The Zenotta Litepaper

an abridged overview of the Zenotta Digital System

Alexander Hobbs

Andrew Kessler

Andreas Furrer

Miles Timpe

Zenotta AG

April 7, 2023

Contents

Chapter 1: Introduction

Ascribing digital value in digital systems

In the physical world, value is easily evident, albeit often subjective. As a society, and as human beings, we are eminently comfortable with the notion that physical objects can possess value, and through the related concept of ownership, how this value can be transferred between individuals and groups. The development of the Internet has, however, given rise to a world that is entirely digital in nature, and our long-held understanding of what can and cannot be assigned value is in dire need of updating. The latest paradigm to emerge from the Internet-enabled machinery of communication – blockchain – is re-defining and potentially introducing the concept of digital value, whether it be digital gold (Bitcoin), money (cryptocurrencies in general), financial products (DeFi), digital goods (NFTs), or digital real estate (the metaverse).

Fundamentally, the digital world does not preserve the "structure of value" in the same way that the physical world does. This introduces unnecessary costs and risk into digital systems, affecting the physical world a myriad of ways – causing procedural headaches and inefficiencies for automation in industry, government, and the private sector alike, as well as interfering with international trade and logistics. Identifying a reliable methodology for ascribing value within digital systems would alleviate the substantial hurdles currently faced by content creators, organisations, and industries in regards to compliance, capital raises, client engagement, cybersecurity, data rights management, and more.

1.1 The pursuit of value in digital systems

Notable attempts at creating substantive value in digital systems include pricing via processing (Dwork & Naor, 1993), Bitgold (Szabo, 1998), Hashcash (Back, 2002), and Bitcoin (Nakamoto, 2008). Each of these technologies represents a step (sometimes a leap) toward understanding value in digital systems. But a general solution, and one that mirrors the structure of value found in the physical world, is still elusive.

When we consider physical world economics, we see why. Economic value is largely a function of supply and demand; however, in the digital world, the fundamental mechanics of supply and demand are not preserved because digital goods can be created, duplicated, and manipulated at virtually zero cost. Fundamentally, the economic value of things in the physical world should be framed in the context of **non-rivalry** and **excludability**[1], two properties which a thing must satisfy in order to possess economic value and to be considered **an asset**.

When we consider legal systems, the discrepancies are even clearer. This is due to the fundamental concept of ownership. Only rival and excludable assets are ownable, while non-rival and non-excludable assets, such as air or water, are public goods available to everyone. Air is everywhere, accessible to all, and in effectively infinite supply, but a tank of compressed air is finite, restricted, containerized, and can be physically transferred in a way that removes it from the ownership of the transferring party. Legal systems must be able to define and protect rights and ownership for digital assets, which they cannot do without a form of ownership that creates such a containerizing concept on the machine level.

[1]Non-rivalry means that consumption by one party of a thing prevents simulataneous consumption by others, whereas excludability means that consumption of a thing can be prevented for certain parties

Value types

Equally important is the requirement for digital value to represent **all** value types, whether *intrinsic*, which is a form of value inherent to the asset and its existence – of which one can classify certain primitive sub-types such as ethical value, aesthetical value, and even metaphysical value (the value associated with self-identity and the relationship between the asset and the owner) – or *instrumental*, which is the utility value of an asset; its purpose, its functionality, or its usefulness as a means to an end.

The source of digital value

The starting point for fixing all of this is to understand the 'thing of value' in the digital space that we need to harness and protect. On a practical level, digital systems consist of *files*, which act as containers for knowledge, and *applications*, which act as containers for logic. While applications can read and, if necessary, extend existing knowledge within the system, it is the file itself that contains the knowledge[2] and the effort and work that has gone into developing and recording that knowledge. This high-level ontology indicates a strong correlative relationship between files and intrinsic value, as well as between applications and instrumental value.

This makes sense when one realizes that there can never be a coin, or a token, that accurately personifies all forms of intrinsic value. However, a file (or files) can. Unfortunately, while digital coins or tokens can 'live' on a blockchain, files cannot – block space is expensive, and files contain far too much data (along with, often, privacy requirements) to be stored and verified.

1.2 Files under blockchain governance: realizing web3

The initial development of the Internet revolved around the dissemination of information. The first incarnation (web1) largely consisted of one-way access to a repository of information for the average user (**read**). Later this developed into a two-way platform for sharing and creating content (**read-write**).

Since then, the Internet has evolved into a social realm where individuals interact, share personal data, and engage in economic activity. This goes far beyond mere social media, and is a fundamental shift towards a digital societal identity, with all of the accompanying societal value and structure, such as rights and privacy.

While many definitions of web3 differ, it is probably described best in this ontology as **read-write-own**. This is not only two-way but also peer-to-peer, with individuals conducting business and personal relationships and transacting, just like in the physical world. The problem is that the infrastructure and base layer protocols of the Internet are not capable of defining or ascribing value – there is no concept of native ownership or transaction security (in short, no solution to the double spend problem). This is where blockchains come in. Solving the double spend problem[3], and more generally, the Byzantine Generals' Problem[4] (BGP) in order to achieve trustless, immutable, distributed group consensus means defining and transacting ownership for the coins or tokens under blockchain management.

[2] here used in an abstract, general sense – a file containing images as art may not be knowledge in a strict sense of the word, but it still contains the fruits of a author's creativity, skill, and imagination

[3] the problem of how to determine whether a given digital asset was spent more than once

[4] fundamentally, a problem describing the difficulty of trusted information transfer without requiring all participants to be trustworthy

Fundamentally, web3 is about getting machines to understand value. Transacting assets in the digital world is largely pointless if vast amounts of human legal manpower has to be brought to bear to resolve disputes constantly. The semantics around value and the relationships they create cannot be interpreted by machines, because under the current web2 paradigm, machines cannot process the ownership and transaction of files.

So what is the solution? While files cannot live on a blockchain, they can be put under *blockchain governance*. Thanks to developments in blockchain and cryptographic protocols, files (and more generally, data) can be managed from the blockchain ledger through a decentralized file format known as **Smart Data**. Zenotta has developed this technology as part of a Layer-1 solution to the double spend problem for data – how to ensure that a file can be traded peer-to-peer in the way that coins and tokens can; and how the rights to the file, and the file itself, can move concurrently from owner to owner.

1.3 The building blocks for a distributed marketplace

The ability to trade a file peer-to-peer opens up the potential for a true distributed marketplace, where trades can occur without going through or being managed by a centralised third-party. Moreover, placing the trade of assets under the consensus mechanism of a Layer-1 blockchain and removing the necessity for smart contracts to govern such transactions reduces complexity, risk, and cost. The use of a universal, two-way ledger (refer to Chapter 3) together with distributed nodes for matching trades between users allows the trade of assets to occur without going through an exchange. The transactions on this distributed marketplace are secured by the distributed consensus that makes blockchains so powerful, and the focus on data, rather than smart contracts, as the key assets around which trade executes provides a framework for compliance and reduced risk when processing the movement of said assets.

With online words and metaverses emerging in the web3 paradigm, distributed marketplaces where the rights of the individual, their digital identity, and the ownership of their assets are preserved in the same way as in the physical world will become ever more vital.

1.4 Transferring value with a native protocol

The Internet, born in 1990 with a suite of technologies that would continue to be refined over the coming years and decades, was focused around the transfer of information across a distributed public network. It is fair to say that it has been extremely successful in achieving this goal. However, in order to transfer value, one cannot use the same protocols that enable the transfer of information. The reason for this is simple: it does not matter if information is 'spent' twice[5]. With value, the prevention of a 'double spend' is absolutely vital, since without this protection, whatever is being transferred loses its value. What is needed, then, at this moment where we are witnessing the birth of an 'Internet for value' is a native Internet protocol that communicates value across a distributed public network.

We call this protocol the Internet Transaction & Trade Protocol (ITTP), and we elaborate on it in Chapter 3. Central to this protocol is blockchain governance of data, as we have introduced above, and a form of data able to retain the properties of uniqueness and identity that give physical objects in the real world value that cannot simply be lost through making a copy.

[5] or multiple times

Chapter 2: Digital Ownership with Smart Data

Programmable ownership through identity

The understanding that files, and the data contained within, are the key repositories of value in digital systems leads us to the key concept: a form of data that can be placed under blockchain governance. Such a form of data would integrate with economic, social, and legal value structures and allow for the realisation of true digital value for the first time.

In our society, the ever-accelerating pace of digitization has led to vast improvements in quality of life, knowledge, and given the individual a truly global reach. However, we live in a world where the rate of technological development often outstrips our ability to preserve fundamental economic and human rights and personal freedoms.

What is needed then is a new approach to the digital world. An approach designed from the ground-up, that natively imparts ownership on a truly digital level, within the data – within the file itself. Imagine a society where you can pay your rent with a fractionalized version of a song that you wrote, or buy groceries with a piece of digital art that you own. Imagine trillions of connected, programmable files, with rights and privacy assigned at the file level. For content creators, for businesses dealing in digital products, or indeed any individual, company, institution, or government, the potential of such a system is vast, and as yet untapped.

To this end, we introduce the technology of **Smart Data**. Smart Data is a decentralized file format under blockchain governance, that is programmable and secured through encryption, encoding, and an immutable blockchain ledger.

2.1 The decentralised file format

A Smart Data file consists of three parts:

1) A cold-stored file (CSF)

An encrypted, encoded file that is under the possession of the owner of the Smart Data.

The CSF contains the content (the image, or the video, or the music, etc.). The CSF lives either on the owner's machine or in their cloud storage. This file cannot be decoded without the DRS (part 2), and cannot be decrypted without the symmetric encryption key (part 3).

(2) A data rights signature (DRS)

A collection of hash values and an encoding scheme that form a fingerprint unlocking the rights to the asset.

The DRS provides demonstrable (identity-based) ownership of the CSF, along with the ability to decode and decrypt the content. Part of the DRS is the unique encoding scheme which acts as the instruction manual, or rosetta stone, that instructs the machine that holds the cold-stored file (CSF) on how to read it. The encoding is akin to digital DNA, which imparts uniqueness to the file itself.

The DRS is visible on the blockchain but unaccessible without the encryption key pair (part 3). It is machine-readable and zero knowledge, which means that its visibility alone does not allow

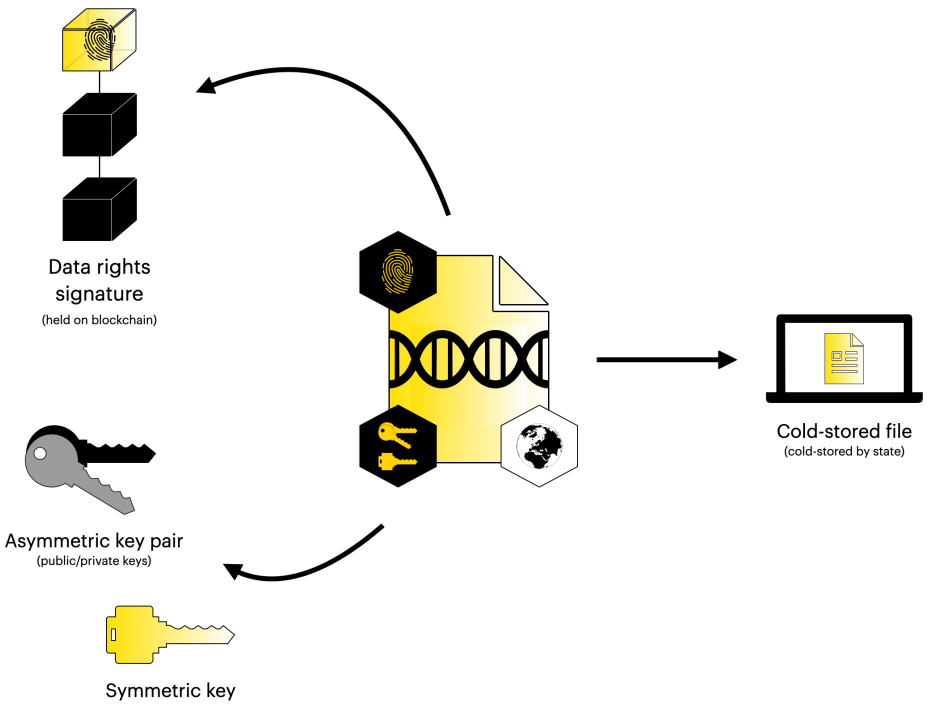

Figure 1: The components of Smart Data, comprising a decentralized file format.

for any party to gain any knowledge about the contents of the file.

3) An asymmetric encryption key pair and symmetric key

A pair of asymmetric encryption keys that sign the DRS on the ledger and a symmetric key that protects the Smart Data content from anyone but the owner.

The symmetric key is held in the owner's wallet, whether this is a wallet on their computer or a hardware version. Once the CSF has been decoded using the DRS, it must still be decrypted by the symmetric key in order to gain useful access to the content. The DRS encoding scheme, which imparts the uniqueness, cannot be moved or spent or in any way transferred without having the asymmetric encryption keys.

Re-inventing Cold Storage

The cold-stored file (CSF) described above is an entirely new approach to cold storage. Instead of being cold-stored by location, e.g., a secure air-gapped server, the file is cold-stored *by state*. This means that is can be held anywhere, or allowed to float freely on the Internet, while still being secure and exclusively the possession of the owner. Anyone who gains possession of the CSF while it is still encrypted and encoded will find it useless, and the only way to (i) decrypt the DRS and (ii) decode the file is to (i) be in possession of the keys and (ii) be the owner of the DRS.

2.2 A paradigm shift in digital assets

The Crypto space undergoes an incredible amount of innovation and experimentation, with new projects and coins being launched almost every day. Accordingly, there are some concepts that have emerged that have similarities with Smart Data. The most relevant of these is that of NFTs, or Non-Fungible Tokens, which have been gaining popularity and activity since approx. 2018.

NFTs are an example of the power of scarcity in a digital asset. By using the Ethereum ERC-721 non-fungible token standard (for example) crypto assets can have property rights assigned to them and become commodities to be bought and sold in areas such as virtual worlds, games, and digital art galleries. NFT standards have also recently been developed in other blockchains, creating a competitive marketplace in terms of choice of infrastructure.

Where Smart Data stands apart from these token standards is the re-invention of the file itself. Rather than having a token with the property of non-fungibility assigned to a particular data file, it is the file itself that contains this non-fungible, scarce property, through the decentralized file format and the interplay of encryption, encoding, and a blockchain-based signature. These properties allow for full control of the file as well as ownership. A good analogy would be that of taking ownership of a new car. Non-fungible token standards essentially give you the 'pink-slip' of ownership, while Smart Data gives you both the pink-slip as well as the keys to the car.

We can see the difference in more specific detail by looking at the relevant properties of NFTs vs. Smart Data. We start with the obvious property that they both share, namely non-fungibility/scarcity.

Relevant Properties of Smart Data

Non-fungible/scarce: The uniqueness of an item is what gives it economic value in the market, allowing it to function as a asset. It is important also that this uniqueness persists over time, and so imparting a rival character (where consumption of the good by one consumer prevents simultaneous consumption to other consumers) to data is a huge step forward in moving towards a data economy.

Smart data extends this property beyond that of NFTs by imparting both a rival and an **excludable** character (where consumers who have not paid for the good are prevented from having access to it) to data. This is an incredibly important property for a data democracy. The owner of the data can decide not only how their data is sold, but also how it is used while it is under their ownership. Integration of existing software with the Smart Data format will allow for rights to be embedded within data, for automated handling of data regardless of a specific application, and for automated compliance checks, reducing lengthy legal procedures at the human level.

The other relevant properties that we need to consider for both NFTs and Smart Data are as follows, starting with the list of properties for NFTs as outlined in a recent Coindesk article:

- ***Non-interoperable:*** *A CryptoPunk cannot be used as a character on the CryptoKitties game or vice versa. This goes for collectibles such as trading cards, too; a Blockchain Heroes card cannot be played in the Gods Unchained trading-card game.*
- ***Indivisible:*** *NFTs cannot be divided into smaller denominations like bitcoin satoshis. They exist exclusively as a whole item.*

- ***Indestructible:*** *Because all NFT data is stored on the blockchain via smart contracts, each token cannot be destroyed, removed or replicated. Ownership of these tokens is also immutable, which means gamers and collectors actually possess their NFTs, not the companies that create them. This contrasts with buying things like music from the iTunes store where users don't actually own what they're buying, they just purchase the license to listen to the music.*

- ***Verifiable:*** *Another benefit of storing historical ownership data on the blockchain is that items such as digital artwork can be traced back to the original creator, which allows pieces to be authenticated without the need for third-party verification.*

(Ollie Leech, Coindesk article, Feb 2021)

For Smart Data this list reads as:

- **Optionally-interoperable:** In the same way as with NFTs, Smart Data is genre-specific; with the caveat that its function can be altered through its property of being programmable (see below).

- **Divisable:** On this property, Smart Data departs from NFTs in an important way. Smart Data can be fractionalised and sold for Zeno coins, which opens up an incredible amount of liquidity in the space and lowers the barrier to entry for investors in Smart Data assets. However, the transaction is atomic, meaning that both sides of the sale or trade of the asset (or the fraction of the asset) must complete in order for it to process. This protects buyers and sellers.

- **Indestructible:** Smart Data is locally stored but under the control of the blockchain via Smart Data contracts and the DRS, which means that it cannot be destroyed, removed, or replicated (see the 'persistence' property below). However, through the compliance property (see below) the 'right to be forgotten' applies, enabling owners to 'burn' the DRS to prevent any further use of this data.

- **Verifiable:** Here the same benefit applies as with NFTs. The signature chain that is built up through a series of 'lockboxes' encypted with each owner's private key ensures that the original DRS remains unchanged, and so the original creator retains their authorship of the Smart Data. Authentication is through the blockchain and does not require a third-party.

To this list we add:

- **Authentic:** Smart Data contains unique data DNA, rather than just an attached signature. This ensures that ownership is authentic and based on identity, and this ownership extends to the file (the asset) itself, rather than just a token that represents the asset.

- **Persistent:** Smart Data is not dependant on trusted third party hosting or on the whims of any prior owner to alter content or previously codified ownership axioms. A seller cannot perform a 'rug-pull' or scam the buyer in any similar way, and since the content of the file is under the control of the owner, rather than a third-party, Smart Data cannot be delisted.

- **Programmable:** Smart Data can be instructed to behave differently under different conditions, through Smart Data contracts. A good example of this would be if an owner wants to restrict the sale of their Smart Data to countries or jurisdictions with a good track record of LGBTQ+ rights, or to prevent the data from being used in a marketing campaign by a company with shady business practices.
- **Compliant:** For any real economy, compliance with national and international law not only cannot be avoided, but is desirable. Blockchains are currently a 'wild west' where anything goes, and while a libertarian philosophy is an important part of the new, decentralized financial system, in order to integrate with and advance society, rights and laws protecting the individual must be upheld. Smart Data enables such compliance through (i) programmable metadata and (ii) receipt-based trade native to the ledger with the ability of user-defined application of sanctions. These are implemented at the machine level, vastly expediting legal processes while ultimately remaining under human control.

These additional properties broaden the notion of value for a Smart Data asset over an NFT from merely economic to (i) social value and (ii) legal value. With Smart Data as the first rival & excludable digital good, possessing economic, social, and legal value, it represents a true paradigm shift in the digital asset space, and constitutes the first ever Non-Fungible Asset (NFA).

Chapter 3: The Internet Transaction & Trade Protocol (ITTP)

Providing a Peer-to-Peer Electronic Trade System

The Zenotta Digital System (ZDS) combines the invention of Smart Data with a next-generation blockchain network & ledger to provide technology enabling the **Internet Transaction & Trade Protocol (ITTP)**. This protocol defines the backbone of web3, in a similar manner to how the HyperText Transfer Protocol (HTTP) defined the backbone of Internet communication. ITTP solves the 'data double spend' problem, ensuring that value, rather than just information, can be transferred across the Internet in a manner that is secure, efficient, legally-compliant, and preserves digital rights and digital identity. ITTP therefore gives birth to a new, data economy and democracy, where digital content and data of any kind becomes a digital asset.

The Internet Transaction & Trade Protocol (ITTP) is built around the following four components/layers of the ZDS:

1) **A data protocol** that gives life to an 'Internet of value' based on ownership of digital goods & services, powered by Smart Data.

2) **A two-way universal ledger** as a means to effect trade of real economic digital goods & services over a layer-1 blockchain defended by distributed consensus.

3) **A hybrid blockchain network** as the backbone for the first distributed marketplace and Smart Data universe, engineered with the next generation of distributed consensus to be scalable, secure, and resistant to mining centralization and monopolies.

4) **A legal framework** that has been developed to be native to a digital system, ensuring all aspects of the transfer of value across the Internet are legally valid, privacy-preserving, and compliant.

These layers exist alongside a governance philosophy that adheres to the principle of governance without control: a community-focused, fair partnership built on a Socratic interpretation of Athenian democracy that ensures compliance with private legal acts and mandatory law.

3.1 The data protocol

Data is the cornerstone of digital systems. In an increasingly digital world, data has become the lifeblood of our technical, social, legal, and economic structures. However, while data can convey information effectively, it cannot be used to reliably prescribe value, in a way that can be transferred digitally. We term this **The Data Problem**.

The Data Problem has its roots in the problem of scarcity. If you can simply copy or duplicate an asset for essentially zero cost, it has no value (or at least none that can be utilised effectively). Up until now, the solution tried by purveyors or custodians of digital goods (e.g., movies, songs, photos, etc.) is to prevent them from being copied, in order to give them scarcity and therefore value. However, this is doomed to failure (and requires huge technical & legal efforts as well as manpower).

At Zenotta, we believe that scarcity can be achieved in a far better way through uniqueness. Making an asset provably unique gives it true scarcity, and thus true value. The Zenotta data

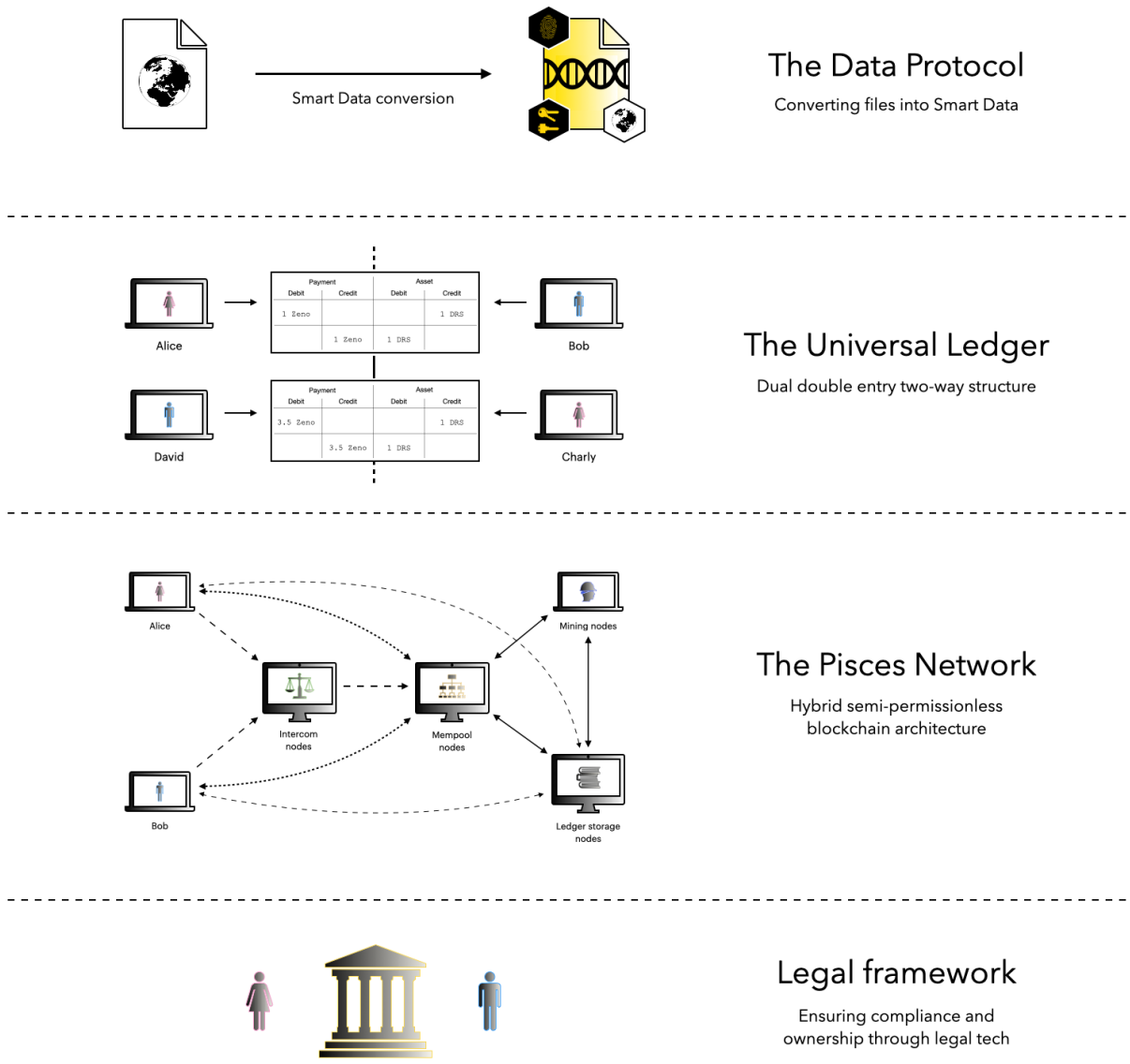

Figure 2: The four components/layers of the Zenotta Digital System (ZDS) that provide the foundation of the Internet Transaction & Trade Protocol (ITTP). The data protocol allows for the conversion of any file or data into Smart Data, part of which contains a Data Rights Signature (DRS) that can be traded for payment tokens (or other digital assets) on a universal two-way ledger with a dual double entry structure. This ledger is secured and defended by distributed consensus through a hybrid blockchain network employing 'Pisces architecture' (see Figure 5) with an off-chain set of nodes and a blockchain set of nodes using a three-tier approach. Underpinning the above layers is a bespoke legal framework, designed from the ground up to integrate with and support the execution of rights in the digital world, through Zenotta's technology.

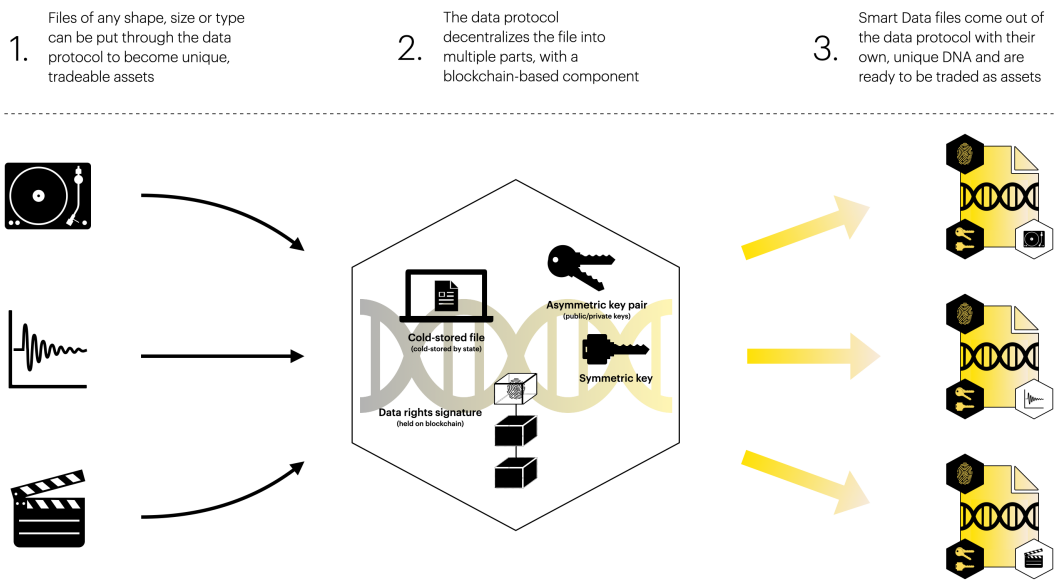

Figure 3: The data protocol converts a file of any type into Smart Data, creating a blockchain-based Data Rights Signature (DRS), a cold-stored file (cold-stored by state, rather than by location) and encryption keys (symmetric, asymmetric) that allow for the movement of the DRS on the blockchain and for the access & control of the cold-stored file, imparting excludability. Smart Data files are encoded, via the DRS, with a unique binary encoding that imparts rival character to the digital asset and its own, machine-readable identity.

protocol is able to assign one or more identities to an asset uniquely and automatically on a machine level.

Digital ownership

This ability to impart a unique identity to data and to consign the record of that identity to an immutable ledger allows for a form of ownership that is identity-based rather than access-based. The Smart Data file is a new approach to data that ensures that access is no longer the defining characteristic of ownership, with a form of binary DNA constituting the unique identifier and allowing for verification of the owner without granting access to the content.

The data protocol employs public encoding and private encryption to create a signing scheme for data, that, when combined with the unique binary DNA of the file, protects the owner and secures the file in an identity-based form of cold storage. The signing scheme carries over the uniqueness of the binary DNA in order to ensure that every part of the file retains its identity and any identity-based data rights that have been programmed into the metadata.

Identity is just one part, however, when enabling data to be owned in the digital world. Blockchains provide decentralized ownership, but files, with their infinitely-variable content, are not suitable to live on a blockchain – they are digital objects, and contain binary data, which needs to be preserved across a communication channel, and properly stored. However, there is a solution: the file can be *governed* from the blockchain, in a way that preserves the key aspects of ownership

that exist in the physical world, which we boil down to the following elements:

1. Being able to demonstrate uniqueness
2. Access & control
3. Protection of content (where relevant)

The first two requirements are fulfilled for on-chain assets on standard blockchains, because the ledger accounting ensures that each is tracked and identified across its entire history (regardless of its fungibility or non-fungibility) and the cryptographic public/private key pair allows the holder of said key pair to move or onspend the on-chain asset. However, they are not preserved for off-chain files. The third requirement does not apply to the typical coins or tokens found on a blockchain, because there is no 'content', in any meaningful sense, to protect. However, this third requirement would apply to a file under blockchain governance, particularly if privacy was a key concern.

The Zenotta data protocol preserves these key ownership elements for off-chain as well as on-chain assets by (i) encoding the file with a unique encoding scheme, which is encrypted and placed on the blockchain as a data rights signature (DRS), (ii) asymmetric encryption keys, allowing the owner exclusive control of the DRS on the blockchain, plus the ability to decrypt the DRS with a symmetric key, and (iii) an additional symmetric encryption key to obfuscate the content of the file from anyone but the owner.

Realizing True Value

In our current digital world, the only value that really exists is in the form of monetary value; cryptocurrency tokens, in-game items, reddit karma points, etc. This is a narrow definition of value. True value can be found not only in an economic form but also in forms such as the benefit of being able to truly own your digital content; the importance of retaining absolute privacy over your data; the legal power of an autonomous file with a unique identity; the freedom to create, and to decide what happens to your creation.

Type of value	Real-world instance
Economic value	Goods & Services
Social value	Identity & Sovereignty
Legal value	Governance, Rights & Obligations

The categories of value listed here constitute the trifecta created by the ZDS when applied to data. Each category has a different role to play in our society, and in an increasingly digital society we must ensure that these roles function as intended.

3.2 The universal ledger

The vast number of innovative projects within the new blockchain paradigm have enabled decentralized money (Bitcoin, and many many others), decentralized contracts (e.g. Ethereum, Neo, EOS), and more recently, decentralized finance (e.g. Augur, Kyber, Compound, UniSwap). Every blockchain up until now has, however, been a form of gifting economy, with only the payment token tracked on the ledger; any movement of the item that was paid for is either down to trust or the engagement of a third party. The Zenotta system provides a bi-directional accounting, through the **universal two-way ledger**[6], of both the payment AND the asset, facilitating a real economy for the first time. The seller pledges to the network a real asset (which would take the form of a Smart Data file created through the Zenotta data protocol) and the buyer pledges some native tokens. Through the dual double entry blockchain ledger, both halves of the trade are authenticated and the transaction is packaged into a block where the Smart Data asset and the tokens used to pay for the asset are exchanged between two wallets simultaneously. In the advent of any error or lack of correct authentication, the trade would roll back to the seller, who would simply retain possession of their provably scarce Smart Data asset, while the buyer retains possession of their tokens.

Ensuring that both the payment, and the goods, are transferred through the blockchain completes the role of blockchain as the backbone of a decentralized economy, enabling **decentralized trade** of goods & services.

3.3 The Pisces network

The Zenotta network protocol consists of semi-permissionless hybrid architecture (termed 'Pisces' architecture, as shown in Figure 5) employing the following node types:

1. **Mempool nodes** that handle block creation, through packaging transactions
2. **Mining nodes** that handle block mining, through next-generation Proof-of-Input and modified Nakamoto consensus
3. **Ledger storage nodes** that handle block writing, adding new blocks to the historical ledger
4. **Intercom nodes** that allow for the matching of trades between users, and maintain a public transaction list
5. **User nodes** that connect to the network in order to submit transactions

The mempool nodes package transactions/trades sent to the intercom nodes by the user nodes into blocks and send the blocks out to the miners. When the miners have completed their mining consensus along with all verification checks, the mempool nodes add the mined block to the blockchain by sending it to the ledger storage nodes. The mempool nodes and ledger storage nodes interact with each other via the Raft consensus mechanism in order to maintain a single chain, while the mining nodes perform Proof-of-Input (PoI) consensus (see next Section) to preserve Byzantine actor Sybil resistance.

[6] technically speaking, a **dual double entry** ledger

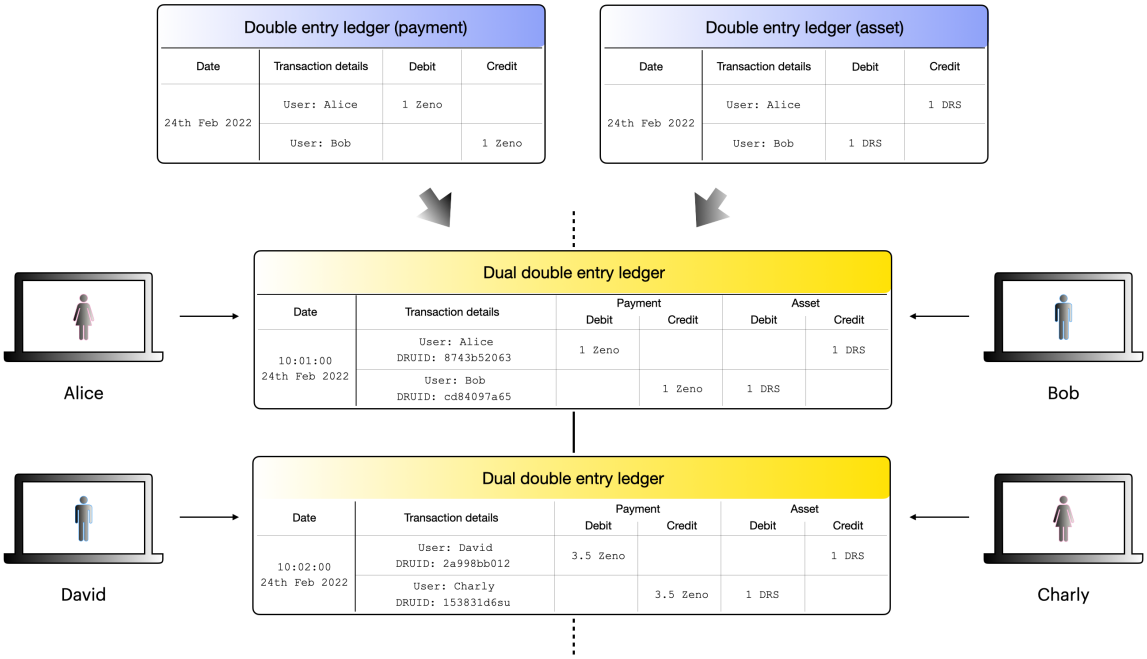

Figure 4: The *dual double entry ledger*, which tracks the payment and the asset separately and combines them atomically. The process of matching the two histories of the payment and the asset, at the moment of trade, enables a dual accounting system and allows for asynchronicity between the two halves of a trade. The unique network architecture that allows the mempool nodes to function as a decentralized trustless transaction notary, timing the two inputs and folding them into a single trade. Note that previous ledger approaches in cryptocurrencies and blockchains revolve around standard double entry ledgers, which only deal with unidirectional information, limiting the function of machine-executable trade for digital assets.

An extremely important aspect of introducing specialized, governing nodes is that they do not invalidate the nature of a blockchain as a decentralized, distributed system for processing transactions. We ensure this through the use of uncontestable randomness (Lenstra & Wesolowski, 2015) in the choices that the mempool nodes make in terms of (i) transaction selection for packaging into blocks (ii) miner selection for each mempool node partition and (iii) winning miner selection from the list of valid submissions. This means that at every stage, any decisions made by the mempool nodes are fully and verifiably fair, without bias or any chance of malicious or selfish behaviour, and can be checked (audited) by any and all nodes in the mining network.

This specialisation allows for transaction block handling, validation and processing to be optimised, taking mining throughput from a few transactions per second to thousands, and allowing the Zenotta blockchain to operate with a 60 second blocktime. The use of sub-networks introduces a novel mechanism to enable compliance without introducing control. Data privacy, trade compliance and service levels as programmable elements introduced through a sub-network with fair, transparent governance properties have the potential to save enterprise significant time and cost while dramatically reducing risk.

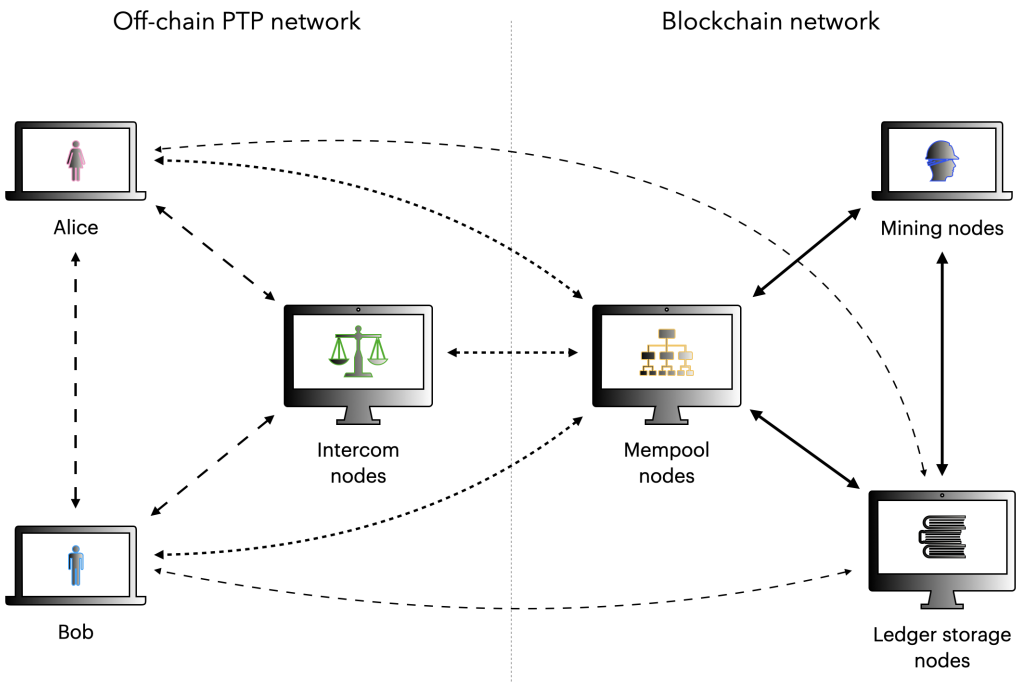

Figure 5: The network 'Pisces' architecture. User nodes Alice and Bob construct peer-to-peer trades via an off-chain pre-transaction processing (PTP) network, employing a series of public, permissionless and distributed intercom nodes, from which a decentralized ring of semi-permissionless mempool nodes randomly selects a transaction set to be packaged into blocks and sent to public, permissionless, distributed mining nodes to perform consensus, before the blocks are written to a decentralized ring of semi-permissionless ledger storage nodes. The choice of transactions is determined by independent contributions from the two distributed permissionless groups (users, miners) to an UNCOntestable Random Number (UNiCORN) seed, with verification and auditing performed by the distributed permissionless mining nodes. The 'on-chain' part of the network employs a three-tiered approach to vastly improve scalability and throughput over traditional approaches.

Optimising blockchain consensus for a real economy

Blockchain networks are rapidly becoming ubiquitous, and have been applied to a vast array of problems and a varied cross-section of industries. The very first blockchain was used in the creation of Bitcoin, and continues to power the leading cryptocurrency to this day. This inaugural blockchain employs the Proof-of-Work (PoW) consensus protocol, an invention that solved a long outstanding problem in computer science and ensures continued security through ongoing resource allocation.

Since the early successes of Bitcoin's blockchain, attempts to find better consensus protocols have spurred a renaissance of innovation. While obviously vital to the growth and development of the industry, there is a danger in abandoning the fundamental consensus philosophy that gives a blockchain network its power – Byzantine actor security through ongoing, operational resource cost. Miners must continue to put work in to secure the ledger against malicious actors, which limits the extent to which malicious actors can execute a sustained attack (namely, that they would have to expend ongoing resources in order to do so).

To this end we feel that abandoning Proof-of-Work is misguided. That does not mean, however that certain aspects cannot be modified in order to reduce the 'race-to-the-top' energy consumption often faced with PoW protocols. Just as in a responsible, functioning, fair society we do not allow runaway greed & monopolistic endeavours to dominate entirely, so too should the PoW consensus mechanism be tempered, to reduce monopolistic tendencies, prevent mining re-centralization, and avert adverse environmental effects (more on this in Section 4.2). However, the first question that must be addressed is that of scalability.

In dealing with data, rather than tokens, a blockchain network must be able to scale to many orders of magnitude higher in transactions per second than current Proof-of-Work setups. Data transactions would have a far higher velocity than monetary transactions, and traditional Proof-of-Work consensus approaches were designed to be deliberately slow, in order to give miners time to act in the event of a malicious party attempting to subvert the blockchain, and to provide a relatively equal opportunity for people to mine on standard spec. CPUs. In order to achieve this high scaling, we first reduce the role of the blockchain to only that vital task that needs to be sufficiently distributed in order to solve the Byzantine Generals' Problem and achieve the required trustless security: block verify (mine). The other two roles, namely block create (package transactions) and block write (store on the ledger) can be handled by smaller, decentralized rings of dedicated nodes (as described above, these dedicated ring networks employ Raft consensus to reach agreement on the state of the information that they contain).

Separating out these three roles vastly simplifies and speeds up the mining throughput. Transactions per second can conservatively reach into the tens of thousands, while the Byzantine security of the ledger is preserved. Specialised nodes fulfilling each of the roles can perform their tasks in a dedicated fashion and communicate in parallel where possible, achieving optimal load-balancing and efficient time utilization.

Proof-of-Input: a re-imagined mining consensus approach

The key innovation provided by Proof-of-Input, however, is that while blockchains typically ensure unbiased randomness in the selection of transactions that go into a block via a resource-intensive race[7] that on average, selects a different random leader to package the block each time, there is another, more direct way to ensure this randomness in transaction selection. The use of an UNCOntestable Random Number (UNiCORN) seed allows for the transactions themselves to be chosen randomly, with the input to the generation of the UNiCORN coming from independent contributor groups (the users and the miners) in the previous block. In this way the role of mining, while still an important part of consensus, is reduced to a contribution set informing the fair, unbiased, verifiable random selection of transactions.

The verifiable nature of this random selection is a key element in ensuring that the decision-making and censorship resistance remains with the distributed, permissionless nodes (the miners). The Pisces network architecture makes use of a modified form of Nakamoto consensus – the heaviest chain rule – via competitor mempool and ledger storage ring pairs. While the main mempool/ledger storage ring pair acts as a single source of truth for the ledger, vastly improving transactions per second (TPS) and throughput, additional 'shadow' rings keep the main ring pair from exerting power over the selection of transactions. In the unlikely event that the Raft consensus fails to stop malicious actors in the main mempool and ledger storage rings, the

[7] or a hierarchy, in the case of Proof-of-Stake

verifability of the UNiCORN process (which includes public data gathering and verification) allow the miners to switch to a shadow ring, within a blocktime, and for the path of the ledger (the block history) to follow such a change when the majority of miners decide upon it. This combination of Raft consensus and modified Nakamoto consensus allows for the Pisces architecture to achieve scale for global economy while remaining secure.

A peer-to-peer electronic trade system

The combination of the data protocol, the universal two-way ledger, and the Pisces network gives rise to the first *peer-to-peer electronic trade system* for the movement of digital goods & services across Internet-enabled communication infrastructure. Solving the problem of transferring items of value across the Internet (the 'data double-spend problem') through giving practical ownership rights to digital assets, moving those rights on a consensus-defended layer-1 blockchain, supported by a scalable network architecture, makes peer-to-peer digital trade a reality for the increasingly digital world.

3.4 The legal framework

The Zenotta Digital System brings the digital and the legal worlds together by accepting that the digital system must comply with legal requirements of the applicable national and international law. Thus, all legal acts executed on the digital level can be drafted and coded in a legally valid manner and kept compliant to the applicable law, and are therefore executable. It is an interesting observation that many other digital systems are conclusively judged by national jurisdictions in conflicts with mandatory law or between participants in these systems. By accepting the primacy of national law, the Zenotta Digital System shall be judged in its own legal system because it can itself enforce applicable law and administrative orders.

We use the term 'law' for any statute of a legislator from any jurisdiction, in whatever form the legislator has expressed its intent, and the term 'private legal act' in the sense of any expression of a legally valid will by a natural or legal person; if two (or more) persons express a mutual will, they are bound by contract, if a person expresses their will in the legally binding form of a vote, this leads to a legally valid resolution by vote if the correspondingly specified requirements of a successful vote are met (e.g. statutes of a company), or a person can draw an option through a private legal act.

Each legally valid right or obligation is embedded in one or more jurisdictions and can be expressed by text, code, and other means of expression such as signs, gestures, plans, documents, or circumstances. Law and private legal acts are binding for both natural and legal persons, which requires a clear assignment to the corresponding (real and digital) identity and an analysis of its legal capacity. A digital legally relevant system must therefore be designed for seamless interaction between both text and code and further be able to integrate these other expressions of intent of legislators and will of persons, so as to maximise the respective advantages of law and private legal acts written in text and in machine-executable code. This allows a future-proof, staggered approach towards a digitalized law without an additional risk to the subjects of the law.

The human understanding of expressed legislator's intention or person's will is the ultimate guideline in the interpretation of law and private legal acts, which finally enables the largely automated digitalized application of laws and private legal acts. After clarification of the actual

intent of legislators or will of persons using the available facts and all methods of interpretation, the execution of the rights and obligations derived therefrom can be achieved in finite time and finite numbers of instructions. Thus, the Zenotta Digital system makes a clear cut between (i) the programming of law, rules, and private legal acts (as Smart Data contracts) in a Turing-complete programming language on a separate system layer, and (ii) the execution layer on the blockchain, where the pure execution commands are programmed in a stack language, so enabling the update during the run-time of private legal acts. These two lawyers linked by various check-modules so that the user can check for himself whether the contract is executable and compliant. For this purpose, not only will the individual program tools be expanded step by step, but a 'LawHub' platform will be set up, which will allow the law community to upload their own codifications of law, rules and terms and also to exploit them commercially.

The Zenotta Digital System implements (i) an efficient dispute resolution process with an inherent human-based arbitral proceeding and a legally valid interface to state jurisdiction, and (ii) an efficient internal enforcement process to comply with administrative orders of state authorities, both to be executed on the execution layer of the blockchain. This integration into the established global legal framework ensures that the digitalized transaction is more than a risk-allocation among creditors and debtors which determines the role of Claimant and Defendant in a court or arbitral proceeding outside this digital system.

In summary, the fully-adapted legal environment for data connects with all three layers and ensures that any and all Smart Data transactions across the network conform with privacy requirements while being fully compliant with any applicable national and international laws.

Chapter 4: The Zeno

A medium of exchange for digital assets

A native Internet protocol for the transfer of value naturally requires a means to assign that value. Moreover, for a thing of value – an asset – to be traded, it needs a medium of exchange. In the blockchain space, the nature of 'asset' and 'coin' is often confused, since most cryptocurrencies treat coins as the assets themselves. With a real economy in the digital space, with distinct assets in the form of digital files, the coins become a medium that enables asset trade, and the Internet Transaction & Trade Protocol (ITTP) becomes the first Internet protocol to employ a native currency in order to effect that trade.

Implementing this approach avoids the paradox whereby the 'token economics' has no basis in the value of assets (and uses as a medium of exchange the 'thing of value' itself – the token (or coin) – creating something of a circular economic motivation). With proper blockchain governance of files and the cryptocurrency used as a medium of exchange, tokenomics can refer to the actual economics of a cryptocurrency; one that is used to pay for goods & services.

Zenotta's tokenomic policy emphasises fairness and maximization of distribution, with long mining timelines (approx. 200 yrs), a large number of coins (10 billion) and a more inclusive mining algorithm (see Section 4.2) The desire or demand for assets rather than purely for coins creates a highly liquid market, and with the Zeno traded for Smart Data, there is a strong incentive to use the currency rather than merely 'hodl' it. This increases distribution drastically over standard cryptocurrencies.

4.1 Issuance schedule

Zeno issuance follows a fixed supply cap mechanic according to the properties outlined in the following table:

	Number of Zeno
Total cap	**10 billion**
Treasury (*Zenotta Holdings AG*)	2.5 billion
Mining cap (*Miners, mempool nodes, ledger storage nodes*)	7.5 billion

The total number of Zeno coins reached will be 10 billion, with 2.5 billion reserved for a treasury that is sub-divided into separate funds/allocations as shown in Figure 6.

Treasury funds as a percentage of the the total supply are a standard feature of any cryptocurrency go-to-market procedure, in order to provide the bootstrapping phase of the project with sufficient funds to develop the necessary technology, and to act as reward and incentivization to the initial developers and founding team for the work put in thus far (which in the case of Zenotta is several years of development prior to going to market). In this regard the issuance and vesting timescales has been designed such that the allocation percentage of the circulating supply that goes to the founding team is at all times less than the amount of coins accumulated by the miners and is at most 10% of the total supply.

The remaining 7.5 billion is mined out via a smoothed issuance curve based on the emission approach employed by the CryptoNote protocol. The smoothed issuance is designed to minimize the volatility seen in standard halving mechanics whereby the reward drops suddenly by half on a particular date. The Bitcoin stock-to-flow model lends support to the idea that this sudden reduction in supply is at least partly responsible for the extreme bull market/bear market cycles.

The sub-unit of the Zeno is the zent. A number with a large number (90) of divisors was chosen as the conversion factor between the zent and the Zeno:

	Coin sub-unit
1 Zeno	25200 zents

This particular conversion factor is the 24th antiprime, or highly composite number, in the sequence of positive integers with a greater number of divisors than any smaller positive integer. This antiprime number has 90 divisors, and 9 prime factors. The use of a number with a large number of divisors facilitates the use of fractional payments without the need for rounding. At the same time we stay within the bounds of the `u64` integer type employed in our codebase for the total cap in zents of 10 billion $\times$ 25200 $= 2.52 \times 10^{14}$.

The block reward in zents is calculated using the total Zeno supply and the current Zeno supply in the market via the following formula:

In a practical network protocol, issuance must be implemented using bitwise operators, in order

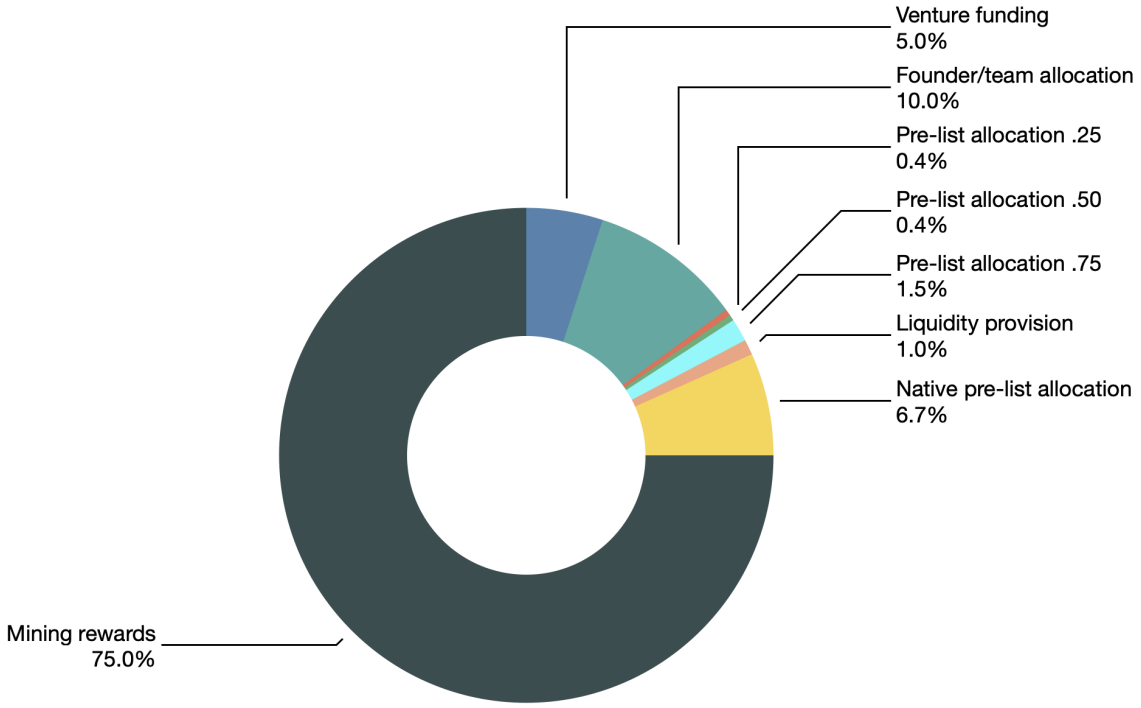

Figure 6: The allocation of the total amount of Zeno issued in terms of mining rewards (74.5%), stakeholder allocations inc. liquidity provision (10%), founder allocation (10%), initial supply (0.5%) and venture funding for projects built on the Zenotta blockchain. Pre-list allocations are specified in terms of the value they are sold at (0.25, 0.50, 0.75, in CHF).

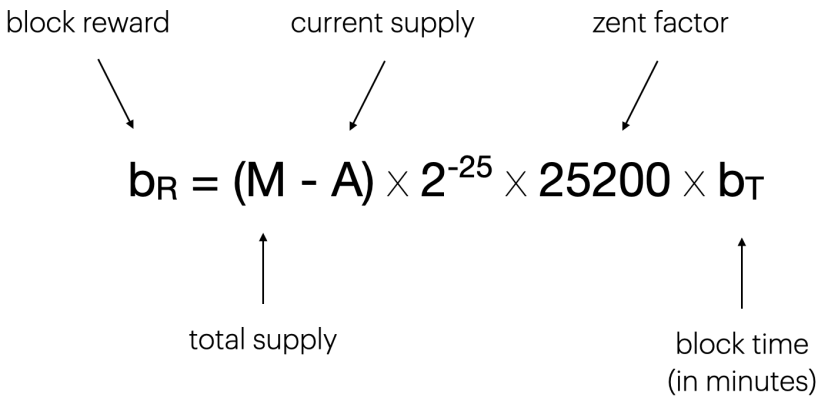

Figure 7: The equation determining Zeno issuance, based on the CryptoNote protocol.

to ensure consistent performance across different hardware types. This allows operations to be

performed on the bit level and therefore proceed at the maximum possible speed. Additionally, this approach ensures the consistency of floating point operations across different architecture types. In Bitcoin and bitcoin-like protocols this manifests requiring the block reward to drop by half (the 'halving') every n blocktimes. This is due to the bitshift operator being applied to the block reward (the left-hand side of the equation). We apply it to the recursive right-hand side of the issuance equation, which allows for a smoothed curve without the sudden halving jumps that likely have undesirable economic properties due to sudden supply shocks. Therefore, the block reward in zents (for a 60 second blocktime) is given in practical terms by

$$\text{reward} = (\text{total supply} - \text{current supply}) >> 25. \tag{1}$$

The issuance curve is shown in graphical form in Figure 8. The emission is divided into two parts, with the miners taking the majority and the mempool and ledger storage nodes being allocated a small percentage that varies over time.

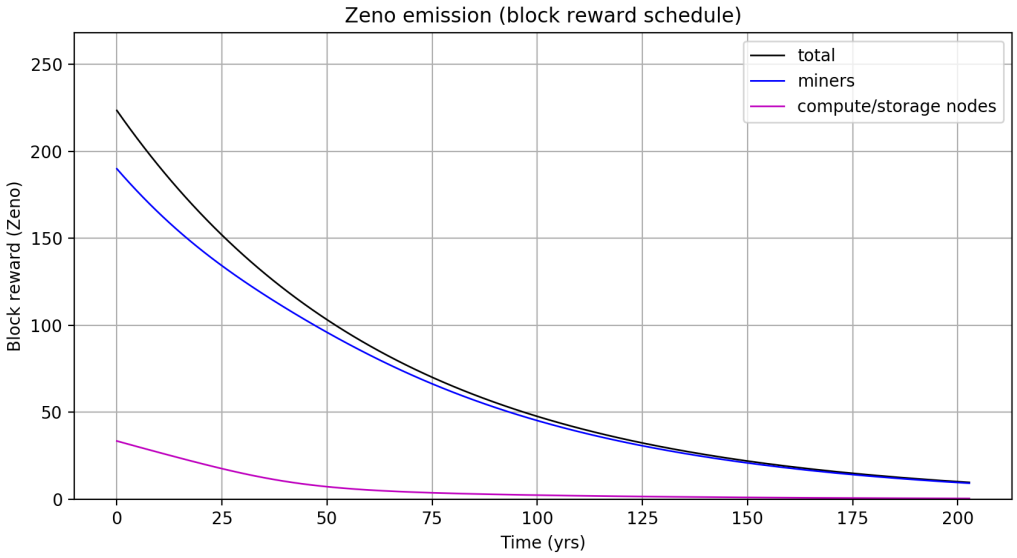

Figure 8: The issuance schedule for the Zeno in terms of the block reward, divided into miners (blue line) and the mempool & ledger storage nodes (magenta line) with the total for the network (black line). The issuance is smooth, rather than proceeding via the standard halving mechanic, in order to minimize the chance of extreme bull/bear market cycles driven by supply/demand shocks.

The fraction of the issuance allocated to the mempool and ledger storage nodes follows a reverse logistic function, starting at 15% and varying smoothly to 5% over a period of approx. 100 years. This is to reward the mempool and ledger storage nodes for the larger role that they play in the initial years of the network, and to recoup large capital costs, and to incentivize miners to play a larger role in the network later on.

4.2 Economic policy

The economic policy of Zenotta is focused around the goals of (i) coin value as a function of real economic activity and (ii) maximization of distribution. The Zenotta data protocol that allows for the creation of Smart Data assets is intrinsically linked to the Zenotta network protocol and the miners via a Socratic approach to democracy – if you put the work in to help secure the ledger, you earn the right to create tradeable assets. This keeps incentives aligned and ensures a healthy level of informed participation.

An economy based on (distributed) goods & services

Boom-bust cycles in the mainstream global economy are largely due to a form of money creation that is funnelled into financial speculation rather than the creation of goods & services or productive innovation. Financial crashes – the 'popping of the bubble' – harm everyone, even those who were the architects of the bubble, unless they are among the lucky few to see it coming and get out at the right time. The trend of the 'too big to fail' banks creating money for risky, speculative investments that do not increase GDP has eroded the function of banks from helping the economy to harming it.

"More than 70% of all lending – actually way more than that – is money creation for financial transactions; for asset transactions; for purchasing ownership rights. Now, then you have a problem. Why? Because you are creating new money, but you are not creating new goods & services. You are simply giving somebody new purchasing power over existing assets, and therefore you must push up asset prices [...] and that also creates the inequality – when the banking sector has focused too much on unproductive lending." – Prof. Richard Werner, episode of RT UK.

The crypto economy is still new and largely untested; however, it is thriving. The problem, though, is that money creation in the crypto economy has similar problems to those described above – when new tokens are created, usually as part of the block reward, there is no corresponding increase in goods & services, beyond the function of the relevant blockchain network as an effective, fair, and efficient money transmitter. Ethereum's world computer (and subsequent variants that have emerged) can arguably be said to funnel money creation into innovation (although most of that innovation to date has been to develop more ways to create money or increase speculative activity).

In the Smart Data economy provided by Zenotta, the creation of new money through mining can quickly and easily feed into the creation of Smart Data goods and services. Smart Data is itself created through the process of either mining or verifying the ledger, through a system of *create credits* whereby miners or those running a full verifying node are awarded the right to create Smart Data assets of their choosing (in other words, they are awarded with the ability to convert files into Smart Data files that can be traded on the Zenotta blockchain). In order to facilitate trade of Smart Data assets (goods & services) the Zenotta blockchain ledger is a new design of ledger that incorporates a *dual double entry* accounting of both the payment and the asset, such that the trade proceeds two-way, with both halves notarized by the blockchain. This makes the Zenotta blockchain a **blockchain for trade** rather than merely for payments.

The nature of data assets; namely, files, as the digital good being traded for in the blockchain ledger ensures a real and considerable level of *a priori* distribution and decentralization. Everyone with a computer has a substantial number of files, and through the *create credits* system of

validating or mining a small part of the network, coupled with the balanced mining approach outlined in the next section that reduces the vast inequality in mining power to acceptable limits, access to the 'thing of value' – the file – is far more distributed than any other type of good or service in any other economy (crypto or otherwise). Therefore, the economy provided by the Zenotta Digital System contains within it the ideal of equality of opportunity from the very start.

The value of an asset in any economy (for example a coin, or a token) can be expressed by the well-known formula below:

$$\text{token value} = \frac{\text{economic activity}}{\text{circulating token supply} \times \text{consumer token velocity}}$$

In the crypto space, the numerator of this equation is something of a problem. Since there is no (or very little) economic activity by the usual definition, assigning value to a crypto coin is difficult. Ultimately it is set by the market, but this is a price-based definition of value rather than a fundamental one. In the Zenotta digital economy, Zeno coins can be used to purchase Smart Data and to provide the 'gas' for Smart Data contracts. With the Zeno coin, the economic activity is real, and therefore the value of the Zeno has a direct link to the value of the Smart Data being traded. The total value in the Zeno currency is therefore more akin to that of GDP, namely the GDP of the Smart Data economy.

The disinflationary mechanics of the issuance (the 'smoothed' halving) employing an extremely long timescale are designed to be preferable to either a pure inflationary or a deflationary issuance approach. Disinflationary mechanics ensure that the purchasing power of the currency is more & more protected over time, while still encouraging spending rather than holding. Inflationary mechanics simply erode purchasing power constantly, while deflationary mechanics act in direct opposition to the use of a currency, namely, to be spent on goods & services.

In our disinflationary issuance approach, the inflation rate starts off initially relatively high in order to encourage the spending of the Zeno currency and kick-start the Smart Data economy. Over time, and as the Smart Data economy matures, the purchasing power of the Zeno becomes more protected. This design focuses on increasing the demand side of the supply/demand equation, which through the provision of actual goods & services, creates a market and an incentive for the average consumer to buy the token, rather than just the risk-taking speculator. This means that the volatility (which of course cannot be predicted) is likely to be less extreme than if the market was driven by speculators alone.

With regard to the value equation, our approach centers around the fact that the key to the adoption of a currency is demand. Purchasing tokens for the purpose of using them to buy goods & services has a strong net positive pressure on the demand side, and is far stronger as a means of value protection than merely swapping currencies, in particular when the goods & services are priced in the token.

A distributed mint

For a blockchain-based economy the 'mint' is not a central body. Coins are created through the mining protocol and awarded to the miners upon winning the block. In this way we have a distributed mint, and so coin distribution begins in an already distributed state (relative to a central bank driven economy). We further optimise this distribution at the mint level by employing a thermodynamic-like protocol that brings the mining power of the entities in the network closer to balance, via a peer-to-peer algorithm. This approach increases the decentralization and distribution of mining power, which increases the security and the efficiency of the network, as well as the decentralization and distribution of the mining reward.

The full technical description of the balancing protocol is the subject of a separate paper, but briefly, the block processing power of the network (the 'node temperature') is moved towards a homogeneous distribution by decreasing the effective hashrate of the 'hot' nodes (the more powerful processors) and increasing it for the 'cold' nodes (the less powerful processors). This is done smoothly, allowing our node temperature quantity η to change between nodes pairwise using a simple differential equation, which for miner A takes the form:

$$\frac{d\eta_A}{dt} = -\alpha\Delta\eta \tag{2}$$

where $\Delta\eta \equiv \eta_A - \eta_B$, and α is a normalisation constant. As a result, the algorithm avoids a centralised controller and operates autonomously.

The desired end-state of the network is not one where the effective hashrate is completely balanced (which would bring its own undesirable economic properties and increase the attack surface for Sybil attacks on the network) but rather in-between the two extremes of the proportional model (where the probability of finding a block is proportional to hashrate) and the homogeneous model (where the probability of finding a block is equal for all participants) at a point where distribution is maximised and excess energy usage is minimised without increasing the net attack surface.

The tendency of the centralization of Proof-of-Work mining to grow over time is caused by an incentive structure that rewards those parties that succeed in gaining an exponential advantage over others. ASICs cost typically 10-100 times what a CPU costs but deliver a hashrate (at the time of writing) some 10^6 times larger. This advantage, and exponential ROI, which plays out on a far larger scale with mining farms, drives huge investment, both financially and in terms of energy consumption, into developing more powerful and effective processors. These processors consume vastly more energy than standard chips (CPUs, GPUs) and come with additional requirements such as heavy-duty cooling and large amounts of space. The race to develop ever more powerful versions also has a high capital cost in terms of resources – financial, energy, components, materials, human labour, etc., driving up the centralisation and the effect on our planet.

Re-aligning and reducing these incentives to put the power back in the hands of individual miners simultaneously reduces these centralization and excess energy consumption tendencies. For more information the reader is directed to the Zenotta whitepaper.

Chapter 5: An Integrated Ecosystem

Inter-layer relationships for a complete, compliant digital system

Naturally, the protocol layers of the ZDS are themselves intertwined, and together form an integrated system that functions as a digital ecosystem. For example, the ability of the network to achieve optimal decentralization through a thermodynamic balancing approach (refer back to Section 4.2) ensures that endogenous bargaining power in the governance layer remains fairly distributed, and provides a means to future-proof this fair distribution by ensuring a persistent, generalized resistance to the 'technology attack'[8]. As argued in her speech entitled *'Running on Empty: A Proposal to Fill the Gap Between Regulation and Decentralization'*, SEC Commissioner Hester Pierce makes it clear that the very nature of compliance and the applicability of securities laws have their roots in the state of the network:

"...token transactions would not be securities transactions if the network has matured into a decentralized or functioning network on which the token is in active use for the exchange of goods or services. To assess decentralization, the team must consider whether the network is not controlled and is not reasonably likely to be controlled, or unilaterally changed, by any single person, group of persons, or entities under common control." – Hester M. Pierce, SEC Commissioner, 2020

The Zeno coin satisfies both of these proposed requirements – the mining network is likely to be fundamentally more decentralized and distributed than a standard Proof-of-Work (or indeed Proof-of-Stake) network due to the anti-centralization pressure exerted by the balancing protocol, and it is used to trade and exchange goods and services based on Smart Data.

5.1 Bridging the gap to traditional finance

A further function of the network protocol layer that arises from the coordinating nodes and subsequent ability for live monitoring of the state of the network is the ability to offer service levels for the transfer of Smart Data assets; a party executing a particularly large or important transfer may wish to ensure that the network has reached a sufficient level of decentralisation and/or environmental efficiency before it is carried out. Such a function is easily programmed into Smart Data assets within the data protocol layer, opening up the playing field for institutions that are required to meet certain standards to issue products on the Zenotta network.

More generally, the nature of Smart Data combined with the universal two-way ledger creates a framework for ownership and trade that is **free of smart contract risk**. The Smart Data asset can be created and traded directly on the Layer-1 blockchain through an application programming interface (API), without a smart contract, with the transaction protected by distributed consensus. The execution of the logic, whether simply for trades or for more complex Smart Data contracts (that may wish to incorporate future conditions) occurs **on-chain** rather than inside a virtual machine (VM). This is made possible by the contracting framework, which uses BitML (Bitcoin Modelling Language), a process calculus that allows for contracts to be written as programs executable via individual (consensus-defended) transactions.

[8] the technology attack, in a similar vein to the 51% attack and the Sybil attack, attempts to gain dominance over a larger section of the network through improvements in processor design, which reduces decentralization in the network and therefore the ability of the network to function as an effective solution to the Byzantine Generals' Problem.

Fundamentally, contractual agreements between two parties require knowledge of what is transferred between both parties, in **both** directions. The two-way ledger enables this. Combined with the form of ownership offered by Smart Data, which embeds the three ownership pillars of (i) uniqueness (ii) access & control (iii) privacy into the data itself (the interested reader is referred to the Zenotta whitepaper) this allows the behaviour of the asset, and the behaviour of the rights to that asset, to move concurrently across the Internet under the direction of the owner. The completeness of the information about the assets and the trades as held on the blockchain ledger opens up a role of the blockchain **as an oracle** for contracts and decentralized apps (dApps). Rather than merely utilising oracle data from external sources to inform the operation of a contract or the execution of a dApp, the blockchain itself contains sufficient information about the history and validity of an asset to function as the source of the input for risk determination/intelligence (e.g., a credit rating).

Putting this altogether means that the entire pipeline of financial products, from (i) risk assessment to (ii) the creation of financial instruments through to (iii) transaction processing can be handled end-to-end by the Zenotta layer-1 blockchain with little to no smart contract risk, and on a machine level, allowing for huge efficiency and scalability. Typically, smart contracts using blockchain technology are complicated to write, expensive and slow to audit, and risky to implement. Zenotta's blockchain network makes use of API integration with coordinating nodes that process data and contracts through direct payment-like instructions. The use of the intercom nodes allows for light touch regulation when listing digital assets on a distributed marketplace, and for the provision of services provided by individuals (anyone can run an intercom server and contribute to the distributed marketplace).

The somewhat fantastical picture of a blockchain as entirely separate from the world around it, and beholden to no laws, is inherently self-defeating. Blockchains exist to be used, but the privacy and sovereignty of the user must be protected as much as possible. Law is inevitably embedded in a functioning society through one or more legal systems that influence all legal relations. The Zenotta blockchain network will give rise to a new, Smart Data economy, and therefore a means to govern the network and ensure legal compliance is essential, a job that will be performed by the mempool nodes. However, the implementation of this governance remains at the behest of the relevant stakeholders (the users and the miners). From the use of UNCOntestable Random Numbers (UNiCORNs), for ensuring fair and unbiased verifable selection of transactions, fully auditable by the miners, to the application of sanction lists at the direction of the user, the use of such specialized nodes enables compliance while ensuring **governance without control**.

References

Lenstra A. K., Wesolowski B., 2015, A random zoo: sloth, unicorn, and trx, Cryptology ePrint Archive, Report 2015/366, `https://ia.cr/2015/366`