AMable

Guide to Blockchain for Additive Manufacturing

Guide to Blockchain in Additive Manufacturing

Blockchain is a technology for a tamper proof registration of transactions in the digital world. Prominent applications today are for example financial services, insurance claim handling or logistics. All applications have in common that data associated to an entity is created over time and that this data or the change of this data needs to be recorded. Signing rules as we know them for conventional contract agreements are implemented in the form of consensus mechanisms.

In this document, we explain the main differences and what you should look at when considering blockchain to be beneficial to you.

Talk to us. We are there to help.

Blockchain

A bit of history

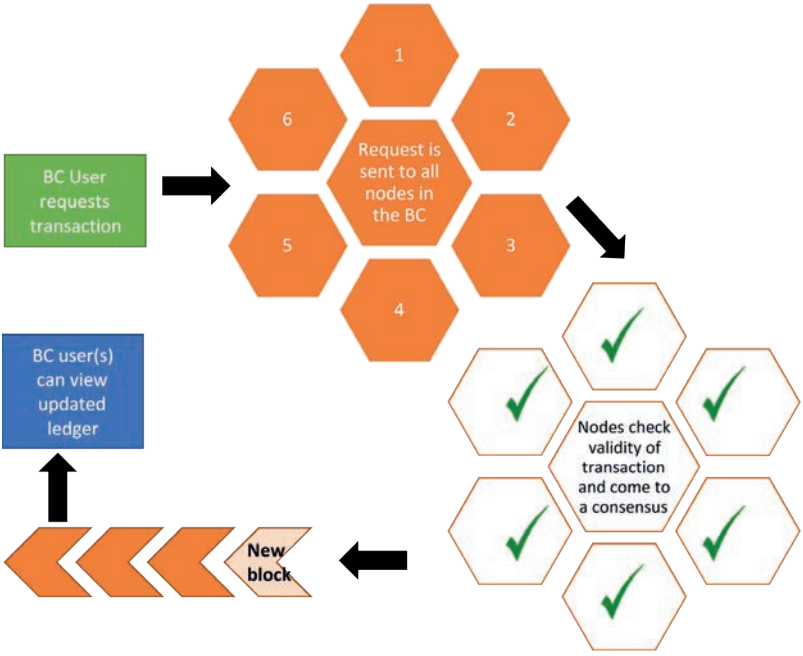
A chain of blocks becomes a blockchain

The basics of what we call blockchain today were invented in the 1990's by people such as S. Haber, W. S. Scott Stornetta, Ross J. Anderson, Bruce Schneier and John Kelsey. They developed principles on how to securely store data blocks that evolve over time. The idea was to use cryptographic algorithms that connect the evolving data blocks in a way that any manipulation of a previous block would be prohibited.

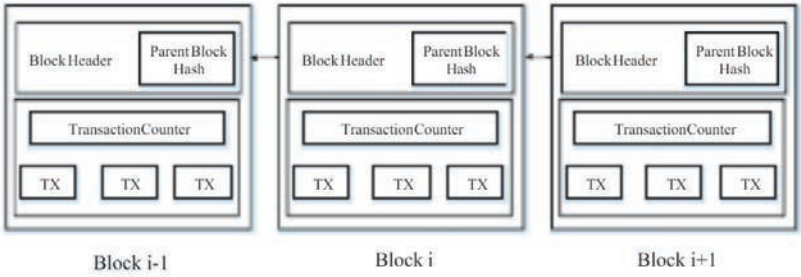
In 2008, the pseudonym Satoshi Nakamoto published a white paper about a distributed data base that would hold such data blocks in multiple places. This proposal opened the door for all the applications that we see today as it prevents manipulation of the database itself.

Consequently, the first implementation was published open source in 2009. Its best known use is Bitcoin and has developed significantly over time. The transaction database today (2019) is 200 GB in size, growing exponentially. As with all new technologies, there are upsides and downsides. Where accessibility, security and traceability are key offerings, energy consumption is a key criticism. The Verge (theverge.com) cites estimates that bitcoin computing with 68 TWh consumes more energy than the entire country of Switzerland with 58 TWh (status July 2019).

People discuss if the estimates on bitcoin energy consumption are realistic but the existence of "bitcoin mining farms" with huge amounts of computes makes clear, that bitcoins do not come for free.



Chaining of blocks based on consenus of the nodes in the blockchain network



Blocks of data (transactions) are connected through linking of hash keys.

Bitcoin calculation is safe due to its open and distributed concept, but this comes at an expensive price and large ecological footprint. Blockchains however do not need to be that expensive. The key factors are influenced by architecture and consensus mechanism. Much of this can be well balanced with a permissioned blockchain implementation.

Blockchain functional principle

Blockchain (BC) is a technology which supports the documentation and administration of transactions between parties without the need of a 3rd trusted party (central authority). It is managed typically in a peer-to-peer network which is able to control and verify transactions within an open and distributed ledger. This makes BC technology a trustworthy and secure solution for recording any type of transaction, since it requires unanimity among the network's majority for any addition to the chain to be approved.

Blockchain is a sequence of blocks which holds a complete history of transaction records forming a chain. Blocks consist of two parts; the header and the body. The header includes the block's specifications like a timestamp, the parent's block hash, and the current transaction's hash (Merkle Root). The body consists of a transaction counter and the transaction data.

When a transaction event occurs, a new block is nominated for addition to the chain. For the new block to be added, the network must reach consensus over this action. One common consensus strategy is the Proof of Work (PoW). The participants that are involved in this this process are known as nodes. Once the addition event has been approved, a block with the characteristics mentioned above is added to the chain. The new appended block

once added to the chain cannot be altered retroactively due to the crypto-algorithmic linking of hash codes.

Decentralise management and be less assailable

Decentralisation/ Disintermediation

Transaction's validation/management and data storage in classic centralized systems, are costly and time-consuming processes. Blockchain does not perform such acts under the scheme of a central authority, but instead uses consensus algorithms to maintain data consistency in a distributed network. In such a decentralized system, the concept of trust is distributed among its members, single points of failure are eliminated, and transactions intermediates are limited.

Data integrity/Traceability

The blockchain utilises an open distributed ledger which is managed by the participants of the network. It is nearly impossible to delete or rollback transactions once they are included in the blockchain. Cryptographic algorithms that link block content to the block's links enables immediate identification of content manipulation. Any transaction must refer to some previous transactions to be linked. The approval of this referral is the consensus that is received from the nodes of the network.

Consistency

The automated processing of the blockchain provides a platform which can perform transactions and data management along its network unceasingly 24/7.

Privacy

Blockchain by principal does not impose restrictions to the transaction data. It can be open or encrypted and access to the nodes can be open or authentication based.

Blockchain types

Get the right architecture for the individual use case.

There are three basic types of blockchain implementations. Their characteristics have an impact on trust, performance and eco-footprint. It is the application and the environment that should influence the decision for the best fit.

Public Blockchain

All records are visible to the public and everyone can potentially take part in the consensus process. Since records are stored by many participants, it is nearly impossible to tamper with transactions. It is very time-consuming to propagate transactions and blocks as there are many nodes on a public blockchain network.

Private Blockchain

A private blockchain is a fully centralised structure and can only be accessed by those who have been pre-approved and have the correct permissions. The network is often administrated by a single body. Transaction visibility depends on the administrator who can determine the final

consensus. The network can be tampered with easily due to its centralised nature. Although the limited number of participants make it more "time efficient" than the public blockchain.

Community/Consortium Blockchain

A community or consortium blockchain is partially decentralised since only a small portion of nodes are selected to determine the consensus. Unlike a public blockchain, where anyone can access the network, or a private ledger where there is a single administrator, a community blockchain has a few pre-selected nodes responsible for validating and managing the transactions. Tampering with a community blockchain would require all node administrators to agree which brings the security down to the selection of trusted bodies. This type of blockchain has the advantages of low computational effort for consensus with a high reliability based on defined administration authorities.

Blockchain for additive manufacturing

Make the technology help your technology.

Blockchain today is mainly used for currencies like Bitcoin but also for transaction management in the financial sector and in logistics. All these cases use the secure and tamper proof recording mechanisms of the blockchain technology to record a status of their data blocks at a specific point in time.

What is the AM benefit from using a blockchain?

In additive manufacturing, data accompanies the entire process of a product life cycle. This makes it an ideal application scenario for blockchain technology. In contrast to logistics however, data in additive manufacturing can be manifold. It is not a parcel that arrives at a specific geolocation at a specific point in time that is administered by a specific entity with some status on

trade tariffs being paid or conformity being signed off.

From a first idea about product functionality and the realisation approach, there is a phase of design, construction, print and post processing before the product is available for use. Data that is created along this path can consist of sketches, drawings, 3D models, simulation loads, analysis results and log files from the production process – these sometimes with considerable file sizes. This prevents data from additive manufacturing to be stored directly into a blockchain implementation.

Hashing algorithms create relatively short number sequences that identify files of nearly any size unambiguously. This technology is typically used to verify the integrity of downloads for operating system updates or program installations. The "MD5" hash code algorithm for example has been developed in the 1990's and creates a 128 bit long hexadecimal number. Since then, numerous computer specialists have addressed the reliability of the MD5 algorithm and discovered weaknesses which make it possible today to create two files that result in the same hash key which is called a collision. As computer hardware develops and knowledge increases, such algorithms will probably see a collision at some time. Algorithms such as SHA-256 are considered safe today. However, as any knowledge about the original file might support an attack, it is best to keep the original file private.

Printing machines

Logging of machine data?

The use of blockchain ledgers in machines has been considered by a number of companies and mostly aim at

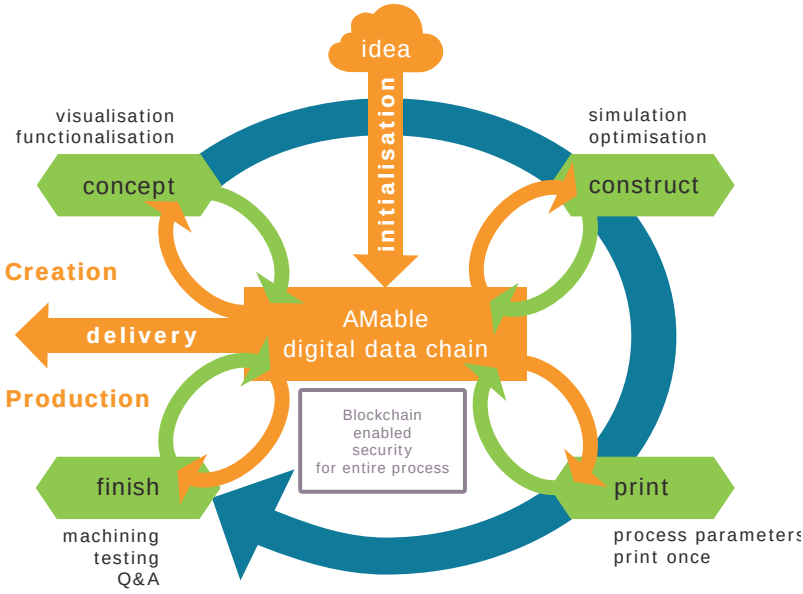
- Documentation of machine usage
- Recording of quality related events
- Logging of number and kind of print parts

Some of these implementations are discussed in research projects and some applications have been filed for patent.

Logging of product data?

AMable Digital Data Chain

One application case thus is to persist the existence of data files (kept private) through storing hash keys of such files (in a permissioned blockchain). The AMable Blockchain as part of the AMable Data Chain allows users of additive manufacturing to consequently document the status of their data with close to zero effort. A simple run of a file through the app creates a hash key, adds a time stamp and chains this data with the registered user account. At any later point in time, this hash key can be retrieved and compared against the newly created hash key of the actual copy of the file. And the best – the file remains under the full control of the user.



The AMable Digital Data Chain enables tracking of data that evolves along the product development process

Resume

Blockchain is a mature technology used well in the financial and logistics sector. Bitcoin was the first and is the best known application yet. But with its large eco-footprint it is also a subject of ongoing discussions which does not support the diffusion into other application areas.

Dynamics of design and development, of data creation and adaptation is characteristic for additive manufacturing.

These characteristics make additive manufacturing a premium use case. Key success factor herein is to keep the data files with the data owner and to only transfer only hash keys of the data files. This allows blockchain to be eco-friendly, to protect IPR and to secure business success through tamper proof continuous documentation and traceable change management.

Talk to us. We support you.

Contact

projectoffice@amable.eu
www.amable.eu

Coordination

Fraunhofer Institute for Laser Technology ILT
c/o Ulrich Thombansen
+49/241/8906-320
ulrich.thombansen@ilt.fraunhofer.de

amable.eu

/company/amable-eu

@amable_eu

Channel: AMable

This project is co-funded by the European Union's Horizon 2020 research and innovation program under grant agreement 768775