University of Tartu

Institute of Computer Science

Research on Blockchain and its Disruptive Potential

(Registry – Management of Assets)

Seminar on Blockchain Technology (MTAT.03.323)

Authors:

Akande Adefisayo Ayodeji

Artur Käpp

Tartu 2017

Contents

1. Overview

1.1 Registry of Things

In order to understand what problems blockchain can possibly solve it is important to understand the vital role of intermediaries in the global economy. Intermediaries are there to help people securely transfer value - they create trust & certainty. (1) (2)

Whether we realize it or not, these intermediaries are a central part of our daily lives. (1) (2) (3)

- Banks maintain a ledger of deposits and transactions.
- Local registries maintain a ledger of property ownerships and transfers.
- The registry of motor vehicles maintain a ledger of vehicle ownerships and title transfers.
- Apple maintains a ledger of purchased applications, songs and movies.

Buyers and sellers need these intermediaries because they might not trust the other party. So they put their trust in the intermediaries to ensure that the transaction is completed faithfully. However the problem with this is that these intermediaries are also running a business so they all charge a small fee from every transaction. Additionally these intermediaries can deny and accept transactions pretty much at their free will. For example they may prevent certain people or organizations from using their platform for personal or political reasons. (1)

Without a proper repository of trusted records, everyone could potentially claim ownership of anything. (2) Imagine losing your car keys and the founder of the keys declaring the car to be their own. Without these trusted records it is not possible to prove otherwise.

1.2 Blockchain

Blockchain, at its simplest, is a ledger or a database open to anyone. The difference between current third-party ledgers is that Blockchain is a fully distributed ledger, with no central governing authority responsible for it. Every participant in the network holds the full copy of the ledger and all parties collectively validate updates to the chain. (3)

All entries in the blockchain network are permanent and visible. Encryption protocols and technology effectively replace third-party intermediaries. Without these third-party ledgers, it is possible to do business, trade goods and transfer value without any government facilities.

Imagine a world without banks, DMVs nor intermediaries of any kind. No need to stand in lines at the DMV and less hassle to fill out all the forms... (3)

1.3 Blockchain problems

Blockchain being a relatively new technology, doesn't come without problems and whilst we don't have solutions to these problems, it is also not yet possible to implement the real potential of Blockchain technology to every use case.

Firstly, the legal system has dealt with issues of ownership for centuries. Whilst some of the rules and laws of ownership may seem outdated they are actually sensible adaptations to the messiness of real life. (4)

Secondly, every kind of system of ownership should be able to guard people against theft. As stated above, mere possession of a car is not the same as owning the car otherwise everyone who can get hold of your keys would own the car. (4)

Let's consider an example. A Cat ate your certificate of title for the car. No worries, because the DMV can reissue new certificates if you can prove your identity. This is possible only because they kept the records and they are matched to your identity. (4)

Now, imagine the blockchain scenario where the only way to prove the ownership of the car is with your private key. Now what if you were to lose that key. Congratulations, your car won't start and no one in the world can help you without rewiring its locks. (4)

Imagine also a hacker getting access to your computer together with your private key. From there, he can transfer the ownership of the car to his own private key. Again, you have no way to prove your ownership and because the block chain says it's his. Also bear in mind that the blockchain has no real names or identities, so it is not possible to trace the theft. (4)

As stated above we need intermediaries mostly to create trust between transactions and to be able to verify transactions and ownerships. Trust will not disappear with Blockchain - Trust is still involved but it is shifted towards the underlying complex cryptography, math puzzles, and distributed/crowdsourcing consensus. (5) Additionally we need people to help us verify that trust and also to convey it to businesses in terms of business value.

2. Appliance and usage

2.1 Everledger (6) (7)

The diamond and jewelry market is a valuable one, which offers a lot of opportunities for fraudsters, thieves and all others who are interested in all kinds of unlawful activities. Eventually, this costs the insurance companies around 50 billion dollars a year. (8)

The problem

Right now when insurance companies assess the diamonds and high-end jewelry, it is often done with more focus on the policyholder instead of the object itself. Unlike high-volume objects like cars there is no central, trusted database to turn to when it comes to diamonds and high-end jewelry. Right now everything is paper based and over time provenance gets lost. (8) This is the problem that Everledger tries to solve - by being a permanent ledger for diamond certifications and related transaction history. (6)

The solution

Everledger is a digital, global ledger that tracks and protects items of value. It's an early stage startup founded by Leanne Kemp. Everledger leverages the possibility to bind data about the diamond to the transaction. Together with adding 40 arbitrary bytes of this data as a secure hash, they can secure the information into the ledger and make it immutable. (8) The record is created by getting a digital "DNA" record from the stone so that altering it would lose so much value that it is not worth it. Therefore it is tamper free, immutable and can therefore be trusted. (8)

With this information it is possible to identify the owner of the diamond together with where it is. It can even trace diamond movements on platforms such as eBay and Amazon. Everledger also assists Interpol and Europol to find stolen diamonds by helping them with tracking the said diamonds - when and where they are crossing the borders and entering black markets. (8)

Additionally, Everledger uses an API and a Smart Contracts platform to facilitate the transfer of ownership of diamonds. These smart contracts will also fundamentally change the marketplace together with how diamonds are financed. (8)

2.2 Provenance (9)

Provenance is a UK-based company founded by Jessi Baker. They provide a platform that empowers brands to take steps towards greater transparency by tracing origins and histories of products. (9) Their goal is to define standards for supply chain data without linking to a proprietary system. They are building a public utility to keep track of our material world.

The problem

According to a study (10) by White Rose Research Online (11), 30% of UK consumers report that even though they are very concerned about environmental and social issues, they still struggle to translate these into purchases. (12) There is an information gap between the consumers and the suppliers. Consumers have hard time ensuring that the company they are purchasing the products from is as green minded as they like them to be or as the company says they are.

The solution

Provenance uses blockchain technology together with mobile devices and smart tags to track the products. It works by linking identity, location, material attributes, certifications and audit information with a specific item or batch and storing it in the blockchain. It is possible to use provenance through their smartphone application or by linking provenance with existing interfaces and systems for data capture along the supply chain. (12)

How it works? On Provenance's website there is a paper (12) published about their 6-month long pilot. The paper is about working together with two local fishermen from two different supply chains and how Provenance helped them collect catch data and track it through to suppliers to end-consumers. To summarize the process with these fisherman looks like this: (12)

1. The product is registered by respective fisherman after a catch. In Indonesia, the fisherman used simple SMS, thus issuing a new asset on the blockchain with each SMS. All relevant data associated with the catch is registered together with the created product ID. By working together with local NGOs and using their data together with Provenance, it was possible to verify the fishermen and their compliance to external standards, thus providing even more provenance information to the blockchain.
2. The fishermen issue a request to transfer the goods to the supplier. As supplier accepts this transaction, a new entry is created on the blockchain. After receiving the goods and confirming the transaction another checkpoint is created on the block chain.

3. NFC-enabled smart stickers are added to the goods from the supplier. These smart-stickers also carry the Provenance marque together with item or batch ID. Touching a smartphone over the sticker it is possible to see the product's journey from the sea to supermarket.

On a more technical side, provenance uses public chains. Although it would be much easier to use consortium blockchains for various reasons they decided to go with public chains. In a consortium chain, trust rests on an assumption that the small number of validators involved cannot collude. They could however still censor certain information if they share some common interest in doing so. Public chains on the other hand make that impossible, thus leaving the core data untouched. Public chains also make it easier to onboard new stakeholders (without changing consensus mechanisms) and also Provenance has stated that they want to use the new empowering technology in an open way. (12)

The technology has sparked interest from some food companies, with the Co-op Food group currently conducting its own trial with Provenance on fresh food products. Thai Union, the world's biggest tuna exporter has also welcomed the development.

Although they might seem to have everything figured out, Provenance is still struggling with some issues. For example they need to come up with better "smart-stickers". As NFC tags and QR codes are both easy to copy. So currently they are exploring ways to avoid duplication and luckily there are some technologies emerging that could probably solve this issue. (12)

According to the founder, "The next challenges are building scalability so that traceability systems can operate across borders and certifying authorities, and educating consumers that it is worth paying more for sustainably-caught traceable fish where workers are paid a fair and decent wage". (13)

2.3 Ubitquity

Ubitquity is a US based company founded in 2015 by Nathan Wosnack. Their objective is to change the real estate world by creating a blockchain-secured platform for real estate transactions as well as reduce the possibility of fraud which is often possible on centralized systems. They offer a SaaS blockchain platform which securely stores property records. They help with real estate as well as title insurance and e-recording companies - everybody who could benefit from a clean record of ownership and increased transparency. (14)

The problem (14)

The ensuing environment of real estate financing and title transfers has resulted in massive amounts of document errors and fraud. Additionally current real world solutions cause innumerable financial and emotional hardships for the citizens.

The solution (15)

Ubitquity provides a permanent way to register your property. Once the data is entered and hashed, it remains permanently on the block chain. Additionally, Ubiquity wants to create trust - as people have done more and more deals on the platform and have hard evidence on the blockchain that they were successful, others get more trust towards that individual.

Ubiquity currently tries to work together with companies that build brand new properties. This way the property is new and it has a clean slate and it is added to a new system. Without involving the government and bureaucrats with their existing properties it is possible to keep the corruption and inefficiency away from Ubiquity. This way in the end people will get more legitimacy and security.

Unfortunately, the current solution isn't without problems. Currently Ubiquity keeps away individuals from the system as they have no blockchain way of proving identity and they don't want to pollute their chains with junk data. Identification is just as import to them as multitude of different emerging blockchain applications. However in the blockchain world, companies are coming up with better and better identification protocols so once some new protocols are implemented to the real world then Ubiquity can also give access to individuals to sell and trade properties. At the moment they only allow reputable title companies to add new data.

2.4 Also Notable companies

VeChain - By combining Blockchain and NFC Counterfeit products VeChain creates a way to verify origin of products. By storing data on the Blockchain it is trustworthy and we can be sure that it remains there. (16)

BlockVerify - By tracking pharmaceutical products they offer a way for customers to ensure that they receive an original product. Additionally they track luxury items, diamonds and electronics. The idea remains the same: each product is labelled with a tag, each product is verified along the supply line and end-users can scan the tag with their smart devices and verify the history and origin of these products. (17)

3. The plan

Remove intermediaries

A common interest between most companies is to remove intermediaries. There are multiple reasons for doing so. Some or all cases apply to the companies listed above:

- **Reduce transaction times -** By removing intermediaries there might not be a need to go to a local government organization, wait in line, fill out forms, and wait for confirmations and so on. By putting the data on the blockchain and nobody being able to modify it there might not be need for intermediaries. As all relevant parties will also store their confirmation of transaction on the chain and it is there forever.
- **Reduce corruption and create more trust -** As it is extremely hard to alter data on the chain then there will be less forgery of documents and thus less corruption and false data.
- **Reduce transaction costs -** Another common reason for removing "trusted" third parties is to reduce transaction costs. As there are no third parties involved anymore then transaction costs would be drastically reduced.
- **More transparency** - Although closely related with multiple points listed here, it is also important to list this. By being able to verify product's history starting from the creation on the blockchain will increase the transparency and origin of the data.
- **More reliability -** By removing intermediaries and keeping the data on a decentralized networks there is no single-point of failure and the data is able to withstand malicious attacks. (18)

Immutable data

All of the above companies are interested in creating an immutable history for products of their interests. Either they are in the property business, diamond business or other consumer products. They do it by utilizing the Blockchain technology where it is extremely difficult to alter data. Although everybody uses the word immutable we don't say that it can't be done, but it is extremely hard to do it therefore we can call it immutable.

4. Comparison

Similarities

Interestingly, the more you learn about blockchain the more similarities you find and all the companies seem to be after the same things. But again the more you think about it; these are all the advantages of the blockchain and how it is introduced to everyone, and why everybody considered it in the first place.

Differences

The main differences are the fields these companies operate on. VeChain, BlockVerify, Provenance and EverLedger mark and track different smaller physical products while Ubitquity is more interested in keeping the integrity of data.

All companies seem to have different problems, although I would say they are all related to some kind of identification and security. Either be it identification of the user or identification of the product. (EverLedger doesn't seem to be as influenced by this problem but probably could also benefit from better identification protocols.)

Advantages

One of the advantages of EverLedger is that it is able to identify diamonds and jewelry by a unique DNA of every piece. Whereas Provenance tries to track a wide variety of consumer products and creating a unique ID for every product that will not be easy to forge is a challenge.

Applying blockchain in the health sector as planned by BlockVerify would save lots of lives. Especially in Africa. The US Food and Drug Administration (FDA) wrote in 2013 that "more than a third of anti-malaria drugs available in Sub-Saharan Africa and Southeast Asia are counterfeit or substandard." [FDA] Additionally fake malaria and tuberculosis drugs cause about 700,000 deaths per year, according to the UN in 2012. (19)

Disadvantages

There probably aren't any notable disadvantages yet as this is still a new technology and everybody is still searching for the correct way to do things.

The only major problem could be its disruptive nature cutting across all sectors of the world economy and eliminating middle men in global transactions.

5. Conclusion

The world of block chains is an interesting one. It has not fully evolved yet as all the companies are still looking for the correct ways of doing things and where to go next. It is good to see that there are multiple companies working on resolving different problems. This way, in the end, there is a greater chance of finding correct and better ways of doing things.

Additionally we see that currently all of the companies are mostly creating, sharing and using data for this to expand even further, more confidence is needed in the technology. More confidence from the general public as well as some larger sectors that are worried about the public nature of blockchains. As confidence into distributed ledgers technology grows then we can truly start creating decentralized ecosystems.

Right now the hype around Blockchain technology has probably settled and companies have started to work with the technology in a more systematic way. During the hype it was all probably fun-and-games but now we start to move onto more serious use cases and there are multiple companies already with working implementations of Blockchain technology. But nevertheless the hype, we still have fun times ahead of us.

References

1. **Forde, Brian.** Quora: What problems can blockchain generalizably solve? *Quora.* [Online] May 26, 2016. https://www.quora.com/What-problems-can-blockchain-generalizably-solve/answer/Brian-Forde?srid=aZhJ.

2. **Back, Anthony.** Quora: What problems can blockchain generalizably solve? *Quora.* [Online] June 8, 2016. https://www.quora.com/What-problems-can-blockchain-generalizably-solve/answer/Anthony-Back-1?srid=aZhJ.

3. **Featherston, Ed.** Blockchain: You Want Me to Trust a "Trustless Trust" System? *Collaborative.* [Online] Collaborative Consulting, April 18, 2016. http://www.collaborative.com/blog/blockchain-trust-a-trustless-trust-system/.

4. **Narayanan, James Grimmelmann & Arvind.** Slate: Bitcoin's blockchain technology won't change everything. *Slate.* [Online] February 16, 2016. http://www.slate.com/articles/technology/future_tense/2016/02/bitcoin_s_blockchain_technology_won_t_change_everything.html.

5. **Wadey, Emma.** Temenos: Is blockchain looking for a problem to solve? *Temenos.* [Online] Temenos, 2016. https://www.temenos.com/globalassets/mi/wp/16/blockchain-looking-for-a-problem-to-solve.pdf.

6. **Donnelly, jacob.** Distributed: Using the Blockchain to Track Assets for Proof of Ownership. *Distributed.* [Online] https://godistributed.com/news/using-the-blockchain-to-track-assets-for-proof-of-ownership/.

7. **EverLedger.** EverLedger: Home page. *EverLedger.* [Online] EverLedger. http://www.everledger.io/.

8. **Huckstep, Rick.** BankNXT: Everledger and the immutable protection of provenance through the blockchain. *BankNXT.* [Online] BankNXT, July 23, 2015. http://banknxt.com/52323/everledger/.

9. **Provenance.** Provenance: Home page. *Provenance.* [Online] Provenance. https://www.provenance.org/.

10. **Young, CW, Hwang, K, McDonald, S and Oates, C.** *Sustainable consumption: green consumer behaviour when purchasing products .* s.l. : White Rose Research Online, 2010.

11. **WRRO.** White Rose: Research Online. *White Rose.* [Online] http://eprints.whiterose.ac.uk/.

12. **Provenance.** From shore to plate: Tracking tuna on the blockchain. *Provenance.* [Online] Provenance, July 15, 2016. https://www.provenance.org/tracking_tuna_on_the_blockchain.

13. **Levitt, Tom.** The Guardian: Blockchain technology trialled to tackle slavery in the fishing industry. *The Guardian.* [Online] September 7, 2016. https://www.theguardian.com/sustainable-business/2016/sep/07/blockchain-fish-slavery-free-seafood-sustainable-technology.

14. **Ubitquity.** Ubitquity: Home page. *Ubitquity.* [Online] Ubitquity, 2016. https://www.ubitquity.io/home/index.html.

15. **McKibbin, Nathan Wosnack & Matt.** Blockchain-Based Real Estate: My Interview with the Founders of Ubitquity. s.l. : @piedpiper, August 2016.

16. **BitSe.** VeChain: Home page. *VeChain.* [Online] VeChain. https://bitse.com/portfolio/vechain/.

17. **BlockVerify.** BlockVerify: Home page. *BlockVerify.* [Online] BlockVerify. http://www.blockverify.io/.

18. **Deloitte.** Blockchain technology: 9 benefits & 7 challenges. *Deloitte.* [Online] Deloitte. https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html.

19. **Sambira, Jocelyne.** AfricaRenewal: Counterfeit drugs raise Africa's temperature. *United Nations.* [Online] United Nations, May 2013. http://www.un.org/africarenewal/magazine/may-2013/counterfeit-drugs-raise-africa%E2%80%99s-temperature.