Blockchain: the solution for transparency in product supply chains

Published 21 November 2015

> "Now, in the hyper-connected and ever evolving world, transparency is the new power."
>
> *Benjamin Herzberg, Program Lead, Private Sector Engagement for Good Governance at the World Bank Institute*

This white paper is by social enterprise Project Provenance Ltd. and describes a prototype that uses blockchain technology to enable secure traceability of certifications and other salient information in supply chains. Provenance enables every physical product to come with a digital 'passport' that proves authenticity (Is this product what it claims to be?) and origin (Where does this product come from?), creating an auditable record of the journey behind all physical products. The potential benefits for businesses, as well as for society and the environment, are hard to overstate: preventing the selling of fake goods, as well as the problem of 'double spending' of certifications present in current systems. The Decentralized Application (Dapp) proposed in this paper is still in development and we welcome businesses and standards organizations to join our consortium and collaborate on this new approach to understanding our material world.

Demand for transparency is increasing

We know surprisingly little about most of the products we use every day. Even before reaching the end consumer, goods travel through an often vast network of retailers, distributors, transporters, storage facilities, and suppliers that participate in design, production, delivery, and sales, yet in almost every case these journeys remain an unseen dimension of our possessions.

> "1,127 people die in Bangladesh garment factory collapse."
>
> *Reuters, May 2013*

The creation, exchange, and use of material things, however, has many potential negative consequences: environmental damage, exploitative extraction, unsafe work conditions, forgery, and the huge amounts of valuable material wasted at the end of product life. Our relationship with the material world is broken.

"50,000 tonnes of meat sold as beef found to contain horse DNA." *BBC, April 2013*

"Without understanding the impacts of goods and services, we buy into systems that deplete natural resources, worsen environmental and social problems and endanger humans and ecosystems. Supply chains are conventionally held secret, limiting the stakeholders who can prevent environmental, social and health and safety problems."

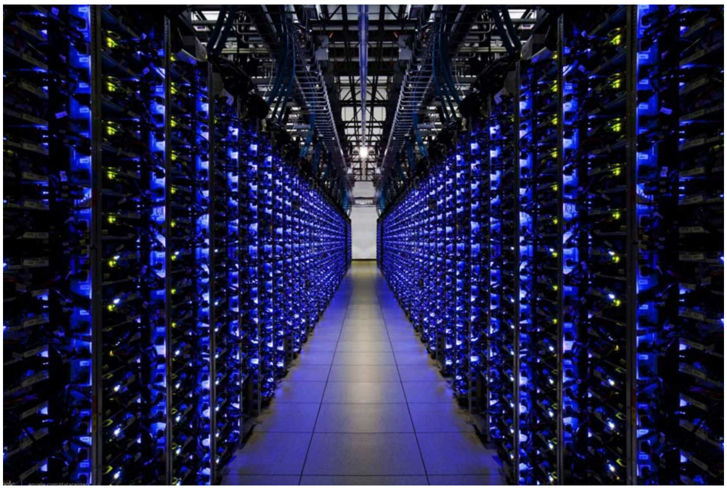
Leonardo Bonanni, Founder of Sourcemap

There is a growing rallying call by customers and governments demanding more transparency from brands, manufacturers, and producers throughout the supply chain. In the UK, 30% of consumers are concerned about issues regarding the origin of products but struggle to act on this through their purchasing decisions. The market for products of proven origin is growing. In the future, regulations like the European directive on non-financial reporting or the UK Modern Slavery Act will require companies to transparently disclose reliable information about their business footprint.

Pioneering companies have long realized the competitive advantage of open, transparent supply chains and sustainable manufacturing. As an example, fish suppliers John West started including codes on their tuna cans to enable a consumer to trace the product back to the fisherman; this initiative alone added £17m to the brand's sales. Sustainability standards and certification (e.g., Fairtrade, Forest Stewardship Council (FSC), Soil Association) have been an important tool to enable choice differentiation and conscientious consumption, yet in the end the outcome of certification is often just an image file or printed label on the packaging whose actual meaning is difficult to know and hard to verify. Guaranteeing the integrity of certificates is a costly process that, despite laborious audits, still struggles to assure the validity of the claims being made. Worldwide expansion of certification schemes in regions with levels of high corruptions further endangers credibility.

Centralized systems can't power transparency

Despite various efforts, full "chains of custody" that tell the stories of products remain largely rudimentary and difficult to verify. Fragmentation of these efforts make them open to fraud. To connect the dots, nominally neutral, not-for-profit or governmental entities are commissioned with the task of creating a centralized data storage to enable a flow of trusted information.



A typical server room storing company system data. In it's current centralized format, there are many weaknesses.

In the face of these efforts, we must ask ourselves: can one organization be trusted to broker all data about every product's supply chain? The truth is that no single organization can, and that relying on one party (or even a small collection of cooperating parties) creates an inherent bias and weakness in the system. If the party were the brand itself, or the most powerful actor in the supply chain, then it would be responsible ultimately for only its own bottom line; this could lead to selective disclosure or, worse, extortion. If the supply chain data were gathered by a third party, it would have to be both totally unbiased and properly incentivized to deliver the technical capability of running the system. Third parties like NGOs or industry associations, however, rarely manage even one of these two, and even if they could, they would become a single point of weakness; this would make them and their operations a vulnerable target for bribery, social engineering, or targeted hacking. Distributing the transaction platform among various third parties would add further difficulties, as the shared costs for its set up and operation would be difficult to apportion and agree on, as benefits to each party are not usually made transparent.

Despite these difficulties, the idea of using a centralized system with a governing third party was, until recently, the only conceivable way to achieve data and transaction transparency along supply chains. Today, however, a new technology called the *blockchain* presents a whole new approach. The blockchain is a recent development in the field of computer science, which uses a global peer-to-peer network to provide an open platform that can deliver neutrality, reliability and security. The basic mechanism was originally proposed as part of a solution for administering the shared accounting ledger underlying Bitcoin ["Bitcoin: A Peer-to-Peer Electronic Cash System", Satoshi Nakamoto, 2008]. Beyond this initial financial application, blockchains can be generalized and used to implement an arbitrary set of rules that no one, neither the users nor the operators of the system, can break. They rely on a completely different system architecture—one that we will detail below—that makes them a unique platform for applications involving multiple parties with little trust in each other; for example, fragmented supply chains. We stress that our approach does not require any particular behavior on behalf of the participants; instead, the underlying technology guarantees the integrity of the system even in the face of dishonesty or idleness. In this way, we provide a technological solution to an organizational problem.

Blockchain technology changes everything

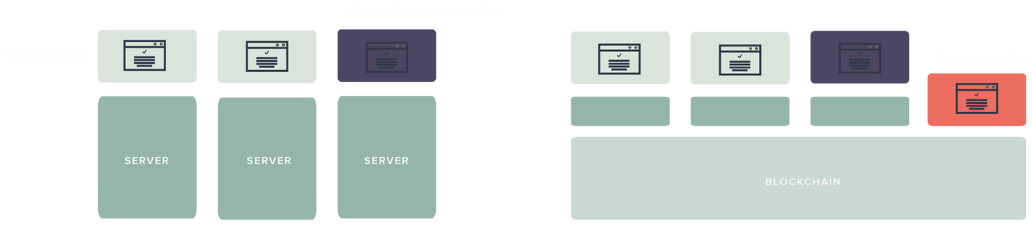
> “The practical consequence […is…] for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate.”
>
> *Marc Andreessen, Inventor of the internet browser*

To grasp the potential that applications built on top of blockchains can deliver, it is essential to understand the three key differences between blockchains and most existing computer designs. We present these below as *non-localization*, *security*, and *auditability*.

Non-localization: A truly global computer running by consensus

Personal computers (e.g., desktop PCs, laptops, and mobile phones) are limited by the physical world. Even though it may seem that modern applications run on several devices, to keep consistency an application’s core program is in fact executed on a single, centralized server, with the client device serving merely as a powerful display.

In contrast, there is no single machine that governs the business logic or the data on which a blockchain operates. Instead, the data on a blockchain is determined by *consensus*, which is a defined convention for how to execute and administer the business logic (e.g., to update the stock of a certain good). The magic of the blockchain and its surrounding incentive structure is such that users can then *unambiguously* discover the state of the system (e.g., the current level of stock or the origin of a particular certificate), not from a single particular authority but rather by independently applying common rules and publishing data openly.



Above: The top row of blocks represent web interfaces and applications, the bottom layer(s) are data handling and storage. Today your data is stored in a silo. With blockchains your data will be stored (publically or pseudo anonymously) in a shared database. This diagram is adapted from a diagram by Nick Grossman, GM at Union Square ventures, however his also includes time.

A machine of unparalleled digital security

Recent years have seen a surge in attacks undermining the protection mechanisms erected around centralized systems. While many attacks exist that directly target the hardware itself, the easiest way to circumvent the strongest security component is social engineering, which targets the weakest human component. By leveraging those with the most elevated access rights, an attack that targets IT and operational support administrators could eventually lead to the system being fully compromised (which is why there are often anti-coercion procedures in place for sensitive financial systems).

With the blockchain, security is different: it does not matter who or where the user is, because all information provided to the blockchain is accepted only if it is *authenticated*. This authentication is provided in the form of an unforgeable digital signature: a cryptographic mechanism that—in a manner analogous to a physical signature but significantly more secure—allows someone to prove their identity without enabling someone else to impersonate them in the future (see call-out box for more details). Thus, it does not matter what your job is or what your access capabilities happen to be, as you simply cannot interact with the blockchain unless you provide the digital “key” required for the interaction that you own (e.g., unless you cryptographically prove the ownership of your account, there is no way for anybody else to change its balance). This means that elevated privilege levels are curbed or removed entirely, and the security risk of the weakest link—in the form of operators and IT administrators—is drastically reduced.

A perfectly auditable system

In any deterministic system, it is possible to strictly verify and audit the actions within the system as correct; indeed, the inputs and outputs of the system serve as a record of the various interactions (e.g., automated bank transfers in the case of a payroll system or ordering additional components in the case of a stock control system) that have led the system into its present state. While this is true in theory, to perform this audit in practice comes with one proviso: *all* information concerning *all* inputs must be provided. In traditional systems, this is expensive, impractical, or impossible. The inputs to a business system typically include heterogenous types of data coming from a wide variety of sources, and the auditing itself, which would essentially require "playing back" such inputs, would be technically challenging. Furthermore, auditing may require strong knowledge and assurance of operator identity, which can often be compromised or flawed in a system with many actors.

A blockchain is different, as by design it is perfectly auditable. Each individual operation or interaction, such as the provision of a new employee or the recording of outgoing stock, is perfectly recorded and archived. Auditing is thus as simple as joining the blockchain network, as this allows one to "replay" the operations of the past in order to build a correct model of the present. Combined with the absolute guarantees of authenticity for every interaction, strong and agile data systems can be facilitated that are at their core resilient to coercion and human factors.

Implementing supply chain certification on the blockchain

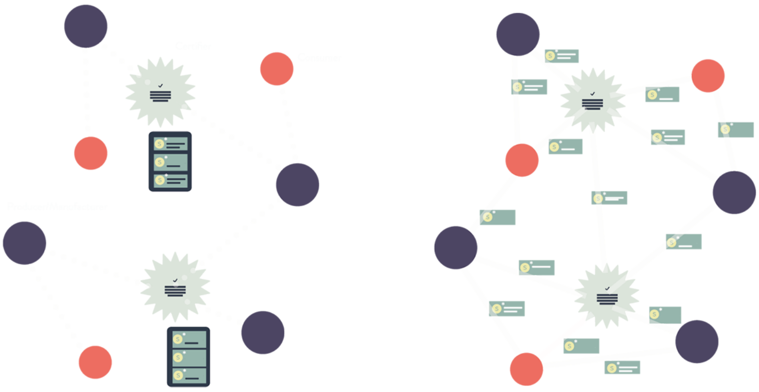
At Provenance, we believe that the use of blockchain technology provides a number of truly unprecedented breakthroughs for certain public-interest information, such as the supply chains of consumer products. By using blockchains, we can create a system that allows an incremental, piecemeal adoption model, gracefully building in utility as adoption increases, but without an inhibiting cost/benefit ratio in the initial stages of usage.

Roughly speaking, the blockchain works much like any datasystem: it takes inputs (for example, the amount of material with a certain grade and the intended recipient) and carries out actions based upon these inputs, changing the database in a manner perfectly determined according to its program (in the same example, the values in the database would be the amount of material of a certain grade resting with each account). The outcome of these alterations may then be inspected and real-world decisions made accordingly.

As an example, we propose an alternative approach to the certification and chain-of-custody challenge in sustainable supply chains: a system to *assign* and *verify* certifications of certain properties of physical products; e.g., organic or fair trade. We will outline a model of the various materials and components from initial production through manufacture and assembly to the final customer. At each point in time, the prototype of our model details four key properties concerning all materials and consumables it covers: the nature (what it is), the quality (how it is), the quantity (how much of it there is) and the ownership (whose it is at any moment). Key attributes may be read and linked from pre-existing datasets such as barcodes, or newly ascribed along the way.

The blockchain removes the need for a trusted central organization that operates and maintains this system. Using blockchains as a shared and secure platform, we are able to see not only the final state (which mimics the real world in assigning the materials for a given product under the ownership of the final customer), but crucially, we are able to overcome the weaknesses of current systems by allowing one to securely audit all transactions that brought this state of being into effect; i.e., to inspect the *uninterrupted* chain of custody from the raw materials to the end sale.

The blockchain also gives us an unprecedented level of certainty over the fidelity of the information. We can be sure that all transfers of ownership were explicitly authorized by their relevant controllers without having to trust the behavior or competence of an incumbent processor. Interested parties may also audit the production and manufacturing avatars and verify that their "on-chain" persona accurately reflects reality.



With blockchains data can be accessed and verified by all actors, rather than solely by the original certifier.

Information architecture for a certification and chain-of-custody system on the blockchain

Here we show how existing certifications and audits of supply chains can take on a new guise implemented on the blockchain. There are six different types of actors involved in our exemplar set-up:

1. Producers (e.g., a cotton grower);

2. Manufacturers (e.g., a maker of fabric or jeans);

3. Registrars, which are organizations that provide credentials and a unique identity to actors (e.g., an accreditation service);

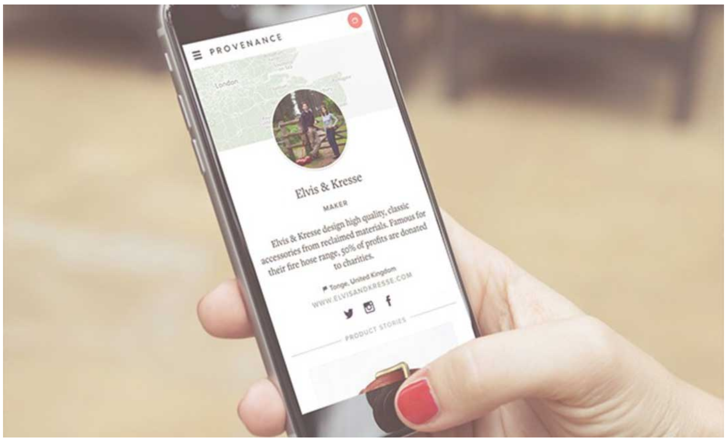
4. Standards organizations, which define the rules of a certain scheme (e.g., Fairtrade);

5. Certifiers and auditors, which are agents—usually separate agents, to maximize security—that inspect producers and manufacturers and verify certain standards, like annual production capacity; and

6. Customers, the buyers of products all along a supply chains, including the end consumer.

Below we explain the principal architecture. The architecture consists of a number of modular programs. Each program is deployed on the blockchain and controlled independently, but because they work within the same blockchain system they are able to interact without friction.

Registration program



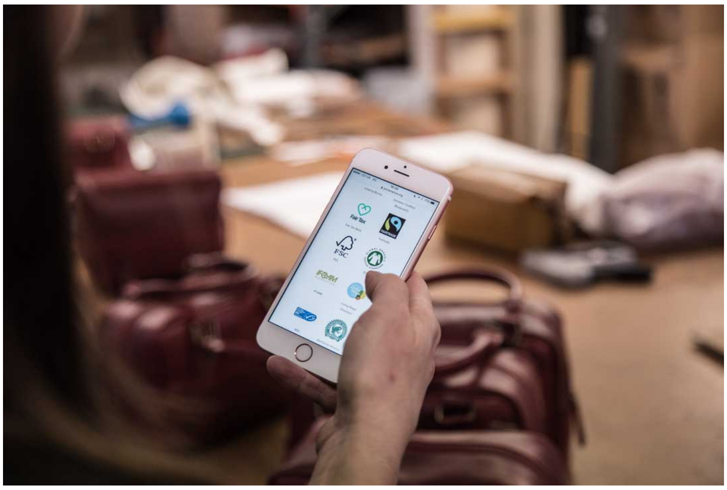
Elvis & Kresse design high quality, classic accessories from reclaimed materials. Famous for their fire hose range, 50% of profits are donated to charities.

On Provenance everyone has a profile accessible with a private key. Profiles can be public or private depending on use case and permissions. Some are rich with information, whilst others simply contain an anonymous ID.

It is this program alone that forms the fundamental trust relationship between the customer and the system as a whole. All other programs derive their "trustability" through their own reputation (which may be imported through their real-world name). This program will initially be deployed by the registrar, who implements a process for the registration of named participants (i.e. certifiers, auditors, producers, and manufacturers). Such participants may request registration of their digital identity (for details, see the "Public- Key Infrastructure" box), which links their real-world identity with their blockchain-based digital identity, thus allowing them to interact with the blockchain using their real-world identity. Upon request, the registration authority verifies their identity and records the result in the blockchain, available for all to inspect.

Importantly, the system could allow participants to remain anonymous, at the cost of opacity at the stage of the supply chain at which that actor operates (although information about earlier stages can remain retrievable). The exception is certifiers, who need to register and identify themselves in order to make the system work.

Standards programs



Marks and certifications that are printed on today's consumer products and shown at the point of sale. On the blockchain certifications can be linked to their real meaning and information verifying their status.

These programs represent the implementation of schemas for proper recognition of a standard (e.g. no animal testing, biodynamic, fair labor). Through these programs, standards organizations provide for the creation of compliant production or manufacturing programs (see below), allowing instances or batches of goods and materials to be added to or processed on the blockchain. Such producers or manufacturers may require inspection by a certifier or auditor of their facilities and processes to be able to obtain and operate a certified program. Successful verification results in the deployment of a production or manufacturing program that is both registered with the certification program and authenticated by an auditor, and allows a producer to create the digitally tradeable equivalent of a good (i.e., a token that shadows the real-world material or product), which acts as its blockchain-based avatar.

Production programs

From cotton growers to gold miners the blockchain presents a method for securely documenting and transferring key information about a raw material.

Deployed following successful certification, these programs are used by producers to prove the creation of materials or primary goods. The program specifies and implements the parameters for each production facility, including:

- the certification of the production capacity for the production of the good (e.g., 500t of cotton/year);
- a taxonomical description of the good, which would include a detailed description of the output, together with any additional "tags" to help identify specific attributes (e.g., fair trade, fair labor, organic);
- the production accounting; i.e., the registration of created produce up to the maximum annual capacity, as well as the registration of their sales.

These parameters can be adjusted according to desired guidelines by certifiers or following the inspection by an auditor, and in case of an unsuccessful audit, the program can be easily (temporarily) revoked if necessary. Since they are principally responsible for the creation of goods, producer programs are the root for the traceability of finished goods, which then link back to the identity provided by the registrar.

Manufacturing programs

Information from the producer is securely cascaded to the manufacturer on receipt.

These programs implement the transformation of input goods from production into output goods. Much as with production programs, once deployed by the certifier the programs are operated by manufacturers, but with one additional constraint: input goods must be "used" for any output to be created, just as in the physical world. For example, the registration of a certain amount of organic cotton fabric requires as input the appropriate amount of raw organic cotton, and after this usage the raw organic cotton should no longer be usable. Because of its auditability, the blockchain provides the same cast-iron guarantee as in the physical world; namely, that creation of an output good can happen if and only if the required input is used.

Tagging—establishing secure links between the digital and the physical world

Label with a unique cryptographic QR code and NFC tag that links to the Provenance of the material, ingredient or product to the physical item.

Beyond the implementation of the fundamental business logic on the blockchain as described above, a method to securely link physical goods to their digital counterparts is also necessary, as well as a user interface that enables informed purchases both along the supply chain and for the customer.

Linking

The technologies by which the physical goods and materials are identified and linked with their digital representation on the blockchain (e.g., serial numbers, bar codes, digital tags like RFID and NFC, genetic tags) is crucial in uniquely identifying a physical good with its digital counterpart. At Provenance we are exploring many new and existing technologies; an overview of recent technologies can be found here. Identities are recorded in production and manufacturing programs, and for simplicity and easy adoption we expect them to take the form of existing barcodes and serial numbers which are linked to blockchain identifiers using a secure hash.

User-facing applications facilitate access to the blockchain

The final owner of the product has access to secure information about the product's supply chain, without having access to identification details.

By design, every transaction along a supply chain on the blockchain is fully auditable. By inspecting the blockchain, smartphone applications can aggregate and display information to customers in a real-time manner; furthermore, due to the strong integrity properties of the blockchain, this information can be genuinely trusted. A thoughtful user interface that sheds light on the digital journey of a product can empower better purchases by giving users a true choice that they can exercise.

There are substantial broad effects of bringing near-frictionless transparency to consumer purchase decisions and product identity; clearly there is likely to be an additional "virtuous" component in purchase decisions, especially among mid-level purchases where a marginal increase of 20% to the price does not affect the willingness to buy. Additional levels of guarantee over genuine articles is a high-value use case. While an initial introduction of this technology may be in the form of a discrete and removable label, easily verified through a smartphone-readable QR-code, a more progressive possibility would be a conspicuous hologramatic or RFID tag, embedded in the brand label, allowing the owner to prove the authenticity of the product at any time by accessing the data on the blockchain through the tag.

Early extensions of the proposed certification system

Interoperability allowing arbitrary schemes to interact with each other could massively reduce the level of trust required for the implementation of a joint system as well as help against concerns regarding adverse cost–benefit trade-offs and privacy. Additional features could securely provide crowd-sourced scrutiny as a complement the formal certification process; e.g., workers themselves could report from farms and factories about the operational processes if they obtain a secure identity in the system.

Public-Private Key Infrastructure

Public/private key infrastructure allows us to mimic a physical signature by way of provably registering our identity with a digital document or instruction without at any time giving others the ability to further produce such signatures for other instructions or documents.

Notionally, physical signatures are difficult to reproduce, especially on demand, leading to their common usage as a way of proving that a counterparty is engaged under a particular agreement. In the digital age where facsimiles are trivial to create and face-to-face engagement no longer the norm for most transactions, they no longer serve their purpose: access to a signature generally leads to ability to reproduce the signature.

Mathematics, however, has provided a fully digital alternative by way of cryptography. Through the use of functions with special properties, it is possible to hold a small piece of data known as a secret (or private key), and use it to demonstrate that you have explicitly sanctioned a particular piece of information (a document, image, order or other such digital item) without ever uncovering that secret to another party. To do so, the secret is combined with the document in question (using a special mathematical function) to produce a signature. This may be freely distributed (usually, but not necessarily, with the document). All secrets have a counterpart public key, which may be published by the secret holder as their identity. When a third party recombines the document with the signature, they are able to retrieve not the secret, but rather the secret's public counterpart, the public key and the secret holder's published identity. This allows them to be sure that the document was sanctioned by the secret holder without ever knowing their secret and thus compromising the fidelity of future signatures.

Anonymity and protection of sensitive business information

The information that's accessible to consumers all along the supply chain depends on the privacy permissions granted. With the blockchain even if the identity of the farmer is not revealed you can still feel secure that verified information is trustworthy.

The success of the proposed systems relies on the registration of identities and recording of transactions and information. This enables actors on the supply chain to carry and prove the defining attributes of their material products to any actor further along the chain. Certain users, however, might be concerned about their privacy or the privacy of their suppliers further up the chain. Technologically, it is possible for identities to be protected in a blockchain-based system, while still transferring other salient information. For example, manufacturers in the middle of the supply chain could securely pass a certificate with full authenticity downstream while keeping their identity private. For customers, the described system provides the ability to check important attributes of purchased goods without necessarily seeing the full intricacies of the supply chain that created them. The system also allows for the trusted proof of ownership thanks to Public-Private Key Infrastructure (see above) without revealing their the identity of owners to the system. In fact, customers could even use the system to sell a good on a secondary market, allowing the chain to continue post sale throughout the product lifecycle.

The blockchain brings significant operational benefits

Interoperable

A modular, interoperable platform that eliminates the possibility of double spending

Auditable

An auditable record that can be inspected and used by companies, standards organizations, regulators, and customers alike

Cost-efficient

A solution to drastically reduce costs by eliminating the need for “handling companies” to be audited

Real-time and agile

A fast and highly accessible sign-up means quick deployment

Public

The openness of the platform enables innovation and could achieve bottom-up transparency in supply chains instead of burdensome top-down audits

Guaranteed continuity

The elimination of any central operator ensures inclusiveness and longevity

Further use cases: From fraud prevention to powering the circular economy

We illustrated a certification example above, but there are many other settings where our blockchain-based system can be applied to provide surprising new benefits. The logging of chain-of-custody on the blockchain, touched on above, can be applied to prevent all kinds of fraud by proving the origins and ownership history of any physical object. Counterfeit goods have had a significant detrimental effect on the global economy for some time: The UK economy alone has lost £30bn and 14,800 jobs, and customers face potentially serious consequences (in, e.g. buying counterfeit medication). As an example, a luxury watch retailer may use the programs described above to prove to buyers that a watch is authentic, or create an “owner’s program” where attributes such as age, repairs, insurance, and valuation can be logged on the blockchain to provide an information log when the watches are handed down or resold.

Electronic waste component reclamation in China: The niche industry employs tens of thousands of people, many of them in small, family-run workshops. Photo by Chien Min Chung.

In general, the afterlife of goods can be dramatically changed through the existence of a full lifecycle record, which could help to power broader efforts such as the Circular Economy. This initiative considers the recycling, (re)manufacturing, and leasing (e.g., Zipcar and Rent the Runway) of existing products, and the Ellen MacArthur Foundation Report on Circular Economy demonstrated that “designing and using durable goods, such as cars and vans, washing machines, and mobile telephones, in accordance with circular principles offers materials savings in Europe that could be worth USD 380 billion in an initial transition period and up to USD 630 billion with full adoption.” All these systems rely on the tracking of the attributes of material things not only during their creation but also their usage. The system proposed in this paper would not only allow the creation (including all materials, grades, processes etc) and lifecycle (use, maintenance etc) to be logged on the blockchain, but this would also make it easy to access this information when products are returned to be assessed and remanufactured into a new item.

Conclusion

> “Beyond the age of information, is the age of choices.”
>
> *Charles Eames*

By design, the blockchain enforces the transparency, security, authenticity, and auditability necessary to make tracing the chain of custody and attributes of products possible, which in turn allows customers to derive the high-quality information needed to make more informed choices. Implementing supply-chain transparency on the blockchain dramatically reduces the high initial cost/benefit ratio for participants, and its naturally distributed design frees a central organization from costly and error-prone operational duties. In the system we have described, the role of the anchoring core organization has been reduced to providing registration and linkage between “blockchain” and “real-world” identities.

The choices we make in the marketplace determine which business practices thrive. From a diamond in a mine to a tree in a forest, it is the deepest darkest ends of supply chains that damage so much of the planet and its livelihood. This new system could be a unanimous source of connected information, secure and incorruptible, to allow the purchasing decisions throughout supply chains and by end consumers to be smarter. The premium cost of ‘Fair trade labour’ and ‘sustainably farmed’, and other socially and environmentally beneficial product and business affordances, are intangible, but increase the value of goods: With Provenance, they can be understood, carried and trusted as they travel the most complex chain of custody.

This paper was written by Project Provenance Ltd. To contact us please submit our contact form or tweet @ProvenanceHQ. Thanks to Dr. Gavin Wood at Ethereum, Dr Sarah Meiklejohn, Aeron Buchanan, Christopher Brewster, Hugh Laughlin, Nicole Green and Patrick Mallet.

Published 21 November 2015

SHARE THIS WHITE PAPER

Quick Key Definitions

Bitcoin The first decentralized application suggested in 2008, a peer-to-peer electronic cash system

Dapp (**Decentralized application**) A program implemented on the blockchain that executes the rules of a particular business application. Usually the term Dapp encompasses both the program’s backend as well as (various) user facing web frontends

Provenance Social enterprise building a system for product supply chain and lifecycle transparency using the blockchain

Ethereum Name of a project and their blockchain platform designed with great generality to allow for easy implementation of arbitrary decentralized applications