WORKING PAPER

MATTEREUM

SMART CONTRACTS. REAL PROPERTY.

Mattereum creates smart contracts
with the legal force of natural language contracts.

Mattereum is an Internet of Agreements project to manage legal rights over physical property, intellectual property, and eventually even real estate, on the blockchain.

We will have met our challenge when these contracts allow you to rent your next car, buy your next house, or sell your next startup.

HOW DOES MATTEREUM WORK?

When you update the state of a Mattereum smart contract, the real-world legal system can see, recognize, and use that change. This is achieved by using natural language contracts which specifically delegate legal authority to two external systems: the smart contract on the blockchain, and an arbitration-based dispute for handling any differences that might arise between the parties. Arbitration decisions are given full legal weight under the natural language contracts, thereby folding smart contract edge cases into established off-chain legally binding dispute resolution. This mechanism is known as a Ricardian contract, and was invented by Ian Grigg, one of the authors of this paper.

Mattereum will produce a set of affordable natural language contracts and corresponding smart contracts to facilitate common legal tasks like buying, auctioning and renting physical property, licensing and assigning intellectual property, and contracting for professional services.

TABLE OF CONTENTS

PREFACE: LAW IN A TIME OF ACCELERATING CHANGE

> *It is a profoundly erroneous truism, repeated by all copy-books and by eminent people when they are making speeches, that we should cultivate the habit of thinking of what we are doing. The precise opposite is the case. Civilization advances by extending the number of important operations which we can perform without thinking about them.*
>
> — Alfred North Whitehead

Law is the product of labour: people have worked at creating it, over centuries. Law, like code, grows into complex assemblages over time that no one human can fully understand. Even if some notional master fully grasped the Linux source code, it is likely that the mysteries of microprocessor design, or the underlying power grid, would elude them. At some point, we must all say 'somebody else's problem' and rely on specialization in society to handle the stuff that our merely human brains cannot contain.

However, the future is a foreign country, and it is also our largest trading partner. New structures which are hard to fit into existing social frameworks pour into reality all the time. For example, SnapChat sets up a new kind of messaging (messages disappear after 10 seconds), new social norms spring up around what can be said in permanent messaging, and what is reserved for temporary messaging. More technical people understand that these temporary messages are, in fact, stored forever. Different groups form different social norms around the new technology.

Eventually it reaches a head. Somebody violates somebody else's trust enough for a lawsuit, or somebody does something which is currently thought to be illegal. The whole matter winds up in court, and the courts must decide – for a technology they have never seen before, used by a youth culture they have only read about in newspapers – what is right or wrong.

Over time, as lawmakers, judges, lawyers and jurors become more familiar with the situation, court rulings and legal norms converge on something that the surrounding culture can live with. The system has adapted. But there is a lag, and the gap between our technical capabilities and the ability of the legal system to integrate new technologies is widening: courts sometimes seem more and more behind the curve.

The intensity of this future stress on our ability to make good law is only increasing. Society changed in radical ways as birth control technology became available, and the legal rulings around birth control continue to be tested 50 years later. Gender reassignment technology is going through a similar process as social, technical and legal systems struggle to represent human will and human identity in holistically satisfying ways.

In the last ten years, public key cryptography has gone from a mechanism for securing the privacy and authenticity of messages to a way to print money. As a result of the creation of Bitcoin, legislators and courts are asked to comprehend and rule on technical systems which have huge economic implications. But these systems are so complicated that only a few hundred people in the world could be said to fully understand them.

As a result of operating at the horizon of their understanding, people make mistakes. Laws either don't get passed for a long time (the ambiguity about the tax status of bitcoins has lingered for years in some countries) or bad laws get enshrined. The result is an uneven landscape of legislation: good law, which will last, mixed with bad law which – although it will certainly be revised in future – is still the law, for now.

Jurisdictions like Zug in Switzerland spin up approaches which may become global legal standards, or ultimately be seen as bold experiments that were later brought into line with a more conservative set of legal norms.

BEYOND PAYMENTS, TO AGREEMENTS

In the beginning of the internet, there was no trade. Commerce was prohibited by a mixture of formal rules, informal cultural values, and the lack of any means of secure payment. The first .com domains were registered in 1985, but these simply indicated that the domains belonged to commercial entities, not that they were places one would go to *buy stuff*. It took until 1995 for the National Science Foundation to relax the rules against commercial activity online, inaugurating the age of e-commerce.

The entire multi-trillion dollar e-commerce economy runs on a handful of core technologies: the credit card and HTTPS web pages secured by SSL encryption. Together they give us the ability to *pay for stuff* on the internet. This gets us lots of things: retail like Amazon or Alibaba, peer marketplaces like eBay or Airbnb, subscription services like Netflix or GitHub; and it makes it worth advertising to people in the hope of attracting their payments, a business model that underpins Google and Facebook. Everything rests on the ability to perform one-shot payments on the internet, and to do so securely. Blockchain technology extends these capabilities further by offering peer-to-peer payments that can be utilized globally without an internet giant intermediating the transaction.

Agreements are more complex than payments. We have figured out electronic payments. How do we master dynamic electronic agreements? Agreements can include multiple parties; they can last for long – or indefinite – periods of time; they can anticipate changing conditions; they can make contingencies or exceptions explicit. If online payments gave us e-commerce, a replacement for handing over cash in a store, then the ability to create and perform agreements online gives us the ability to create digital equivalents to wages, complex property transactions, many financial instruments, and other complex chains of value, obligations, and rights.

An agreement sets out the roles that each party will play, the actions that are permitted, mandatory or forbidden, and what the consequences for each of these will be. We also set out a within the agreement a mechanism to resolve any differences that arise over whether the rules are observed.

WHAT IS MATTEREUM?

Mattereum is a smart contract platform and related support services that aims to provide a high degree of certainty about the legal frameworks which will be used to handle issues arising from new technology in business. The first horizon is making possible the legal transfer of property using a smart contract.

For the first decade of e-commerce, courts debated jurisdictional issues around the use of the internet in business. For example, it used to be a topic of active debate whether an ecommerce transaction occurred in the jurisdiction of the person making the purchase, the company selling the goods, or the physical location of the server. If something went wrong, one common recourse was the 'chargeback' operation, where the credit card company (which might inhabit yet another country) would simply pull the money back using the legal authorizations it had made vendors sign in exchange for processing their payments.

In practice most of these queries are now resolved using another mechanism: centralized hubs like Amazon or eBay who have powers much like those of credit card companies, granted to them by legal agreements signed by people when they start to use these services.

The terms and conditions (T&Cs) posted on the websites of internet giants have become a sort of loose de facto law of the internet enforced by legacy courts worldwide. For example, eBay's T&C allows governs trade that happens on eBay's servers, and is loosely subject to eBay's authority for most non-criminal matters. When something criminal happens, nation-state law kicks in to resolve the issues in the usual fashion, but the rest of the time eBay's (or Amazon/Google/Alibaba/etc.) rules form an additional layer of regulation on top of the existing nation-state laws. If your account is frozen, or eBay or Amazon decide they do not want your business, you have little recourse in many jurisdictions.

Mattereum aims to build a system to facilitate the use of blockchain technology in commerce. However, as befits the blockchain space, a somewhat complex mix of different legal, technical and social norms have to be combined to get this result. The integrity of the resulting contracts

should be significantly higher than ordinary terms of service too, thanks to the concept of an independent dispute resolution panel.

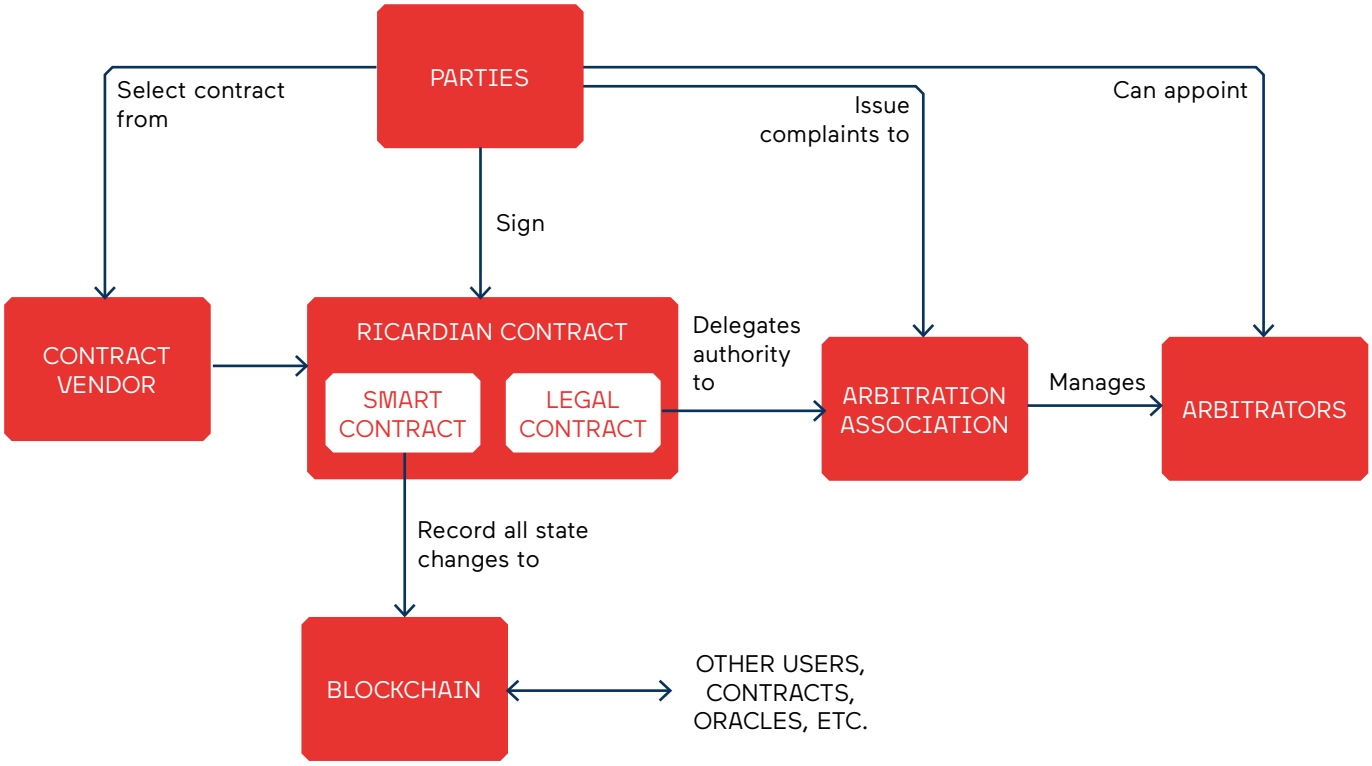
T&C-type 'jurisdictions' are relatively weak because, although we can clearly see that the person using eBay or Amazon is legally bound to obey the terms of service, these terms are seen as being one-sided and mainly interpreted to benefit the company which published them. In counterpoint, the Mattereum system uses negotiated contracts, which properly represent the interests of both parties, and independent arbitrators (paid by the parties themselves) to efficiently resolve any disputes that arise. A higher standard of integrity will be rewarded with better acceptance of decisions as fair and reasonable. The fairer, more equitable nature of the Mattereum contract suite provides an additional set of benefits on top of those which naturally follow a decentralized trade environment.

To effect Mattereum, we will need a body of law, people to arbitrate disputes, a way of getting nation-states to recognize what we have done as legal by their own norms, and of course we will need contracts. All of this can be done by correctly constructing the natural language contracts between the parties. Most jurisdictions recognise arbitration clauses, with 157 states having contracted in to the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (the 'New York Convention') under which local courts recognise and enforce arbitration awards made in other jurisdictions in all but a limited number of circumstances.

This paper will explain how this can become a reality.

A key component of trade is the formation of contracts. A contract aims to represent the wider agreement in all its detail between two or more traders. Sometimes this can be simply reflected in a paper document, other times it can be complex, contained in many documents, many additional promises, some verbal and some implied, and many events including some related to performance. But before we can run, we have to walk.

A single printed document containing all agreed terms within what some lawyers call 'the four corners of the page' is a key element in resolving any dispute. Such a document is typically on paper (or an electronic presentation of a document that could equally well exist on paper) because we as parties needed to read it and agree to it.



THE RICARDIAN CONTRACT

There are a number of techniques, all combined, that allow us to make much more modern representations of our agreements. These days all documents are already stored in digital form, in the format of Word documents. Most lawyers work with Microsoft Word and will send you a copy to 'redline' as their version of negotiation. We also know how to sign a digital-but-readable document by means of cleartext signing, an invention of the PGP community.

But we are not out of the woods yet. Unfortunately there are so many Word documents flying back and forth that we do not know which is which.

The Ricardian contract solves the above problems. It takes the legal prose of the lawyers or the legally adept business person, incorporates the signature, and then hashes the agreed document.

It is that last step which is the 'magic' – the secure or cryptographic digest or hash for short. This algorithm produces a one-for-one number that perfectly relates to the document. Only that document can reveal that hash, and that hash always refers to that one document. Blockchains now allow us to store those hashes in a permanent form,

and to represent substantial parts of the logic of the contract as a smart contract.

Then, whenever we do things together relating to the contract, we include the hash. Not the document, not the name or meaning, not an extract, not the many terms and conditions – just the hash. This forces the developer to keep a full contract repository (easy) and also forces the user to always have the contract in her contract repository.

Forcing the software to always have the contract in a digitally accessible fashion is an incredible benefit: because the transactions just refer to on-blockchain objects, they are almost totally meaningless without the natural language contract. For example, what is 5213 that you just sent? Refer to the contract which will say that you have paid £52.13. Why do I have a receipt for some 321 of a hash? The contract will tell you that you have received 321 loyalty points from Blockchain Airlines. What is my process for disputing the result?

As with a natural language contract the smart contract indicates that arbitration is the dispute resolution mechanism. You have to file a notice at the specified forum which your software will help you to do. The contract will tell you whether smart code prevails over the prose or the prose prevails over the code. And so on and so forth.

Many contracts are more complicated. Some contracts will need many more signatures; we also need ways to record events such as payments and delivery, and to formally vary the T&Cs. In particular, contract formation is a messy business, being in essence a negotiation with many positions trading back and forth before settling on the final agreement. Yet, all of those negotiations are potentially important to the contract, and a court can bring them back into consideration in the event of ambiguity. Negotiation is part of the contracting lifecycle, as is the dispute when something goes wrong.

Such dynamic change is more the domain of the smart contract than a traditional paper contract. A Ricardian contract can simply point (by hash, of course) to some automated code. Or vice versa. But two things mitigate against just linking prose with code. First, as mentioned above, we want the technology or process to capture the initial phase of formation – the negotiation – and also the ultimate phase of dispute as it

happens. Secondly, we want to use a standard piece of code over and over again, and we want to use standard legal prose over and over again. Those standards cannot be standard unless they leave parameterisation as an external responsibility.

Thus a Ricardian contract that incorporates smart code and negotiating looks like {prose, code, parameters}, being three separate components. Practically, it starts out very lightweight, empty even – we negotiate to add all things as we go. But that takes us into technicalities and also open experiments that today's blockchains are still working through.

The Ricardian Contract is a form of digital document that captures the contract between parties, ensures by its hash that the right contract is identified and also always present, and includes all the necessary components to keep up with trade as users want it.

THE BENEFITS OF CERTAINTY

In many places there is a hesitancy to 'write things down' in the form of invoking natural language contracts. Some, largely oral, cultures feel that it would be a breach of trust between the parties to write things down. Other sub-cultures have had overly negative experiences with legal systems and feel that they are expressly built to subjugate and reduce the 'freedoms' of individuals. However, as commercial activity has evolved over thousands of years by utilizing contracts legal certainty has become a highly valued attribute.

Human societies are some of the most complex systems on earth. As humans we span the spectrum from rational to irrational; sometimes we follow through on our promises and sometimes we do not. When we do not follow through on our promises sometimes there is a reason, and sometimes there is not. Sometimes that reason excuses us not following through on our promises; other times the reason does not excuse our behaviour. This complexity leads to innumerable instances of what coders call 'edge cases' and 'corner cases' that must be dealt with by legal systems.

When a dispute arises that is based upon this complexity, legal systems have a few options. They can resolve the dispute in favor of one party according to precedents that have been established within the jurisdiction. They can resolve the dispute in a creative manner based upon the adjudicator's desire to 'right a wrong'. But what the legal system cannot do is throw up its hands and not resolve the dispute. Even if the adjudicator does not understand the technical background of an agreement, the commercial context in which an agreement was signed, or have a deep understanding of the particular personal circumstances of the parties to the dispute – the adjudicator still must resolve the dispute. How that dispute is resolved in many countries then provides further background to the ever-evolving corpus of 'law'.

Thus we now have a background understanding of why contracts exist at all: to provide parties to an agreement with a modicum of certainty as to how a dispute about their agreement would be resolved. This certainty provides a systemic background across society that provides huge efficiencies to both the 'operation' of an agreement as well as to the resolution of any dispute. As an example, if both parties know that if a good was

shipped from a producer to a consumer and was destroyed along the way that it is the responsibility of the producer to send a new good to the consumer, then there is little incentive to incur the costs of a legal dispute. The producer should just send a new good. On the other hand, if in the jurisdiction in question the opposite is the case, then the consumer should just order a new good. In the real world this simplified example rarely holds, but it provides an illustration.

The second predominant reason for leveraging contracts is that humans do not always remember what was agreed. In oral cultures where families get together to form a business, when there is a stress to that business it can lead to rifts within the family as different members of the family remember what was agreed differently based on their own subjective biases. Written contracts reduce this systemic strain by providing a baseline understanding of what was actually agreed between the parties.

The final major reason for utilizing natural language contracts is to cleanly build a certain rule-set for the agreement. Law, like code, is typically built modularly and in layers. The layers in the legal system differ tremendously from, say, a software stack that operates an application. However, the fundamentals are largely the same. Natural language contracts are typically built to invoke what software engineers would call 'macros' or 'libraries'. These invoked 'functions' have stood the test of time, have had the edge cases and corner cases softened by adjudication, and have been proven to provide a high degree of certainty to the 'users'.

Taken together the benefits of leveraging natural language contracts in complex agreements and transactions largely outweigh the counter-arguments for not using them. This holds not because there is some authority insisting that natural language contracts be used, but rather it holds because it provides tangible benefits for the parties that are using the contracts. It is private parties that move contract law forward much more than the 'state' does. Thus it is not a stretch to say that, in the pre-blockchain world, contracts were the closest thing that existed to 'decentralized law'.

Ricardian contracts, as described above, extend further what a legal contract alone can do. They give us not only the benefits of certainty over the transaction or agreement but they also give us machine readability, API invocation, and scalability in formulating our contracts.

If the Ricardian contract is the narrative, we still need the story-tellers and the audience. Let us turn to that.

THE MATTEREUM PLAN

The Mattereum plan is to bootstrap the necessary legal and technical structures to make the legal transfer of property possible online.

We will have met our challenge when we can rent our next car, buy our next house, sell our next startup on the blockchain.

Meeting the challenge has three key components:

1. A population of 'blockchain aware' dispute resolution professionals, particularly arbitrators.
2. The necessary legal infrastructure to accommodate the new technologies.
3. Deployment and use of particular contracts

Mattereum will build out a set of legal and smart contracts to enable the transfer of ownership of an expanding set of different kinds of property. In parallel, part of this project is to build the ecosystem on the other side of this infrastructure: companies and clients ready to embrace and profit from the new technology, and mechanisms for ensuring that dispute are handled by suitably equipped dispute resolution professionals.

The other task is to build the natural language contracts and the smart contracts which actually manage the legal rights in property. This is where the majority of the set-up work for the Mattereum system resides.
For this task, the plan is to engage a spectrum of established law firms to write the natural language contracts, and to contract with various technical service providers in the Ethereum space to provide the smart contracts.
In almost all cases, a sketch of the legal contract (an outline mainly focused on the possible states the property can be in) and the smart contract will be developed in parallel, then the full legal complexity attached to the paper side.

Only a very limited pool of experience in marrying natural language contracts and smart contracts exists.

Our team (and network) represents a significant fraction of that global pool of experience.

We expect this process to be a significant hill to climb, and we expect iterative review and revision of both the legal and technical norms that will enable the smooth, unified functioning of the Ricardian contract triple. However, once a few base cases have been prepared for the simplest cases in our suite, the rest should come more quickly.

What kinds of ground might these contracts cover? There are many different kinds of legal property: personal property (shoes, pans), real estate (land, buildings), intellectual property (copyright in text and sound recordings, patents, trademarks), shares in a business, and so on. Some kinds of property have complex and specific legal frameworks associated with them – music is a case in point here. In addition, there are different sets of operators which apply to various kinds of property: lending, leasing, licensing, buying, mortgaging, auctioning, insuring, options to buy, etc. are all possible, and different contract clauses apply (and, indeed, different laws in some cases).

By spreading the work around multiple legal firms and technical firms, we hope to foster broad understanding of how to create these Ricardian contract triples (legal template prose, smart contract code, transaction-specific parameters). We hope our initial efforts to get the first suite of contracts written will be augmented by other firms (including those we have paid to write a contract or two) finding new areas and forms of property for which to create a contract triple. In this way we aim to create a systemic transformation, where legal firms become used to the idea of creating Ricardian contracts and will offer this as a service to their clients in the future.

The result may well include a set of markets for different kinds of property which have just been brought to the blockchain. It is easy to imagine analogues of existing services like eBay or Amazon, but these take little advantage of the unique properties of the blockchain environment. A wider imaginative scope might see futures markets for charter jets or airline seats, fine wine or antiques shipped with their full history and provenance tied to the transfer of goods, complex option schemes allowing a whole set of purchases (say renting house and furnishings from a variety of different sources) to be locked in as a single transaction, and so on.

Broad adoption of any of these schemes is likely to be challenged by two

factors: transaction fees and low transaction rates on the current Ethereum blockchain. There are two solutions: in theory, permissioned blockchains could be used to host the smart contract aspect. However, these systems may be less stable and permanent than the public chains, causing future problems. The other, more likely solution, is that scaled blockchain technologies will rise to meet the need. Demand for property transfer will take a while to get going, and as it gets faster, easier, cheaper and less mysterious, demand will grow. But we are definitely aimed at the future if we consider running entire supply chains on Mattereum.

We see Mattereum as a system which will start with relatively high value transactions for types of property closely associated with the blockchain ecosystem, but which will branch out as time passes and more work is done to bring new kinds of property to the market.

The Mattereum organization will get the system bootstrapped by investing in the legal and technical work required to start the system and to represent the initial property types and transfers. Additional strategy, marketing and other kinds of work may be necessary as time passes, and the Mattereum organization undertakes to get what is necessary and possible done to encourage the growth of the ecosystem.

THE BUSINESS MODEL

Mattereum sits in an ecosystem with many kinds of value flows.

1. Arbitrators can charge for hearing a dispute
2. Institutions can charge a fee for services such as appointing an arbitrator and administering the dispute resolution process
3. A fee can be charged when a Smart Contract is instantiated, and/or for operations carried out
4. Smart Contracts can charge a percentage of value exchanged using them
5. Customers can pay each other using this smart contract ecosystem
6. Insurance can be offered for various potential costs (including dispute resolution)
7. Investment possibilities

However, several of these value flows will have the effect of slowing the growth and adoption of the ecosystem – in particular, schemes around charging percentages of exchanged value will tend to create competitors or simply drive people to private arrangements.

We believe that the correct approach to this space is not to directly intermediate any of the value flows (this is, after all, meant to be a decentralization exercise!) but rather for Mattereum to have a dual nature: setting up the infrastructure, and then acting as a (lead) investor in the companies that are coming into the space to build businesses in the ecosystem.

This approach tightly aligns our interests with the overall health and growth of the ecosystem, without giving us any kind of incentive to raise the transaction costs for using the system; in fact, our interest is to keep the costs and risks as low as possible, while keeping the system fully healthy. We trust the arbitrators to look after their own interests; the market for arbitration services will include higher and lower cost options, depending on the specific needs of the parties. Large scale commercial adoption of arbitration is common in other industries, and arbitration systems are well understood in industry.

We anticipate a complex and integrated ecosystem of services (many

being investment opportunities) will form once the ability to transfer legal property on the blockchain is well established. What market adoption will be of that ecosystem is hard to predict: the ecosystem is filled with surprises. Adoption could be slow, with gradual adoption in obvious areas, or it could be sudden and unexpected as Magic the Gathering cards or some other physical commodity suddenly leaps online with the blockchain as its primary trading venue. It could be short leases on real estate, or some as-yet-untraded object like hotel bedroom futures.

Human creativity about ways to make money is not in short supply. Our hope is that there will be no shortage of interesting and creative investment opportunities in the space we are about to create.

ARBITRATION ASSOCIATIONS

An arbitration association is an institution which publishes a list of proposed arbitrators, appoints arbitrators when the parties cannot agree on the arbitrator to be appointed, and publishes rules to be followed in arbitrations. The contract will include a term which requires disputes to be decided by an arbitrator, who will either be selected (by agreement) by the parties themselves, or (in default of agreement by the parties) will be appointed by the association from the panel of arbitrators. There will be a variety of options for arbitration, including low cost options. These kinds of mechanisms are standard in the commercial ecosystem, and there are tens of thousands of practising professional arbitrators.

BOOTSTRAPPING THE ECOSYSTEM: WHAT'S THE SIMPLEST THING THAT COULD POSSIBLY WORK?

The next challenge is to get a simple test system built. The simplest test system we can imagine is a copyright assignment contract. A simple web form calculates the hash of a piece of text pasted into a box. This hash is written to a smart contract, claiming ownership of this work by the current operator. Assignment of the ownership of this work, in exchange for a payment, is made possible on chain using another smart contract method. To get this to be legally binding requires a contract to be assented to by the parties (perhaps using an approved online representation of a natural language contract – DocuSign type services.) Similarly, a copy of the work itself should be assigned/stored somewhere.

Let's break this system down into its constituent parts.

The system must include:

1. an arbitration procedure.
2. a natural language contract which delegates some authority to:
    a. a smart contract, and
    b. an arbitration procedure to resolve any dispute.
3. a smart contract which adequately represents the legal transfer of copyright ownership as a technical operation.
4. a proven link between the author's assent to the natural language contract, the smart contract, and the work in question (all identified by hashes)
5. secure storage for the original contract signatures, or other equivalent proofs.
6. a set of transactions on the blockchain corresponding to a sale.

In a sense, the static starting conditions of the game are laid out in the natural language contract: I am the author of this work. In return for a fee of $500 I will transfer ownership of this work to you, whoever you are.

The payment which actually makes this happen is done on the blockchain:

a function is called which accepts a payment and changes the state on the smart contract to indicate a change of ownership has occurred. No new natural language contract is created. Rather, the agreement that a sale is possible is conducted in the paper world, and the events which make the sale final happen on the blockchain. If a non-technical person wants to interpret this situation in the event of a dispute, they have the option of raising a dispute about the contract, and asking for the decision of an arbitrator.

The arbitrator musters whatever technical resources are needed to ascertain the current status of the copyright. Because both buyer and seller have committed to giving the arbitrator authority in this matter in the natural language contracts, the arbitrator's decision is legally binding. In some countries there are limited rights of appeal, for example on the ground of lack of jurisdiction or serious irregularity which causes substantial injustice.

What if something has gone wrong, like a bug in the smart contract has destroyed the $500 payment made in ether, but the blockchain still shows that the buyer owns the copyrighted work, even though the author never got paid?

The answer is: it's complicated. There is a body of law which applies to situations of this type, and the job of the arbitrator is to apply the law to our case and come up with a solution or remedy which in an ideal world will be both legally correct and satisfactory from a technical point of view.

COMPLEXITY AND MATTEREUM CONTRACTS

To build a substantial and functional Mattereum ecosystem is going to require a very solid structure. Although it is tempting to conceptualize the smart contract ecosystem as mainly being an ecology of code, the majority of the complexity of the real world is beyond the real capacity of code to represent. Take goods in container shipping: there must be 500 different legal conditions that goods can be in as they go from a factory in China through to a retailer in America – impounded by customs, lost on the docks, trapped on a ship that has been ruled unseaworthy, flood damaged, lost, lost-believed-stolen, sitting on the bottom of the sea, and many more states, and each of those states could be in any country in the world (more or less). A sea of possible states, and transitions between those states exists largely in the paper world – a container is found, or a ship is certified as lost at sea for insurance purposes. Attempting to jam this complexity into a smart contract results in a *lossy abstraction* in which the paper reality isn't quite married up correctly to the smart contract reality. If it's close enough, people expect the mapping to be perfect, but instead the mapping is just a little off and edge cases slip through. For this reason, the Mattereum plan mainly focuses on natural language contracts. Smart contracts exist to register the subset of state transitions which can be well represented by current or near-future blockchain technology. An additional factor is that if the granularity of the system is too fine, transaction costs will price the use of smart contracts out of the market. So rather than representing the passage of goods through a shipping system with 500 possible conditions and 75 possible mechanisms for triggering a transition from one condition to another, each transition managed by a different set of cryptographic keys, the system might be reduced to half a dozen states (owned by A, bid offered, bid accepted, goods shipped, goods arrived, goods accepted) with the parties keeping their own records of the full complexity of the system, ready to be presented to arbitrators in the event of a dispute.

Such a system is clearly a step on the way to systems which can truly model and accept the complexity of the real world. Some of that software exists already: SAP (for example) has those comprehensive models

in place for much of manufacturing and some other industries. However, it is more likely in the near future that bridges will be built between existing repositories of complexity management know-how (i.e. law, legacy software etc.) than that the full complexity of the real world will be internalized into the blockchain space.

TOWARDS FLEXIBLE CONTRACTS

If we let the imagination run wild, we can envisage a future where we perhaps look beyond the proposed triple – prose, code and parameters – where now the first two components are essentially static templates. Each such contract might be made up of building blocks, both for prose and for the smart contract code. Each contract might have plugins and each plugin might have a set of parameters associated with it.

To get more specific, imagine a contract that represents the interaction between a seller of shoes and a buyer. This main contract would be very simple: buyer pays, seller delivers. A new feature to this contract would be the ability of the buyer to return the shoes within a specified period of time. A bulk of prose text would be added and also a counterpart smart contract piece that now needs to add a couple more states to the internal automaton to model the returning of the shoes and the issuing of the refund. Of course, this futuristic platform would handle all the complexity of auto-generating the contract(s) with the end users only needing to tick one more check-box to add this feature together with the parameter which specifies the time to return.

Further on, the seller might want to take off some of the risk of the shoes getting lost in transit and might want to buy an insurance for the parcel. Because most likely the insurance contract would be quite complex as well, it would be added into the main one only as a reference. In case of an insurance claim, the main smart contract would be paused in a Pending state and continue execution inside the insurance smart contract until it gets resolved. As such, linked contract networks would be formed.

Another example that illustrates the usefulness of having a flexible contract is the process of buying a house. In the simplest of cases, the seller owns the house, the buyer already has the cash to buy the house, transaction occurs – money gets exchanged for the house ownership title. But if the buyer doesn't have the money, he would need to borrow from a third party. The introduction of the third party and the part about borrowing the money, with all the implications of a mortgage charge would come as additions to the main contract. The newly formed contract would also contain the schedule of mortgage repayments with automatic execution

of the house ownership charge in case of default.

If the lending third party is an established blockchain business with their own [smart] contracts in place, we could also think about composition of contracts again, where the main contract ends with the exchange of ownership title and would continue execution into the mortgage repayment contract with a remaining charge in the main contract for the case of default.

ASSETS AND CAPABILITIES

Ecosystem transformation investments are complex, subtle things. Let us break this down into a set of assets and capabilities.

The first asset is a body of arbitrators and the defined procedures to handle disputes. Without them, the Ricardian contract pairs hang in space – if something goes wrong, we have little recourse. A system could be stood up with general commercial arbitrators, but a high quality, consistent, service would be hard to find without technical competence on the part of the arbitrators. So building technical knowledge among arbitrators is critical to quality of ruling, which is critical to the function of the system.

The second asset is a very considerable portfolio of natural language contracts, written in specific ways which make them suitable for precise integration with smart contracts. The preparation of that contract suite is a big job, and will be spread among many different law firms. The base of skills and experience created will likely result in many more such contracts being written by these firms for their clients as they begin to feel more comfortable with the Ricardian contract approach, and the arbitration association. Broad adoption may be driven as much by the lawyers as by the startups. Professional networks that understand what we have to offer are significant assets.

The third asset is a body of hard-won understanding on the technical side. This is partly a suite of smart contracts, but more fundamentally it is a nuanced model of how the contracts are created to fit the natural language contracts, and vice-versa. There has never been a broad-based effort to climb this particular hill, and in all probability at the end of this process we will have the world's best body of understanding of this critical area.

The fourth asset is our network of investments. We anticipate using some very solid new models for keeping together a tightly socially integrated set of startups, with good recycling of talent from projects which are stuck to projects which are fully viable. We also anticipate cutting edge approaches to risk management for entrepreneurs, including equity pools. In short, we believe the VC side of this operation will be fully adapted to the new world

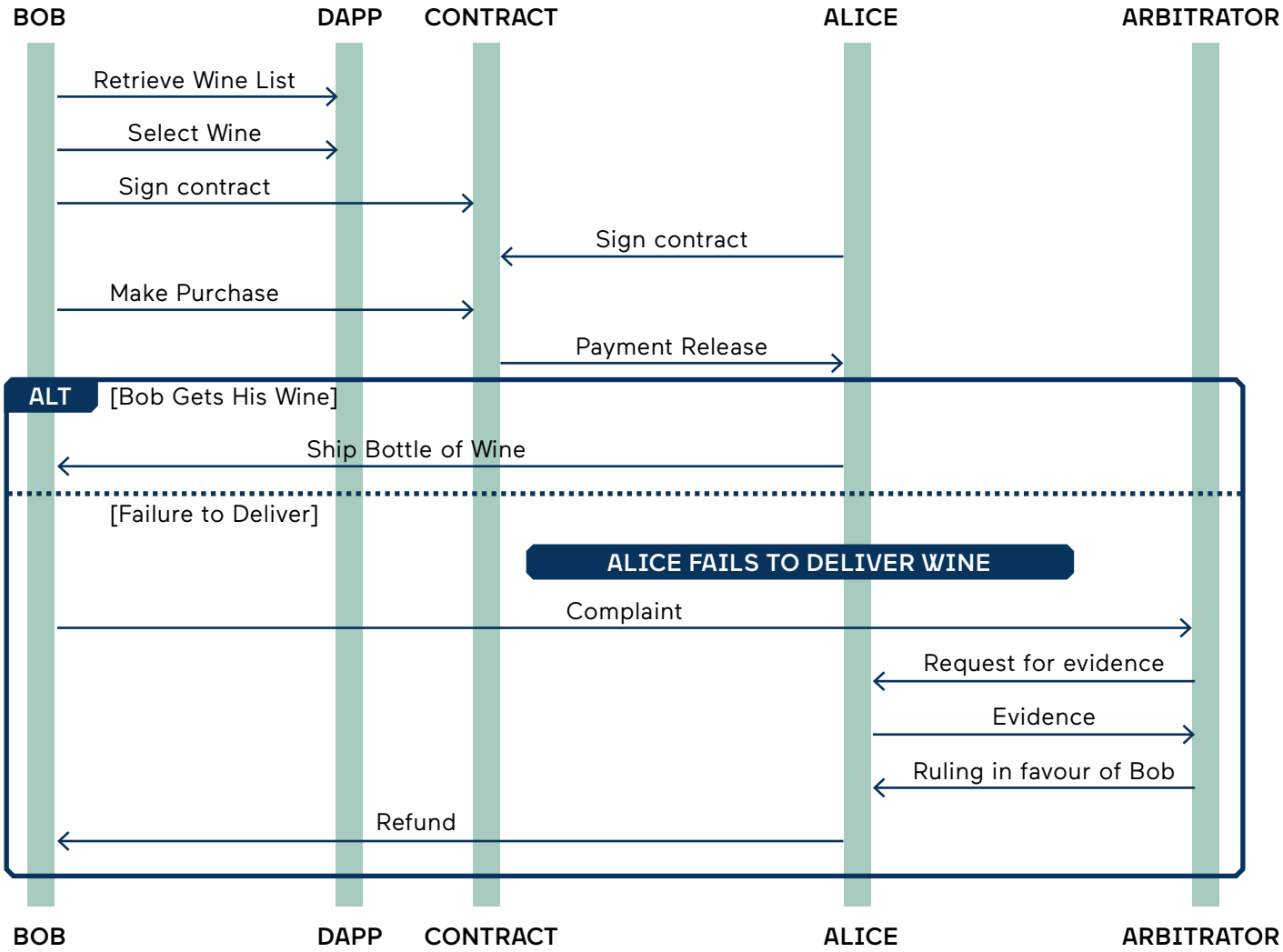
VC operates in. We believe the entrepreneur network we invest in will be a huge asset.

Together, we feel these assets will deliver a very substantial change in the position the crypto ecosystem has relative to the conventional world of law, finance and regulation.

CASE STUDIES

PURCHASE OF FINE WINE

Alice's Fine Wine Emporium wishes to sell a variety of fine wines to customers via their dapp. The dapp allows customers to browse the currently-available wines, with provenance information recorded for each step of the winemaking process.



Bob wants to buy wine. After selecting a particularly expensive Médoc, Bob signs up to make his purchase.

Alice and Bob both sign a Ricardian contract which details the terms and conditions of Alice's Fine Wine Emporium. It explains how purchases, returns and refunds are handled, how shipping and delivery will be arranged,

and how purchases will be invoiced. Once signed, this contract covers all purchases Bob may make in the future, so the signing only needs to happen once.

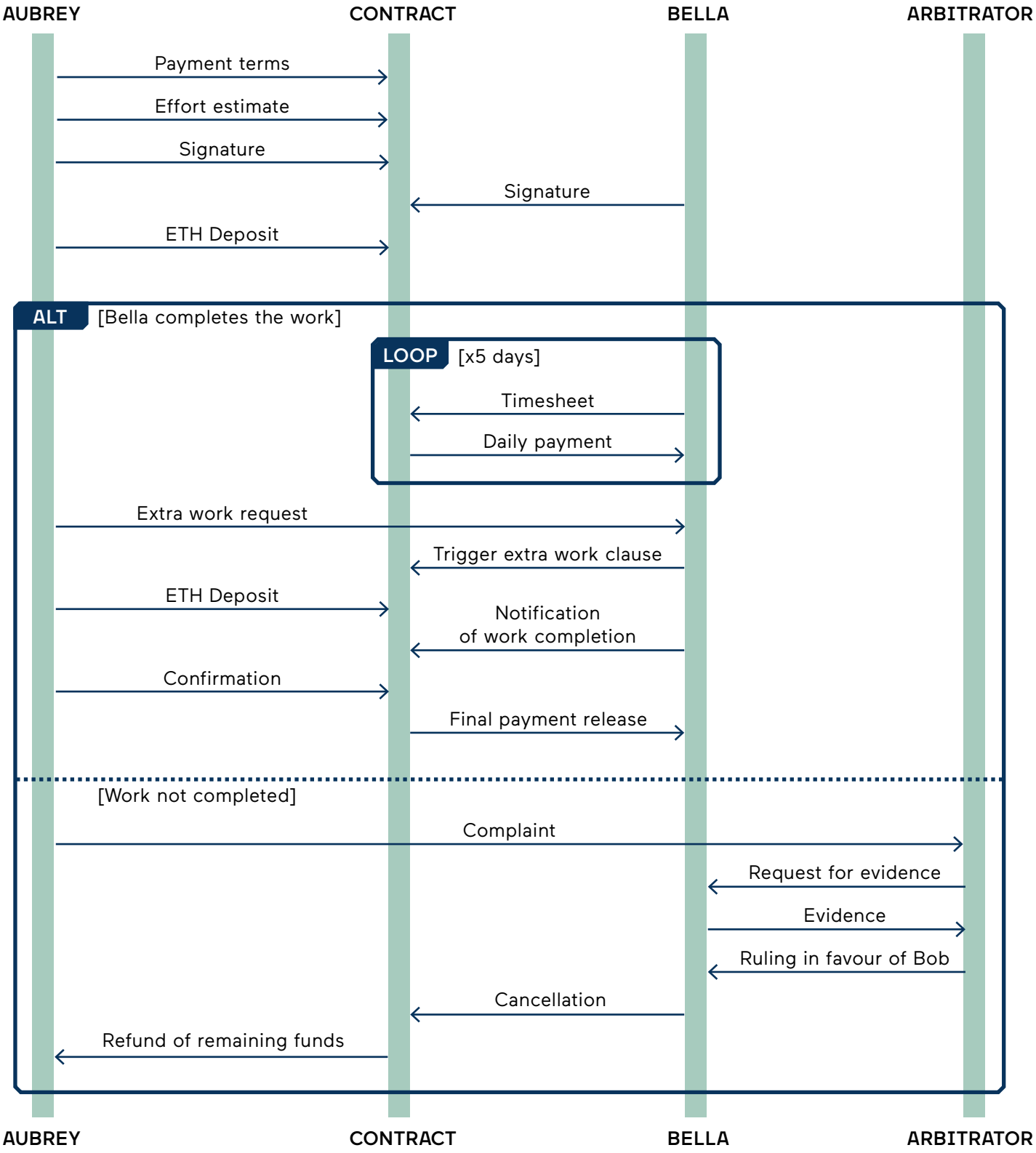
How Arbitration Affects Outcomes

In this example, Bob has recourse in the event that Alice fails to deliver the wine as advertised – either by failing to deliver any product, or delivering a product that is deficient under the terms of the contract. Bob has the ability to ask the arbitrator for a ruling, and the arbitrator can gather evidence from both parties before making a decision. If Alice cannot provide evidence to counter Bob's claims, the arbitrator will rule in Bob's favour, forcing Alice to pay Bob back.

In reality, the mere knowledge of the fact that Bob can request arbitration would encourage Alice to resolve the situation before reaching arbitration. As the costs of arbitration are normally borne by the losing party, Alice has a strong incentive to reach a satisfactory conclusion with Bob before arbitration becomes necessary.

WORK-FOR-HIRE CONTRACT

Aubrey has a great idea for a new startup business. With his MBA and extensive business contacts, he's convinced that he can build the next Facebook – or, at least, the next LinkedIn! All he needs is someone to code the prototype.



Bella is a web developer, and a friend of Aubrey's cousin Cerys. Aubrey asks Bella to build the prototype, in return for payment. Bella agrees, and her estimate is that it will take her 5 days to complete the work. Aubrey is also concerned that Bella might work slowly and costs might spiral out of control. They agree that Bella should be paid her normal rate of 5 ETH per day for the first 5 days, with both parties aiming to finish the work by then. They agree that any further work will be charged at 2.5 ETH per day, giving Bella an incentive to finish and move on to other work, without allowing Aubrey to request further modifications without paying anything at all.

With the help of Bella's friend Lawson, they draw up a contract specifying the payment terms and the intellectual property rights (all work produced will belong to Aubrey once completed).

Aubrey deposits 25 ETH to cover the first five days of the work. After each day, Bella writes a record to the smart contract indicating that a day's work has been completed along with the hash of the latest commit in GitHub. 5 ETH is paid immediately to Bella.

After the five days is completed, Aubrey requests a further day's worth of changes. He deposits 2.5 ETH to cover the cost, and Bella notifies the smart contract when she is finished, releasing the final payment.

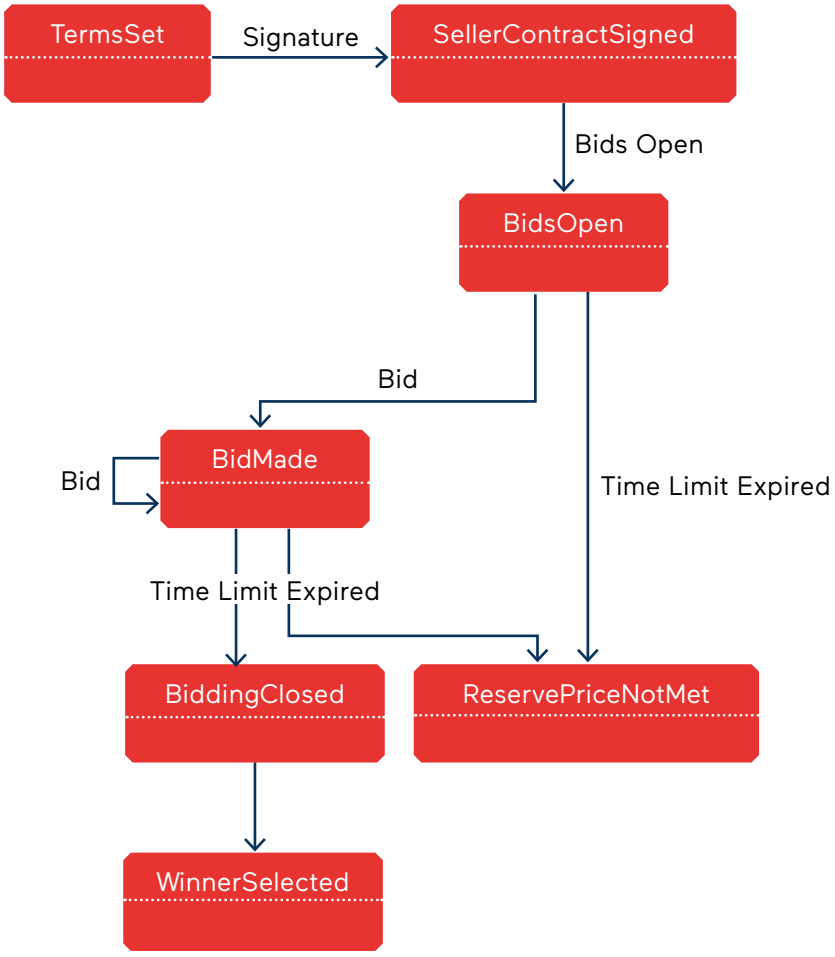
How Arbitration Affects Outcomes

In this example, Aubrey deposits funds in escrow before Bella completes the work, so there is no risk of Aubrey refusing to pay. However, there is a risk that Bella does not complete the work, and Aubrey needs to seek the return of escrowed funds.

In this case, Aubrey can ask the arbitrator to order the return of either escrowed funds or funds already released to Bella (the legal contract should stipulate how partial payment is handled in the case where Bella completes part, but not all, of the work). Bella can be instructed either to repay directly to Aubrey, or to withdraw her offer of work thus triggering the release of the escrowed funds back to Aubrey.

AUCTION

Arjun owns a Lamborghini Aventador. Following a decision to switch to a more environmentally-conscious form of transport, he also decides to sell the Lamborghini. Aware of high demand for Lamborghinis within the Ethereum community, he decides to auction the car via a smart contract. To ensure legal enforceability, he uses a standard Mattereum auction contract.



The contract allows him to specify a minimum reserve price, and a time limit on bids. Once these have been set, the auction can be opened. All bids are openly visible on the Ethereum blockchain, and a competitive bidding process ensues. Eventually, Zadie emerges as the person willing to bid the most, and she is named as the winner of the auction, immediately becoming the legal owner of the car.

The diagram below illustrates the contract as a state machine. This simple model of the possible states of a contract, and the possible outcomes,

can help to ensure that both the smart contract programmer and the legal contract author agree on the expected behaviour. As state machines are well-understood, they can provide simple but useful documentation.

How Arbitration Affects Outcomes

In the simple example above, there are relatively few opportunities for arbitration. As the entire auction is conducted on-chain, there is no risk of payment being withheld. The main risk is failure of the seller to provide the item listed for auction, in which case the winner of the auction is entitled to pursue to the seller for compensation.

ADVANCED TOPICS

IDENTITY

Natural language contracts require legal identity. Smart contracts require key pairs, and protection of one's private keys. Bridging these two different kinds of identity is at the heart of making smart contracts legally binding.

There is no doubt that to make it possible to transfer legal property on the blockchain requires the paper half of the contract pair to be signed by a legal entity: there is no mechanism which can make a contract enforceable against a public key. However, there are many legal methods used to protect the privacy of property owners, usually involving having a corporation own the property, or some kind of legal intermediary like a legal firm which acts as a nominee. These systems are legal and heavily used. Of course, one's degree of comfort contracting with such an entity might vary with its reputation and its history of prior contract counterparty performance. A brand new, never-seen-before legal entity without an obvious human owner might be much less trusted than one with thousands of transactions to its name.

We do not propose to enumerate or classify what can and cannot sign a contract. Mattereum does not purport to be able to engineer out this complexity: it is part of the legal world, and while we hold out high hopes for general blockchain identity schemes which will resolve these issues in a categorical form, those systems are not here yet. So instead we propose to leave these questions to the lawyers, who are expert in assessing these risks. If your lawyers are uncomfortable with their ability to identify the counterparty should a dispute arise, this is not a risk that we can hedge without insurance. However, we think we can do a little better than 'buyer beware' even in the absence of comprehensive and standard blockchain-native identity solutions.

We do not propose a single method to accomplish this binding between legal persons, keys, and contract counterparties. It is clear that blockchain identity systems are under very heavy development, and changing all the time. Similarly, state-run identity systems, like the Estonian e-residency approach,

are also in constant flux. If we establish an identity system ourselves, we are simply locking out all the people who have better ways of managing the identity problem than we do. This is not productive.

However, if we leave identity unaddressed, we have a system in which one of the hardest problems of the day is simply marked 'buyer beware.' If we pick a technology, we are too early. If we do nothing, we are creating insurmountable problems in an unacceptably wide range of use cases.

Our chosen method for managing identity is to classify misidentifying individuals as an 'insurable risk.' If you suffer a loss because the person you thought was selling you shoes or wine turns out to have given you a fake identity and run off with the money, an insurer steps in and covers your losses. That's not the same thing as covering your losses to other classes of fraud or theft: rather we take the specific risk of identity fraud, and find specialized insurers who can insure that risk. This represents a new class of e-commerce insurance.

We know that (for example) having a notary public (aka legal notary) check identity documents and witness the signing of a contract is a reasonably high standard of identity validation for many purposes. However, getting this act on to a blockchain requires either that the notary is comfortable with digital signatures and key management, or that an intermediary takes this input from a notary – verifies the notary's legitimacy, for example – and then posts this information onto a blockchain. These specialized intermediaries could work in a variety of ways – attaching this kind of validation to a uPort profile, for example. It could also leverage the existing Know Your Customer / Anti Money Laundering work done by (for example) exchanges like Kraken and Poloniex. Under the right circumstances, exchanges could act as data sources for identity providers, or even act as identity providers themselves.

To unify these various sources of validation, we propose that trust in identity is measured by the amount of third party compensation that the counterparties can attach to the transaction in hand. Suppose that I have notarized copies of my passport, and 20 years of bank statements and other substantiating documents together; if I ask a third party to examine these records, and vouch for my identity, they might feel they are taking a very small risk. People are incentivized (i.e. paid) to vouch for the fact they have examined these records and believe them to be valid. To pay

for the risk they are taking by insuring the parties against misidentification risk, the notary charges a fee of 1% or even 0.1% of the funds staked as payment, depending on the risk. This could be framed as an insurance contract in some jurisdictions: 0.1 ETH paid to the insurer buys me 10 ETH of funds which the insurer will stake against any fraud which results from them misidentifying me.

This is not a conduct bond; for an insurer to guarantee my behavior is a different kind of trust. We think that kind of trust is also very much worth exploring, but it is a different thing.

Rather, the identity assurer simply examines the available records, including perhaps their own transactions with the identity customer, and in return for a payment posts a bond indicating they will pay a fee (as part of an arbitration award) in the event that the contract signed with BOB HOWARD turns out to have been signed by somebody else masquerading as Bob.

Identity insurance of this type can be layered, and backed up by bonds. I could have KYC/AML data with two or more exchanges, a family lawyer who has known me for years and who has recently become crypto savvy, and a couple of whales in the space who have been to my house and know my face. Each of these individuals might be willing to stake significant funds against the very, very small risk that I am not who I say I am. The resulting identity bond is presented as an asset to contract counterparties: a total sum of 200 ETH are available from the following parties at the discretion of the arbitrator if the person who signed this contract is not BOB SMITH. If I was much less well known to the person making the bond, or the documentation was thinner, they might charge a much higher fee for the identity bond they are providing: perhaps up to 20% of that bond, or no bond at all.

This simple way of resolving trust into identity bonds should make it possible for identity systems of all kinds to work smoothly together to help contract counterparties identify each other, with real consequences for misidentification, and real protection for counterparties, all subject to the jurisdiction of the arbitrators. None of this precludes fraud prosecutions against people lying about their identity, of course: the law is still the law. But the ability to feel secure while involved in a transaction

is as much about insurance if things go wrong as about trust that they will not go wrong, and we feel the correct approach for an environment with such rapid change is to make identity about the one thing which everybody can agree on: money changes hands to manage the risks which technology cannot yet eliminate.

This basic paradigm that trust in systems and people is expressed by bonds, escrows or other promises to pay in accordance with an arbitral decision is likely to form a backbone by which pieces of trust we have spread across different technical systems can be brought together to provide actual support for our transactions.

We will establish the basic contractual frameworks for some of these use cases, and do our best to encourage widespread market adoption of these mechanisms. If a different dominant solution emerges, we will (of course) move to adopt it as quickly as possible.

CONTRACT MANAGEMENT

Contract validation and fees

It is unreasonable to expect arbitrators to adjudicate poorly written contracts, or smart contracts which have not undergone sufficient security testing. While unforeseen events are always possible, the purpose of arbitration should so far as possible be to handle the unforeseen, and malfeasance – not gross ambiguity in the underlying instruments. In many cases, a poorly written contract that fails to adequately express intent will leave arbitrators forced to interpret words like 'reasonable' in the absence of a solid context to put those words in.

To ensure against this situation, contracts which are part of Mattereum will have been reviewed before a contract can be entered into and any consequent dispute referred to arbitration. The initial suite of contracts we create will be registered as a matter of course, and additional contracts can be registered after they have been examined and a fee paid.

This fee covers inspection of the contract, and an audit of the smart contract, to ensure not that they are free from defect (we cannot vouch

for that, not being omniscient) but that they form a suitable basis for arbitration: intentions are clearly stated on paper, and the smart contract passes a basic sanity check as an expression of those intentions. The fees for this process are not handled inside of the system: rather, Mattereum has a set of professionals on file who can provide the service, and people with new contracts must contract one of that set to do the inspection and report back that the contract is either a reasonable basis for arbitration (should arbitration be necessary), or needs work to clarify ambiguities or further secure value in the smart contract.

Contracts which have been validated in this way are added to a whitelist.

Contract fees

Contracts are protected as copyrighted works, and are licensed to parties who wish to use them: this applies both to natural language contracts and to smart contracts. There is a small fee associated with contract use: one part goes to the Mattereum organization, and another to the owner and maintainer of the contract (if the contract was created by a third party.) The first part helps cover the costs of training and accrediting arbitrators as technically competent.

Contract fees will typically be at least partially anchored by the price of goods in the real world, or against fiat currency charges for goods and services. This makes the volatility which is common to cryptocurrencies somewhat problematic. If, for example, contracts have fixed prices denominated in ETH, and there is a rapid rise in prices, a 'nominal fee' of a dollar or two to register a contract suddenly becomes 5% or 10% of the contract value.

To avoid this problem, prices to register contracts are set on a dynamic basis, so that their fee (when translated to fiat) remains at their chosen level. We do not anticipate that contract signing functions can fluctuate wildly in price without impacting the ability of the ecosystem to use the arbitration mechanisms of Mattereum for day to day trade, which is the goal. Price volatility is the enemy of predictability.

To resolve this issue, contract registration will be priced dynamically: Mattereum will operate a price oracle which will set the cost of registering

a contract so that it stays roughly constant in fiat terms.

Contracts themselves may specify payments any way that is acceptable to all parties: Mattereum does not constrain the parties' contracts, including their choice of payment instruments.

CONTRACT ORGANIZATIONS

This approach is very much an attempt to bootstrap the next phase of transformation in the smart contract ecosystem, giving rise to many new users for the blockchain, and forming one of the backbones of the entry of the blockchain into the day to day business lives of ordinary people working in conventional businesses. These kinds of businesses may already have contracts that they are using every day which could be rendered usable in a Ricardian contract triple with a little work, opening the door for existing businesses to streamline their operations using Mattereum. This is even more true for standard contracts which are shared inside of an industry, or are common to the operations of a company with many thousands of customers, some of whom are sophisticated enough to make the transition to the Mattereum system.

Natural language contracts and smart contracts will accumulate profile data over time – how often the contract is used, parallel versions of legal text which have been translated and certified as accurate renditions of the original contract, audit reports on smart contracts and so on. Total value transferred or managed by the contract would be another useful trust metric.

Over time we anticipate that some of these contracts will wind up with institutions which support the contracts, including managing and producing new metadata in support of a contract pair – legal contract prose and smart contract code. A good example is the International Swaps and Derivatives Association (ISDA) Master Agreement, the foundation for derivatives trading. ISDA supports the users of the contract, manages the contract text (including keeping it up to date) and generally supports the industry which has grown up around the contract. Although we would be surprised and delighted if the contracts in our system grew to be ISDA-sized, it's not at all unreasonable consortiums might form to manage keeping

a specific natural language contract up to date, make improvements over time, handle versioning issues, modifications to the smart contract paired with the legal contract, and so on. We would anticipate that some of these contract consortiums would be profit-making enterprises in their own right, competing for advantage in areas like making real estate or corporate debt instruments available for buyers on the blockchain. Mattereum does not intend to compete with contract organizations: access to arbitration is open for all parties who get a contract audited and cleared by Mattereum.

In fact, Mattereum is highly in favour of the formation of contract organizations, and interested in facilitating the formation and profitable operation of new contract organizations within the Mattereum frameworks. The objective is to create large-scale systems transformation of how certain classes of contract are administered, and that cannot be done with any mechanism except a broad-based engagement of many talented people working for their own goals, with their own vision, under their own guidance.

The objective is not to create a monopoly, but to set an initial set of templates and standard contracts up to prove that the field is viable, and then provide the core services necessary to all the people doing business in the synthetic jurisdiction that we have established.

THE FUTURE: A STATUTORY REGISTER TRANSITION

In the long run it is likely that the blockchain, or a technology derived from the blockchain, will be used for many statutory registers. Statutory registers are things like publicly visible ID numbering schemes.

The Icelandic Kennitala is a single global ID number used by citizens of Iceland for everything from library cards to tax records. This number, because it is so public, is tied to careful selective disclosure methods: everybody in the country can figure out your library card number, so the library card number alone will not reveal any private information under any circumstances. The number is public, but the data stays private. This model gives some interesting insights into how privacy matters might be managed on the blockchain in future. It is old, well established, and a good fit for the privacy properties of the blockchain as it currently stands.

As things stand, property can be divided broadly into two main categories: registered and unregistered. Registered property lives on statutory registers: registers the government maintains by law. These typically include cars, motorbikes, houses, land plots, company shares and directorships, copyrights, patents and trademarks. Unregistered property is everything else: bottles of scotch, cigars etc. are typically not registered, but this is not to say they are not controlled: no sale to minors, taxes in addition to sales tax. But, for our purposes, it's not these additional control structures that matter, it's the question of whether the government maintains the list of who-owns-what, and how that list is updated. Right now, most of the statutory registers are updated by complex multi-stage paper processes. By far the biggest and most complex of these is the process of buying a house: fees can pile up to a few percent of the cost of the transaction. And these are not small ticket items.

So while the system remains in this condition, there are limits to what can be done elegantly using contract law to transfer ownership. There may be a set of legal approaches involving companies which own property, and rights like usufruct being transferred rather than ownership outright, but all of these things are legal bridges towards a future which has not yet been built: a future where the statutory registers have machine readable forms, and APIs allowing software to transfer ownership of property.

It may take upwards of a decade to get statutory registers online in a way which permits online updates. Various problems have to be solved: identity, authentication and authorization, legacy records stretching back to parchment (goat skin!) and large amounts of off-book property that is not traded, and so has not made it into the government's statutory registers yet. There is very little we can do, Dubai Blockchain Strategy notwithstanding, to get these registers online.

However, Mattereum, can provide an interface to a small subset of registered property like cars, houses and patents. This is perhaps the trickiest issue we will face as the project moves forwards: just how far can we get towards a pocket universe which mirrors the situation that everybody will get when the statutory registers finally move online? For unregistered property this is an easy situation: people sign bills of sale on the back of napkins, and anything which improves on that situation will work.

But getting towards a situation where it's possible to cruise around London in an Uber looking at houses, and buy the one you like for ETH using a smartphone wallet? It's not impossible that the legal research will find mechanisms which actually allow and enable that sort of future, but odds-are it will be a multi-stage process involving building out more infrastructure in the form of intermediaries (i.e. entities which hold the property on paper, on behalf of the beneficiary owner.)

This is the fundamental research component of the Mattereum plan: getting the best possible interface to the statutory property registers for real estate etc. that we can build inside the current legal system we have. And this, of course, will vary from jurisdiction to jurisdiction. It may be that we will find clever approaches which only work in France or Germany or Luxembourg, but cannot work in New York. This kind of lumpiness does not affect most simple property, or property rights which have been created recently. But land law is old law, and as such it is very lumpy and irregular.

The poor may inherit the earth, but at least in some jurisdictions they will not be getting the mineral rights.

Transparency

Earlier on, we discussed the Kennitala, the Icelandic ID number which is used for so much in their society. It acts as an index to sensitive data, but simply knowing the number tells people little or nothing.

Can blockchain identities work like this? Should they?

We don't know yet. Opinions on this vary widely, and technology is moving fast. Some people see the future as homomorphic encryption everywhere, others favor ZK SNARKS. Some suggest the chain will be split into multiple components some containing data, others identity. We do not know which way this will go, so we have to have a strategy which is largely independent of the technology of the day.

Here's what we know to start. In the initial context, the minimum which can be on-chain is a contract ID and a couple of counterparty signatures. If those signatures key to only this contract (i.e. the users have multiple keys, and only use this key for this contract) information leakage should be

minimal. The arbitrators (or more likely some intermediary acting as a lawyer) holds the legal identities of the participants, and so very little is revealed on chain. This leaves lots of repositories of useful (even critical) information off chain.

The next step might be to encrypt a lot of this information and put it on-chain. The full text of contracts would only need to be stored once, and referred to by contract address. The same might be true of identity information: it could be put on-chain, which would allow a person to see that a given key had signed a lot of contracts, but without knowing the parameters (what is being sold, for example, would likely be encrypted.) The bottom line is that there are multiple possible technical approaches to these issues, each with a slightly different balance of cost and complexity.

Our proposal is that we are going to spread around the initial smart contract work to a variety of vendors – some big firms, some small firms, some individuals – to get a variety of models built out and tested. This is a profoundly complex area: the technology is far from trivial, and the product-market fit questions around contract privacy are deeply non-trivial.

For example, consider an auction. There are certain classes of auction where seeing bids is necessary for the auction. These could be approached in a very straight forwards fashion, and work well. Another class of auctions require sealed bids, and at that point the cryptographic approaches come in. But in this context, how are we to know which class of auctions will be more popular? Are sealed bid auctions going to be rarities, or the dominant auction format? Product-market fit is non-trivial in a market moving this fast.

Our expectation is that this will be an evolving endeavour. Relatively open systems, without deep privacy measures, will probably come first in test systems. From there, it will be a choice of levels: in which cases is privacy protected by intermediaries like lawyers or nominees, and in which instances is it protected cryptographically by (for example) N-of-M secret sharing schemes and multi-party arbitration teams having the keys?

Different kinds of contracts will have different requirements. Other vendors are working very hard on contract privacy. Intermediaries who might escrow identity using various technologies are also forming. This suggests active

engagement with the issues, and a sharp eye on the changing technology front rather than a dogmatic hold on a currently-available technology solution.

Across this entire project, the question of what to handle with smart contracts and other technology, versus what to handle using additional layers of intermediaries and trusted humans will be tricky. We have already discussed the need for simple smart contracts, with the majority of the work being done by the natural language contract. But all of this is dependent on the current state of the art in both the underlying platform and infrastructural support services provided by vendors and other third parties. This kind of messy, complex environment with multiple moving technological parts intersecting with marked dynamics and fundamental platform innovation requires teams much larger than a single person to manage. Multiple specialities have to come together to make optimal decisions in such a terrain, and building this kind of pool of deep expertise is why our initial team has the cross functionality it has.

ECOSYSTEM INVESTMENT

Mattereum is a platform, not a product. To deliver on the full promise of decentralization – a transformation of business, governance and administration – will require a vibrant ecosystem of many products, powered by Mattereum.

Ethereum's existing smart contract infrastructure has already enabled many new businesses, but these are limited in scope by the fact that smart contracts can only enforce on-chain outcomes. With Mattereum, that scope is expanded by orders of magnitude: smart contracts to manage everyday sale, lease, lend, and auction of simple property, real estate, vehicles, land, energy, labour, and time will become possible. Built on Ethereum's programmable blockchain substrate, applications composed of connected smart contracts and Ricardian contracts will become possible. New ways of managing the systems that run our lives are enabled, and it will become possible to program our reality.

Imagine a young musician, creating her first pieces of music for sale. With Mattereum, she can register her copyrights herself, enter deals

direct with distributors, promoters and concert venues. Her fans, too, can participate directly – crowdfunding new music, tours, and videos. With instant payments on-chain, not only does the artist get paid directly, but so do her producers, backing singers and session musicians.

This is the possibility that Mattereum exists to enable. To build it will require an ecosystem. For that reason, Mattereum's aim is to create *infrastructure* to support the efforts of others, and to generate an ecosystem of startups, partnerships and joint ventures around it.

This involves a lot of very early stage investment in small enterprises, and quite possibly standard incubator/accelerator/lab type arrangements for getting these startups together. Much of the thinking from hexayurt. capital comes straight across to the Mattereum ecosystem, and we expect to work with our network of experienced VC fund managers to enable rapid uptake of these services.

TECHNOLOGICAL COOPERATION

Understanding the parameters, boundary conditions and thresholds for action in a complex environment with a lot of moving parts, with legal issues at the heart of the process, is a job for a specialized entity which solves exactly that problem. There are few teams anywhere in the world which could bring together this cross-section of expertise, and as time goes on that expertise and the network which supports it will grow wider and deeper. The intention is to build the fundamental gateway between the legal and the technical, but this is as much a social structure as a technical one. As Sun Microsystem's Bill Joy said 'no matter who you are, most of the smartest people work for someone else.' This means keeping the door open to other teams with alternative models, finding markets for innovators while not attempting to drown them out or lock them out of our core business, and so on. It's a fully cooperative-competitive environment, where our ability to license and collaborate with others who have technological break-outs is matched by our ability to absorb and integrate new technologies into our operational expertise to get our fundamental clients – Mattereum users – the best possible legal agreements so they can get on with their business.

This kind of structure is typical of frontiers. Nobody knows exactly who will come out ahead in the end, and whether it will be a few large players that dominate in the long run, or complex networks of smaller actors in networks. This margin is partly set by cooperation and transaction costs – what you might call Coasean factors – but also by the fundamental technical complexity of the market. Sometimes innovation is easy to build on, sometimes you have a breakthrough and then wind up locked to it while other people innovate as you are bogged down building out the details of the initial invention. Frontiers of this kind require and provoke a cooperative response – in a sense, all the people innovating at this edge are working together to effect a global transformation in the center – and it is in this spirit that we continue our labors. We have far more to gain by cooperation than competition.

This is an imperative which is as much strategic as aesthetic. Our understanding of the complex nature of frontiers is that those who thrive on them tend towards a cooperative response whenever possible: we are in this together, or we perish alone.

AUTHORS

Vinay Gupta is the founder of Hexayurt.Capital, a fund which invests in creating the Internet of Agreements. He was instrumental in creating the Dubai Blockchain Strategy, managed the Ethereum blockchain platform release, and invented the hexayurt refugee shelter. His first involvement in commercial software development was in 1992, and continued through the 1990s in medical imaging, flight simulators, cryptographic applications and the web. His areas of expertise include disaster management, energy policy (5 years at Rocky Mountain Institute), and computer graphics.

Rob Knight is an experienced software engineer, architect and Chief Technology Officer. He has led teams building large-scale logistics, financial regulatory compliance and intellectual property management systems for organisations including the BBC, ITV and Royal Mail Group. He has also founded several businesses and is a speaker and author on software development, management, and blockchain technology.

Dr. Aeron Buchanan received his doctorate from the Robotics department of Oxford University in the field of Computer Vision, after reading Engineering and Computer Science for his undergraduate degree and working as an algorithm designer for the special effects industry. He has since designed algorithms for UAVs, started tech companies building light show controllers and blockchain technology, plus acted as a consultant to economics professors and ecological research laboratories. He is currently a technical advisor to the blockchain world, aiming to continue the advancements in consensus platform technology and more readily bring the benefits to the economy and society in general.

Christopher Wray is a lawyer and commercial mediator, and cofounder of companies developing self-adjustable spectacle lenses for distribution to populations without access to conventional eye care. He read physics and philosophy at Oxford University and later law, and he writes on the cognitive science of decision-making and dispute resolution.

Ian Grigg is a noted financial cryptographer, having entered the space in 1995. He invented the Ricardian Contract as a process to capture all of the prose in a legal contract of issuance, and permit unique identification

among many competing issues without the need for a centralised registry to allocate numbers. He is co-inventor of triple entry accounting, which has been termed by some as the most significant change to accounting in 500 years. As well as doing seminal work in digital payment and issuance or registry systems, he has created models for identity and community which have been trialled successfully in low trust environments. Ian has worked for R3, and consults with leading firms in the blockchain space. He is currently partner at block.one.

Casey Kuhlman is the CEO of Monax specializing in the legal applications of blockchain technology. Prior to cofounding Monax, Casey was the head of legal information systems at the US Open Data Institute. A lawyer and international development practitioner for nearly a decade, Casey has worked extensively in the Horn of Africa, including cofounding the first law firm in Somaliland. Casey has also been a New York Times bestselling author, an infantry officer in the Marines, and is an avid participant in open source software development.

Dr. Mihai Cimpoesu is a computer scientist with experience in computer security and machine learning. He holds a Ph.D. in Computer Science with his thesis focused on applied Machine Learning algorithms towards proactive detection of online threats. He worked for companies like Bitdefender, Amazon.com and Thomson Reuters and for the last two years, he focused entirely on blockchain related projects through his consultancy company dltlab.io.

Professor Michael Mainelli FCCA FCSI FBCS Co-founded Z/Yen, the City of London's leading commercial think-tank and venture firm, in 1994 to promote societal advance through better finance and technology. A qualified accountant, securities professional, computer specialist and management consultant, educated at Harvard University and Trinity College Dublin, Michael gained his PhD at London School of Economics where he was also a Visiting Professor. He is a non-executive director of two listed firms and a regulator, Alderman of the City of London for Broad Street, Emeritus Professor & Trustee at Gresham College, Fellow of Goodenough College, trustee of several charities, and Senior Warden of the Worshipful Company of World Traders.

Clive Freedman FCIArb FBCS is a barrister, arbitrator and mediator at 3 Verulam Buildings, specialising in information technology, banking and financial services. He is a fellow of the Society for Computers & Law, and co-wrote the chapter on Fintech and blockchains for the forthcoming 4th edition of Banking Litigation.