Real-World Blockchain – Four examples of the future of DLT

Bitcoin Suisse Themes - Industry

By Tom Lyons and Dr. Raffael Huber

January 2021

Contents

Key Takeaways

- As blockchain technology matures, we get a clearer picture of the role that blockchain protocols and the cryptocurrencies that fuel them will play in shaping our increasingly digital economies and societies. This paper illustrates four use cases where advances that exploit blockchain's strengths are showing the way the industry will likely evolve.

- Advances in IoT and AI, which are helping machines become increasingly autonomous, are being matched by significant advances building interfaces between the real world and the blockchain. This will allow blockchain to act as the payment, contracting, identity and data verification platform for large-scale, machine-only economies.

- A new approach to blockchain-based shared business processes, known as "baselining", may have solved the key challenge for enterprise blockchain – how to synchronise data between stakeholders in a value chain without revealing the actual data or investing in expensive new systems. This will open the door to wide-scale adoption of public blockchain infrastructure by the corporate world.

- New, modular approaches to decentralised autonomous organisations (DAOs) are making this technology enterprise-friendly as well, allowing companies to "parametrise" decentralised governance and automation of business processes. A future ecosystem of DAO modules will dramatically reduce the time and expense to get a small company off the ground, and make it easier for larger companies to introduce decentralised setups where they make sense. It could also lead to a healthy competition for ever-better organisational templates.

Introduction – Blockchain enters its adolescence

On October 31, 2020, blockchain turned 12 years old[1]. While still young as a technology, at this age we can speak of it entering into adolescence. And as is often the case with adolescents, it is becoming clearer what blockchain might look like when it grows up.

Few technologies have generated as much exuberance – both rational and irrational – as blockchain. Understandably so. A technology expressly designed to provide trust in data among large groups of strangers, it can enable new ways for people to exchange value and collaborate without the need for third-party intermediaries. That seems tailor-made for a world in which trust is an increasingly rare good, and in which people are becoming wary of the power of large intermediaries like the giant technology platforms[2] that currently act as the gatekeepers and primary profiteers of the digital world.

From first-world financial services to the billions of unbanked, from global supply chains to medical care, from software development to luxury goods and digital art, from corporate and country governance to local activism: since its early days there has hardly been any sector of the economy or society that blockchain proponents have not claimed could be transformed for the better through the magic of decentralisation, tokenisation and group consensus.

We know better now. The truth is blockchain cannot fix everything. Looked at objectively as a technology, it still has many flaws, from performance to security to usability. These stand in the way of its wider adoption, particularly in business applications where legacy technology is often superior and is likely to remain so for a long time. Looked at philosophically, we have learned that decentralisation and transparency have their limits: intermediaries, it turns out, are often useful, and the crowd is not always wise.

That said, in the right setting, blockchain can play a pivotal role in shaping our increasingly

1 Counting from the publication of the Bitcoin White Paper on that date.
2 See Blockchain, not Bitcoin?, Dr Raffael Huber, Bitcoin Suisse Decrypt, 2 March, 2020.

technology driven economies and societies. This will be both a function of the technology itself as well as of the cryptocurrencies that were blockchain's first use case, and remain its most important.

On the one hand written off as a fad or demonised as a tool for criminals, on the other almost worshipped as digital gold and the only reliable store of value in a rapidly disintegrating global monetary system, people often forget the central role that cryptocurrencies play in blockchain protocols. By providing incentives for running the network, they are an essential element of decentralised blockchain platforms. Whatever one may think of their utility in the real world, it is clear that bitcoin, ether and their close relatives are here to stay, and will be key in helping blockchain reach its potential.

This paper aims to showcase this potential by examining four use cases in which blockchain as a technology and an approach can and will have a major impact in the near to mid-term future in ways that exploit what is special about blockchains. They are by no means the only examples that could have been chosen. But they can serve as good indicators of where the strengths of blockchain technology lie, and therefore the direction in which the blockchain industry is likely to go.

“Look mom, no hands” – Blockchain for autonomous, machine-to-machine payments

One very promising use case for blockchain is in supporting machine-to-machine (M2M) payments, and with it the creation of large-scale, autonomous, machine-based ecosystems.

Such machine ecosystems are already evolving around us. Thanks to advances in technology including smart devices and the Internet of Things (IoT), artificial intelligence and machine learning, big data, ubiquitous digitisation and global communications, machines are becoming increasingly sophisticated and independent, able to assess their environments, make decisions, and carry out actions on their own. To create a human-free, M2M economy, however, machines will also need a way to enter into agreements and carry out economic transactions with each other.

Blockchain meets this need quite nicely. The technology was invented as a means of exchanging natively digital value in a trustless way on the open Internet, exactly the kind of environment a machine economy would be operating in. Whether via a cryptocurrency, or a tokenised version of a fiat currency, blockchain can easily handle the payment part of machine-to-machine interactions, including micropayments. With smart contracts, blockchain can be used to program agreements between machines and automate the processes around carrying them out.

Blockchains can also be used to provide identity services as well as assist in the secure transfer of verifiable data, ensuring machines can trust each other. They can be deployed as open protocols on public networks allowing machines of different makes and models to join and leave the network at will. That makes such networks very flexible, able to grow organically and adapt to changing technologies and environments.

There are, however, two crucial prerequisites to making blockchain-based machine-to-machine payments workable. First, while there is nothing to stop machines from paying each other in cryptocurrency, widespread adoption will likely only occur once tokenised versions of fiat currencies are available. It is telling that last year's Commerzbank pilot with Daimler, in which a blockchain-based platform allowed electric trucks to pay for power at a charging station without any human intervention, used a tokenised version of the euro that Commerzbank provided as "cash on ledger" to the trucks.[3]

The second prerequisite is a means to create a secure, unbreakable and unique link between machines and the blockchain. This is challenging for the simple reason that – unlike with digital information, which can be secured on a blockchain by means of a cryptographic hash – it is not possible to 'hash' a physical object.

One company working on this challenge is the Vienna-based Riddle&Code.[4] Among other things, the company has developed blockchain-enabled crypto chips, similar to those used in credit cards, that can be permanently embedded in a machine or any physical object. This creates a blockchain-compatible, unique digital identity for the machine, meaning anyone or anything communicating with that machine can be sure it is indeed what it purports to be.

These chips can do more than just provide identity, however. They can contain crypto wallets which can hold funds as well as smart contracts, helping machines to not just exchange data, but also enter into agreements and make direct payments to each other. The chip can also be used to hold verifiable credentials of various types, for example quality certificates or proof of provenance, that can be helpful in providing confidence in the transactions.

These capabilities are available now. Looking to the future, Riddle&Code is building virtual versions of its secure hardware that will allow machines to store data and execute blockchain-based transactions safely in the cloud. This would allow for much larger, more diverse groups of machines to interact and transact together in more complex ways than is possible with direct M2M interactions. This in turn could serve as the basis for large-scale, machine-based biotopes based on a kind of circular data economy – all orchestrated by blockchain.

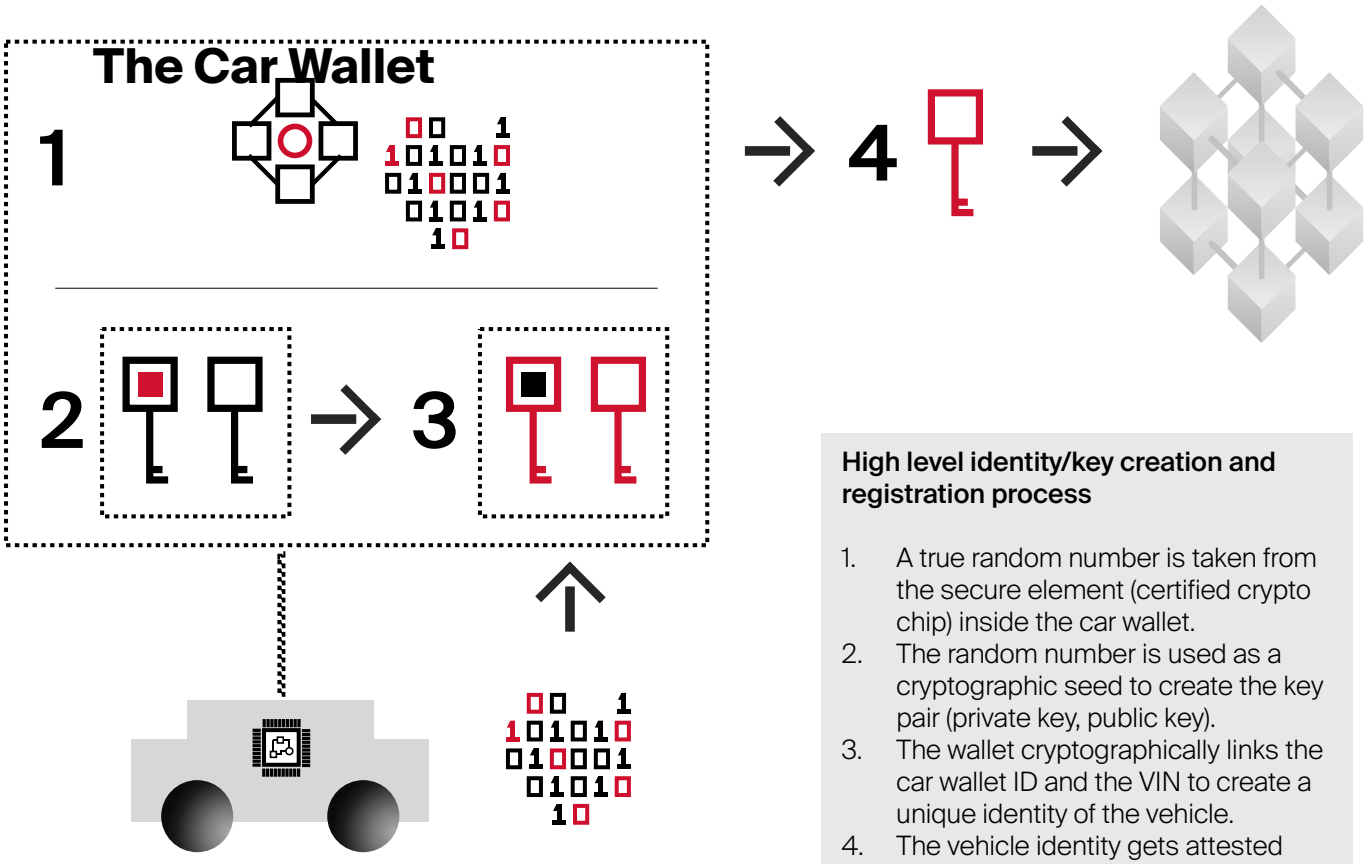
To get an idea of how such a biotope could work, consider a manufacturing robot that produces a steel rod with certain chemical properties suitable for building bridges. Along with the rod the machine creates a verifiable certificate of those properties as well as manufacturing data on the particular rod. Buyer robots could check the provenance of the rod, pay for it, and even if necessary provide feedback. For example, they might order new rods with slightly different properties. The manufacturing robot would receive this order, produce a new set of rods to spec, and deliver them along with verifiable quality certificates, all with no human involved. Blockchain would be part of each phase of this value chain, providing the digital identity, the smart contract automation, verifiable credentials and certificates, and of course tokenized payments allowing the transactions to be settled immediately.

"If you want to have a machine economy, you have to have a data economy too. And that can only happen if you have the right security and trust in data, which in turn can only be achieved by blockchain and within a token economy."

- Thomas Fuerstner, Founder & CTO, Riddle&Code

3 No Humans Required: Commerzbank Develops Blockchain Payments for Automated Trucks, Coindesk, 8 August 2019

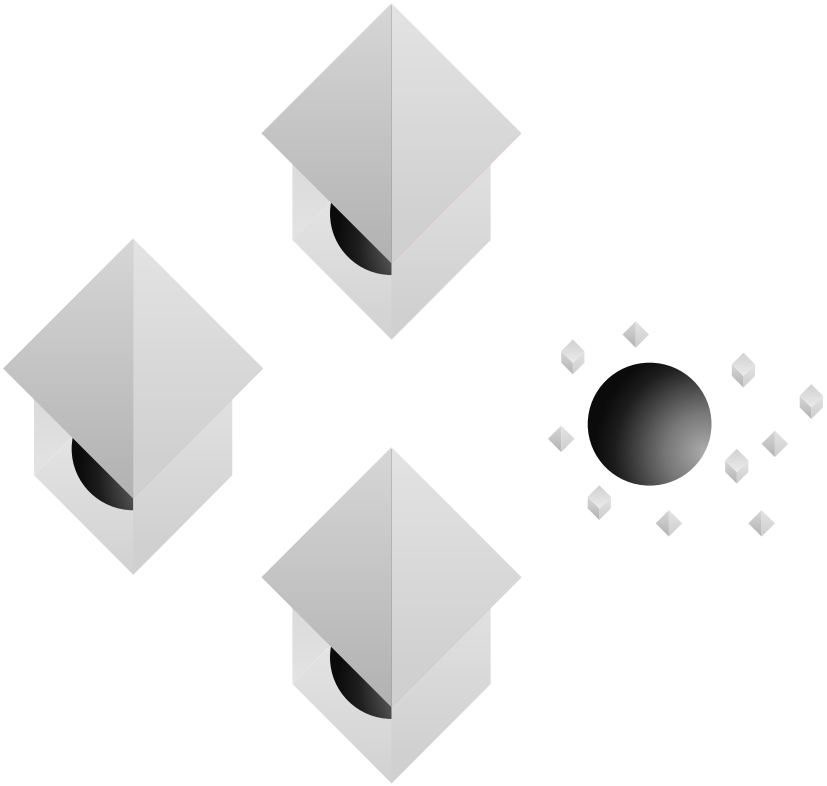
4 This section is heavily indebted to an interview with Thomas Fuerstner, Founder & CTO of Riddle&Code. See also the company's excellent report on The Automotive Sector and Blockchain.



High level identity/key creation and registration process

1. A true random number is taken from the secure element (certified crypto chip) inside the car wallet.
2. The random number is used as a cryptographic seed to create the key pair (private key, public key).
3. The wallet cryptographically links the car wallet ID and the VIN to create a unique identity of the vehicle.
4. The vehicle identity gets attested on the ledger infrastructure and becomes indisputable and tamper-proof.

Source: Riddle&Code



Blow your house down – Blockchain for parametric insurance

The insurance industry has famously been resistant to digitisation. Today it still relies on outdated, often manual and expensive processes, ultimately resulting in higher-than-necessary prices and reduced choice for consumers. It comes as no surprise that large insurance incumbents find themselves seriously challenged by innovative newcomers, or that blockchain is playing a part in this revolution.

Blockchain can be deployed to disrupt insurance in many different areas. A promising one – which also highlights the unique qualities that blockchain technology can bring to this sector – is parametric insurance.

In parametric insurance, payouts are not made based on loss or damage, but rather on pre-agreed external triggers. If there is a drought, a farmer receives a pre-arranged amount. If a flight is cancelled, a passenger gets reimbursed for the ticket, no questions asked. In both cases there is no need to prove the damage. Reference need only be made to some reliable data source such as weather or flight records.

While parametric insurance has been around for a long time, blockchain is breathing new life into it. And for good reason. To work, parametric insurance policies need trusted data. If a payout depends on the weather at a certain place and time, the insurer needs more than just a reliable source of information. It needs to be sure that the data it receives actually comes from that source, and has not been tampered with. Blockchains can help to provide such assurances. The agreements underlying parametric insurance policies also tend to be fairly straightforward: if X happens pay Y the amount Z. This makes them suitable for automation via smart contracts. With automation, of course, comes lower costs, lower premiums, and happier customers – at least in theory.

This potential has long been recognised and is currently being exploited. Back in 2016 the blockchain startup Etherisc[5] made waves when it presented its plans for a blockchain-

5 www.etherisc.com

based, parametric insurance dApp covering risk to passengers from flight delays. The dApp was tied to official airline flight data that served as the "oracle" (as trusted data sources are referred to in the blockchain world). Since then, it has developed a whole platform for building blockchain-based, decentralised insurance products, including a recently announced parametric crop insurance for farmers in Kenya using weather data provided by Chainlink, a company which specialises in oracles for blockchain platforms.[6]

As more and more real-time information about the world becomes available through developments in IoT and big data, it will become easier to create more sophisticated types of parametric insurance. According to one industry source[7], we can for instance imagine parametric insurance against hacking that pays out directly upon proof of a data breach. With tools to measure sentiment and emotion on social media, we could imagine parametric insurance against reputational damage from mobbing and trolling. We can imagine climate change insurance tied to rises in sea level or temperatures. The list goes on.

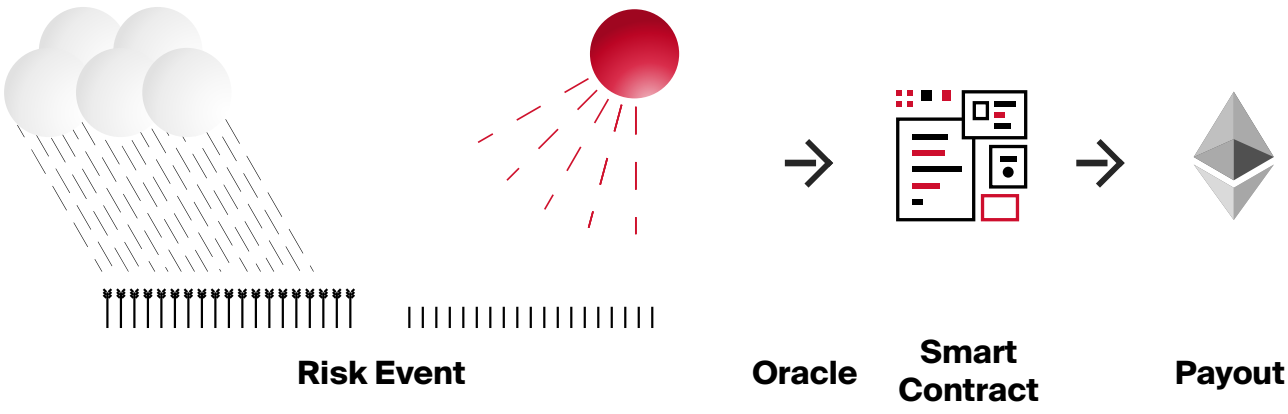
Looking farther ahead, we can imagine a world in which these kinds of parametric insurance policies could be purchased on-the-fly based based on where we are or what we are doing at any given time, often without our intervention. Blockchain-based dApps could be configured according to our preferences to automatically purchase flight insurance when we book air travel, or payroll insurance when we contract for a freelance job, or even reputational risk insurance when we post to Facebook or Instagram.

Blockchain could bring radical automation and decentralisation to the insurance industry as well, in the form of decentralised autonomous insurance companies (or Insurance DAOs - more on DAOs below). In this scenario large groups of people would contribute to a pool and self-insure themselves using the same combination of oracles, blockchain and smart contracts that is powering the parametric insurance policies mentioned above. By eliminating the company in the middle and automating processes, such insurance cooperatives could have much lower margins than traditional insurance companies. If done correctly, this could mean lower premiums and better service.

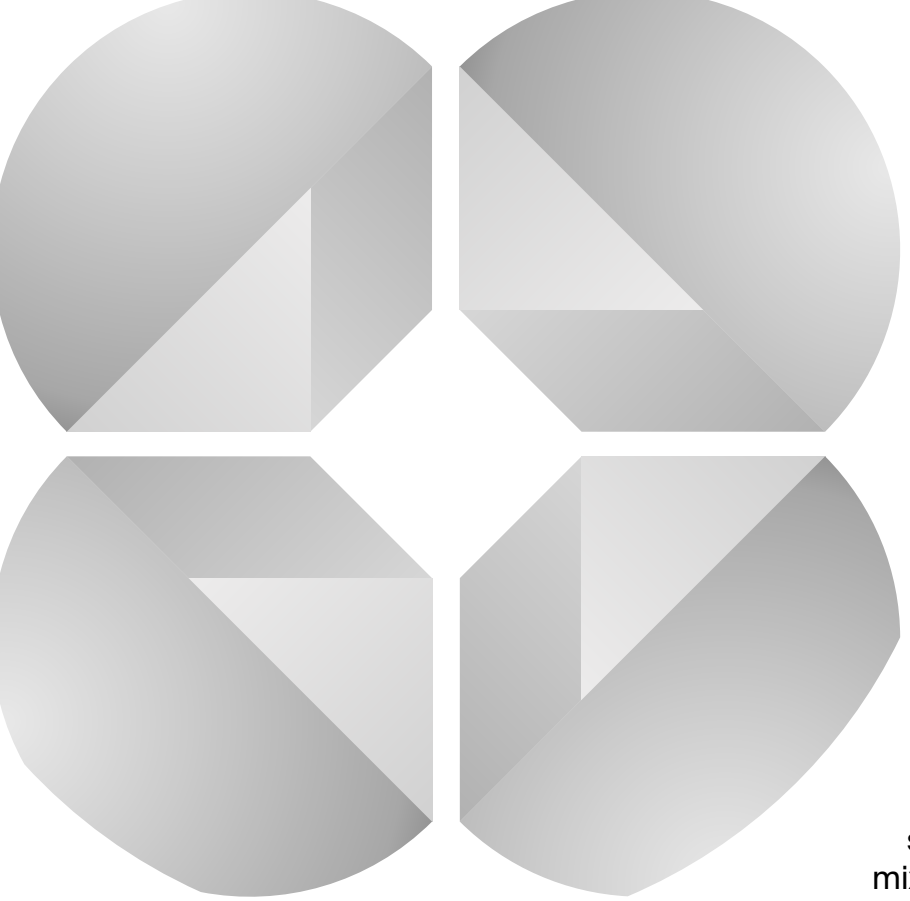
Over time such decentralised insurance products could grow into large, decentralised general insurance companies. If so, in the future we may all be both policy holders and policy issuers at the same time. And all of it orchestrated by and on the blockchain.

6 Etherisc teams up with Chainlink to deliver crop insurance in Kenya, Etherisc blog, 14 November 2020.
7 Trends in blockchain-based parametric insurance, International Travel and Health Insurance Journal, 3 June 2019.

How Parametric Insurance Works



Source: What is parametric insurance? And why on a blockchain?, Etherisc, 10 November, 2017



We've got a secret – Shared, privacy-preserving business logic

Trust in multi-party business processes almost always boils down to the ability of companies to agree on information along a value chain of some sort.

If, for example, Company A offers Company B a 20% discount when it purchases 100 new Widget Xs in a calendar month, to be delivered by Shipping Company Q and quality checked by Provider R, all parties need to keep the relevant information in sync or the arrangement will not work.

This is not always easy to do. Companies spend hundreds of millions of dollars a year on sophisticated IT systems just to share such flows of information regarding orders, agreements, deliveries and payments – a fair amount of which goes towards reconciling data and clearing up the inevitable errors that result from the lack of interoperability between the myriad different systems and processes currently in use.

In the early days of blockchain, many thought that distributed ledgers could help solve the problem. By agreeing on and then recording business data on a shared ledger, the thinking went, companies involved in a joint business process could be confident they were all on the same page. Add smart contracts to the mix, and agreements as well as shared processes could be automated in a way all parties could trust. That made things look even better.

But there was a huge catch. The whole point of a blockchain is to create a permanent, immutable, public record of transactions. Data on a public blockchain is available for all to see, forever. Even if it is stored on chain in encrypted form, or stored off-chain and referred to by a unique identifier – generally a cryptographic hash – data written to a blockchain leaves traces that can be used to glean information about the contents, often in surprising detail[8]. The same goes for smart contracts saved to a blockchain, which can be examined by all in ways that can also reveal sensitive information.

Enterprises cannot afford this kind of uncontrolled transparency. Strict data protection regulations compel them to keep information safe. So does good business sense: Company A may not want Company C or anyone else to know about its discount offer to Company B.

To reap the benefits of public blockchains in an enterprise setting, what is needed is a way for businesses to synchronise data between

8 This is not just a problem with blockchains. These days any data sent via the Internet leaves traces of some kind, for example in the metadata that accompanies messages and is used among other things for identifying and routing them. This messaging "exhaust" can reveal a great deal about the contents of the message without having to encrypt the actual data.

their systems without actually exposing that data – a seeming paradox.

A new approach, known as "baselining", may offer an answer. Currently being developed as an open source project by a large consortium under the name of the Baseline Protocol[9], it was born of the realisation that the blockchain should not be used as a shared database to store common data. Rather, it can be a powerful tool for enforcing data consistency and workflow synchronization by recording verifiable proofs that all parties are in possesion of the same information. This is a subtle, but very powerful, difference.

In slightly simplified terms, it works like this. If two companies want to share a document, for example a purchase order with delivery and payment terms, they first share the document directly between each other via some form of secure messaging. This document is then baselined, meaning that a special type of digital signature of the document is created, one that uses sophisticated cryptographic techniques to ensure there is no inadvertent leakage of data or metadata[10]. Now each party knows what this signature looks like, information they keep to themselves. The signature of the baselined record is then written to the blockchain. The result is publicly accessible, immutable proof that all parties had the same understanding of a specific piece of information at a certain moment in time – but saved in such a way that only the parties involved know what this seemingly random signature represents. To all other observers, it is simply so much digital noise.

This approach has many advantages. For one, all parties can stay in sync without anyone revealing any actual data. Because all parties can continue to use their own internal systems of record, there is no need to invest in expensive, proprietary third-party platforms or trust an expensive intermediary. Instead the Ethereum Mainnet serves as a common infrastructure – a global, publically available, censorship-resistant, decentralised platform that is open to all, relatively inexpensive to use, and available 24/7 around the globe.

While still in its very early days, baselining may prove an extremely significant development in enterprise blockchain. Above all, it appears to have squared the circle between transparency and data security that has bedevilled enterprise blockchain solutions until now. It is also a good example of exploiting blockchain's strengths. In Baseline, blockchain is a small part of the equation, but an essential one - filling a need no other technology or method can.

For those interested in the development of enterprise blockchain applications, the Baseline Protocol is therefore worth keeping an eye on. It could be the missing ingredient to widespread adoption of this technology in the enterprise world.

"In the Baseline world, you don't have a single version of the truth but rather a common frame of reference. It is not about 'I have a secret that I can prove to you I have', but rather that 'we all share the same secret.' "

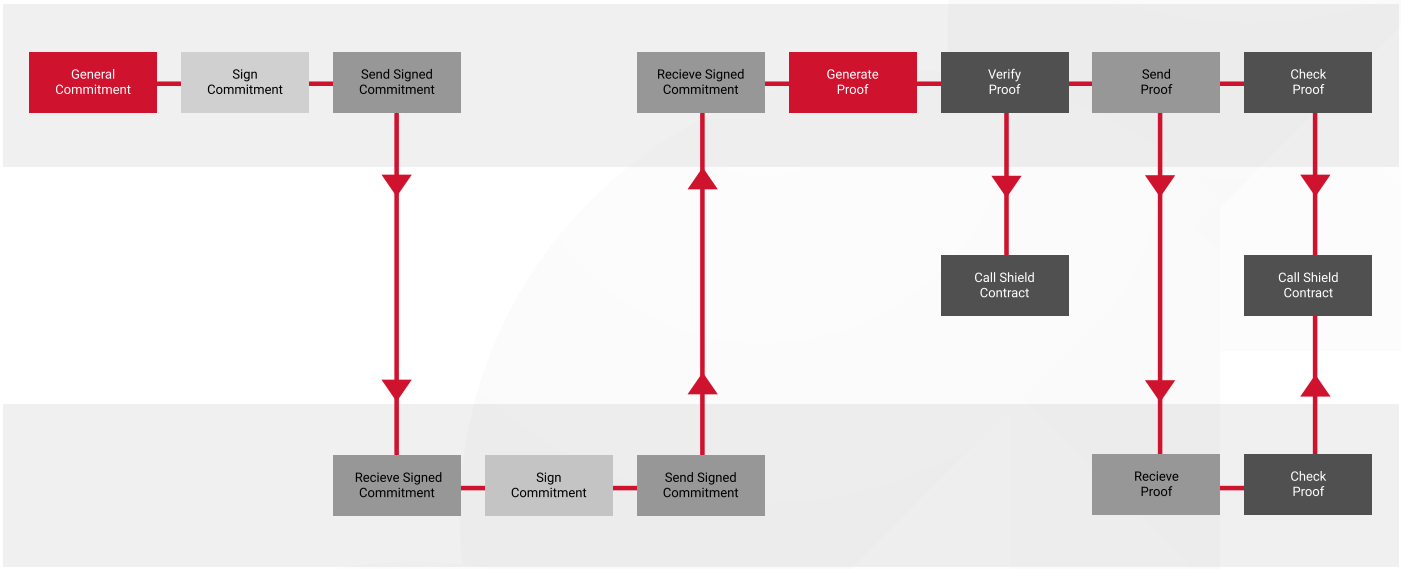
- John Wolpert,
Group Executive, ConsenSys
Chair of the Baseline Technical Steering Committee

9 See baseline-protocol.org.

10 This is technically a normal cryptographic signature with an extra type of obfuscation method, known as a zero-knowledge proof, added on top to ensure there is no inadvertent data exhaust.

> **“Baseline will make the choice by enterprises to use public blockchains simple: all the privacy offered by a closed network with the security, low costs, and immense ecosystem of a globally scaled, public utility with thousands of nodes and nearly a million developers.”**
>
> **- Paul Brody, Global Blockchain Leader, EY**

Baseline Protocol: The Business Workflow



Source: baseline-protocol.org.

Boss code – Enterprise DAOs

We have already seen that blockchain can be used to help autonomate interactions and transactions between machines. Since the early days of blockchain, people have wondered if it could be used to automate certain types of interactions between groups of humans, for example those take place within a company. This gave rise to the notion of a Decentralised Autonomous Organisation or DAO – a company or other type of organisation that is run to a large extent, if not completely, by code.

DAOs offer many advantages. The process of coding the governance and procedures of an organisation requires describing these things in detail. This can increase transparency, as procedures in code are likely to be more precisely documented, and less ambiguous, than those described in natural language. Similarly, code can make decision-making much more transparent and democratic, for example by specifying voting procedures. It can also heighten confidence in company processes, as it is generally easier to predict what a program will do with the instructions given to it than what a human will. Coded policies and processes are also easier to enforce and harder to evade than those administered by humans. This can help mitigate errors and fraud.

Having an organisation in code also allows processes to be automated. This can add efficiencies and reduce costs, freeing up staff to focus on the more difficult problems. Last but not least, code behind a DAO is also replicable. If a certain type of DAO works well, others can copy it. Or modify the code to make it even better.

But there are problems too. An organisation expressed in code can be rigid, unable to adapt to new conditions as quickly as humans can. The code can also become quite complex, increasing the risk of bugs and making it harder for people to understand what is really going on. There is also a fair amount of legal uncertainty around decentralised organisations at the moment, especially those that have no clear owner or fixed abode. For these reasons, while DAOs today are gaining popularity in certain settings – for example crowdfunding via cryptocurrencies – they have yet to gain any traction in the business world. Considering their potential, that is a shame.

One way to make DAO technology more palatable to enterprises, and more accessible to startups and SMEs, would be to make it more modular, allowing organisations to deploy DAOs selectively and "parametrise" levels of decentralisation and automation. This is the thinking behind LAOLand, a project from the blockchain-based legal technology company OpenLaw that provides a good glimpse into what may be the future of DAOs generally. [11]

11 See https://github.com/openlawteam/laoland. LAO stands for Legal Autonomous Organisation.

In LAOLand, there is no single, overarching DAO, but rather a flexible hub-and-spoke architecture composed of DAO modules. The hub is known as the Core module. It acts as the master agreement upon which the DAO is built, and serves to keep track of the members of the organisation, its bank accounts, proposals that have been submitted, decisions that have been taken, and other information that captures the state of the organisation over time.

The hub is surrounded by spoke modules known as Adapters. These are written for specific purposes. An organisation might have a Financing Adapter that allows individuals to request funding for specific projects. There could also be Voting Adapters, HR Adapters, Accounting Adapters – anything representing some policy or procedure important to the organisation.

There are several advantages to this approach. Changes in the requirements or procedures for a specific process can be made simply by updating the Adapter. There is no need to touch the code of the core module or any other Adapter. This saves time and effort and is also safer, as it mitigates the potential for introducing bugs. Like apps, Adapters can also be swapped out if better ones come along. This makes upgrades easier. It could also pave the way for an "app store" of DAO components.

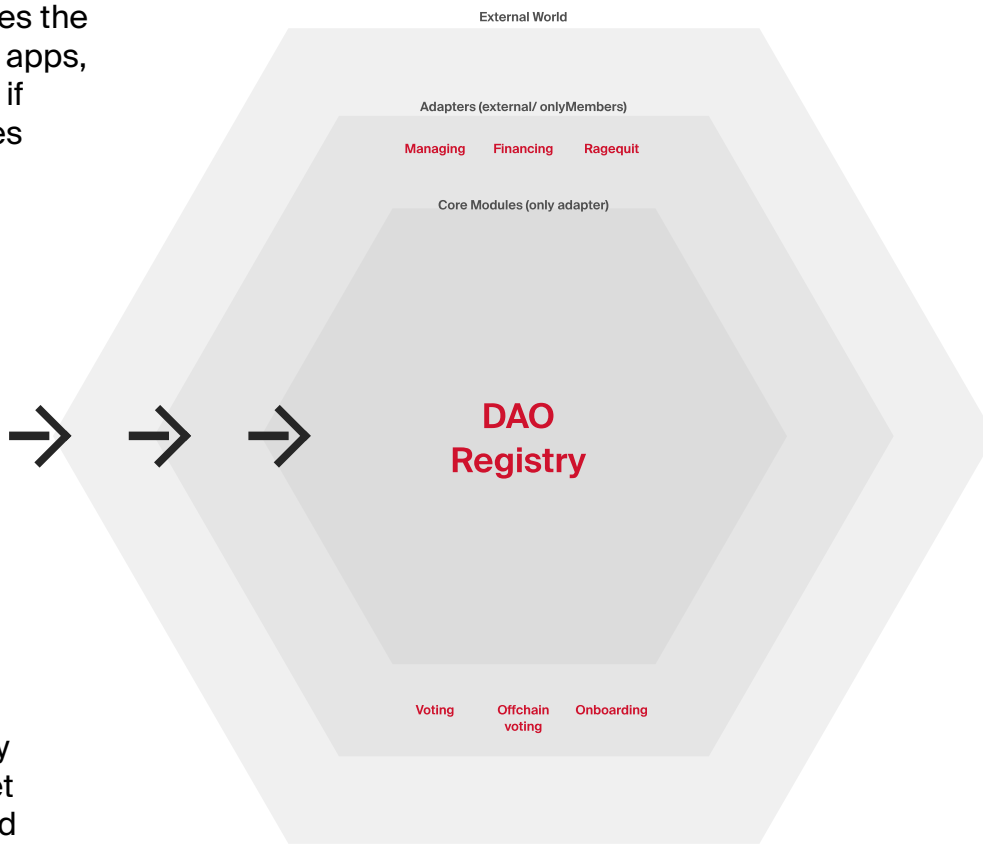
An ecosystem of off-the-shelf DAO modules is a tantalising prospect. Just as startups use cloud services like AWS for out-of-the-box IT infrastructure and Google's GSuite for out-of-the-box office infrastructure, a LAOLand-type setup would provide out-of-the-box, customisable organisational infrastructure. This could drastically reduce the time and expense to get a small company off the ground and would make it easier for larger companies to introduce decentralised, autonomous setups in areas of their business where

"In future, blockchain-based DAOs could make it easier for organisations to swap out their governance structures. This could lead to a healthy natural selection, where only the best governance and process models survive."

- David Roon, Co-Founder of OpenLaw

such things could make sense. It could also foster competition for templates, leading to an evolution of ever-better organisational structures over time.

LAOLand: Building A Modular DAO



Conclusion

As blockchain enters its second decade of life, much of the initial hype around it has settled. It has also gained exposure far beyond the crypto community. Today it is not uncommon to find developers, academics, policy makers, executives, product managers and others in a wide variety of sectors who have heard about blockchain and started down the path of learning what it is about.

All of this activity is making it easier to understand what blockchain can – and cannot – do. This is healthy, and necessary. While blockchain will not solve all the world's problems, as some of its more zealous adherents have claimed, it is likely to live up to its billing as one of today's important emerging technologies. As we have hopefully shown by the examples in this paper, where there is a need for digital trust, there will be a need for blockchain – a need that likely cannot be filled by any other technology. So while blockchain still has a fair amount of growing up to do, its career prospects in adulthood look very good.

Tom Lyons

Tom Lyons is an independent communications consultant based in Zurich. Previously an Executive Director at ConsenSys Switzerland, he currently advises the European Commission on its blockchain-related communications.

Twitter

LinkedIn

Dr. Raffael Huber

Raffael Huber joined Bitcoin Suisse AG in June 2019. He is currently a member of the Institutional Services and Products department and is conducting research on a broad variety of topics ranging from blockchain data analytics to market opportunities.

Before Raffael started at Bitcoin Suisse AG, he completed his doctoral studies in chemistry at ETH Zurich. Fascinated by blockchain technology and cryptocurrencies from a technical as well as an economic and game-theoretical point of view since late 2016, he is committed to transferring his extensive knowledge of the tools of research in traditional science to the crypto space.