Daniel Van Eijck

Ethereum blockchain mining

In traditional centralized currency systems, trusted third parties such as banks are needed to keep a ledger of all transactions and financial records. However, in a blockchain system the ledger is public and decentralized. This means that instead of the ledger being handled by a central figure, the new transactions are verified and added to the ledger by the entire network. In order to achieve this, a trustless and distributed consensus mechanism called "proof of work" is used [4]. Using a proof of work consensus mechanism, no one has to trust a central third party to validate transactions, because everyone has their own copy of the ledger and can directly verify the information written.

The proof of work consensus mechanism is driven by mining. Mining refers to an expensive computer calculation that needs to be performed in order to add new transactions in into a block on the blockchain. Mining serves two main purposes: to solve the double spending problem and rewarding miners with new digital currency for solving this problem [4]. The double spending problem is a problem especially linked to digital currencies. This is because digital information is easily copied and distributed to multiple sources. It is important that crypto currency is not double spendable, meaning that the same coin can be used in multiple different transactions, because this would heavy loss of trust in the currency, making it worthless. When a new transaction is proposed, miners use their CPU power to solve a mathematical puzzle known as the "proof of work problem". The process of solving this problem involves a brute force approach, which means continuously guessing the answer until it is correct [4]. The first miner who guesses the answer correctly adds the transaction to the next block on the chain.

Daniel Van Eijck

Proof of work consensus

The proof of work problem is a mathematical puzzle that has a key feature: asymmetry. Asymmetric encryption uses two keys to encrypt and decrypt data: a public key and a private key. The keys are two large numbers that have been paired together but are not identical. The key feature of the asymmetric puzzle is that it is moderately hard for the answer to be solved [3]. This means that there is competition between miners too see who can solve the puzzle first so that they can be rewarded with new coins. The mining process is an operation of inverse hashing. Miners continuously try to come up with a 64-digit hexadecimal number that is less than or equal to a certain threshold. This threshold is called the mining problem difficulty. As the demand for the crypto currency increases, the difficulty of the proof of work problem also increases. For example, when Bitcoin launched in 2009 the difficulty of the problem was set at 1. As of November 2019, the difficulty is over 13 trillion [3]. This difficulty parameter is updated every 14 days to keep the nature of mining competitive. As the difficulty of mining increases, miners must use more hardware (graphics cards) to make their mining attempts more efficient. Therefore, the higher the difficulty the more electricity is used by miners as they attempt to solve the proof of work problem first. There is a growing concern in the cryptocurrency community that the high energy usage involved with a proof of work consensus is leading to a constant downward pressure on the digital currency value, since the power used to perform mining must be paid with traditional currency. Data from 2015 showed that a single bitcoin transaction required the same amount of electricity used to power 1.57 American households for one day [3].

Proof of stake consensus

Just like proof of work, proof of stake is a kind of consensus mechanism that can be used in a blockchain system. Instead of miners, participants in a proof of stake system are called validators. Rather than everyone in the network competing to create a new block, a selection algorithm (based on an individual's stake in the currency) is used to pick a single validator that gains the rights to producing the next block [3]. This means that there is only one person mining the next block to put on the chain, instead of a large number of participants competing to be the first to solve the problem. This dramatically reduces the electricity used when creating the next block on the chain. Just like in proof of work, the validator will receive some reward tokens upon adding the next block. The size of this reward is proportional to their stake. If the validator misbehaves, then their stake is taken away, which incentivizes the validators to behave honestly [3].

The Proof of stake consensus mechanism intensely reduces energy consumption compared to Proof of work. Using PoW, Bitcoin alone consumed 22 terawatt-hours of energy in a year [6]. The majority of this energy is wasted because only one miner is rewarded with new coins for each block added to the chain. Using proof of stake, it is estimated that the power consumption would be equal to the power of a Raspberry Pi [6].

Daniel Van Eijck

Permissioned vs Non-permissioned blockchain

There are commonly two types of blockchains: Permissioned and Non-permissioned. A non-permissioned blockchain allows anyone to join the network. This means that everyone in the system can interact anonymously and without having to trust each other. In a permissioned blockchain, a user requires access in order to join the network. This feature eliminates the ability to interact with the blockchain in an anonymous way. Permissioned blockchains are crafted to take advantage of blockchain technology without losing the central authority aspect of a centralized system [2].

Permissioned blockchains often have a much smaller number of nodes in the system compared to a normal blockchain. This makes the process of verifying transactions much more efficient, because permissioned blockchains often have pre-determined nodes for performing the consensus mechanism. However, due to the small number of nodes in a permission blockchain, this makes it easier for the security of the system to be compromised. The security of a permissioned blockchain is proportional to the member's integrity. If enough members work together, then information on the blockchain can be modified [2].

Permissioned blockchains have a proper governance structure which comes with a few benefits. Updating the rules of the network can be completed much faster compared to a public network due to the smaller number of nodes [2]. Every node in a permissioned blockchain works together to move the updates faster. However, there are also some drawbacks that come with having a governance structure and regulations. Having regulations on the network introduces censorship. An example of such censorship is where the central authority can choose to restrict a transaction or even stop it from happening. This is a major threat to any of the organizations that are part of the system, because their cashflow can be interrupted at any time by the central governing authority.

Permissioned blockchains are much more cost effective than public blockchains, especially when using a consensus mechanism like proof of stake with pre-determined nodes for performing validation.

Scalability

In the domain of blockchain technology, scalability refers to the ability of a Blockchain to accommodate a growing number of users while still retaining a fast consensus. Currently, public blockchains are unable to scale up because of the inefficiency of consensus protocols when used with large numbers of users. This inefficiency results in a longer "block time" which is the time it takes for new blocks to be added to the chain. A long block time means that transactions on the network take longer to verify and complete. Permissioned blockchains often have much smaller block times compared to public blockchains. For example, Bitcoin has a block size of 1 megabyte which fits 2000 transactions in it [1]. It takes approximately 10 minutes for one block to be mined and added to the chain which results in a transaction throughput of 7 transactions per second. The Ethereum blockchain can process a maximum of 20 transactions per second. In contrast, the permissioned HyperLedger blockchain can process up to 100,000 transactions per second [1].

Daniel Van Eijck

Proof of authority consensus

The Proof of Authority (PoA) consensus mechanism is an algorithm that is currently being implemented that attempts achieve a much higher rate of transactions per second. PoA is a reputation-based consensus algorithm that provides an efficient solution for private blockchain networks [5]. This consensus mechanism leverages on the value of certain entities of the system. Similar to proof of stake, not everyone on the network competes to mine the next block and instead, a single node is chosen based on an algorithm. In proof of stake, this algorithm considers a participant's stake in coin, however in PoA the algorithm considers the participants reputation score. Reputation is considered to represent trustworthiness in a system therefore the pre-determined block validators are trustworthy nodes that act as the moderators of the system [5].

There are a few things that a system needs to be able to run a PoA consensus:

- Valid identities: the block validators need to confirm their real identities (permissioned blockchain)
- There must be some level of difficulty to become a validator. If it is someone difficult to gain reputation in the system then this reduces the risk of selecting bad validators and incentivizes a long-term commitment.

A major limitation of this method is that it eliminates the true decentralized nature of the blockchain. Since it has such a high transaction throughput and the need for identity confirmation, it makes it an attractive solution for large corporations with logistical needs [5]. However, with the system being moderated by a few individuals with high reputation, this introduces the possibility for censorship and blacklisting. Another downfall is that because the block validators are publicly visible and identifiable, it is possible for people to try and influence the block validator to act dishonestly in order to comprise the network. In conclusion, PoA sacrifices decentralization for better scalability and higher transaction throughput.

Daniel Van Eijck

Decentralized autonomous organizations (DAO)

A decentralized autonomous organization (DAO) is a network of agents interacting with each other according to an open source self-enforcing blockchain protocol. In traditional organizations, all agents involved with the organization have some kind of employment contract that states their relationship with the organization and with each other. If an agent breaks the rules of their employment contract or something else goes wrong, the legal contract will be enforced in a court of law according to the law of the country the organization resides in. However, in a DAO, there is no legal contracts that determine the relationships between agents. Instead, agents are steered by incentives tied to the network tokens and fully transparent rules that are written into smart contracts.

DAOs have many advantages over traditional organizations:

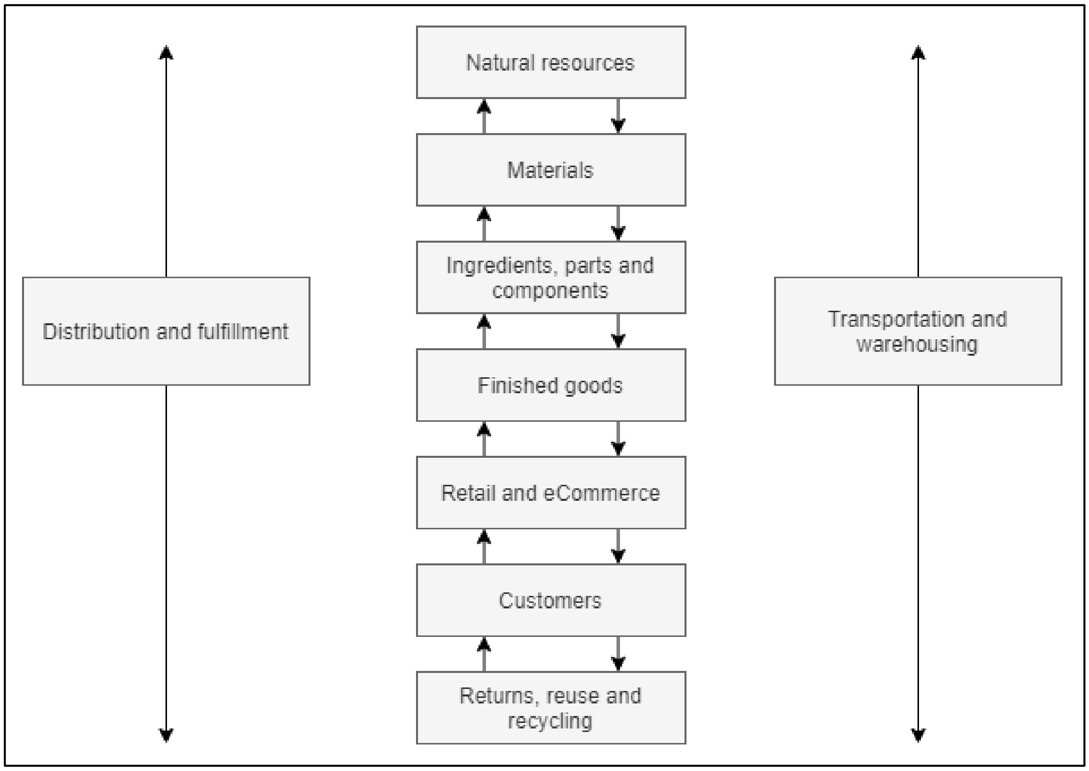
- Coordinating resources when not all parties know/trust one another
- Aligning large number of stakeholder contributions towards shared goals
- Running organizations in a way that is resistant to censorship
- Tracking and validating participation and contribution to a project
- Accommodating a variety of levels of contribution
- Allowing people and entities to contribute work in a jurisdiction-agnostic fashion

So far, there is two generations of the development of blockchain technology. The first generation was the introduction of Bitcoin. Bitcoin created a decentralized eco-system for holding and transferring currency. The second generation was the introduction of Ethereum. Ethereum also provides a decentralized currency system but with the additional ability to add business logic to smart contracts. An example of such business logic would be: if company X completes task Y then automatically transfer Z amount of crypto currency to them. For this reason, Ethereum is the most popular platform for DAOs to be built upon.

Supply Chain DAOs

It is often desirable for companies in a supply chain to track physical assets digitally to be informed about location, trigger processes, certify ownership and perform the corresponding payments. The reason blockchain technology is a good candidate to store supply chain data is that there are many different parties involved in the supply chain network. Although it is often stated that certain organizations in the same supply chain are in “trusted partnerships”, at the end of the day they are still two different organization each pursuing their own interests which means there is only a limited amount of trust [7]. Parties in a supply chain maintain contractual relationships. In the simplest case, the contract involves one party buying x amount of y at a time t and a price p. When there is a high rate of exchange of goods it becomes hard to monitor, especially at a global scale. In traditional systems, this information is stored and used in many different systems that are most likely in many different countries. This is one of the key problems that using the blockchain can solve: the tracking and tracing of exchanged goods at a global scale. However, one challenge is having a trusted source of input data that translates events in the real world into data on the blockchain. One method to doing this is by using an Oracle. Oracles translate events in the real world into transactions on the blockchain.

Basic hypothetical system


Natural resources
Materials
Ingredients, parts and components
Distribution and fulfillment
Transportation and warehousing
Finished goods
Retail and eCommerce
Customers
Returns, reuse and recycling

The hypothetical supply chain consists of many components that interact with each other in order to produce and deliver a product to consumers. Interactions should also be able to move backwards up the supply chain to support returns and refunds. Each component in the system requires stakeholders that perform distribution and fulfilment of the products needed at each step in the supply chain. Transportation and warehousing are also needed throughout many levels of the supply chain.

Let’s imagine a hypothetical supply chain for the production of PVC products.

Natural resources: The raw materials required to make the product. In cases such as PVC production, this may be things like water or oil.

Materials: The production or procurement of materials such as Naphtha, Ethylene, Chlorine.

Ingredients, parts and components: Combining the materials into parts and components for the final product. In PVC production, this would be combining the materials in order to produce the PVC resin.

Finished goods: Combining the parts and ingredients to form the final PVC product ready to be distributed.

Retail and Ecommerce: The PVC product is distributed to shops and advertised online.

Customer: The customer buys the product either in a shop or online.

Returns, reuse and recycling: The PVC product supply chain needs to support the ability for customers at any level of the chain to return products if they are not happy with them. To promote sustainable practices, the products will either be reused or broken down for recycling.

The interactions between these components will be achieved through implementing supply chain management. Supply chain management can be broken down into three things: Material flow, Information flow and Financial capital flow between the stakeholders in the system. The supply chain management system must support each stakeholder in the chain to trade goods and services between each other while maintaining an immutable ledger of all transactions. If you can properly implement supply chain management then you can increase sales, decrease fraud and overhead costs, improve quality and reduce the cost and complexity of the manufacturing process [9].

A supply chain DAO can solve many problems faced by supply chain solutions. The DAO enforces trust between parties with different interests, so that they can work together towards a shared goal in a unified way. The DAO allows products to be tracked and traced throughout the supply chain and this provides an immutable dataset of history for each product that is open and transparent. However, one challenge is finding a reliable way to update the product data in the blockchain. Oracles are used to translate events in the physical world into transactions on the blockchain.

Key features of a basic supply chain management system:

Digital ownership certificates: A digital mirror asset that links to the physical asset. The blockchain maintains information about each asset such as a unique ID or serial number that links the physical asset and the wallet address of the owner [10]. The blockchain is immutable, so only legitimate transactions can take place and therefore the ownership of an asset cannot be stolen by manipulating the blockchain.

Asset tracking: used for tracking assets as they move along the supply chain. For each transaction, you can see the timestamp and which parties were involved for free [10]. In order to implement asset traceability, smart contract trees are used to link different assets to a common product. Transactions become expensive, because each time a product is passed on, the ownership certificates for each asset linked to that product need to be updated.

Proof of origin: This allows both producers and consumers to validate that an asset is genuine. I.e., an original and not a pirated product. This can solve problems such as clients asking for manufactures warranty while having a fake product.

Trusted maintenance tracking: The lifecycle of a product does not end as soon as it is in the hands of the customer. Maintenance of products is an important part of the supply chain for many different reasons such as ensuring safety and providing additional services to the consumer. For warranty concerns, it is important that maintenance events are stored with a timestamp and remain unmanipulated. Smart contracts can be used to issue maintenance work to a worker via the products unique ID. The worker then completes the work and records the work tasks and required work effort and submits a confirming transaction on the blockchain [10]. The owner then signs the transaction, confirming that the work has been done.

Integrated financial transaction: Because smart contracts allow for atomic linking of data transactions and financial transactions, it is possible to make payments to agents in the network as soon as the task is completed. For example, as soon as a PVC material shipment is scanned as delivered, the payment for the shipment can be executed immediately.

Daniel Van Eijck

Distributed product master data: Places such a retail stores that are selling products that come from the supply chain can use the blockchain to get a comprehensive overview of product master data, such as title, description, pictures, serial numbers and a breakdown of where each component of the product came from.

Components that enable these features:

Trusted devices (Oracles): devices that change the state of the blockchain. For example, a device that spawns a digital mirror asset on the blockchain at the moment the physical asset is produced. Another example would be a mobile phone scanning a product QR code in order to confirm the delivery of a product.

Asset management platform / in-the-field interface: A portal that allows manufactures or owners of assets to manage their assets. A place to manage everything from checking transaction history to transferring assets to a new owner. However, this should not just be designed to run on a standard desktop computer. The use of NFC and QR codes allow assets to be physically scanned in the field to access information.

Existing solutions:

There are many supply-chain projects in development that utilize the blockchain. The field of supply chain solutions built on blockchain technology is very recent and there are new developments arising very day. Below is an overview of some of the most important projects in this domain.

Everledger is an independent technology company that provides businesses with secure technologies including Blockchain, Artificial intelligence and Internet of things [11]. Everledger has a range of industry solutions that are being used today. An example of one of their solutions is Everledger minerals. This platform provides traceability throughout the lifecycle of high-risk products and helps to support reuse and responsible recycling of material such as portable electronic batteries. One of the key features of the system is the ability to monitor sustainability. Being able to trace assets through the production line enables higher visibility and control over responsible and ethical sourcing throughout supply chains.

Transparency-One enables companies to discover, analyze and monitor all suppliers, components and facilities from source to store. It is built on Microsoft Azure's blockchain service which uses the Ethereum protocol to encrypt data [8]. Transparency-One claims to help companies identify potential issues in their supply chains such as Modern slavery and product fraud. Companies have complete access to information on where and when assets are modified and exchanged, which helps them prove that their products come from ethically sound sources.

Daniel Van Eijck

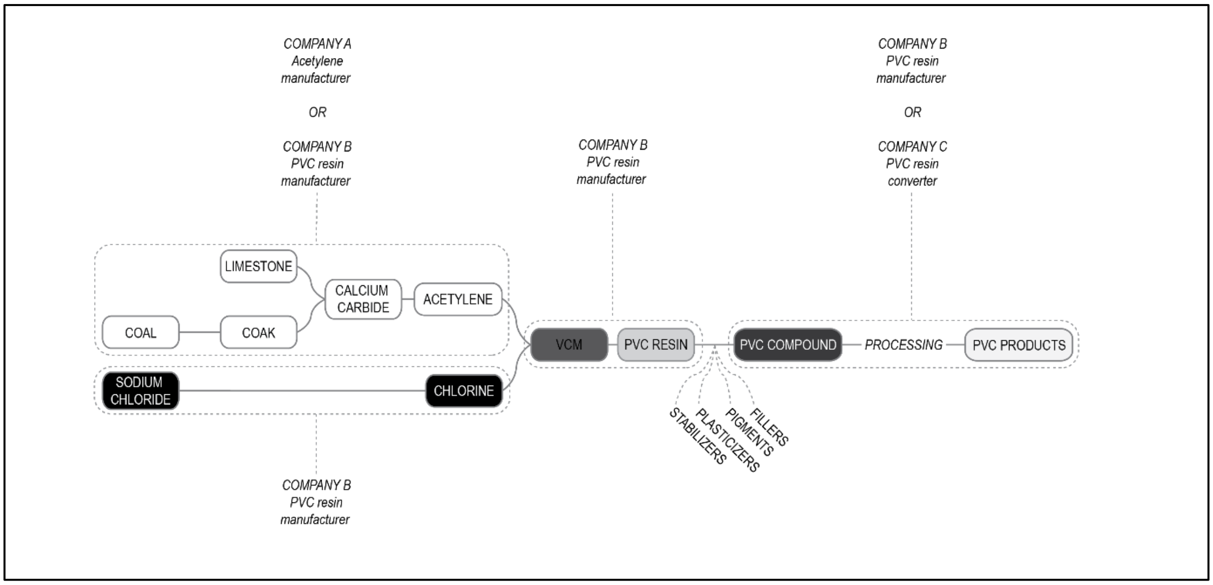
VeChain is an open source blockchain platform made to enhance supply chain management and business processes [12]. The whitepaper for VeChain [13] states that the dream of the platform is “Building a trust-free and distributed business ecosystem platform to enable transparent information flow, efficient collaboration, and high-speed value transfers” [13]. The VeChain platform consists of two tokens called VeChain Token (VET) and VeChainThor Energy (VTHO) [12]. VET is used as a currency in order to transfer value across the network and VTHO is used as gas to power the transactions. VeChain’s whitepaper states that the platform allows authorized stakeholders to view a full breakdown of information linked to a product and its business processes such as storage, transportation and supply. In order to accomplish this, VeChain uses Radio Frequency Identification tags and smart sensors which broadcast relevant product information onto the blockchain network. VeChain uses a Proof-Of-Authority consensus mechanism to validate transactions and incorporates a unique governance structure and voting mechanisms for deciding on changes to the platform. VeChain uses a permissioned blockchain, meaning that all nodes are validated and approved by a central trusted party (the VeChain foundation) which means that blocks can be validated faster and more efficiently compared to Proof-Of-Work or Proof-Of-Stake consensus mechanisms.

The VeChain economy consists of the two coins VET and VTHO. VET is used to store and transfer value, while VTHO is used to pay for interacting with the blockchain (transaction fees). Users are rewarded with VTHO for holding VET. Currently, 1 VET will generate 0.000432 VTHO per day [13]. This essentially allows users to use their VET for free as long as own an adequate amount of VET that is generating VTHO. As more parties begin using VeChainThor blockchain, the demand for VTHO will also increase, along with its price. This will also drive up the price for VET, since it can be used to generate VTHO.

A unique feature of VeChain is its transaction model. As we have seen, other blockchain projects such as Bitcoin and Ethereum struggle to solve scalability issues such as congestion on the network and huge increases in transaction fees. As a result, VeChain has moved away from using Ethereum and instead have their own blockchain called VeChainThor. VeChainThor solves the network congestion issue by allowing subsequent transactions to be processed even after one has failed. The failed transaction can simply be re-sent after the rest of the transactions in the pool have been processed. VeChain also allows the user to set an expiration time to their transaction. If the transaction is not validated by the expiation time, the user can resend it with a higher transaction fee. VeChain solves the problem of high transaction fees by setting a limit on how high the transaction fee can be. On platforms such as Bitcoin, spammers can prevent transactions with low fees from being processed by flooding the network with transactions with high fees. VeChain sets the limit of the transaction fee to 2x the current market price, which makes the transactions costs more stable and predictable [14].

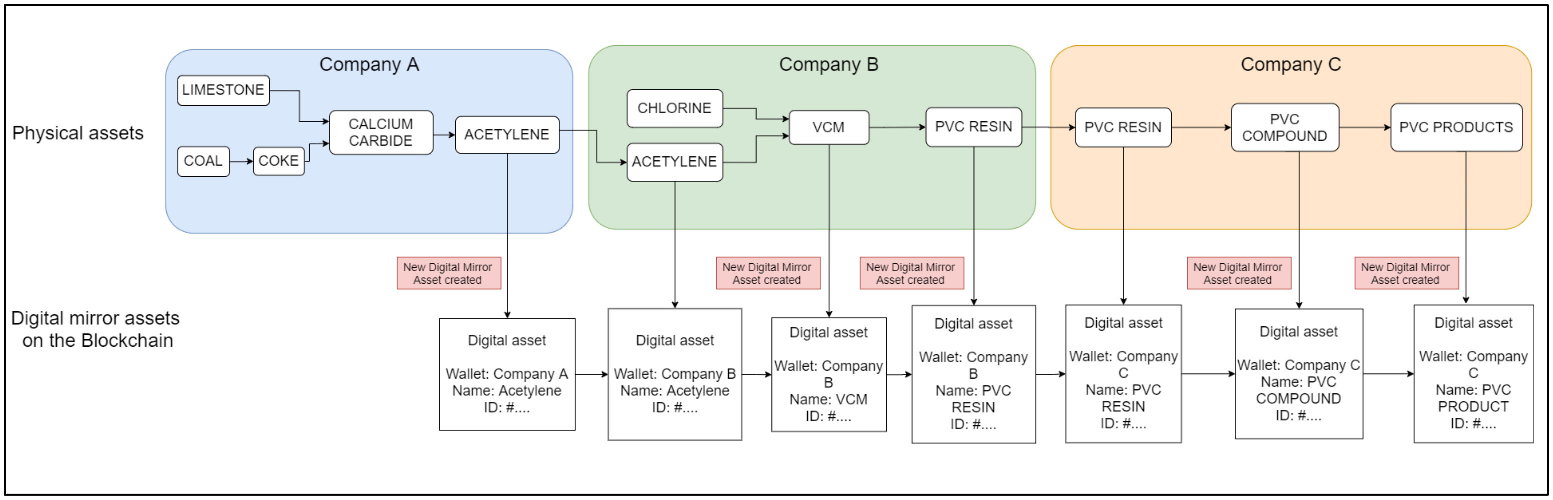
Daniel Van Eijck

Hypothetical PVC supply chain solution with blockchain



The above figure shows an example of a supply chain for the production of PVC products in China. There are many different methods for the production of PVC products. In some methods, the production is "fully integrated", meaning that all of the materials can be acquired and processed by a single PVC resin manufacturing company. However, in China it is common for PVC resin manufacturer companies to use a process that is only "integrated up to chlorine", which means the company must purchase Acetylene from another company. Once the PVC resin manufacturer has produced the resin, that company or a separate company will convert the resin into PVC products.

Our blockchain supply chain system can be utilized most effectively in the cases where assets must be transferred between different companies. We will focus on the method where 3 separate companies are involved. Company A will produce the Acetylene. Company B will buy Acetylene from Company A in order to manufactory the PVC resin. Finally, Company C will buy the PVC resin from Company B and convert it into PVC products. From there, the PVC products will be distributed to the retailers.



The above figure demonstrates how the blockchain would be utilized to keep track of assets in the PVC manufacturing supply chain. The first digital mirror asset that is produced is for Acetylene. In order for the digital asset to be created, a set of trusted oracles are needed that can capture the information associated with the physical asset and upload this information to the blockchain. These would perhaps be a set of measurements such as weight and chemical content of the Acetylene batch collected by hardware oracles, which a software oracle could then verify and upload to the blockchain. Once the digital mirror asset has been created, some kind of tag such as a Radio Frequency Identification tag or a QR code would be attached to the physical asset, linking it to the digital one.

Then the Acetylene is purchased from Company A by Company B through a transaction. In the physical world, the asset is picked up for transit and sent to Company B. It would be possible for the courier to scan the physical asset's tag upon pickup and then use special oracles to upload information to the blockchain such as live location tracking and confirmation of delivery. Once the asset has been marked as delivered, smart contracts can be used to automatically send the digital asset to Company B's wallet. When Company B processes the Acetylene with Chlorine to produce VCM, a new digital mirror asset is created for VCM. This digital asset is linked to the digital asset of its ingredient Acetylene. The link between digital mirror assets is needed for the ability to track production history of an asset. Company B then produces the PVC resin, along with its own digital mirror asset which is given to Company C through another transaction process.

Company C then converts the PVC resin into the PVC compound, and a new digital mirror asset is created that contains information on what additives were used to convert the resin into PVC compound. Then PVC products are produced, with their won digital mirror assets that are linked to the batch of PVC compound that was used to produce them.

Finally, when the PVC products make it into the hands of the consumer through the retail process, information of each product can be accessed through the Radio tag or QR code that is attached to the physical product. The consumer will be able to see a complete history of the manufacturing process that was used to produce the product.

Energy consumption

The energy consumed by a blockchain supply chain solution comes down to two main components: the energy used to process each transaction on the blockchain and the energy used by the hardware and software oracles that capture information and upload it to the blockchain.

In the hypothetical PVC supply chain described on the previous page, the most suitable solution would be a permissioned blockchain using a proof-of-authority consensus mechanism, as the system is comprised of a set of verified and trustworthy stakeholders as participants. Unlike with proof-of-work consensus, there is no technical competition between block validators which means that P-o-A requires almost no computing power and therefore almost no electricity for its operation [15].

As for the energy consumption of the hardware and software oracles used in the system, this is entirely dependent on a number of factors that will be specific to a real-world setup. It is hard to estimate the energy consumption of these oracles without knowing the exact way in which they are setup and used. Factors to consider would include:

- The power efficiency of the hardware being used. This hardware could include things such as:
    - Engravers used to engrave unique IDs onto physical assets
    - Printers used to print unique IDs onto physical assets
    - Devices such as scales, thermometers and/or other machines for measuring chemical composition
    - GPS devices for live location tracking
- The throughput of the supply chain. Energy consumption would be influenced by how many physical assets are being mirrored and tracked on the blockchain each day.

Without knowing the exact equipment and material throughput associated with each part of the supply chain, it is difficult to estimate an accurate figure of energy consumption. However, we can conclude that using a permissioned blockchain with a proof-of-authority consensus mechanism for verifying blocks uses next to zero energy compared to the more well known consensus mechanism bitcoin uses which is proof-of-work.

References

[1] https://www.climateledger.org/resources/Blockchain-Potentials-Climate-Policy_2019.pdf

[2] https://101blockchains.com/permissioned-blockchain/

[3] https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

[4] https://www.investopedia.com/tech/how-does-bitcoin-mining-work/

[5] https://www.binance.vision/blockchain/proof-of-authority-explained

[6] https://dzone.com/articles/the-proof-of-work-vs-proof-of-stake-an-in-depth-di

[7] https://blog.codecentric.de/en/2017/09/unblocking-supply-chain-blockchain/

[8] https://www.transparency-one.com/wp-content/uploads/2018/10/SGS-AFL-Transparency-One-White-Paper-EN-HR-18-10.pdf

[9] https://blockgeeks.com/guides/blockchain-and-supply-chain/#Components_of_a_Hypothetical_Supply_Chain

[10] https://blog.codecentric.de/en/2017/10/blockchain-in-the-supply-chain/

[11] https://www.everledger.io/about/

[12] https://www.investopedia.com/terms/v/vechain.asp

[13] https://cdn.vechain.com/vechainthor_development_plan_and_whitepaper_en_v1.0.pdf

[14] https://vechaininsider.com/vechain/how-vechains-advanced-transaction-model-solves-the-problems-bitcoin-and-ethereum-are-facing/

[15] https://www.coinhouse.com/learn/blockchain/what-is-proof-of-authority/