Utilising Financial Blockchain Technologies in Advanced Manufacturing

White Paper

August 2008

Colin Andrews

Daniel Broby

Greig Paul

Ian Whitfield

Contents

1. Introduction

Blockchain is commonly associated with the transfer of digital assets. It is explained in technical detail in Appendix 1. It is essentially blocks of programing code that are securely linked together. In this way, a blockchain can deliver an immutable and irreversible record for digital assets and as such offers advanced manufacturing the promise of several practical applications. These include distributed record-keeping and online database management.

In this paper, blockchain is explored from the perspective of what can been learnt from research conducted in financial markets.[1] It is concluded that the digital aspirations of what has come to be termed *"Industry 4.0"* could be enhanced by the application of blockchains in advanced manufacturing. Our core finding is that blockchain can be used to provide advanced manufacturers with secure ownership verification, parts and order validation.

We have learnt from financial applications that blockchain can offer a robust and resilient method of record history indexing that can be distributed and stored over the internet. We advise, however, that It is not as scalable a storage tool, as is widely perceived. Stored information must be carefully considered by manufacturers. We suggest that it is its data management capabilities that make it useful in the advanced manufacturing.

In creating added value advanced manufacturing needs to create an audit trail. The blockchain aids in the identification and therefore elimination of counterfeiting. Also as a result of its digital record keeping properties, blockchain has many other potential applications. Its use adds rigour to the measurement and traceability that is required in manufacturing. We also believe it can facilitate mass customisation and can be used to track both "use" and "effect" in the supply chain, some examples of which we provide latter.

As in finance applications, manufacturers can utilise blockchain to see the status of payments, invoices, documents and digitalised data. In this way, it enables detailed visibility of a product's progress through the supply chain. The value to the supply chain is enhanced by the financial ability of the blockchain to store and process in different currencies. Through our research we have shown it can also provide a real time exchange of production information and documents.

As no one party can modify or delete any record without consensus, the level of transparency provided by blockchain helps reduce fraud and errors. We believe it can also reduce the time products spend in both production and storage. Blockchain therefore has the promise to improve inventory management, possibly even reducing waste, forgery and redundancy.

This paper proposes four advanced manufacture use cases to illustrate the potential of blockchain. The technology offers manufacturers a secure and transparent shared network. We believe blockchain also gives advanced manufacturers the ability to include suppliers in the production and supply chain. In this respect, it benefits from end-to-end visibility based on the level of permission granted by the manufacturer. Both the manufacturer and the supplier can use

---

[1] The testing we have done on the importance of precision timing in financial markets can be found in Appendix 3.

blockchain to view the status of goods through the value chain. This in turn sheds visibility on where components are in the value added process.

2.   What has been learned from finance

A number of lessons can be learnt from the research we have conducted into financial blockchains. This research focused on the analysis of time series, but we identified some cross disciplinary applications. In advanced manufacturing, time series are used in the control and service functions. The variables monitored in finance are digital assets.n manufacturing such diverse items as the diameter of precision components, the length of time to deliver the finished components, as well as the composition or concentration of those components.

The use of control charts which include time series with upper and lower limits is similar to financial time series. Variables such as the time it takes to process an order, the time when an order was received, and the shipment time are all incorporated into such data, although we appreciate that it is not a scalable storage tool.

Financial applications of blockchain can be divided into three core approaches dependent on how distributed their *modus operandi* is. They are either: (1) decentralised and based on proof; (2) hybrid based on validation; and, (3) centralised based on validation. The first is termed a public blockchain, the latter a private one, with the hybrid being a combination. The centralised version requires a high degree of coordination with suppliers. In our opinion, this is the most scalable for advanced manufacturing use cases.

The research on which we base many of our findings was very focused on time and order, rather than cryptographic properties. The research is documented and explained in Appendix 3. We undertook an investigation into the importance of precision time and the relevance of precision time stamping blockchains. Our focus was financial markets, order driven transactions, done over distributed ledgers using digital instructions. That said, we extrapolate the impact of our findings for advanced manufacturing in a cross disciplinary way.

One issue we identified which we believe is not widely appreciated is the impact of forking on the blockchain. This is where two valid blocks are produced at the same time and therefore tension is created in the network as to which of the next block lines is valid. We recommend case specific research be done in order to address this in advanced manufacturing usage.

Another financial lesson is the deflationary impact of disintermediation, the effect of cutting out the "middleman". We believe this will be the case in advanced manufacturing (see the case study on the £500 nut).

Blockchains relevance to advanced manufacturing is in the potential for distributed architecture marketplaces as well, as in linking the supply chain. This will be explained in the use cases below.

3. Litmus test

As with many new technologies, there is much hype surrounding blockchain and as such we apply a litmus test to our analysis.[2] A product or process must be logically improved upon (have value added) compared to other information management technologies to be regarded as something that can benefit from blockchain.

One clear thing we have learnt is that there are many mores ways in which Blockchain 'could' be used than there are ways in which it 'should' be used. Early implementers (Greenspan 2015) suggest using a checklist to help verify whether a proposed blockchain is viable and its usage a appropriate and we adapt this as our litmus test:

1. **Database** - we ask why an activity should use a database.
2. **Multiple writers** - we check that the manufacturing process involves more than one entity generating the instructions that modify the database.
3. **Absence of trust** - we consider the nature of trusted counterparties. If multiple entities are writing to the database, some degree of mistrust between those entities can be resolved by the use of blockchain.
4. **Disintermediation** - we apply the concept of disintermediation from finance. Blockchains remove the need for trusted intermediaries by enabling databases with multiple non-trusting writers to be modified directly. A good reason to prefer a blockchain-based database over a trusted intermediary might include lower costs, faster transactions, automatic reconciliation, new regulation or a simple inability to find a suitable intermediary.
5. **Transaction interaction** - we look for transfer interaction as blockchains are more useful to advanced manufacturing processes when there is some interaction between the transactions created by these various counterparties.
6. **Set of rules** - we ensure that there is a defined protocol. This is an inevitable consequence of the previous points. If we have a database modified directly by multiple writers, and those writers don't fully trust each other, then the database must contain embedded rules restricting the transactions performed.
7. **Sponsor** - we investigate what the nature of the assets being moved around is and who stands behind the assets represented on the blockchain? The complexity of advanced manufacturing demands that the blockchain have a trusted and defined sponsor.

8. **Validators** - we identify the validators because no matter which consensus scheme is used, the validating nodes have far less power than the owner of a traditional centralised database. Validators cannot fake transactions or modify the database in violation of its rules. Nonetheless there are still two ways in which validators can unduly influence a database's contents:

---

[2] Peat, J, Kelly, O & Broby, D 2017, *Fintech: Hype or Reality?* International Public Policy Institute Policy Brief, University of Strathclyde, Glasgow.

a. ***"Transaction censorship"*** where the validators collude maliciously, they can prevent a particular transaction from being confirmed in the blockchain, leaving it permanently in limbo.
b. ***"Biased conflict resolution"*** where two transactions conflict, the validator who creates the next block decides which transaction is confirmed on the blockchain, causing the other to be rejected. The fair choice would be the transaction that was seen first, but validators can choose based on other factors without revealing this.

Because of these problems, when an advanced manufacturer decides to use blockchain-based databases, they need to have a clear idea of who their validators are and why they trust them.[3]

Blockchain technologies are already being deployed in manufacturing. Some examples of blockchains usage include Rolls Royce and Keysight. Rolls Royce have developed it for online parts concessions and Keysight as a cloud based test and measurement tool, providing traceability.

4.   The benefits of using blockchain as an enabling technology

Blockchain is an enabling technology that can help to reduce the manual burden of compliance and inspection processes. It is valid wherever there are trust based relationships in the supply chain where performance must be transparent or is verified by a third party while maintaining confidentiality and/or intermediation.

An example is a company looking to source a logistics service where the shipment, say frozen food, never gets warmer than zero celsius. This can get an automatically verified via IoT technologies. Blockchain shows where this is the case, rather than selecting suppliers based on the judgement process of a human-based Quality Assurance procedure backed up with compliance audits (again human based).

Blockchain is a foundation technology that allows new value to be added in the product and service value chain. While the 'cost out' opportunity above can be postulated and initial trials made to closely model the costs and benefits we have learnt from finance that there is a 'value-in' opportunity that is much harder to identify and quantify before it has been invented. These opportunities are the province of tech-leading entrepreneurs but some potentials include:

- Better value realised from end-of-life product through an open market for 'cores', the term used for products to be remanufactured or recycled. Blockchain provides transparent

---

[3] Depending on the use case, the validators might be chosen as: (a) one or more nodes controlled by a single organization, (b) a core group of organizations that maintain the chain, or (c) every node on the network.

information on the cores' life history. The implication is that better maintenance of a product through life will lead to a greater return at the end of life.

- More responsive Maintenance Repair Operations where 'anyone' with access to the right blockchain can provide the services required at a given point in time. Payment flows with completed service or even individual service steps.
- Greater collaboration within industries to make most efficient use of available capabilities without the need to build trust with new collaborators OR trust in the judgement of existing collaboration networks.

4.1   Smart Contracts

Considerable attention has been paid upon the potential for blockchain technology to be used for smart contracts. A smart contract is essentially an agreement written in programing code and delivered by a blockchain. One of the most notable models for smart contracts is that proposed in the Ethereum project. While a full analysis of smart contracts is out of the scope of this document, a brief overview is given for context, in Appendix 2.

One key limitation of smart contracts is they cannot help enforce physical ownership rights. This is clearly an issue that advanced manufacturers need to be cognisant about. That said, we can see from financial blockchain that a party having possession of an item may still deprive another party of access to property, even if they themselves are unable to use it.

While this may render the property useless in some limited cases (such as a part cannot be manufactured), it cannot prevent the retention of the property (such as part stopped in production, or a part which has been placed into a shipping container). In such cases, the smart contract serves as a cryptographically signed proof of agreement between the two parties, and the matter would likely require escalation to a conventional court for resolution and remedy.   These can be used in advanced manufacturing, in an example learnt from financial applications, in multi-contract letters of credit.

From a technology perspective, smart contracts are often viewed as being outwith conventional jurisdiction, yet from a legal perspective, smart contracts must fall under a certain jurisdiction, such that there is a right to access to justice via a court of law, a fundamental element to ensuring the rule of law. The process of allowing a court to rule over a smart contract, where the terms cannot be altered, therefore presents a significant challenge for future research.

5. Existing Manufacturing applications for Blockchain.

In this section we explore uses of blockchain that have already been deployed in manufacturing. Some of these are commercially available at the time of writing, some are in use and some have been proposed but are not yet implemented.

5.1 Retail Product Provenance

Provenance is defined by the Oxford English Dictionary as "the fact of coming from some particular source or quarter; origin, derivation". There are a number of products and services on the market today whose value is linked to a greater or lesser degree by their 'provenance'. This may be fairly traded goods, or food stuff produced in a sustainable way, or products that do not come from textile sweatshops. Blockchain technology can be used to establish the provenance of advanced manufactured products.

There are a number of firms already operating in the context of blockchain technology being used for provenance[4]. Such companies focus on supply-chain accountability for products, work with suppliers to gather information from the supply chain process, and share this information with customers at the point of sale of the product.

Using this approach, blockchain can be used for the tracking of materials and products, and works at item-level. It provides a user-oriented experience, detailing key steps in the production of a product. For example, a specialist component part may see a registration of precise specification given by an end manufacturer to a supplier, and the resulting transfer and processing stages shown. The focus of Provenance.org (an established service provider) is on the user-facing experience, however there is little technical detail given of the implementation or capabilities of blockchain technology to the product, or indeed how this can be used for verification.

In this paper the supply chain is modelled as consisting of producers, manufacturers, registrars, standards organisations, certifiers and auditors, and customers. Registrars act as trust roots, verifying the identity and credentials of other named participants. Standards Organisations define requirements for a given approval (for example, no animal testing in pharmaceuticals), and these organisations allow for batches of products to be added to this group. The process of approval of a manufacturer for a given standard may require a certification or audit, which would be carried out by an auditor. A successful verification results in a manufacturer who is registered with the certification organisation, as well as a process that has been approved by an auditor.

---

[4] There has been relevant work by companies such as Provenance.org, BlockVerify, mPedigree, Chronicled, BitSE/Vechain, Raketa, Cubichain, and BlockRX.

Following certification, a producer now has an approved production programme, which is certified for a given production capacity over a period of time, such as a year. A description is then created of the goods, as well as any appropriate tags or certifications (Fairtrade, the Ethical Trading Initiative and/or theMarine Stewardship Council). As production occurs, produce is registered against the certified production capacity, Transfers of goods to manufacturers are recorded, and a manufacturing process requires the consumption of a given quantity of the raw material, which prevents that raw material's electronic record from being reused in another process.

Commercial providers of this technology instead claims to focus on the detection and prevention of counterfeiting, with an initial focus on pharmaceuticals, luxury goods, diamonds and electronics. They hope to identify counterfeit goods, prevent duplication of products, and to allow companies to register their own products and monitor their own supply chains. Specifically with regard to counterfeiting, such companies claim to be able to determine if a product in someone's possession is counterfeit, if a product was diverted from its original destination. If merchandise was stolen it can be traced using blockchain to track fraudulent transactions. While little technical details are given of the solution, and it appears to not yet be on the market, each final product is given a tag, and verified along the supply chain. Customers are able to verify and activate the products they buy, which appears to be designed to prevent counterfeits from cloning the identities of real products. What is not covered is how to prevent rogue registrations of a product which someone has access to, such as on a shelf.

Another commercially offered product is a supply chain provenance system.. One example for this incorporates a mobile phone-based platform integrated with a central registry of pharmaceuticals and drugs. Manufacturers using the technology upload information about each pack of medication they produce, and customers may use a no-cost SMS message to query the database at point of supply, to verify whether a particular packet is from a legitimate source. Each product has a unique serial number, beneath a scratch-off tamper-evident panel, allowing for verification to be carried out by customers at point of sale through a mobile phone. Successful validations return details about the manufacturer and expiry date of the medication, and unsuccessful verifications will alert the user to re-check the code, as it was not recognised.

An existing service aims to offer a digital identity and presence for physical devices. A secure microcontroller, incorporating a unique private key, is embedded into a label or sticker, which is designed to be damaged if tampered with or removed. Verification of the integrity of an item can be carried out by interrogation of the microchip, either through Near Field Communications (NFC) or Bluetooth Low Energy (BLE). One limitation of this is that while NFC is passive, BLE requires a power source. BLE is necessary however for support with iPhones, since they only allow NFC to be used for Apple Pay, and do not permit use of NFC by third party applications. The providers claims to use the blockchain to underpin the offering, building messages signed by the secure microcontroller of a device, to create timestamped and verifiable blockchain-based records of possession and provenance. The platform has been used for verification of authenticity of high-price trainers, helping to verify ownership, and to enable buyers to ensure they are buying legitimate trainers in second-hand markets, rather than fakes.

There is a further offering just coming to market that also involves the placement of a NFC tag within a product. An Android smartphone is used to read and verify the identity of the device. The public key within the NFC tag can be identified within the blockchain, and the private key can be used to attest to the identity of the product. Public keys are checked against platform providers servers, which appears to be a centralised process, in order to determine if a signed public key belongs to a genuine product. When products are moved or transported or otherwise manipulated on the supply chain, their identity is scanned, and this is used to form a blockchain-based history and trace of movements and processes. This can be used to track and verify luxury items such as designer clothing and handbags.

A final example is a luxury wristwatch manufacturer, which has incorporated blockchain technology into their manufacturing process, using technology from Emercoin. Each watch has a serial number assigned to it during production, and these are enrolled digitally into a blockchain-based registry. While few details are available of the solution, it appears that the manufacturer's approach is to use unique keys which identify each watch as being produced by the company, and enabling buyers to ensure serial numbers are not fake. Service and repair history, manufacturing information, and owner information can be included on the blockchain-based record if desired.

5.2   Generic product-centric use cases

The section above shows a number of blockchain-enabled services that are already on offer. There is also a growing number of generic use cases for blockchain within a manufacturing environment that have been identified in academic papers (e.g. Abeyratne and Monfared 2016) and internet blogs. Some key examples are below.

Transparency   in   the   supply   chain

The offerings above seek to make the provenance of goods more available to the end-user. This is a special case of a more general use for blockchain within a manufacturing supply chain – transparency.

As was noted in the introduction, advanced manufacturing provides an enhanced amount of 'value add' for the customer through its activities. This is achieved through the deployment of high levels of technology, skill and knowledge. In a traditional supply chain this is accepted by the customer based on trust in the OEM, and has led to some scandals in recent years involving global brands.[5]

The use of distributed ledgers and blockchain provides a way to address this gap between perceived trustworthiness and actual behaviour.   For example, an index of the parties involved in producing a product can be indelibly recorded in the product's blockchain. This capability can be extended to provide some supporting evidence of any claim made about products or services provided.

---

[5] Nike & child labour, VW and emissions testing

It is easy to imagine that as this type of verification becomes more prevalent, so the demand for it will increase.

Traceable Service history

Using blockchain enabled records of service activity on a capital equipment asset has already been identified as a potential use for the technology by a leading IT provider.[6] In the long life of a commercial vehicle the service history and parts used grows to be a complex pattern of use activity, servicing and parts replacement. With current technologies this requires discipline to maintain and is not difficult to counterfeit.

Blockchain solutions help by being essentially automated. Admittedly, the stakeholders still have to agree use of the blockchain but it maintains an unalterable index of events in which the sequence is maintained. This will support a more informed assessment of asset values throughout their life.

IoT enabled manufacturing

The Internet of things (IoT) is a developing technology trend that has been widely predicted and is now gaining traction with internet enabled 'app' controlled central heating for houses being a clear example.

The application of IoT within manufacturing is a natural step and examples of 'app' based interaction with production machinery exist today. A typical example is a CNC machine texting an operator when support is required for an upcoming tooling change. It can be considered part of the next generation of industry evolution (industry 4.0). Blockchain has been identified as a supporting technology for this.

Bahga and Madisetti (2016) propose a general purpose platform for blockchain use in the industrial IoT which enables 'on-demand' manufacturing. This has been variously described as cloud manufacturing and distributed manufacturing, and is typically considered to offer significant flexibility and cost advantages over typical manufacturing.

Blockchain-enabled Timing

High precision time stamping has proven to be critical within FinTech to remove one of the ways to circumvent market mechanisms during high volume trading. It is not envisaged that the same requirement will exist within advanced manufacture however it is clear that timing of transactions is important at some level of accuracy. The ability to agree the order of transactions on the blockchain will support better learning for continuous improvement activity, problem solving and issue resolution. If a 'bid - ask' market develops, the order in which bids were received will be important.

---

[6] IBM - https://www.ibm.com/blockchain/business-use-cases.html

5.3 Key features of Distributed Ledger use

Distributed ledgers have a number of advantages over traditional databases. Key features in terms of manufacturing in general (and advanced manufacturing in particular) are:

- Tamper resistance. The distributed nature of the database makes it very difficult to change records of past transactions.
- Built-in traceability. A corollary of tamper resistance is that traceability of transactions can be 'built-in' to the blockchain. Each transaction is recorded and cannot be altered in practice, so there is a trace of such transactions.
- Transparency in place of trust. Building upon the previous 2 features, the blockchain can be seen as a 'transparent' history of what has happened. This transparency can be managed to an appropriate level through the use of cryptographic keys e.g. the identity of parties involved in a whole supply chain can be revealed or it can be shown that a particular organisation was involved in many transactions without revealing who they are

These features are not yet all 'proven' in the manufacturing context. We attempt to assess the technology readiness level of these features below:

	Description	Blockchain Features
TRL 1.	basic principles observed	
TRL 2.	technology concept formulated	
TRL 3.	experimental proof of concept	
TRL 4.	technology validated in lab	
TRL 5.	technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)	
TRL 6.	technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)	Transparent not trusted: Technology shown by platform developers
TRL 7.	system prototype demonstration in operational environment	Traceability of transactions: IBM platform for transportation compliance, and multi-party interrogation of Product status

| TRL 8.	system complete and qualified	
TRL 9.	actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)	Tamper-resistance: BitCoins used in commercial environment. Tamper mechanisms proven not worth it for 'normal value' transactions

6.   Advanced Manufacture Use Cases

We chose our use cases based on the lessons we learnt from finance and the litmus case we applied. We begin with the circular economy, as an audit trail is something that is central to this concept.

6.1   Circular economy / Remanufacture

The term 'circular economy' implies a move on from a linear worldview where raw materials are extracted, processed, made into products which are then used and disposed of into one where the loop is closed by product value and material being recovered at the end of life.

Remanufacturing offers the potential to greatly reduce the resource burden of modern consumer lifestyles, while still providing the function and guarantees of new products. It is a growing industry with aspects apparent in many industries including automotive, electronics, capital equipment and aerospace and activity being carried out both by the original equipment manufacturers (OEMs) and third party service providers.

The figure below shows how remanufacture sits within the broader circular economy.
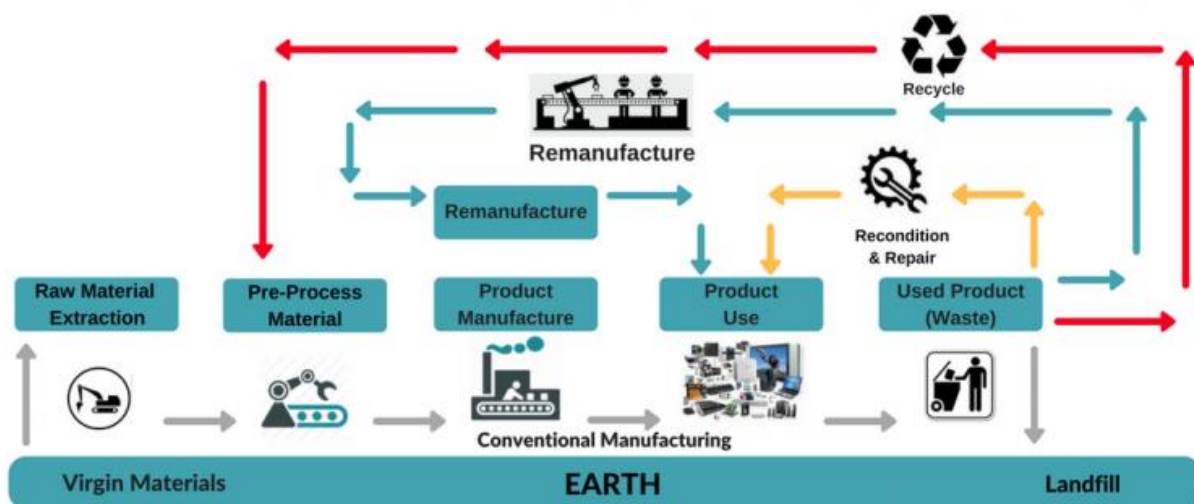
Adapted from W. Ijomah et al 2007

- **Remanufacture** returns a used product to at least as new performance specification and gives the resultant product a warranty that is at least equal to that of a newly manufactured equivalent.
- **Reconditioning** returns a product to a satisfactory working condition that may be inferior to the original specification and a gives a warranty less than the newly manufactured product.
- **Repair** corrects specified faults in a product and gives a warranty less than the newly manufactured product that may not cover the entire product.
- **Recycle**: Recovers materials for the original purpose or a new purpose.

A key success factor in any remanufacture chain is the condition and status of returned 'cores' - the items which will be remanufactured. Value chains where where remanufacturing activity is beginning to accelerate tend to be business to business as the more stable relationships provide some 'trust' that the returned items are correct.

A distributed ledger that records use and service records for a product offers a number of attractive features to a remanufacturer:

- A record of the specification of the core that is unchangeable (and accurate)
- More transparent information about the status of the core
- Clarity of the status of the core after remanufacturing (in support of warranty)

One of the contentious issues with remanufacturing is the status of the intellectual property around remanufactured product. Where the product is remanufactured by the original equipment manufacturer this is generally unimportant, but where the product is remanufactured by a third party, there are already disputes about using the OEM's name in association with the remanufactured product. Blockchain offers a mechanism to address the IP issue by:

- Providing secure access to product data that doesn't lead to counterfeit products. Remanufacturers can agree a maximum volume of products to be remade in a given period of time in return for access to product specification and performance data.
- Identifying that remanufactured products meet original specification / testing requirements (potentially through third party testing) and logging this information permanently into the blockchain.

6.2 Through-life Engineering Services

Complex products e.g. commercial aircraft, ships, power stations, are characterised by long operational life cycles during which the semi-independent systems which make up the product may need to be modified, repaired or replaced. Currently the management of the product configuration and related data is done via centralised Product Lifecycle Management (PLM) systems. These require sophisticated processes to maintain and manage and often need to be restricted in scope to be practical. Cases where PLM systems have been effectively deployed have tended to be in industries with long term stable customer / supplier relationships e.g. defence, power generation, rail.

Existing proposed uses of blockchain and distributed ledgers (product centric approach to data (Matilla et al 2016)) have given consideration to maintaining product information in a way that is independent of OEMs and can be updated through experience and service results by third parties. These proposals demonstrate that it is a possible use of blockchain and show how some disintermediation benefits can be accrued. An example might be for wind farm operators who have issues with operational data as Wind Turbine Generators complete their warranty period and are handed over to in-house operations from the original equipment manufacturers. A blockchain indexed service record would give a higher degree of assurance of what work had been done.

In complex products there are foreseeable benefits to blockchain use that reach beyond the PLM data environment:

- Validated data for condition monitoring. One of the limitations for data mining of operational logs is the fidelity of sequence data. The use of blockchains to record data has the impact of maintaining the sequence of events. With precision timing as used in finance applications, this can be maintained to a high level of resolution.
- Disseminated learning across dissimilar projects using common sub-systems. In the long lifetime of a capital project there will be a number of third party organisations working on the subsystems that comprise the whole. Any experiential learning will, at best, be applied to the site where it arose. A distributed ledger of the service history of similar subsystems in different products gives a huge learning resource and the mechanism for anonymously sharing it. Potential outcomes include updated running specifications across a fleet of subsystems (e.g. pumps).
- Maintained HAZOP validity. There is substantial complexity in maintaining the validity of the safety of operations in hazardous environments. Currently this relies on a combination of auditable processes and informed human judgement. In principle one can imagine a blockchain enabled Safety Management System that both confirms the validity of operating conditions and logs the activity in an unalterable system of events. This would be analogous to a flight data recorder for use when lost time incidents occur.

As can be seen, through life processes are well suited to blockchain adoption.

6.3 Product Service Systems

There is a growing trend for products to be provided as a service instead of sold to customers. The Rolls Royce aero-engine 'power by the hour' is one example as is 'software as a service' e.g. Office 365. These commercial propositions have their own logic and do not *require* a distributed ledger system to operate. However the use of blockchains does offer a number of potential benefits to Product Service Systems:

- Extension of product service systems to wider markets e.g. personal transportation. A single source engine supplier is able to control all the elements of the product service system centrally. In other markets it may be desirable to have a more complex product service system e.g. delivery transportation with multiple vehicle choices and distributed

service centres. In this case it is easier to produce an evolving and adaptive service using a distributed ledger across multiple parties.

- Disintermediation capability removes the brokerage role in a market. In any market where there is a brokerage role being applied, there is an opportunity to remove this (or greatly reduce it) through blockchain use. The broker is acting as a disinterested party between customers and suppliers, neither of whom trust the other, but both trust the broker. There are many trading platform examples such as the obvious Amazon and eBay, but also companies like Uber. Similar structures exist in the Finance sector, and blockchain has been shown to disrupt these.
- In a more general case, it is possible to envisage product / service solutions that are far more flexible and user focussed. This may be truly bespoke solutions, or mass-customised solutions based on mass manufacture elements. Users would submit requests for service into an ecosystem of service providers, equipment manufacturers

6.4   Blockchain and the Supply chain

Manufactured goods of all sorts are the product of lengthy and involved supply chains and this is especially the case for advanced manufacturing. The development and management of these supply chains has become a specialism in its own right, the techniques of which have more recently been adapted to incorporate digital and collaborative techniques. Such supply chains can be conceptualised according to the supply chain operations reference model (SCOR).

Each link in the chain has similar processes that are required to make the supply chain function e.g. planning activity, sourcing, making, delivering etc. The enabling activities cover all the other functions of each organisation e.g. personnel, finance, research and development. The end customer's plans are interpreted by the manufacturer in developing its plans and these in turn are developed by the supplier. These plans may be communicated at a range of detail from essentially none all the way to completely shared information.
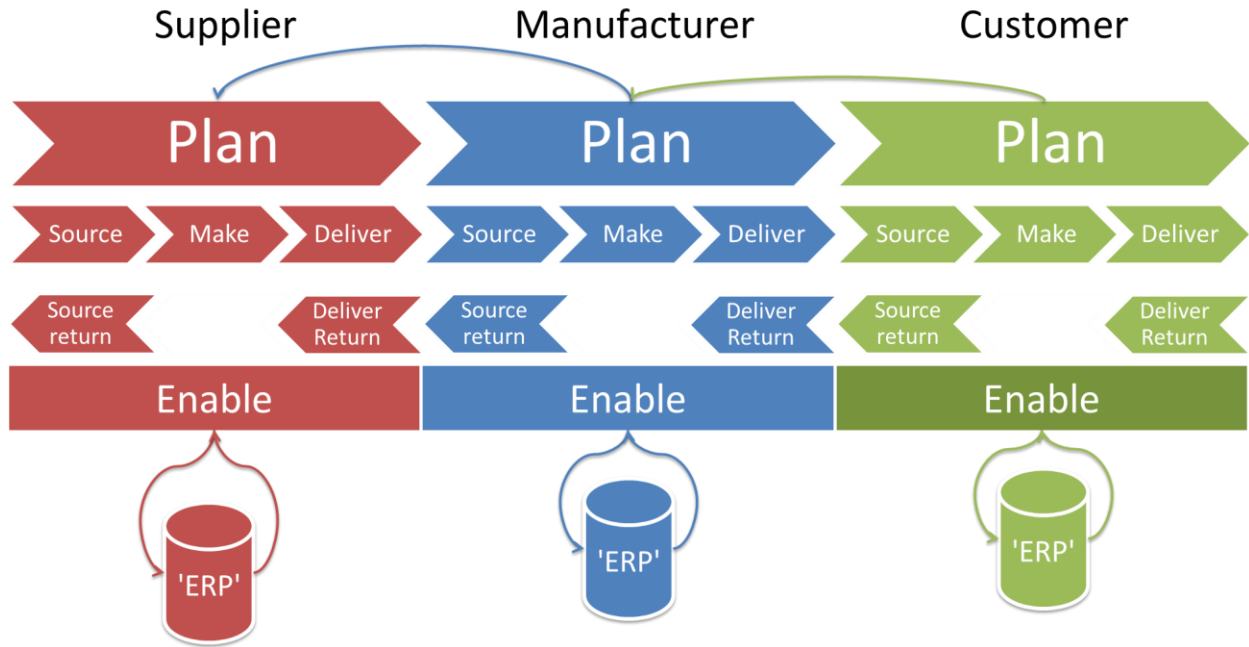
The figure above shows a very simple one - one - one arrangement. Real supply chains are of course much more complex, typically many - one - many. Part of the strategic management of supply chains is to balance the overhead of managing a large number of suppliers with the resilience and flexibility of multiple sources of supply.

Each of the linkages between the actors involves a degree of trust, such as in the accuracy of forecast orders. In mature supply chains there may well be an element of intermediation, where the 'manufacturer' role is to handle product from multiple smaller suppliers on behalf of the customer.

There is clear potential for blockchain technologies to play a role in this. The following table lays out some of the activities that rely to a greater or lesser extent on the trust between the parties. The sample is not exhaustive but is intended to show the spread of trust elements across the supply activity.

Trust element	Description	Supplier Processes	Customer processes
Product pricing	The price agreed for product is a fair balance between cost of goods sold and value added	Pricing strategy, negotiation, selling	Pricing strategy, negotiation, buying
Orders	The order for product conforms to the negotiated pricing, quantity, lead time etc.	Sales and Operations	Sourcing

		Planning, credit checking	
Product quality	Does the sourced part conform to specification	Quality assurance, process control, metrology	Vendor auditing, in-coming goods sample inspection, metrology
Invoicing	The payment for product supplied	Invoicing, credit control, invoice financing	Invoice matching, payment runs

Each of these can be addressed by blockchain type technology. Indeed, new business models can be envisaged. To illustrate one such example, an extreme model is proposed (figure below)
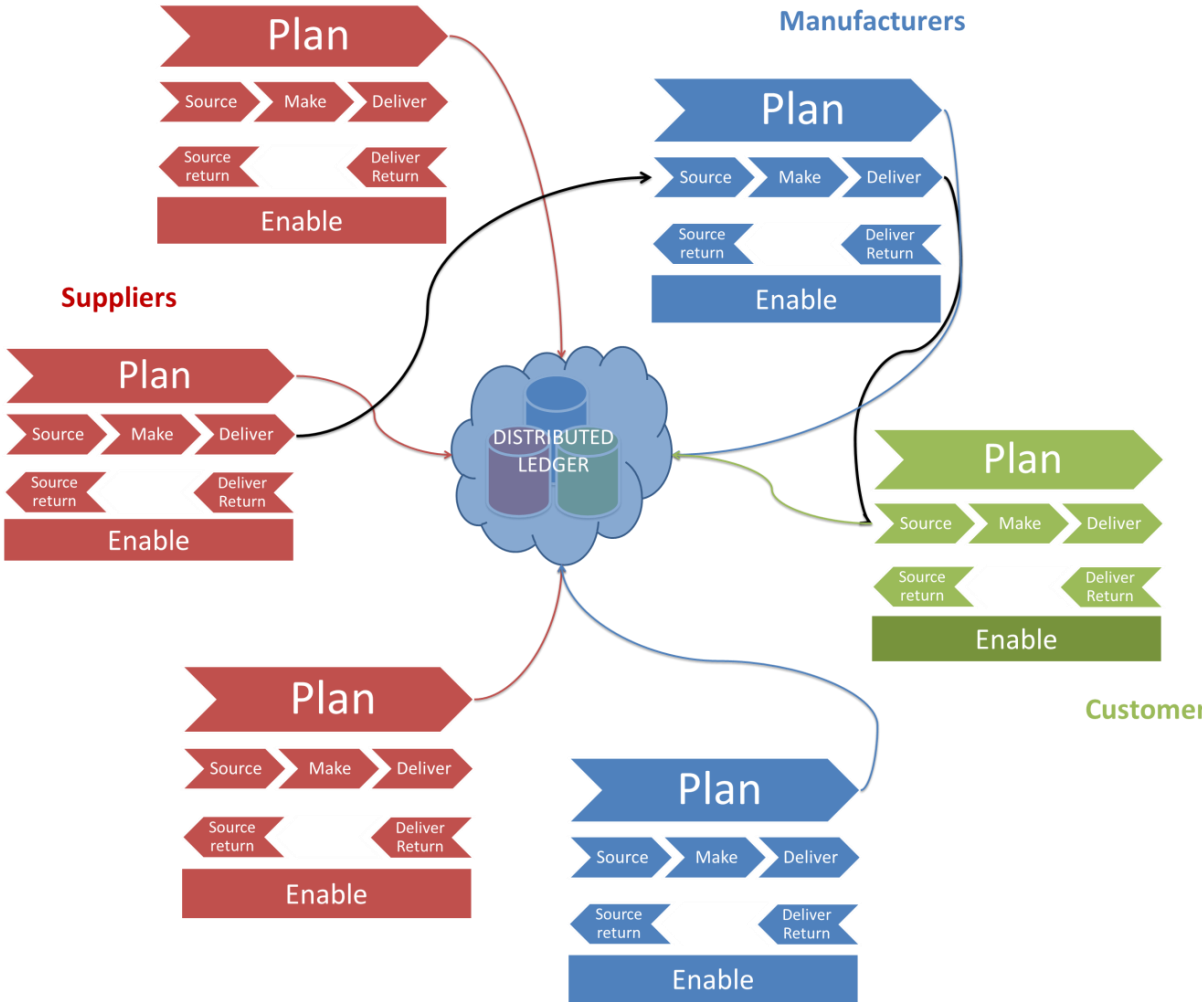
In this model, the 'ERP' databases of the previous model have become instances of a distributed ledger. The customer adds an order for a product that includes a desired specification, quantity

and lead time. Manufacturers can access the order and prepare their own bids against the order, including posting orders of their own for componentry. At the same time suppliers can see that customer orders are being placed and make their own plans in parallel with the manufacturers. The validity of orders (credit worthiness of customer, mechanism for payment, specification of product, process for delivery) is checked and maintained by the distributed ledger. Pricing is set by processes analogous to pricing discovery in high frequency trading. Bidding is anonymous and transparent, with orders under the control of smart contracts.

The physical production and fulfilment of the order is managed within the respective suppliers' and manufacturers' copies of the distributed ledger but is traceable and transparent for any 'valid' customer. This includes a growing record of the process control, validation measurement and calibration of equipment used.

Payment is made via smart contract as soon as the customer takes ownership of the delivered product.

Each of the described elements is, in principle, possible and would have the following impact on the trust elements described above.

Trust element	Description	Supplier Processes	Customer processes
Product pricing	The price agreed for product is a fair balance between cost of goods sold and value added	Transparently managed via a bidding process that sets the most efficient price at the time	
Orders	The order for product conforms to the negotiated pricing, quantity, lead-time etc.	Order validity maintained by the distributed ledger automated processes	
Product quality	Does the sourced part conform to specification	Data demonstrating this are part of the blockchain for the delivered product. The question can be automatically answered	
Invoicing	The payment for product supplied	Automated via smart contracts	

The blockchain enabled model allows for a very lean supply chain as described. This can potentially facilitate new agile cost effective manufacturing processes. It is the wider implications of this that make it beneficial. These are enhanced by its:

● Flexibility: To be efficient in terms of transaction costs most supply chains trade a degree of flexibility to work with known, trusted participants to avoid the need for costly time and resources that require negotiation. This model allows for maximum supply flexibility.

- Market access: Established supply chains can make it difficult for a new supplier to break into new markets. Even establishing that they have the required technical capability can be problematic. This model removes this barrier to entry.
- New Product Venture: A key block for product based entrepreneurs is sourcing the capability to produce product. This model cannot address every element of this but supports the development of an ecosystem that would greatly improve the situation.

This is of particular relevance in Advanced Manufacture environments where data about the product (whole product, sub-systems, components) is as valuable as the physical entity itself. Ensuring the correct documentation is produced and available in accessible ways is a human editing task which can be both costly and prone to human error. The cost difference between a standard part (e.g. a nut) and the same part with full validation of its material, processing parameters, inspection reports and storage (e.g. for an application where the nut is a critical part for safety, reliability, performance) can be several orders of magnitude. The automatic recording of this data into the blockchain, and the algorithmic checking of the blockchain for each part, provides a lower cost, lower error rate solution.

7. Challenges for Blockchain use in Advanced Manufacturing

The value of blockchain technologies comes from the the ability of a large and unconstrained group of stakeholders to interact in ways that build a shared history of activity with independently testable provenance.

To make this happen there a number of challenges that can be broadly categorized into;

- Technological Requirements: the new technical capabilities required to make use of blockchains
- Integration Requirements: the new processes and linkages needed to gain value from blockchain use

7.1 Technological requirements

Bahga and Madisetti (Bahga & madisetti 2016) propose a blockchain platform for an Industrial Internet of Things (based on smart manufacturing machines) that sets out the key technological requirements. These can be summarised as:

- Processing equipment that can write to the blockchain. Process equipment has had the capability to electronically register and transfer process data for many years e.g. CNC milling machines, process check weighers, instrumented torque wrenches. This information is typically managed by a SCADA (Supervisory Control And Data Acquisition)

system. The requirements for blockchain go well beyond this level. Process equipment will require sufficient 'smart' capability to access existing blockchains and be able to write to the blockchain all relevant information for the operation they carry out.

- Process-connected equipment that can interrogate the blockchain. This is a natural extension of the previous requirement. The difference between a read / write capability and interrogating the blockchain is that the equipment is doing some form of processing in the later case e.g. comparing the blockchain history of incoming parts against the requirements embedded in a specification blockchain. Reading the blockchain is a relatively slow process that does not 'scale' well.
- Each piece of machinery has its own unique identity. This is one of the more straightforward uses of a distributed ledger. As the internet of things increases its scope, the scale of machinery that constitutes a piece of machinery will reduce. Initially it is easy to see how a flexible machining centre would have a unique entry / identity in a distributed ledger of assets. As affordability of 'intelligence' and desirability of more finely resolved information increases, one can imagine the individual tools within the machining centre having their own unique entry.
- Linking the digital to the physical. Possibly the most challenging element is the link between the physical item and its electronic fingerprint. The opportunities for counterfeiting are dependent on the security of this link. There are a number of existing technologies available for this from simple printable identification labels (eg. barcodes and QR codes) through smart labels (RFID and NFC) to embedded identification chips (e.g MAC addresses on network interface cards). There is also a large amount of experience in counterfeiting such systems.
- High fidelity coding of Smart Contracts. One of the features of the use of blockchain is that it makes for a permanent (unalterable) record. When the blockchain is used for storing an algorithm there is no way to update the code to correct 'errors' in the code. Indeed where the coding is a smart contract, there is not a way to say the code is in error. (there are already legal cases testing this). It is thus hugely important that the coding is to a very high standard, and that processes exist to withdraw and replace smart contracts that are not functioning as intended. Developments in Computer Aided Software Engineering have a significant role to play here.

7.2 Integration requirements

Part of the litmus test for the suitability of blockchain technologies is that the function should not be equally able to be implemented via a centralised database system. Blockchain implementations by their nature then must include a significant amount of integration actions impacting all the actors in the system.

- Replacement of human judgement with algorithmic validation. One of the key benefit areas of the use of blockchain is to automate the acceptance of a transaction (production of a product, delivery of a service, transfer of ownership). This is a change that has significant impacts on organisational roles. For example, in current goods receipt processes, there is a human judgement made that a correct product has been received

within a delegated scheme of authority. This would be replaced by a blockchain comparing algorithm - who is responsible for the functioning of this algorithm?

- Modifications to end-user interactions with products and services. This can be seen in the difference between getting into one's own car and driving to office, compared to being allowed into the car outside one's home and being assessed and invoiced based on the duty cycle of use of that car.
- The process of disintermediation. The current state where there are a number of trusted intermediaries who provide assurance of the correct functioning of the supply chain is familiar and broadly understood. The future state where the correct functioning of the supply chain is verified via blockchains stored on distributed ledgers is understood in principle. The challenge comes in moving from current state to the future state when trying to operate in a mixed environment.
- Setting up and operating the blockchain machinery is a non-trivial matter. The less information held on a blockchain, the more efficiently it can be handled and the more flexibly it may be used. BitCoin blockchain transactions only record participants, value transferred and time. There is a 'Catch-22' like situation to the setting up of a blockchain. If the number of participants is small, reaching a consensus on the makeup of the blockchain is easy, but there is likely to be a simpler solution amongst a group that broadly trusts each other. The great value of a distributed ledger comes when there are large numbers of participants who have reason to not completely trust each other (conflicts of interest etc), but who need to have a consensus on what has happened. This makes it difficult to agree on the set-up of a blockchain. It is possible that use of blockchain may need to grow with the development of new industries, rather than be added to those that are more mature.
- A final integration challenge is to consider dispute resolution. Although blockchain use is identified with situations where participants don't wholly trust each other, blockchain does not remove the need for trust. In a blockchain environment trust is 'distributed' so that a lower level of individual trust is required. Each use case needs a set of 'miners' who will maintain the validity of the blockchain. These entities provide a check against each other but they need to have a vested interest in the system working. In the case of digital currencies, these miners are paid a small amount per transaction to carry out the validation process (proof of work). Similar arrangements may be appropriate for supply chain blockchains.

8. Roadmap

	Near term	Mid Term	Long term
Technology	Key agreed parameters of product indexed to industry group	The blockchain applies end-to-end within a products supply chain	IoT products come with a life history to transparently prove

	blockchains		identity
Business Model	Reduced supply chain transaction costs e.g Supplier Quality Assurance	Disintermediation of trading platforms. Just-in-Time enabled across ad-hoc networks	Highly responsive global capability base with ultra-low transaction costs for mass-customised product
User norms	Trade trust in corporations for richness of provenance information	Ever growing customer expectations of substantiated claims for products and suppliers	Intermediaries help identify what you need (curation and advice), rather than deliver what you've decided upon

9. Conclusion

We conclude that blockchain and distributed ledger technology offers significant and disruptive opportunities for advanced manufacturing. We have learnt from finance that such innovation can occur rapidly but that there is some resistance to the roll out and adoption by incumbent market leaders. To avoid this happening in advanced manufacturing, early adopters must avoid treating the technology as if it is just a technology roll out. There are substantial changes in business activity implied by its use. There are also significant limitations built into the underlying method, such as that while reading the blockchain is quick, writing to the blockchain takes time.
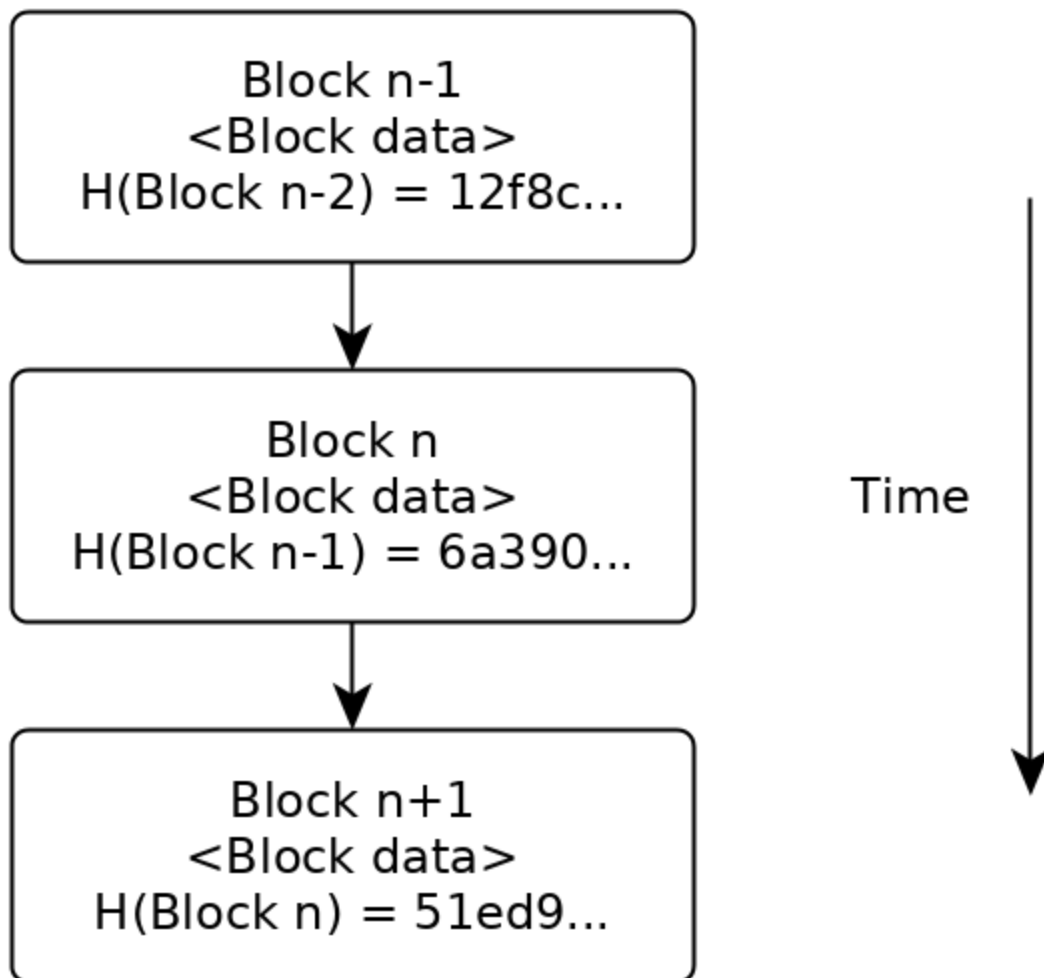
The opportunities that we identify come from cost reducing factors, such as reducing audit and validation costs. They also come from value increasing opportunities, increased responsiveness, added value in the final product, and new services based on blockchain information. We find that new technology compatible with industry 4.0 trends needs to permeate production and metrology equipment in order to achieve the fullest benefit. We believe the intermediate stages can be accommodated via blockchain interfaces on ERP systems at a corporate level and SCADA at on operational level. We also find a major benefit in avoiding counterfeiting by using this technology. Linking the digital to the physical remains a critical issue. Blockchain technologies will reduce the value of 'cloned' copies.

We have provided a roadmap for the adoption of blockchain. Realistically, the benefits in the near term are largely focused on the supply chain, whilst in the long term they are more related to the life cycle of the product. Finally, we urge the adoption of blockchain where it facilitates a more efficient and secure manufacturing process.

Appendix 1: Blockchain primer

Blockchain was a concept that gained significant attention with the rise of decentralised digital cryptographic currencies. It was first presented by Nakamoto in 2008 as a secure way to transfer financial assets over the internet using decentralised ledgers to verify their authenticity and avoid the "double spending problem". The protocols it uses can be applied to digital assets that can be recorded on a decentralised and transparent platform. It can be used in advanced manufacturing and supply chain networks where security, service reliability and an audited record of value added are required.

Blockchain technology is based around the concept of a chain of cryptographic hashes. It was first used within the Git version control software, first released in 2005. In it, data is stored within blocks. The integrity of these blocks is protected by a self-verification process, whereby each subsequent block contains the cryptographic hash of the previous block. This cryptographic hash provides assurance as to the integrity of the block, since as a checksum, any change to the contents of the block will result in a completely different cryptographic hash being produced. With each block referring back to the previous block, it is not possible to insert a new block or alter an existing block's contents, thus providing a range of guarantees as to the integrity of the historical records. This is shown in Figure 1.

Block n-1
<Block data>
H(Block n-2) = 12f8c...

Block n
<Block data>
H(Block n-1) = 6a390...

Block n+1
<Block data>
H(Block n) = 51ed9...

Time

The key properties provided by this chaining of blocks are integrity, verification and order verification. Clearly, it is not just financial markets that require such properties. Previous blocks' content cannot be altered without breaking the chain of hashes, thus revealing alterations have taken place. To make a change to an earlier block requires every subsequent block to be updated, since an alteration to block N will require the hash of block N within block N +1 to be altered, which will affect the hash of block N +1, stored within block N +2 and so on. This preserves integrity of previous blocks, since any changes to previous blocks will cascade forwards. Similarly, the order of blocks is preserved and unchangeable. This is because since the next block contains the hash of the previous block,it is not possible to swap the order of blocks.

The above properties only hold true under a scenario whereby manipulation of the blockchain will be detected. In the absence of such a system, a party carrying out modifications would be able to simply create a new chain of fully valid blocks. Therefore, it is also necessary for a second layer of verification to take place. This can either take the form of a distributed consensus mechanism, or through the manual verification of the blockchain at certain points in time — for example, by having a trusted party publish the hash of a recent block regularly through a reliable means of publication. All interested parties could verify their history of events by comparing their own copy

of the blockchain against these published validation block hashes. Validating block hash N provides assurance of the integrity of each block x, where 0 < x N.

Where a truly decentralised and distributed approach is desired, or there is no trusted third party or reliable means to communicate block hashes, a decentralised consensus protocol can be used to ensure that the blockchain contents is correct. This is the approach taken in the Bitcoin blockchain. Under such a model, it must be assumed that there may be multiple different parties attempting to produce their own competing views of the blockchain. The objective of this consensus protocol is to ensure that a consensus is fairly agreed between all parties, such that no one party is able to unfairly force their own view of events upon other participants. Figure 2 illustrates the concept of such rival chains.
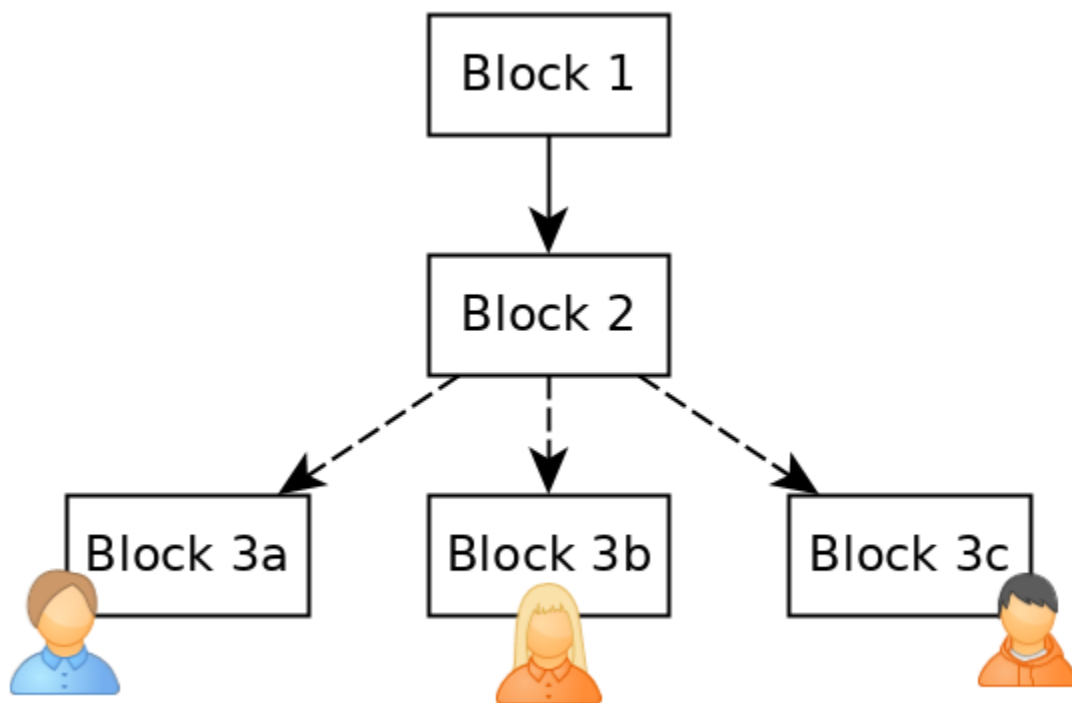
To ensure that the process of selecting the next block is fair, a computing challenge recognised by all parties as being fair and equally difficult is selected. Within Bitcoin, this challenge is based around a cryptographic hash function, where the one-way property of such functions is used. All cooperative participants in the blockchain reach agreement on an expected rule of validity over the next block. Participants wishing to propose a block must then create a new block, incorporating data they wish to include, and carry out the inefficient process of modifying padding data within the block until the hash of the block meets the requirements of the network. For example, the Bitcoin network requires valid blocks to have a given number of the initial bits of the hash output to be zeroes. Since the output of an ideal cryptographic hash is uniformly distributed, and an ideal cryptographic hash is effectively a one-way function, this task is of equal complexity to each participant.

The first participant to generate a valid block, according to the rules of the network, then broadcasts this block to all other network participants. They are able to verify the block against the network's rules, ensuring that it links correctly to the previous block. At this point, the next block is stored and appended to the previous blocks. At this point, any subsequent blocks aiming to take the same position in the chain will be rejected, on account of an earlier block already having held this position. Since the process of generating a block requires work to be carried out (and thus providing a proof-of-work having been executed), a participant must, on average, put in more work to successfully mine more blocks.

To make pre-mining of blocks impractical (where a single party may attempt to pre-compute its own future block), the difficulty of generating a block should set such that the chain will regularly advance. A new block must contain the full hash of the previous block, ensuring that any party mining the next block has knowledge of the contents of the previous block; this prevents participants from pre-mining blocks effectively, since the window to mine a given block only opens when the previous block is created.

Appendix 2: Smart contract primer

Smart contracts are self-executing contractual programs, stored on the blockchain, which nobody controls and can therefore be trusted as they are pre-programmed. Smart contracts evolved from finance and were first proposed as a result of the formulation of a transaction. The manufacturing process can benefit from the protocols they bring.

From an advanced manufacturing perspective, smart contracts facilitate:

- Greater Accuracy. Smart contract transactions are faster and less prone to manual error.
- Less intermediaries. Smart contracts can reduce reliance on third-party verification between counterparties.
- Lower cost. Smart contracts require less human intervention and fewer intermediaries and will therefore reduce costs
- Lower execution risk. Smart contracts eliminates the risk of manipulation, nonperformance, or errors.

We suggest thinking of smart contracts as mimicking the legal process but in written program code. In effect they have automatic dispute resolution built into them. More technically in finance, smart contracts incorporate the concept of *"an unspent transaction output (UTXO) as the building block for all future transactions"*. A UTXO contains a validation script, which is executed to determine whether a transaction has been suitably authorised to take place by the legitimate owning party. A basic form of script is executed within each transaction to ensure that the recipient of a UTXO signs any spend operation from that UTXO. Nonetheless, more complex validation scripts can be used[7], such as those permitting N from M multiple signatures (commonly known as multi-sig), by using a custom validation script to enforce other rules for the transaction.

These scripts are relatively constrained in their scope however. Bitcoin's validation scripts are only able to approve or reject a transaction, and offer no ability to granularly disburse partial contents of a UTXO. Bitcoin's transaction validation scripts are also entirely stateless, and can only validate within the context of a given transaction; each script is evaluated as a one-off operation, cannot call other scripts, and cannot access information about the block header, such as block number or hash (which precludes time-locking of transactions based on block numbers and the network's predictable block generation rate). The script must ultimately return a boolean for whether a transaction is permitted.

Within Ethereum, these limitations are removed, and this platform is therefore a facilitator of smart contracts. Ethereum enables two types of account; externally owned accounts, and contract accounts. Both are equal in capability and are capable of carrying out the same operations. Each account contains a balance, optional contract code, and an account-specific area of storage, to allow for the persistence of state data. Externally owned accounts are accounts controlled by the human holder of a private key corresponding to the account, like a Bitcoin address. Contract

---

[7] Such as those permitting N from M multiple signatures (commonly known as multi-sig)5, by using a custom validation script to enforce other rules for the transaction.

accounts do not have a specified owner or private key, and instead contain contract code, which acts as the authority controlling the funds within the account.

A contract can be triggered by a message being sent to the account, and this will cause execution of the contract's code, potentially resulting in the transfer of funds to other accounts, based upon the rules specified within the contract. A message is similar to a transaction, but may contain arbitrary data, making a contract in some ways similar to a function within computer programming, as the contract may return a response, as well as carry out actions.

Smart contracts offer potential in a number of areas that are applicable to advanced manufacturing. Firstly, they facilitate the creation of self-enforcing agreements between two parties, without necessarily requiring the engagement of a trusted third party in the event of a dispute. For example, in most financial transactions it is necessary for one party to trust the other to deliver as promised, while providing funds in advance; an example would include the purchase of digital content on the internet. Contracts are used to form a basis of protection for the buyer, by providing an agreement between the two parties, showing a mutual agreement on the goods or service to be delivered, timescales or other terms, and the fee or other compensation due in return. In the event of a dispute, this contract may be used as evidence in court proceedings to attempt to seek enforcement of the contract against the party in default of the contract.

As a result of this, contracts are often complicated, requiring professional drafting and careful review by lawyers. This quickly becomes expensive, and in many cases will require lawyers to be involved at multiple stages of the process, possibly at considerable expense, such as to ensure all terms are satisfied during delivery of a large contract. This clearly presents a significant cost, and impracticality for smaller scale contracts, such as one-off low-value purchases. In such scenarios, while a customer may be provided with a form-contract by the seller, stating what will be provided, short of seeking redress through the court system at a cost likely significantly exceeding the value of the contract, the buyer is often left with little means of recourse. Where reversible payment methods such as Visa or Mastercard are used, the card provider may offer charge-back facilities, or other guarantees, although these are not practical within Bitcoin or other blockchain-based payments which are, by definition and design, irreversible.

Smart contracts offer a potential solution to this problem, especially within the distribution of digital goods, whereby delivery can be measured or controlled as a result of the execution of the contract. Funds could therefore be disbursed to the seller at the time of delivery of the goods to the buyer, preventing the need for a payment escrow provider or other intermediary. The need for a trusted third party intermediary can therefore be reduced in some scenarios.

Another area of potential use for smart contracts is within smart property, or tokens. Such tokens can be used to convey and prove ownership of a physical asset, where such a form of electronic proof may be desirable. Constrained or otherwise limited tokens may be used by owners of smart property to delegate access for a limited period of time. For example, smart property techniques could be used to provide proof of temporary right to use a rented vehicle, or to occupy a given rented property, with the token signed by the property owner, and expiring at an agreed point in time based on blockchain progression. Such a token could be used, for example, to unlock the door of a rental property via NFC (Near-field communications), or to prove outright ownership of

a vehicle when attempting to borrow money with the vehicle used as collateral, and issuance of a verifiable token of collateral to prevent other debts being secured against the vehicle.

Appendix 3: Distribute Ledger blockchain testbed

This appendix details the research in finance that we conducted and from which the lessons for this paper were extrapolated. A distributed Ledger testbed was created in collaboration with Strathclyde University, the National Physical Laboratory (NPL), ZYen, and the Toronto Stock Exchange (TSX). Research was conducted to evaluate "*market microstructure*" and *"price discovery"* when using blockchain orders directed at *"distributed ledgers"*. The aim was to show how securities orders need to be processed when sent to distributed ledgers rather than a central stock exchange via a blockchain or other programed digital instruction.

In financial markets, it is important that such internet based trading platforms reflect the timing and order of trades. At the nanosecond level, it is necessary to know which order to process first. We therefore created a protocol for this, the time of order of receipt and execution being subject to nanosecond stacking. Our approach incorporated both transitory and permanent price discovery components and allows for the efficient processing of ordinal blockchains as they are received by a market clearing distributed ledger.

In order to establish a trading protocol to clear the orders, it was first necessary to establish a Distributed Ledger Test-Bed demonstrator. This was used to test high frequency trades and price discovery using blockchain like trades sent to a distributed marketplace. Such distributed market databases are capable of operating without a central validation system.

The research was relevant because current research in finance focuses solely on stock-market clearing, which itself has a central marketplace and validation system. Advanced manufacturing typically does not have a central marketplace and as such there are conceptual areas where the same technology can be applied. The distributed ledger blockchain testbed was used in our research to get insights into the role of timestamping blockchains. The test utilised market test data gathered over 24 hours for the whole of the Toronto Stock Exchange for level one and level two transaction date. By using financial market data the research established the importance of the time-stamp to distributed ledger technology in a real world scenario utilising an NPL Time signal.

The impact of the research was primarily focused on the regulatory framework. Financial market clock synchronization and time-stamp requirements mandate that both trading venues and market participants synchronize their clocks to Coordinated Universal Time (UTC). At present the regulators prescribe different time stamp granularities for venues depending on their processing speed as well as dependent upon the type of activity engaged in. The lessons on validation and timing can be extended to manufacturing and other applications. In order to prove that a blockchain generated order was executed with all sufficient steps, best execution required a

measurement methodology. Current regulatory guidance suggests that trades need to be recorded in microseconds. The quantitative research on order routing demonstrated that speed matters. Millisecond and sometimes microsecond timestamps are critical in the evaluation of order routing.

Appendix 4: Financial Blockchain Applications

A number of key areas of application for Blockchain have been identified in previous work and peer reviewed papers. These can be broken down into applications into the two key areas of currency and the provision of financial services:

Currency and Money Transfer/Exchange

Blockchain is widely associated with currency and/or money exchange. Bitcoin was the original implementation of the current blockchain, and is the largest and most widely cryptocurrency, although it is only one of many hundreds of such offerings. We don not see many money applications for advanced manufacturing, although of course all invoicing and payments are made using such mediums of exchange.

Bitcoin was built as a decentralised cryptographic currency, whereby issuance of the currency is issued according to a set of rules able to be followed and validated by all participants on the network. This is in stark contrast to most other currencies, including previously-proposed electronic cash schemes, whereby a central issuing bank, or other trusted third party is relied upon to control issuance of funds. In this paper, we have used this validation as a litmus test as to whether blockchain is applicable for advanced manufacturing. It should be noted that security, data validation and authentication can be achieved without a blockchain.

Within Bitcoin, since the full contents of the blockchain is publicly visible, it is not possible for any party in a position of trust to arbitrarily generate their own funds. Non-compliant blocks would be detected and rejected by other participants in the network. This means a malicious user would only be able to trick themselves. This made Bitcoin the first truly cryptographic currency, where funds cannot be spent without access to the correct cryptographic keys to sign transactions, and is in stark contrast to regular centrally-issued currencies, where fractional reserve banking and quantitative easing policies can be used to arbitrarily create new funds to issue. Within advanced manufacturing, payment and invoicing can benefit from many of the protocols used in blockchain facilitated currency and/or money exchange.

Financial Services

There is much hype and indeed potential for innovation around Blockchain technology within financial services and financial products. One of the most muted is the creation of authenticated secure money transfer of existing fiat currencies such as Sterling. While such a currency would clearly not be a truly decentralised currency in the same way that Bitcoin is a decentralised currency, free of central control, it may offer opportunities for advanced manufacturing. By facilitating the purchase of a digital version of currency, one-for-one exchangeable with regular physical currency, there may be an increase in user confidence and adoption, and increased abilities for users to trade online. Such a currency may attract foreign investors seeking to diversify their currency holdings with a digitally tradable form of another currency however, potentially resulting in challenges for the management and issuance of supply. Security of such a currency would also be critical, as any security breach of a one-for-one tradable currency would result in potentially adverse consequences for the underlying physical currency.

Other areas of potential interest to advanced manufacturers may relate to smart property. In finance, listed or unlisted stocks can be traded on a decentralised and distributed trading platforms, eliminating the need for a centralised broker and stock market to exist for the purpose of carrying out trades. Such a platform would not necessarily replace all use-cases for a stock exchange, such as high-frequency trading (HFT), where the significant delays to confirm transactions on the blockchain would be unacceptable. This is the basis of our collaborative use cases for advanced manufacturing.

Centre for Financial Regulation and Innovation

The CeFRI was established in 2016 as a centre of academic excellence in Financial Regulation and Innovation. Its vision is to provide a strategic link between academia, policy-makers, regulators and other financial industry participants.

The mission of the Centre and of its members is to foster policy relevant research to support the practical application of innovation in Finance.

The CeFRI aims to foster better regulation in the face of its academic and practitioner focused innovation in capital markets. It promotes insights in innovation, market efficiency, risk management, investment benchmarks and corporate governance to a wider audience. CeFRI's activities are funded by industry partners.

Contact details:

Daniel Broby

Centre for Financial Regulation and Innovation

Stenhouse Wing

199 Cathederal Street

Glasgow G4 0QU