Abstract —
Rapid advances in decentralised technologies such as blockchains have put within grasp solutions to complex information asymmetry problems found in supply chain management; and solutions which may be Pareto-optimal and have a Nash equilibrium.

We have proposed a radical implementation of a new supply chain management architecture using blockchain 2.0, P2P storage, and RFID technologies. This implementation, called Zillerium, would further act as an infrastructure for a supply chain management economy with marketplaces, price aggregation services, reputation systems, business intelligence, data mining, supply chain finance, and P2P insurance. This information economy would use Zillerium tokens as a currency to buy and sell services.

1. Introduction

The supply chain is a complex global network of companies providing finished articles and commodities to consumers which is managed by Supply Chain Management (SCM) architectures. We propose a new SCM architecture called Zillerium which optimises supply chain integration using emerging and advanced technologies such as RFID, blockchains, P2P storage, smart contracts, and oraclizes.

We have designed an architecture which combats counterfeiting, enables better stock control, lowers costs, reduces wastage, and increases trust throughout the supply chain. Our design especially allows companies in developing nations to more safely trade, and provides a bedrock for a raft of new architectures to be built on top of Zillerium such as ones enabling marketplaces, data mining, price aggregation, P2P insurance, business intelligence, reputation systems, and better communications. These additional architectures are outside the scope of this document, and their mention is only to underline that Zillerium is the basis of considerable further growth and trade.

We therefore propose a Zillerium token called the Supply Sovereign to be the basis of the Zillerium architecture which would be used to reward active participation in Zillerium. This token would then be usable to pay for services connected to Zillerium and using the range of Zillerium based services including SaaS (software as a service), DaaS (Data as a Services), APIs, SDKs, and RFID management systems. Hence a BI provider would be able to utilise data via Zillerium by using DaaS and paying a fee based on time or data flow. This fee would be payable in Zillerium tokens. In this way, an economy around Supply Chain Management would develop which would extend to value chains, and consumer based systems such as e-commerce.

The structure of this document is to introduce high level theories which underpin the theoretical basis of supply chain management; and then to describe the supply chain, and aspects of it; we then will outline some of the key elements of blockchain related technology; and finally propose our solution.

2. Information Asymmetry

Information Asymmetry refers to unequal information available to two parties in a contract. It is part of information economics. Information Asymmetry is described by Gresham's Law, signalling, and principles of trust.

2.1. Gresham's Law

Information in a sales of goods process is asymmetric, favouring the seller [15] which gives rise to the opportunity that a bad seller may drive market prices down by misrepresenting the goods they sell (Gresham's Law [14] as applied by Akerlof [13]). This impact is so severe that honest traders may be forced into insolvency by the dishonest ones and hence the entire market is affected. The impacts of dishonesty are especially felt in developing nations.

Akerlof considered that trust is a key factor in sale of goods and trust may be strengthened via a guarantee to offset the effects of Gresham's Law. Trust when not reciprocated drives the market to distrust (as the trusted party is betrayed and their trust is used against them) [16]. Therefore only when trust is reciprocal can a market built on trust exist.

2.2. Signalling

Signalling refers to observable actions taken by economic agents to convince the opposite party of the value or quality of their products [17]. Therefore, we would expect a seller to provide information to their advantage at the expense of the buyer's interests.
2.3. Information

Information alone has limited impact on the supply chain but information accompanied by trust and trustworthiness has a significant impact [12].

3. Game Theory

Game theory is the methodology of using mathematical tools to model and analyze situations of interactive decision making. These are situations involving several decision makers (called players) with different goals. This interactively distinguishes game theory from standard deviation theory, which involves a single decision maker, and is its main focus [68] [69].

Game theory may be applied to Theoretical Economics and Supply chain management [?].

3.1. Nash Equilibrium

Pareto - Optimal Nash Equilibrium.

4. Supply Chain Theory

Inventory cost is a significant cost to a retailer and optimising this cost is vital to lowering their costs. The optimal case for making decisions is when the retailer has access to all information via centralised control. But in a supply chain, there is no agent who controls it, and each agent acts to according to their own incentives and hence we have decentralised control. The main purpose of the supply chain contract is to overcome double marginalization. This may be achieved by channel coordination: i) determine optimal solution under centralised control, ii) apply game theory to the decentralised model and determine if a Nash equilibrium exists, iii) match the decentralised solution to the centralised one. We refer to Chinchuluun et. al. for this analysis [67].

Consider retailer orders \( x_i \) sold at \( r_i \); the manufacturer has a cost \( k \) for the product and supplies \( x_i \) units at a cost \( c_i \).

\[
R_i = w_i + \beta_{ij}(w_j - x_j)^+ \tag{1}
\]

Theory of Constraints
Utility Theory
Push, Pull Contracts, ADvance Option contracts
Satisficing - decision making

5. The Supply Chain

The supply chain (SC) consists of suppliers of raw materials, food producers, manufacturer of finished articles, component manufacturers, warehouses, distributors, logistics companies, and retailers. They add value via their individual value chains and hence the supply chain is a combination or chain of value chains, each value chain adds value to goods [48] [46].

Virtually all agricultural, energy, and industrial commodities must undergo a variety of processes to transform them into consumables. These are classified as transformations in: i) logistics, ii) storage, iii) form (e.g. refining) [47].

Components are used to construct a finished product, for example electronic parts in a computer, or engine parts in a car. Logistics is very expensive and considered to be unsustainable in its current form [44].

5.1. Supply Chain Levels

The supply chain is broadly classified into 4 levels describing the level of integration.

<table>
<thead>
<tr>
<th>Supply Chain Levels</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Limited integration</td>
</tr>
<tr>
<td>2.0</td>
<td>Digital Internet Integration</td>
</tr>
<tr>
<td>3.0</td>
<td>Physical Internet Integration</td>
</tr>
<tr>
<td>4.0</td>
<td>Industry 4.0 integration</td>
</tr>
</tbody>
</table>

The Physical Internet is an open global logistics system founded on physical, digital, and operational inter-connectivity, through encapsulation, interfaces and protocols [44]. Just as the digital internet achieved integration via standard protocols (TCP/IP) between heterogeneous networks, the physical internet can achieve integration via standard containers and smart objects allowing improved logistics.

Supply Chain 4.0 is defined as the supply chain managed by Industry 4.0 Innovations, with increased customer satisfaction [45].
5.2. Food Safety

Food contamination is a serious problem in the supply chain accounting for widespread illness and death ([54]). The WHO reported that 600 million people get ill from food contamination.

5.3. Fake Medicines

Fake medicines have been a serious problem for decades ([52]). Measures to combat fake medicines include the implementation of e-pedigrees and electronic product codes (EPCs). Mackay et al. established that blockchains could be used to: i) trace raw materials in an immutable and shared e-pedigree based digital ledger, ii) authentication by blockchain users, iii) IoT devices to prevent fake medicines, iv) open standards technology to enhance information sharing.

5.4. Bullwhip Effect

5.5. Industrial Revolutions

We have observed four industrial revolutions take place, with the fourth one impacting the world at an exponential rate [55]. Industry 4.0 is concerned with smart devices, nanotechnology, Internet of Things, Industrial Internet of Things, and quantum computing.

6. Supply Chains & Currency

6.1. Appreciation & Depreciation

Currencies may be affected by actions of central banks. As currency exchange rates change, so do the aggregate imports and exports. We may say: A currency depreciation should raise net exports and therefore increase aggregate demand; conversely a currency appreciation should reduce net exports and therefore decrease aggregate demand [71]. This is because currency appreciations and depreciations affect international relative prices of goods.

6.2. Central Banks

Central banks affect currency depreciation by buying a foreign currency for example US dollars. The People's Bank of China has done this to undervalue the RMB against the USD [71]. For example, this was done by the central bank in China instructing large state owned Chinese banks to aggressively buy the US dollar [72].

As an example we may consider the soybean market. RMB undervaluation has had significant effects on the world soybean and soybean products markets [73]. Therefore currency affects the supply chain and so does the role of central banks.

7. Internet of Food

As food is such an important commodity, we present a section detailing the food chain and its inadequacies.

7.1. Food Chain

The food supply chain is global and complex, and demands on integration are so high that competition is seen in terms of supply chain A competing with supply chain B. Consumers now demand such high levels of food safety that food safety is a requirement and not an advantage [28].

These changes and evolutions in food supply have placed pressure on all actors to share information, and the entire market of traceability has developed leading to the concept of “farm to fork.”

7.2. Food Traceability

Consumers today demand verifiable evidence of traceability as an import criterion of food quality and safety [30].

Traceability was researched by Lindh et al. [28]. It consists of two key elements: local and chain. Local traceability refers to tracing ingredients in one branch of the supply chain; chain traceability refers to movement of products within the entire supply chain.

To effect traceability in the supply chain is challenging and requires information integration between actors in the supply chain.

7.3. Inefficiencies

Waste can be reduced via supply chain integration [29]. Waste is a significant problem in the supply chain with approximately one third of all food produced for human consumption being lost or wasted [26].

7.4. Additive Manufacturing

Additive manufacturing (AM), the process of joining materials to make objects from three-dimensional (3D) model data, usually layer by layer, is distinctly a different form and has many advantages over traditional manufacturing processes. Commonly known as "3D printing," AM provides a cost-effective and time-efficient way to produce low-volume, customized products with complicated geometries and advanced material properties and functionality [34].

Although separation of product design from manufacturing capabilities is a major advantage of Additive Manufacturing (AM), the impact of AM is not only...
limited to the design and manufacturing stages. In addition to the freedom of design such as elimination of design constraints, material saving, and free complexity, AM offers other potential benefits to the manufacturing industry as well. One of the most immediate potentials of AM is the possibility of more efficient logistics and improvement in production systems [35].

Therefore, with customization we have the prospect of an infinite number of goods being accessible to the consumer via additive manufacturing. This raises the question of identity for the new products and trust related to their identity and their quality. For example, a decentralised AM process could be contaminated and the consumer would be placed at risk. Hence the trust issue then relates to the actual process, the machines used and the condition of them. This is how the traditional supply chain is assessed as a parallel, in that the equipment is also part of the supply chain.

8. Supply Chain Management

Supply chain management (SCM) is the management and control of all goods and information in the logistics process from acquisition of raw materials to delivery to the customer [50]. We describe some of the key issues hindering SCM enhancements.

E-commerce is part of SCM in terms of web e-commerce and EDI [25].

8.1. Communication

Costs of communications in the SC are high and poor sharing of information and data across the SC has hampered efficiency and provided a significant barrier to cost improvements and benefit to the consumer. Suppliers are sharing information but they still distrust information from other suppliers, and one poorly managed supplier can impact the entire SC due to the interdependent nature of the SC [8].

Trust is an important factor in a buyer-supplier relationship which may enhance performance [18]. Khan et. al considered that real-time integration of information systems between the buyer and supplier was important to improving performance along with improving the buyer-supplier partnership; they also discovered that technological advances impacted the delivery of real-time information sharing systems.

8.2. Trust

Trust is defined as an expectation that an actor will be relied upon to meet their obligations in a predictable manner and they will negotiate fairly [19]. Trust speaks therefore to future events. It is a measure of confidence that an expected action will happen. Trust is an important factor in the SC and it mitigates risk from opportunistic actions. Trust will improve efficiency and performance in the SC.

8.3. Market Demands

SCMs gained acceptance following Forrester's paper in 1958 [7], and during the 1960s onwards to the 1990s, SCM was more widely adopted. Following an increased global market demand causing consumers to expect lower prices and quicker delivery times [6] pressure has been placed on SC participants to innovate their SC.

8.4. Synchronization

Synchronization across the supply chain has been identified as a step to reduce costs and meet market demand from the supply chain [8]. Fredendall et al. concluded that to treat the entire supplier chain as a single entity meeting market demand would improve costs and benefit to the consumer. Such an synchronized architecture would use constraints management and synchronous flow.

Information Technology would play a central role in integrating the supply chain especially with real-time information sharing to improve transparency [9]. Pareto analysis has shown that an uncoordinated SC is not efficient as a Nash Equilibrium may not be Pareto Optimal [22].

There are a number of ways to optimise supply chain stock and costs: 1) Quantity Discounts, 2) Backup Agreements, 3) Buy Back, 4) Return Policies, 5) Quantity Flexibility, 6) Incentive Mechanism, 7) Revenue Sharing. These optimisations may be effected using supply chain integration of information.

8.5. Globalization

The supply chain has greatly grown in complexity as globalisation has increased 140 times since the mid-1800s and world's population has grown six times during the same period [61].

The ownership and growth in the use of smartphones (more than 25% from 2013 to 2015 in many countries [62]) is also affecting the supply chain as users get more access to information, finance, and buying options.

9. User Identity

9.1. Internet of Identity

The term "internet of identity" was stated as a requirement to counter lynchpin concerns expressed in an MIT report following a meeting between AT&T; MIT; IBM; Mastercard; Qualcomm; and US Department of Treasury and Commerce officials. The concerns were
based on a person’s or an organisation’s inability to own and assert identity attributes [27].

The MIT report also cited that identity plays a crucial role in enabled blockchain technology. Auditability and credibility are needed to form robust and trusted identities.

9.2. Identity Management Systems

A number of identity management systems are available using blockchain technologies, such as uPort and shocard [40] [41].

uPort works via a proxy smart contract in Ethereum, and that address is the user’s unique 20 byte string which is persistent and global. Interactions with other smart contracts are via the proxy contract and the user’s private key; hence the user’s identity is known to other contracts.

10. Product Identity

10.1. GS1

GS1 is a neutral, not-for-profit, international organisation that develops global standards and solutions to improve efficiency and visibility of supply chains across industries [42]. The Aberdeen Group discovered that of 100% of top performers only 20% had full compliance to GS1 standards, and 80% maintained just 25% compliance.

10.2. Barcodes

One-dimensional (1D) bar codes have existed since the 1970s, and they typically refer to a key in a database. Two-dimensional (2D) barcodes increase the capacity of 1D barcodes [64]. 3D barcodes have developed too.

10.3. RFID

RFID and NFC have gained widespread adoption due to their capability to act as a ubiquitous computing tool [65]. The cost of RFID is high compared to barcodes but costs are predicted to fall as cost in microelectronics and low-power semiconductor technologies drop.

11. RFID

An RFID system uses radio frequency (RF) to communicate between receivers and transponders. An RFID system has three basic components: i) tags (transponders), ii) readers (receivers), and iii) a database [49]. There are three types of tags: active, semi-active, and passive. Passive ones are the most popular as they do not require a power source and they are the lowest cost ones to make.

RFID technology implemented on the supply chain has been far more effective than barcodes ([?]): accuracy, reliability and efficient are all improved. There are some problems with RFIDs related to cost (higher than barcodes), interference when numerous tags are read, and privacy invasion. Also metals and liquids may disrupt RFID signals.

11.1. Barcodes

RFIDs are superior to barcodes. Barcodes have limited data storage capacity and are susceptible to counterfeiting ([52]).

11.2. Matryoshka Implementation

The Matryoshka concept proposed by Gaith et. al. ([49]) may counter some of these problems. Their proposal consists of classifying tags by levels, and assigning a mute/un-mute function to prevent various RFID tags being read and hence interfering with the reading of large numbers of tags.

Under the Matryoshka implementation goods are all tagged, and then tags assigned to pallets, and then finally to the container of the pallets. Therefore, there are three levels of tags. The lower level ones are muted after being read and they are linked to the higher level tags.
11.3. Large-Scale Systems
Since the cardinality of the products can be extremely large, collecting the tag information directly from each of those tags could be highly inefficient. Zheng researched large-scale RFID systems using compact approximators to reduce for scans [66].

11.4. Authentication
Authentication may be achieved by using crypto-tags with secret keys. But these tags may be resource intensive for the RFID system and also they may be compromised by side channel attacks [53].

12. Blockchain Ecosystem

12.1. Permissioned and Permissionless
Blockchains may be permissionless (open to everyone) or permissioned (controlled access).

12.2. Transparency
Presently many companies maintain their own proprietary database systems which are not shared with other companies. A blockchain implementation would allow a company to use data which was shared by all participants of the blockchain. If a permissioned one were used, then the blockchain could be private. Such an implementation would negate the need for companies to maintain their own databases and hence they could significant cost reductions.

The blockchain also provides greater transparency and hence issues such as notary and provenance may be confirmed.

12.3. Sybil Attack
A sybil attack is one based on an entity forging multiple identities to subvert a network [23].

12.4. Zero-knowledge
Zero-knowledge proofs are proofs under which is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true.

Everything is provable by zero-knowledge proofs [24].

12.5. Hash
A hash function takes as input an arbitrarily long document D and returns a short bit string H. The primary properties are ([36]):

- Computation of Hash(D) should be fast and easy, e.g. linear time.
- Inversion of Hash should be difficult, e.g., exponential time. More precisely, given a hash value H, it should be difficult to find any document D such that Hash(D) = H.
- For many applications it is also important that Hash be collision resistant. This means that it should be hard to find two different documents D1 and D2 whose hash values Hash(D1) and Hash(D2) are the same.

A hash is a cryptographic primitive.

12.6. Hash Pointer
A hash pointer is pointer to the storage location of some data and also a cryptographic hash of it the data [37]. Since hashes are collision free we can confirm the data was not changed by checking the hash was not changed.

12.7. Hash Chain
A hash chain is the successive application of a cryptographic hash function to a piece of data. Hence is we have some data (s) and we have a Hash function, then $h_1 = H(s)$, and $h_2 = H(h_1)$ [38]. As the hash pointer to the previous element is stored in the current element, if one link in the chain is changed, the hash pointer will be invalid and hence the change will be detected.

12.8. Merkle Tree
A merkle tree is a data structure to store hashes of data elements to form a root which may then be checked to confirm the integrity of the all the data elements. To construct this tree, we can consider a data element $D_i$ in a collection of data elements N. If we split the population of elements into pairs and then recursively hash the pairs we will eventually get just one hash [39].

For example, if we had 10 data elements, we can create 5 pairs and then 5 hashes. We duplicate the last one to make an even number of hashes, and hash again to get 3 more hashes. Then we repeat to 2 more and then finally one hash. Therefore, the entire data structure of 10 elements (transactions) may be reduced to just one hash.

If we have two sets of transactions we wish to compare to ensure they are identical then we may just compare the root of their respective merkle trees to confirm they are identical.

12.9. Blockchain
The blockchain is made up of blocks and each block has a header which has a merke tree root. This may
be used to confirm that any two blocks have the same data. This concept is then applied to store the hash of the block and the header in temporally later blocks and hence a chain of blocks are created which are integral. This creates the immutably characteristic which is widely associated to blockchains. Simplified Payment Verification (SPV) is an implementation constructed from just headers and hence just the merkle tree root is used in verification that a transaction exists via an merkle path.

12.10. Private Key

A private key is a random number. It is hashed to form a public key which then hashed again to form an address for the blockchain [39].

12.11. Trust

Blockchain represents a technology innovation that enables transparent interactions of parties on a more trusted and secure network which distributes access to data. Although the technical components have been in existence for decades, blockchain qua blockchain is a novel, resilient, and ubiquitous approach to data, transaction analytics and networks. It holds the potential to address inefficiencies, reduce cost, unlock capital, improve trust in societal fabric, and open new business models. It also could accelerate the growth of the informal economy or even criminal elements of societies, complicating efforts of governments to provide security and safety to their citizens. Like any new technology, it holds the potential for good and for harm, and benefits from an enlightened, informed, and ethical application by its users [63].

13. Blockchain Enterprise

The limits of ethereum were discussed by Marek Laskowski ([33]) and he underlined the need for an Enterprise Ethereum. The Enterprise Ethereum Alliance (EEA) was founded by Accenture, Banco Santander, BlockApps, BNY Mellon, CME Group, ConsenSys, IC3, Intel, JP Morgan, Microsoft, and Nuco, with a view to provide enterprises with resilient secure systems and a robust controls environment under Ethereum.

13.1. Offchain Solutions

The scaling inabilities of well known blockchains such as Bitcoin and Ethereum are well documented [31]. Solutions for this problem were led by the Lightning Network team [32] in 2015, and more recently by Brainbot Technologies with the development of the Raiden Network.

13.2. Raiden

Raiden is a technology that leverages off-chain state networks to extend Ethereum with properties for asset transfers: i) Scalable: it scales linearly with the number of participants (1,000,000+ transfers per second possible) ii) Fast: Transfers are confirmed and final within the fraction of a second iii) Confidential: Single transfers don't show up in the global shared ledger iv) Interoperable: Works with any token that follows Ethereum's standardized token API v) Low Fees: Transaction fees can be 7 orders of magnitude lower than on the blockchain vi) Micro-payments: Low transaction fees allow to efficiently transfer tiny values Technology

The technology enabling this is similar to the proposed Bitcoin Lightning Network. The basic idea is to switch from a model where all transactions hit the shared ledger on the blockchain (which is the bottleneck) to a model where users can privately exchange messages which sign the transfer of value.

Raiden uses a network of p2p payment channels and deposits in Ethereum to preserve the guarantees expected from a blockchain system.

Raiden is implemented as an extension to Ethereum. A Raiden node runs alongside an Ethereum node and communicates with other Raiden nodes to facilitate transfers and with the Ethereum blockchain to manage deposits. It offers a simple API which makes it easy to use Raiden in DApps.

13.3. Raiden Applications

Micropayments for content distribution: Alternative to Paywalls, Ads and Subscriptions. (Figure a decentralized youtube where the creators of a video are paid for every second watched) Decentralized M2M markets: especially in IoT where tiny chunks of bandwidth, storage, cpu time, energy, sensor data, etc. can be traded.

Frictionless Token Systems: Game Tokens, Reward Tokens, Private Currencies API Access: Accessing and monetizing APIs on a per use basis is at the core of the upcoming Machine-to-Machine economy Fast Decentralized Exchanges

Complementary to Ethereum Vitalik Buterin: "State channels are an important technology that has the potential to greatly improve the scalability and privacy of many categories of blockchain applications; in conjunction with sharding and other privacy-preserving cryptographic technologies, they are an important ingredient in helping decentralized systems to achieve the properties that mainstream individual and institutional users expect and deserve."
14. Zillerium Solution

14.1. Raw Material

14.2. Component

Components are used to build a finished articles. Components have their own supply chain. To show how Zillerium would treat data about components, we consider an example. Part Number 36309000 identifies the Digital Controller from Grohe. This item is a component of the 36292000 but we have no further breakdown of the 36309000. Often suppliers do not reveal their sources of components or they do not know them.

We propose storing in P2P storage component details in sufficient detail to identify them.

14.3. Product

A product is an article which is manufactured to sell. A product may certain defining characteristics, such as a description, photograph, technical drawing, part number, spare parts, ingredients list, list of the materials used in its construction, weight, size, certificates of approval (eg CE), links to other products, brand name, installation guides, and other similar details.

This level of detail will vary depending on the nature of the product and the nature of the manufacturer.

If we consider an example, of a Grohe product called - F-digital Veris F-Digital Digital controller for bath or shower - with part number 36292000 and an EAN 4005176894640, we find that a wealth of information is available. The table shows the components making up this product.

<table>
<thead>
<tr>
<th>Components</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. MOTOR</td>
<td>42337000</td>
</tr>
<tr>
<td>2. retaining ring</td>
<td>47765000</td>
</tr>
<tr>
<td>3. Thermostatic compact cartridge 3/4</td>
<td>47881000</td>
</tr>
<tr>
<td>4. Solenoid valve</td>
<td>42340000</td>
</tr>
<tr>
<td>5. Non-return valve</td>
<td>47753000</td>
</tr>
<tr>
<td>6. Digital Controller &amp; Remote Controller</td>
<td>36309000</td>
</tr>
<tr>
<td>7. Connection wire</td>
<td>47727000</td>
</tr>
<tr>
<td>8. Transceiver</td>
<td>36356000</td>
</tr>
<tr>
<td>9. Plug power supply 230 V</td>
<td>65790000</td>
</tr>
<tr>
<td>10. Plug power supply 110-240 V</td>
<td>36078000</td>
</tr>
<tr>
<td>11. Uninterruptible power supply</td>
<td>36394000</td>
</tr>
<tr>
<td>12. Connection wire</td>
<td>65815000</td>
</tr>
<tr>
<td>13. Socket Spanner</td>
<td>19332000</td>
</tr>
<tr>
<td>14. Holder plate for Digital Controller</td>
<td>40710000</td>
</tr>
</tbody>
</table>

This main unit consists of 14 components. When the consumer buys 36292000 and gets all the components.

In our solution, the component list, and all details are recorded on a P2P storage system such as Swarm, or IPFS. A product identity is created and stored from key defining information, such as brand and part-number. The hash of this key data is the Universal Product Identifier (UPI).

The UPI is used to define the catalogue entry for this item.

A part often has options such as colour, finish, size, and these would all generate a new UPI.

14.4. Catalogues

Finished products are described in a product catalogue. A catalogue is therefore a collection of products from a particular brand. Catalogues are important for retailers who will have contractual rights to sell a particular brand. If for example a retailer is entitled to sell Grohe products (thousands of products) [57], then the retailer could list all the products at an e-commerce solution provider such as Shopify [58] or via the retailer’s own website using a Content Management System [59].

As we have already defined how product details may be stored on P2P storage storages and identified by a UPI, we can then store all UPIs in a Merkle Tree for a certain brand, to obtain a root hash which is for the entire brand catalogue. This tree may be distributed to retailers who can then immediately confirm the entire catalogue is genuine (by comparing the root with a known root sent under contractual conditions) and also the entire tree defines the UPIs for the brand which enables the retailer to find all the UPI data and all the CMS data on P2P storage. This is an example of Data as a Service (Daas) [60].

Therefore, a retailer may be able to immediately build a CMS via DaaS and by using established services such as Shopify may very quickly build an entire e-commerce selling service at low cost and very quickly, and also without the need to employ specialists in software development. Additional services could filter data based on contractual conditions, so that the retailers sells only certain more profitable items and this opens the door to a range of additional services to filter data.

In this design, we store UPI data which is hashed to
form a root hash, which is then appended to a UBCI (Universal Brand Catalogue Identifier) with a version number, which consists of the hash of brand key data with the catalogue identifier (root on the Merke Tree) and a version.

If an attacker changed the UBCI it would be detected on the blockchain. Hence if a retailer knows the version number, and key identifiers (hashes) sent via a secure means under contractual conditions, the retailer has access to all the catalogue data which is immutable, shared, and global.

<table>
<thead>
<tr>
<th>Data Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>UUI</td>
</tr>
<tr>
<td>UPI</td>
</tr>
<tr>
<td>UPD</td>
</tr>
<tr>
<td>UBI</td>
</tr>
<tr>
<td>UBD</td>
</tr>
<tr>
<td>UBCI</td>
</tr>
<tr>
<td>IPI</td>
</tr>
</tbody>
</table>

### 14.5. Tracking Products

A product moves through the supply chain and in each segment of the SC, value is added by a respective value chain. The movement would be recorded by RFID scans, which generate a transaction stating the location of the product. Therefore, we can obtain the following:

Location Txn = Time, IPI, UUI, Location

This txn data forms part of an event chain which is recorded.

### 14.6. RFID Volume

One of the key challenges in processing RFID data is volume.

### 14.7. Blockchain Volume

We propose using the Raiden Network to handle the volume of transactions generated in the SCM.

### 14.8. Blockchain

### 14.9. Oraclize

Zillerium provides access so the SCM can access KPIs such as stock levels. The Oraclize [11] can record and respond to queries. If a supplier sells an item, then the sale could be record by a transaction or a delivery scan and this is feed into the Oraclize and then recorded. The SC Blockchain has data relating to the product and the product sale. For some data a permission restriction could apply. The UI has event listening and all NSCs are updated when there is a change in the blockchain.

Just as the nodes in a blockchain get blocks of data to confirm consensus, a similar concept with a different context applies to the SC in which NSCs all get access to KPIs on the SC and some of this data will be repeated (at least for two NSCs).

Hence, we are applying a similar consistency principle to the blockchain design. If nodes in the SC had differing information, then a real world error would have happened (eg goods not delivered but invoiced).

### 14.10. Data & IPFS

We propose using data designs already established by Mediachain [3] (open source at github). IPFS has certain characteristics and data in IPFS is: immutable, implemented in reverse-linked lists, and serialized to CBOR.

### 15. Tokens

The fundamental purpose of Zillerium is to move SCs to Pareto-optimality with a Nash equilibrium.

#### 15.1. Supply Sovereign

Each SC player may gets benefit from a transaction (selling) and a loss from buying. The difference between buying and selling is the gross profit. The selling price is driven by a market price but the buying price is affected by a price in the SC and subject to national factors elsewhere.

This creates risk. We propose create a SC token to reduce this risk, so buying and selling would be in a SC token.

#### 15.2. Asset Class

We recognise a new asset class - Supply Chain Efficiency.
15.3. Example

Information integration is a key element to making that happen. Therefore, participants who assist Zillerium in reaching its main purpose will be rewarded. The degree of reward will be calculated based on the degree to which others are affected and how much further optimisation they achieve (e.g., lower costs, better customer service).

Therefore, we apply the theories in Contract Theory, Utility Theory, Game Theory, Information Economics to determine the degree of benefit and this is quantified in tokens.

As an example, it is known that transparency improves efficiency. If therefore, a manufacturer in China open up its products to RFID tagging, that would be a benefit to others. Hence the manufacturer would receive a reward. The reward paid in tokens would be calculated by the impact of that action on the rest of the supply chain and calculated using information economics. If the action caused retailers to gain enormous benefit and generated higher profits, then the reward would be high.

Zillerium will charge transaction fees, and hence the increased volume would enrich Zillerium. Therefore, under this example, the manufacturer sells more goods and earns more profit, Zillerium gets more income from more transactions, and the retailers get more benefit, and the entire market grows.

Similarly providers could add services to Zillerium which when used would be rewarded. The resulting economy would be one based on optimising supply chain management as shown in the figure.

16. Summary

17. Conclusion

References


