoption truly began.

Granted, the field of AI started in the 1950s and has known its fair share of highs and lows. We perceive distributed ledger technology, including blockchain, as a new installment of the larger field of distributed computing, which originates in the 1970s. This makes blockchain an offspring of the internet, e-mail and peer-to-peer file sharing.

Most products that include a component of machine learning, deep learning or another form or AI, do not put focus on this trait. Instead, AI works in the background, enabling or improving the applications it empowers. The emphasis is on the functionality and how this can benefit potential users. This is in sheer contrast of our field, where "using the blockchain" is voiced as a merit on itself.

The path to mass adoption starts with baby steps, including low impact, well received solutions that clearly show the benefits of the blockchain to organizations and the general public.

3. The path to mass adoption

We envision a progressive strategy for introducing new features, each taking the mark a bit further. The steps to adoption are not determined by technological advantages, but rather aimed to be a natural progression, minimizing resistance. Below we take you through the different steps.

The **difficulty** score assumes all previous steps have been implemented and adopted. The **impact** and **cost saving potential** score are absolute.

3.1 Anchoring: Enabling data verification

When explaining the blockchain to business leaders, the word "immutable" particularly strikes their imagination. Data integrity is a major concern to large organizations.

Of course, this immutability doesn not come from cryptographic ingenuity alone. The data on a single system can always be changed or destroyed, but share this data with thousands in a peer-to-peer network and you always have a valid backup.

Organizations are not keen to put business data and client information on a public blockchain. While a private blockchain might work, storing a hash of the data in a public blockchain, also known as anchoring, could be a better option. Adding a new layer of trust to existing applications is easy to integrate, as it allows anyone to verify the integrity of the data in a reliable way.

Introducing hardened audit trails and "notarized" documents will not change the world, yet this is the first step towards a decentralized ecosystem.

Anchoring
enabling data verification

Cost saving potential - 40
Impact - 30
Difficulty - 10
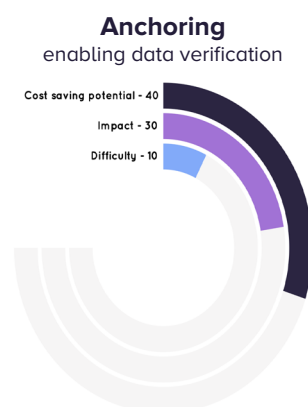
3.2 Cryptographic authentication

Passwords have been the de facto standard for application authentication since the birth of the internet. Ironically, while the internet is a global decentralized network, we are stuck to siloed systems which hold our personal information separately.

But there is hope: Organizations and governments increasingly switch to public key infrastructures (PKIs). While this is mainly for security reasons, it also enables decentralization. Unfortunately issuing and revoking certificates is cumbersome, as it relies on a central authority (CA). If PKIs want to become as established as password authentication is now, it must be easy to integrate and ready to use.

The blockchain shows that the use of a CA is not necessary for using cryptography. On the other hand, we also see blockchain beginners struggling to keep their private keys safe.

Before decentralized and blockchain applications can become mainstream, we must improve the user experience for public key authentication. It needs to be embedded in every internet browser and key management services should be as common and as reliable as password managers.

By creating the tools required and highlighting security benefits, we will kickstart this shift towards cryptographic authentication and open the door for decentralization.

Cryptographic Authentication

Cost saving potential - 50
Impact - 40
Difficulty - 70
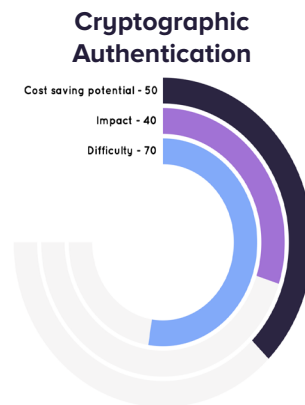
3.3 Chain of trust: on-chain authorization

Whereas public key authentication is a great step forward, it may not be directly useful for organizations. Employees come and go and positions change often, while they would be able to hang onto their private key forever. With PKI certificates you can revoke a certificate, but that does not apply to these self-generated key pairs as there is no Certificate Authority (CA).

This could be made possible in a PKI environment through the chain of trust, on which there is visible a hierarchy of certificates. We can recreate such a concept using the blockchain and even improve upon it, so that an organization is able to publish a trust relationship on the chain. It can do that for an employee as well as for a division or subsidiary.

That division could also publish a trust relationship to, for instance, a team. On its turn, the team will issue a relationship for each individual member. We create a chain of trust as such, where an account can be seen in multiple unrelated chains, where people freely choose who to trust and relationships can be as quickly revoked as they are issued.

This simple but effective use of the blockchain means that anyone can easily and effectively validate if a person is authorized to act on behalf of an organization. This simplifies business processes and mitigates some of the most costly cyber scams, like CEO fraud.

Chain of trust
on-chain authorization

Cost saving potential - 70
Impact - 50
Difficulty - 40
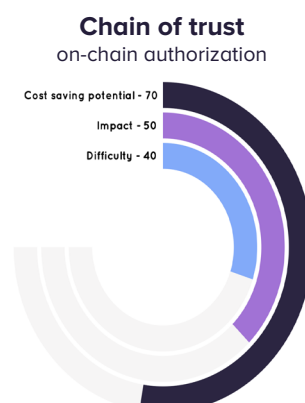
3.4 On-chain certification

With the chain of trust, organizations issue digital certificates to create a relationship. This does not stop at defining employees. Organizations may also issue certificates such as academic credentials, professional certifications, workforce development and quality standards.

Paper certificates are unreliable. For as little as €50, you can purchase a novelty degree certificate online. Pick your university, course and qualification and within 48 hours it is yours, completed with seals and crests. Most employers do not check qualifications, taking CVs and certificates at face value.

With certificates on the blockchain, verification is done independently and can be automated, sifting out the fakers at forehand.

Chain of trust
on-chain certification

Cost saving potential - 60
Impact - 50
Difficulty - 20
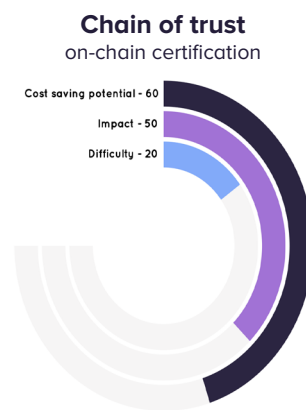
3.5 Self-sovereign identity (SSI)

Certificates on the blockchain are useful, but also very public. Self-sovereign identities allow a similar form of validation, leaving the control firmly in the hand of the individual.

Common methods of identity assurance, the act of verifying a user is the real-world person he or she claims to be, have simply been copied from the offline world. As you can imagine, this does not hold up well in the digital world. Online KYC procedures are a joke. A digital copy of a passport and letter of a utility company is childishly simple to falsify and vulnerable to fraud.

Identity theft is one of the most common form of fraud, costing organization billions of euros per year. Some western countries have created federated identity services, but as with DigiD (the identity management platform which Dutch government agencies use), it is nearly impossible to be allowed to connect to this centralized, government controlled service. Considering the number of different services deployed by countries across the world, this is not a feasible solution for the global economy.

Self-sovereign identities switch the concept around. A person can make any claim, for instance about a name, address, age, employment history, medical insurance, etc. Organizations that provide information, like the insurance agency, or assess the claim offline, may submit the acknowledgment to blockchain. This allows the person to proof the claim is valid.

In contrast to a federated identity, this solution is fully decentralized. An organization can only verify information that the person provided, rather than getting information from a central source. The organization is also free to choose which auditors to trust upon and which not.

By the time we are already to use cryptographic authentication, chains of trust and on-chain certificates, using SSI will feel natural. Without noticing we, as a community, have changed the way the public view their online identity.

Self-sovereign identity
(SSI)

Cost saving potential - 70
Impact - 70
Difficulty - 60
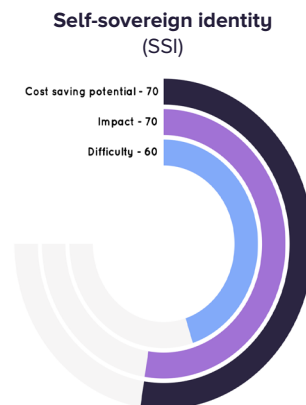
3.6 Proof of acknowledgement

Tokenization has captured the imagination from the blockchain community, from tokenizing real estate and loyalty points to carbon emission rights. On the other hand, both government bodies and established organizations are rather sceptical of the so-called benefits.

One of the major issues is that anyone could create a token out of thin air on Ethereum, Waves or one of the many other blockchain platforms. It only takes a bag full of money and a few spare minutes. The issuer can claim that this token represents any value they come up with.

A certificate of acknowledgement is a notary attachment to a deed. It is acknowledges the authenticity and ownership the object described in the deed. Similar to SSI, submitting such an acknowledgment to the blockchain enables the holder of the deed to proof it is authentic.

In this case the acknowledgment must be connected to the token rather than a key pair. The LegalThings One platform creates strong tie between the token and the deed, by referencing the token in the deed. As approval, the notary or other authoritative party generates the certificate of acknowledgement from the deed and injects it into the token.

To sell the asset, you require both a token and a copy of the deed. Proof of acknowledgement allows the seller to prove the authenticity of the object, using the deed and the token to prove their ownership.

Connecting real-world assets to tokens is an essential step, if we want to move beyond to adopt the blockchain only for cryptocurrency and authentication.


Proof of acknowledgement

Cost saving potential - 60
Impact - 60
Difficulty - 40
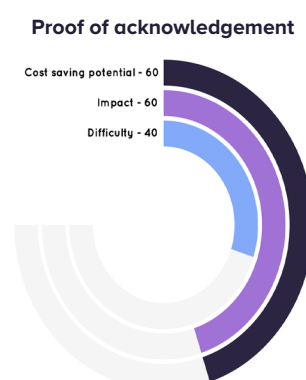
3.7 Non-fungible tokens

As blockchain has been in place since the existence of cryptocurrencies, we are familiar with fungible tokens. From an economic standpoint, fungible tokens are interchangeable and uniform. Non-fungible tokens are the opposite; non-interchangeable and unique. An example: money is fungible, whereas your birth certificate is not.

For several industries, non-fungible tokens can be a solution to their most tangible problem: counterfeited goods. For electronics, fashion and most other goods, the damage is merely economic. However, one in ten drugs sold in developing countries is fake and toxic, causing tens of thousands of deaths a year.

Anything printed on a box or even a blister pack can be easily copied. A non-fungible token has a unique hash that may serve as serial number for such a specific package. Transferring ownership of the product always goes hand in hand with transferring the token. This not only allows the consumer to verify the authenticity of the product, but also closely observes the whole supply chain of the product.

Two-thirds of pharmaceutical manufacturing is outsourced. To allow third parties to issue tokens, but still ensure a high quality and authentic product, the organization can employ proof of acknowledgement together with quality control on their product.

Non-fungible tokens

Cost saving potential - 90
Impact - 90
Difficulty - 80
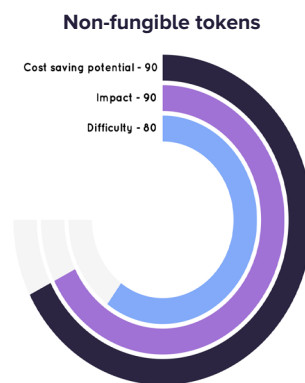
3.8 Stable currencies

Many organizations want to experiment with automating cash flows and financial products. Smart contracts are a perfect means to allocate and automatically distribute funds without the involvement of third parties. Healthcare budgets, salaries and debt obligations can all be managed through smart contracts. But is it a good idea to do this with billions worth of Ethers?

As cryptocurrencies are too volatile, organizations rather prefer to take a traditional currency. It is unlikely they would be able to pay their expenses in cryptocurrency. Interesting advancements, like Tether, have come about in the field of stable coins, but these currencies either lack scale or trust.

While Bitcoin has started as reaction to failing banks and a dysfunctioning financial system, the reality is that we always need a stable currency being backed by (central) banks in order to get to the next stage.

Although many banks are still reluctant to blend into the blockchain scene, some have already started doing so. Noteworthy, powerful Dutch parties like ING and ABN AMRO within the blockchain community are trying to infiltrate the financial market by buying competitors or setting up so-called FinTech startups.

Accepting euros, dollars and yens on the blockchain will likely be a challenge. However, demonstrating that true value of the blockchain could be created via identity assurance, tokenized assets and supply chains, will swing the public sentiment around in favor of the blockchain technology.

Stable currencies

Cost saving potential - 80
Impact - 90
Difficulty - 100
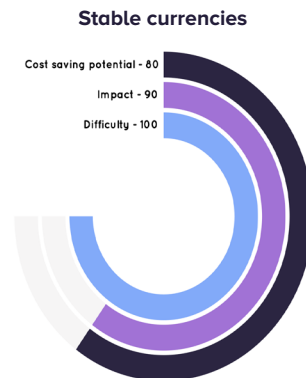
3.9 Smart contracts

Smart contracts are probably considered the holy grail of the blockchain technology. These contracts define the terms of the agreement encoded on the chain. Without the approval of a third party, the contract is automatically executed upon predefined terms have been met.

Smart contracts offer a lot of benefits in regards to the flows of money, such as its ability of self-execution.Almost every initial coin offering (ICO) runs on (Ethereum based) smart contracts. Yet, the real-world applications of these smart contracts for organizations are limited.

The self-enforcing nature of a smart contract is both the most important asset and largest limitation at the same time. Unlike legally enforceable contracts, parties are free to abandon a smart contract. In order to make a contract useful, it either needs to control the flow of money or holds something of value. Smart contracts only holding tokens have limited use for organizations.

Once a stable or fiat currency is put in place on the blockchain, we could expect an explosive growth in smart contracts. Simultaneously, it will mainly be a game of cutting out the middlemen, as in-game payments could automatically be distributed under beneficiaries in real-time circumstances

At that point, blockchain would be fully integrated into our lives. As with any new technology, this, however, is only the beginning. We expect that blockchain will bring about many more groundbreaking developments.

Smart contracts

Cost saving potential - 80
Impact - 90
Difficulty - 60
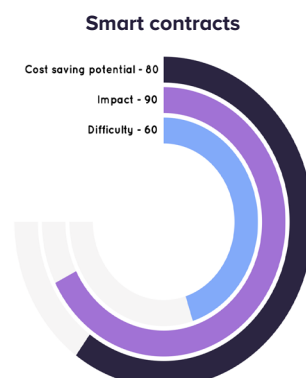
4. Conclusion

This visionary paper is intended to offer the community a different perspective on the blockchain technology. Having held talks with numerous enterprises and governments in recent years, we have experienced that leaving the echo chamber is crucial for the organizational adoption of blockchain and the creation of strategic business value. By offering a helping hand to incumbent organizations, the fundament of a fruitful ecosystem can be laid down in order to make blockchain work for both the community and innovative companies.

However, rushed and forced implementation of blockchain into organizations should be avoided, since it will be doing the feasibility only more harm than good. Recent failed proof of half-baked concepts aimed to transform industries have mostly led to desillusion for organizations. If we want to make blockchain a success - regardless of who we are - we should manage expectations and create a long-term realistic plan, without scaring decision makers that blockchain immediately disrupts their organization and jeopardizes thousands of jobs.

By pursuing baby steps in a long road to mass adoption, we can change the way organizations view the current state of blockchain, making them understand and embrace the numerous advantages the technology has to offer. As mentioned earlier in this paper, we ought to see that the adoption of blockchain technology is similar to that of the internet in 1995, when the technology behind it raised more questions than answers.

Trusting upon blockchain to handle day-to-day business processes is a necessary first step towards mass adoption and the creation of strategic business value. Contrary to previous messages, organizations have to experience that blockchain could play a key supportive role, before even becoming the next big disruptor. In many cases, a fusion among existing digital infrastructures, middleware solutions and blockchains has already significantly lowered the costs of certain workflows. As noted, reducing expenses is not the only benefit blockchain has to offer.

In the light of future short-term developments, we will be updating this paper accordingly.