THE BLOCKCHAIN FOR SCIENCE

Whitepaper 2.0

May 2022

Contact:
info@bloxberg.org

Authors:
Friederike Kleinfercher kleinfercher@mpdl.mpg.de
Sandra Vengadasalam vengadasalam@mpdl.mpg.de
James Lawton lawton@mpdl.mpg.de

Table of Contents

Keywords {blockchain, distributed ledger technology, timestamping, global consortium, science, ethereum, POA, bloxberg}

Disclaimer:

The bloxberg infrastructure is defined as a research project. All consortium members work forcefully towards establishing bloxberg as a sustainable globally functioning network. Nevertheless during the research project phase interfaces may be modified, the governance model may change and data might get lost.

ABOUT

The bloxberg infrastructure is a secure scientific global blockchain established by a consortium of researchers and research organizations to provide science with decentralized services worldwide. It broadens the scientific landscape of regionally and nationally governed blockchain networks, and is the first truly globally maintained scientific decentralized network for scientists.

The bloxberg consortium aims to foster collaboration among the global scientific community, empowering researchers with robust, autonomous services that transcend institutional boundaries. The excellent reputation of the participating research organizations encourages scientists throughout the world, to utilize the bloxberg network and the applications built on top of the infrastructure.

BLOXBERG FOUNDERS

The bloxberg consortium was initiated in February 2019 at the invitation of the Max Planck Society together with the founding research organizations. Each of the participating research organizations has an in-depth knowledge of the groundbreaking possibilities of DLT in science and recognizes the enormous potential of a truly decentralized global scientific infrastructure like bloxberg for the scientific community worldwide.

With the 11 bloxberg founders, 9 different countries are represented with at least one renowned research organization:

Organization	Country	Contact
Max Planck Society	**Germany**	Sandra Vengadasalam
University of Nicosia	**Cyprus**	Soulla Louca
University College London	**UK**	Tomaso Aste
IT University of Copenhagen	**Denmark**	Roman Beck
University of Kassel	**Germany**	Walter Blocher
Georgia Institute of Technology	**USA**	Vijay K. Madisetti
Carnegie Mellon University	**USA**	Sevin Yeltekin
University of Johannesburg	**South Africa**	Maria Frahm-Arp
University of Sarajevo School of Economics	**Bosnia and Herzegovina**	Zlatko Lagumdzija
ETH Library at ETH Zürich	**Switzerland**	Sven Koessling
University of Belgrade	**Serbia**	Aleksandar Markovic

Authority Nodes: https://validators.bloxberg.org

Boot Nodes: https://github.com/bloxberg-org/bloxbergValidatorSetup/blob/master/validator/bootnodes.txt

IRON THRONE

The Iron Throne is the temporal executive of the bloxberg consortium.

2019 - 2020
Max Planck Society
0xaa84378fa41da83a9b6523ba46e45a664fbebfc8

2020 - 2021
Max Planck Society
0xaa84378fa41da83a9b6523ba46e45a664fbebfc8

2021 - 2022
Max Planck Society
0xaa84378fa41da83a9b6523ba46e45a664fbebfc8

2022 - 2023
Max Planck Society
0xaa84378fa41da83a9b6523ba46e45a664fbebfc8

BLOXBERG INFRASTRUCTURE

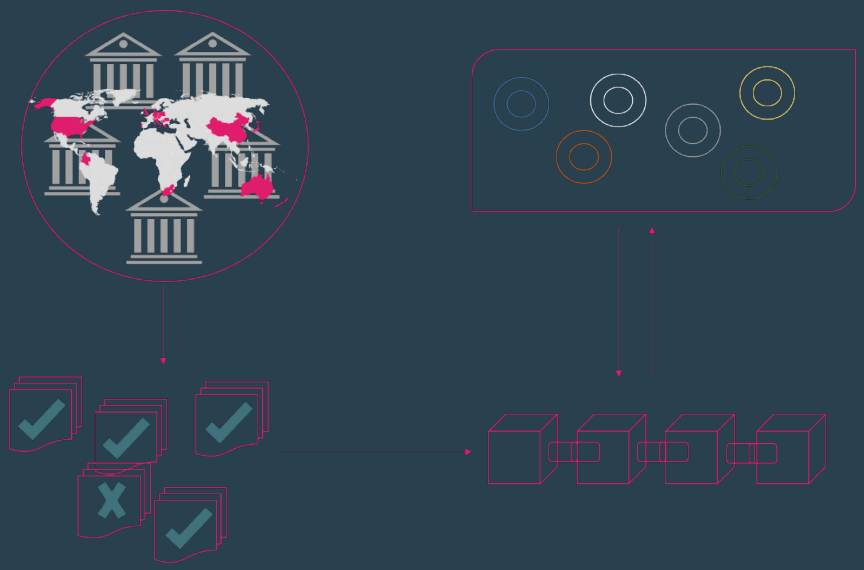
The bloxberg infrastructure consists of the two main components which are explained in this chapter, first the bloxberg technology (nodes, smart contracts, etc.) and second the governance model which defines the ground rules of the network. The bloxberg infrastructure is developed on top of a permissioned Ethereum blockchain network driven by Proof of Authority consensus (see chapter Consensus Algorithm). Ethereum was chosen because it has one of the strongest communities out of any blockchain network and it has been shown to be resilient and stable against many attacks while running on the mainnet. The growing number of productive applications and networks relying on the Ethereum blockchain has proven the readiness of this new technology and has become apparent to handle the requirements of a fully decentralized and global network on a high scale level.

The bloxberg infrastructure relies on the Proof of Authority (POA) consensus algorithm which assures the greatest combination of security, efficiency, and decentralization, available on the Ethereum chain. Efficiency is achieved because the amount of Authority nodes processing transactions is kept relatively low, so block confirmations happen quickly, without the long confirmation times commonly see in other blockchains. Security is guaranteed through the fact that Authority nodes are distributed among different entities and are numerous enough that they prevent against a malicious 51% attack. Finally, decentralization is realized through limited control of the chain from any single institution, once more Authority nodes which joined the network can vote and add other Authority nodes independently of the Max Planck Society (see chapter governance model). Candidate institutions will be vetted through a peer review process from entities already part of the network.

BLOXBERG PROTOCOL

The bloxberg network is based on a public, permissioned implementation of Ethereum (https://www.ethereum.org/), featuring smart contract functionalities and using the network of nodes from the bloxberg consortium.

Every consortium member maintains one Authority node in the bloxberg network and approves transactions by the Proof of Authority consensus algorithm. Independent dApps or Apps can be built on top of the bloxberg network by using the open bloxberg API.



The consortium consists of research institutions who run nodes. Each research organization will be restricted to running one authority node on the network. The consortium is responsible for running and maintaining the underlying infrastructure of the network. All rights and duties are defined in the detailed bloxberg governance model

Decentralized applications running on top of bloxberg can be developed by third parties, consortium members, scientists, amongst others. The bloxberg Consortium fosters the development of apps that benefit the scientific ecosystem.

bloxberg API: Scientific dApps communicate with the bloxberg blockchain to provide services to scientists and researchers

bloxberg consensus is governed by a Proof of Authority algorithm. This algorithm was chosen based on consistency, availability, performance, and previous use in large networks. A detailed protocol audit is available for review.

The blockchain itself is based on a permissioned implementation of Ethereum

NODES

The bloxberg network consists of two types of nodes; Authority nodes and non- Authority nodes.

All members of the bloxberg consortium have to commit to run one Authority node, and hence build together the essence of the bloxberg infrastructure. Thereby it is guaranteed that all Authority nodes of the network are distributed throughout various research organizations around the world.

Authority nodes carry out the computational activities in the network to validate and store blocks and transactions of the distributed ledger of the bloxberg network. All Authority nodes in the bloxberg network are considered equal and use the same consensus protocol to remain consistent. The hardware requirements for running a Authority node in the bloxberg pilot phase are relatively low (see https://github.com/bloxberg-org/bloxbergValidatorSetup), during this phase only the transactions are stored on the bloxberg blockchain, but not the data itself.

Non- Authority nodes communicate with the network. Every entity can run a non- Authority node and connect it to the bloxberg network, e.g. a 3rd party company, running an application on bloxberg. With the growing number of consortium members and the corresponding growth of Authority nodes and non- Authority nodes in the network, the capacity and security of the bloxberg will grow.

CONSENSUS ALGORITHM

The bloxberg consensus is governed by Proof of Authority (PoA) based on the Authority Round (AuRa) algorithm (https://wiki.parity.io/Aura). This algorithm was chosen based on consistency, availability, performance, and previous use in large networks. A detailed protocol audit is available for review (https://github.com/poanetwork/wiki/wiki/Aura-Consensus-Protocol-Audit).

A PoA consensus algorithm does not depend on nodes solving arbitrarily difficult mathematical problems (mining), but instead uses a set of "authorities" – nodes (in bloxberg called Authority nodes) that are explicitly allowed to create new blocks and secure the blockchain. The chain has to be signed off by the majority of authorities, in which case it becomes a part of the permanent record (finalization). Some advantages of a PoA consensus compared to a PoW consensus:

- Increased security (a node which is not registered as a validator or a hacked Authority node cannot overwhelm the network, potentially reverting all transactions)
- less computationally effort (no mining required)
- more performant (Aura consensus provides lower transaction acceptance latency)
- more predictable (blocks are issued at steady time intervals)

Block creation and signing

The Authority node, who is next to create and sign a block, is called the primary. All Authority nodes in the network keep track of the steps in the chain. A step is the unixtime divided by the current block creation time. The primary is calculated from the step modulo the number of all Authority nodes in the network.
Primary = (unixtime / block creation time) mod #Validators

Example:
Primary = (1579169080 / 7) mod 11 => Authority *node number 3 creates and signs the next block*

Finality

Finality in AuRa is defined by a simple majority vote. Finality is reached when at least 51% of all Authority nodes signed the same chain twice.
If there is a valid chain *Chain1* where #signedValiatorNodes > #allValidatorNodes / 2, then *Chain1* and all of its ancestors are finalized.

SMART CONTRACTS

The bloxberg consensus algorithm and the bloxberg governance model are computed into smart contracts and were deployed on the bloxberg Genesis.

All smart contracts for the bloxberg network are open source (https://github.com/bloxberg-org):

- bloxberg genesis file
- bloxberg consensus algorithm smart contract
- Voting application compliant with the bloxberg governance model

Additionally, research organizations, developers, and users of the chain are free to deploy smart contracts as they see fit.

BERG – THE BLOXBERG CURRENCY

bergs (△ U+25B3) are the currency of the bloxberg network. In order to interact with bloxberg blockchain applications or to deploy smart contracts, bergs are utilized for these interactions. The berg symbol stands before the value, e.g.: △0.00134

The smallest unit is called a ‘brox’. The full table is:

Unit	brox Value	brox
brox	1 brox	1
Kbrox	1e3 brox	1,000
Mbrox	1e6 brox	1,000,000
Gbrox	1e9 brox	1,000,000,000
microberg	1e12 brox	1,000,000,000,000
milliberg	1e15 brox	1,000,000,000,000,000
berg	1e18 brox	1,000,000,000,000,000,000

bergs are not traded; all transactions in the bloxberg network are free of charge. The bloxberg network provides a faucet app to distribute bergs among all entities who wish to build on the bloxberg network or utilize the functionality of bloxberg apps.

GOVERNANCE MODEL

Compliance:
All members must follow the guidelines; not following the guidelines may result in exclusion.

Stakeholders

Stakeholders are the main entities, which participate in the bloxberg network and are relevant for defining governance rules.

Consortium members

Consortium members form the governing body of bloxberg and are responsible and accountable for the directing and control of the bloxberg blockchain. Consortium members are equal, no hierarchy exists by design. Institutions can apply as a bloxberg consortium member if they are a:

'Science organization, specifically academic, higher education and primarily publicly funded research institutions.'

Consortium members can be a natural person (affiliated with an institution), or a legal person (the institution itself). Each institution can only be represented by one entity in the network, either a natural or a legal person. All members are known and identified by their authority node address in the bloxberg network (https://validators.bloxberg.org).

Iron Throne

The Iron Throne is the temporal executive of the bloxberg consortium. It has the following duties:

- Execution of votes on adding and removing nodes from the bloxberg network
- Setting up proposal voting
- Commuinicate decisions of governance voting to the consortium
- Organizing at least one bloxberg summit for the bloxberg consortium per year
- Organizing regular bloxberg consortium meetings
- Handing over keys, accesses, and relevant documents to a succeeding Iron Throne

For the first year after the genesis of bloxberg the initiating research organization 'Max Planck Society' will inherit the Iron Throne. The next holding of the Iron Throne will always be elected on the bloxberg summit for one year. The acting Iron Throne can reapply for the next period; there is no upper limit of succeeding periods.

Decision Making

Decentralized decision-making processes are essential for the sanity and growths of bloxberg. bloxberg differentiates between two basic decision-making processes. Governance decisions, carried out off-chain, after intensive discussion, as the nature of governance decisions are more likely to be ground-breaking and fundamental for the consortium, and proposal decisions, are made by an on-chain voting.

Governance Decisions

Governance Decision Voting Model

one member – one vote
(Members representing the same institution must choose a single member to vote on their behalf.)

Iron Throne Voting

1. The voting of the Iron Throne is executed off-chain at the annual bloxberg summit.
2. The bloxberg consortium requires a quorum of >50% of the participating organizations at the annual bloxberg summit to execute a valid voting, but a minimum of three voting organizations.
3. An Iron Throne candidate needs > 50% of the valid votes to be appointed as the Iron Throne until the succeeding bloxberg summit.
4. The voting is executed off-chain by the acceptance of all consortium members.

Governance Model Changes

1. Changes of the governance model are discussed off-chain at the annual bloxberg summit.
2. The bloxberg consortium requires a quorum of >50% of the participating organizations to execute a valid voting, but a minimum of seven voting organizations.
3. For changing the governance model, the proposal needs >50% of acceptance.
4. The voting is executed off-chain by the Iron Throne.

Solving Consortia Conflicts & Forking

Consortium members are urged to solve conflicts in the best manner for the good of the network. The Iron Throne can be called as a mediator on demand. Intractable disagreements in the consortium can be resolved by initiating a 'fork'.

If the acting Iron Throne refuses to fulfil their duty and is not willing to hand over the Iron Throne, forking of the bloxberg network will be executed to restitute power back to the bloxberg consortium. In this case, a new Iron Throne will be voted independent to the bloxberg summit.

Proposal Decisions

Proposal decisions are executed via an on-chain voting through bloxbergs voting application (https://voting.bloxberg.org/). Proposals can be set up at the beginning of every month and are up for voting during the period of one month. The voting on proposals is executed according to the Proposal Decision Algorithm.

Proposal Decision Voting Model

The proposal decision-voting model follows the proposal decision algorithm to incentivize consortium members to execute their duties in the bloxberg network. All bloxberg founding members start with a voting power of 25% (100 voting weight), new consortium members will start with a voting power of 0% (0 voting weight).

For each voted on proposal, weight is added to the current voter weight. Each missed proposal results in a deduction of weight. The function that governs the adjustment of voting weight per proposal is:

$$CurrentVoterWeight \pm \frac{100}{TotalProposalsinBatch}$$

The maximum possible voting power of one organization is 100% (400 voting weight); the minimum possible voting power is 0% (0 voting weight).

Voting for new consortium member

1. Applicant fills out a form on the official (bloxberg.org) website.
2. The Iron Throne adds the applicant to the voting application.
3. The voting is executed on-chain after an off-chain discussion.
4. The voting is executed according to the proposal decision algorithm.
5. The bloxberg consortium needs a quorum of >50% of all voting power, to execute a valid voting, but a minimum of 3 voting organizations.
6. If > 50% of the valid votes are yes, the new member is accepted. If not, the new member is rejected and can reapply at a later time.
7. After a positive vote the Iron Throne is instructed to add the new member as an authority node to the bloxberg network.

Voting for exclusion of a consortium member

1. A voting for exclusion will be triggered if a consortium member does not fulfill his or hers accountability.
2. The voting is executed off-chain.
3. The voting is executed according to the proposal decision algorithm.
4. The bloxberg consortium needs a quorum of >50% to execute a valid voting, but a minimum of seven voting organizations.
5. If > 50% of the valid votes are yes, the member is excluded.
6. The Iron Throne is instructed to remove the member from the bloxberg network.
7. The excluded organization can reapply for a bloxberg consortium membership.

bloxberg Improvement Proposal

1. Every consortium member can create a BLIP (bloxberg improvement proposal).
2. Every BLIP must contain the voting option ‚reject'.
3. The voting is executed on-chain after an off-chain discussion.
4. The voting is executed according to the proposal decision algorithm.
5. The bloxberg consortium needs a quorum of >50% of all voting power, to execute a valid voting, but a minimum of 7 votes.
6. The option with the most votes wins.

Inclusion & Transparency

All bloxberg consortium members are fully included in the decision-making processes of bloxberg, as they can:

1. create a BLIP (bloxberg improvement proposal) at https://blips.bloxberg.org/
2. initiate governance decisions at a consortium meeting

The decision-making process of bloxberg is fully transparent for all consortium members, as:

1. information on new member votes is provided by the Iron Throne and discussed in the consortium meetings.
2. all consortium members can access the voting application of bloxberg to see upcoming votes and the results of past votes.
3. BLIPs are published on https://blips.bloxberg.org/ .

Accountability

Accountability is particularly useful for permissioned blockchains where all parties know each other, and hence, accountability incentivizes all parties to behave in a way that benefits the whole network.

Validator Node

1. Consortium members must furnish and maintain up-to-date contact and node information to the consortium, (https://validators.bloxberg.org). Members must furnish and maintain cryptographic information, identifying the respective node that they maintain, to the consortium.
2. Each consortium member runs one authority node in the bloxberg network.
3. The node may not be offline longer than three months.
4. The consortium member performs necessary security updates on the nodes, takes reasonable actions to prevent spamming of the network and implements certain protocols, promulgated from time to time by the consortium.

5. The consortium member will perform updates and install releases as decided by the bloxberg consortium.

Legal Implications

A consortium member is responsible for the legal compliance in the respective jurisdiction, for running a bloxberg authority node.

A consortium member shall not be liable inside and outside the consortium for the transactions and content, which are distributed to the network through its node, and in this regard be indemnified and held harmless by the bloxberg consortium.

Incentives

Incentives influence the system participants to behave in a way that benefit the whole network.

Consortia participation

1. Members of the bloxberg consortium have voting rights on governance and proposal voting.
2. Active participation in proposal voting will be incentivized by an increase of voting power.
3. Members of the consortium gain 'Bergs' for processing transactions.
4. Members give a strong statement towards decentralized and autonomous services to support science and the global scientific community.

Conclusion

These are the governance rules for bloxberg, which were discussed and and passed at the annual bloxberg summit in May 2022. The rules will very likely be adapted in future by governance decisions of the bloxberg consortium.

BLOXBERG CONNECTIVITY

Scientific dApps and Apps communicate with the bloxberg blockchain to provide services to scientists and researchers. Therefore, various research institutions will run a hosted node to provide access via an API to the blockchain for interested parties to connect to. An initial access point can be found on the bloxberg website (https://bloxberg.org) with more to come. It is expected that individual applications will run their own non- Authority node to communicate with the bloxberg blockchain to ensure performant communication.

BLOXBERG SUMMIT

In February 2019, on the initiation of the Max Planck Society, leading research organizations from around the world came together to formally constitute the bloxberg consortium for the ground-breaking and secure bloxberg network to build truly global, decentralized and autonomous services to advance science.

The bloxberg Summit is an annual meeting of all consortium members to vote the Iron Throne, discuss the governance model, and define synergies and strategies for further consortia cooperation.

BLOXBERG MANIFESTO

The bloxberg Manifesto describes the direction, purpose and commitment of bloxberg. It is a requirement for all members that they publicly endorse the manifesto and whilst being a member, apply it to their practices. The manifesto should serve as an accountability function: while members are not legally required to commit efforts to the initiative or apply it in their practices, the signing of the manifest is a moral mechanism for enforcing the definition and purpose of bloxberg.

At the first bloxberg Summit in February 2019 all founding consortium members (see chapter bloxberg founders) signed the bloxberg manifesto and therefore constituted the bloxberg consortium genesis.

BLOXBERG APPLICATIONS

The aim of bloxberg is to instantiate the bloxberg network and promoting the implementation of applications on top of it, that will benefit scientific research. bloxberg will host a suite of scientific applications in order to enhance research. The vision of bloxberg is to have sufficient representation from globally distributed scientific entities participating in the network, such that the network itself can replace traditional scientific infrastructure like closed-access publishing amongst others.

BLOXBERG HOMEPAGE

The bloxberg website is up and running at www.bloxberg.org. It contains basic information on the bloxberg project, the technology and the consortium members. Utilizing the bloxberg website it is also possible to see the suite of apps developed by the bloxberg consortium.

APPS/DAPPS

Third parties, consortium members, and scientists, amongst others, develop apps or dApps running on top of bloxberg. The aim of the bloxberg consortium is to encourage development of apps that benefit the scientific ecosystem. The bloxberg network itself provides the blockchain infrastructure for the suite of applications that take advantage of blockchain technology. The following applications are ensuring the bloxberg network core services. For a full overview of applications on the bloxberg blockchain visit the bloxberg website (will follow).

Certify and Verify
With bloxberg, research claims need not be limited to one institution alone, but can be confirmed by the whole trusted network. Additionally, researchers can leverage bloxberg to create a transparent footprint of their work, without revealing its content. You can then generate a certificate that proves you uploaded this data at a certain time, therefore protecting you from being scooped or IP stolen. At a later date, this application can be utilized to confirm that research data was certified at an earlier time.

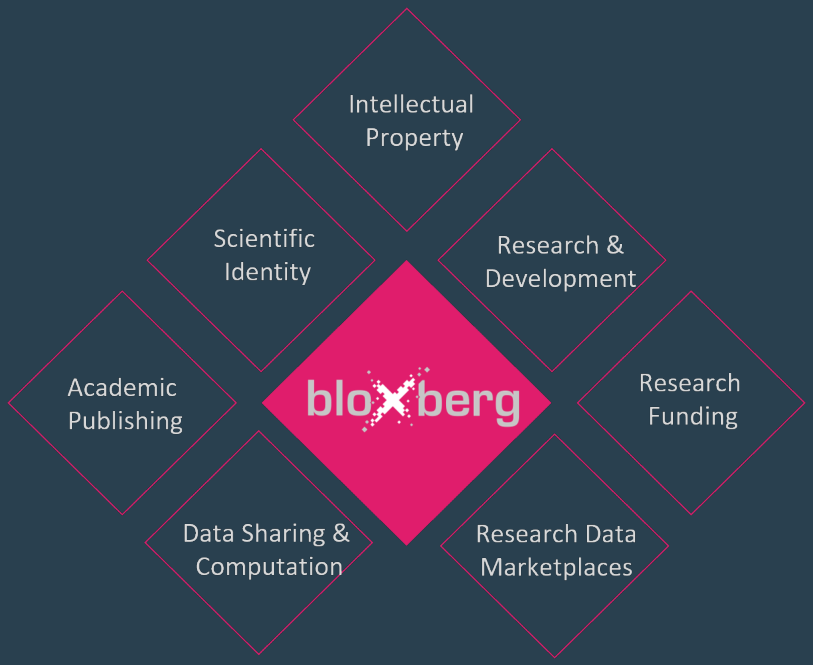
bloxberg Faucet
The faucet dApp is primarily for providing bergs (the bloxberg currency) to users of the blockchain. In order to interact with blockchain applications or deploy smart contracts, bergs are utilized for this interaction. The faucet guarantees that people who wish to build on bloxberg or utilize the functionality of the apps will be able to do so.

bloxberg Explorer
Here you can see a wealth of information detailing current transaction status such as pending or confirmed, smart contracts that have been deployed and can be interacted with, and a detailed and transparent look into the overall activity of the network.

bloxberg Validator
The bloxberg validator app can be utilized to connect authority public addresses to basic information about each validator, for instance the research institute, address, and research field of each responsible member.

FUTURE OUTLOOK

Ultimately, the vision of bloxberg is to be the foundation for a suite of applications utilizing blockchain technology to benefit the entirety of the research process. These could include applications like innovative ways of research funding, a decentralized journal, expanding and securing the peer review process, and much more. Consortium members, third-party organizations, and scientists are encouraged and invited to build on top of the bloxberg infrastructure – secure in the fact that it is run by scientists, for science.



APPENDIX

The bloxberg Research Data Certification

bloxberg

Research Object

Certificate

This bloxberg certificate serves as a proof of existence that the data corresponding to the cryptographic identifier were transacted on the **bloxberg** blockchain at the issued time.

Cryptographic Identifier

620c00d82bb9e49e4dead633d8791aa37fb58a058793056bdc2f1f893bbfb39b

Transaction ID

0xc09d14494b7fc93bf5af166aaa183dfd4c787add6fd58dbd73d720e1199ccdf4

Timestamp

2022-06-29T07:10:21.882713

Merkle Root

9afe0347dbf26acf2e21acf1ca422684f49e9cae7e95930b2cd993f43a2751b6

View the transaction at https://blockexplorer.bloxberg.org

Verify the certificate at https://certify.bloxberg.org/verify

The annual bloxberg summit


Fourth bloxberg Summit
for Consortium Members
May 3 - 4, 2022
UCL | London | United Kingdom
Couch | Home | Worldwide
bloxberg
The Novel Blockchain Consortium for Science


Fifth bloxberg Summit
for Consortium Members
October 26 - 27, 2022
Protaras | Cyprus
Couch | Home | Worldwide
bloxberg
The Novel Blockchain Consortium for Science