The Trusted Research Infrastructure

Whitepaper 1.0

February 2019

Contact:
info@bloxberg.org

Initial authors:
Dr. Sandra Vengadasalam vengadasalam@mpdl.mpg.de
Friederike Kleinfercher kleinfercher@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 (February 2019 until February 2020) interfaces may be modified, the governance model may chance and data might get lost.

About

The bloxberg infrastructure is a secure global blockchain established by a consortium of leading research organizations to provide scientists with decentralized services worldwide. The bloxberg infrastructure broadens the scientific landscape of regionally and nationally governed blockchain networks to become the first truly globally maintained scientific decentralized network for scientists. By establishing the permissioned, public blockchain **bloxberg** the network is safeguarded against the cryptographic power of third entities, as the credibility of the research organizations maintaining the network, constitutes trust in the system.

The bloxberg consortium aims to foster collaboration among the global scientific community, empowering researchers with robust, autonomous services that transcend institutional boundaries. For example, with consented transactions on the bloxberg infrastructure, research claims need not be limited to one institution alone, but can be confirmed by the whole trusted network. The excellent reputation of the participating research organizations will encourage scientists worldwide to utilize the bloxberg network and the applications built on top of the infrastructure. Researchers can leverage bloxberg to create a transparent footprint of their work, without revealing its content. Each institution can integrated the bloxberg infrastructure into existing institutional services for their scientists, and therefore easily expanding centralized services with decentralized components such as DLT (distributed ledger technology) timestamping.

Commercial companies and especially Start Ups are encouraged and supported by the bloxberg consortium to build new and innovative services on the bloxberg blockchain whereas maintaining the network and validating transactions is only administered by the bloxberg consortium of scientific organizations.

bloxberg Founders

The bloxberg consortium is initiated in February 2019 with the founding research organizations on the invitation of the Max Planck Society. Each participating research organization has deep knowledge of the groundbreaking possibilities of DLT in science and recognizes the huge potential of a truly decentralized global scientific infrastructure, such as bloxberg, for the scientific community worldwide.

With the bloxberg founders 10 different countries are represented with at least one renowned research organization:

	Organization	Country	Contact
	Max Planck Society	**Germany**	Sandra Vengadasalam
	University of Nicosia	**Cypress**	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

Validator Addresses

Max Planck Society
0xaa84378fa41da83a9b6523ba46e45a664fbebfc8

University of Nicosia
0xb1A7419Acd652d5F70d2480A4B6F2609fA996308

University College London
0x9387fC4cb0f7d0250Cc696e08c2A4289a4Bfd53b

IT University of Copenhagen
0xe659bc6A60Ba2091c08F7df623BA6057349B6980

University of Kassel
0x599c3F2CCBb96Ff55378fF902fE7c8d6a7c8592a

Georgia Institute of Technology
0x8De281f47B137979e55B6CEa598179737574C774

Carnegie Mellon University
To be added

University of Johannesburg
0xf2f99defc0045875806abdb85af3822860afc8de

University of Sarajevo School of Economics
0x1d90d67b4978149e9c43e93090e740197c32e13d

ETH Library at ETH Zürich
0x1ef319db1930e3420fcff90c376d9cf515b34876

University of Belgrade
To be added

bloxberg Infrastructure

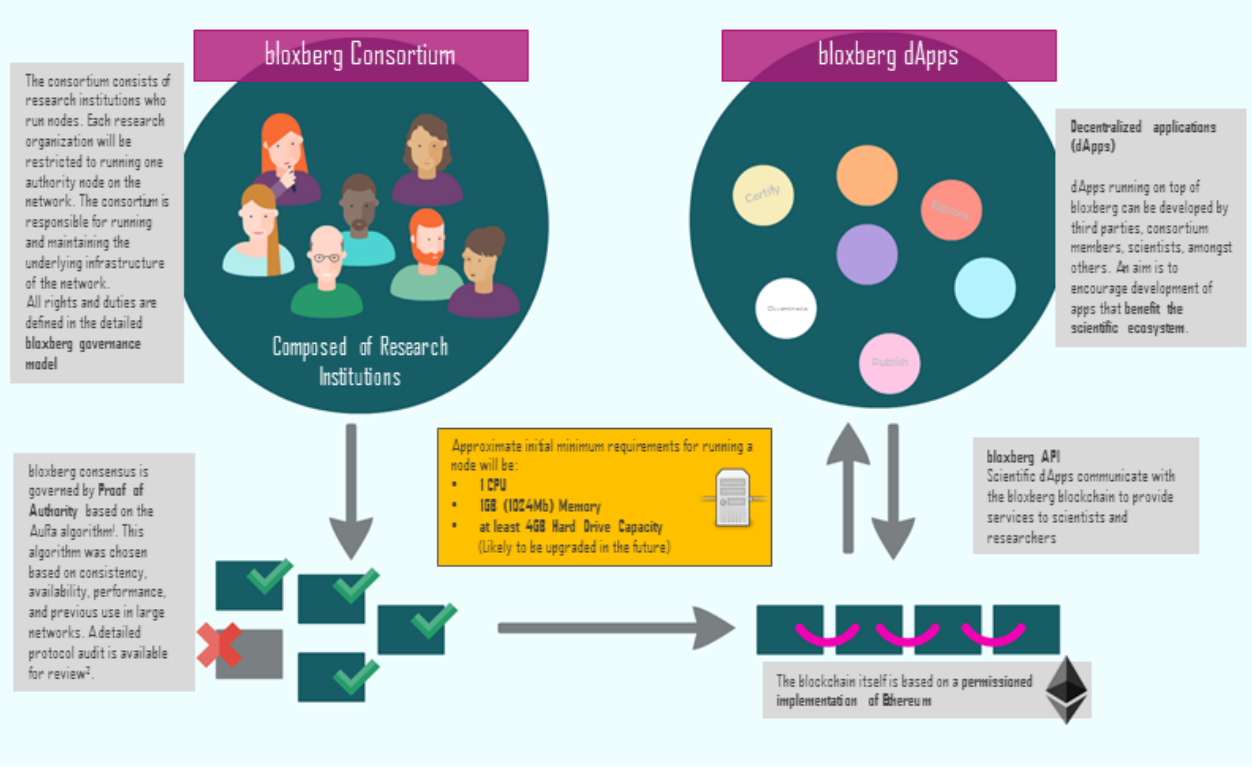
The bloxberg infrastructure consists of the two main components which are explained in this chapter, first the bloxberg technology (nodes, smart contracts, etc.) and second the governance model which defines the ground rules of the network. The bloxberg infrastructure is developed on top of a permissioned 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 Network

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



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 an authority-node in the bloxberg pilot phase are relatively low (1CPU, 1GB memory and about 4GB of hard drive capacity), 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, like a startup 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 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).

The PoA consensus algorithm does not depend on nodes solving arbitrarily difficult mathematical problems (mining), but instead uses a set of “authorities” - 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. This makes it easier to maintain a private chain and keep the block issuers accountable. For consortium setting there are no disadvantages of PoA network as compared to Proof of Work (PoW). It is more secure (since an attacker with unwanted connection or hacked authority cannot overwhelm a network potentially reverting all transactions), less computationally intensive (mining with difficulty which provides security requires lots of computation), more performant (Aura consensus provides lower transaction acceptance latency) and more predictable (blocks are issued at steady time intervals). PoA deployments are used by the enterprise and by the public (e.g. popular Kovan test network).

(https://wiki.parity.io/Proof-of-Authority-Chains)

Smart Contracts

Governance of the bloxberg blockchain is controlled via smart contracts to ensure transparency into the network and fairness for the participating nodes. To facilitate this, foundational smart contracts are deployed on bloxberg Genesis. Additionally, research organizations, developers, and users of the chain are free to deploy smart contracts as they see fit.

berg – the bloxberg currency

Bergs 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.

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.

bloxberg Governance Model

The bloxberg governance model is formulated into a set of rules, or by-laws, which need to be followed by all consortium members. They are created to encourage desirable behavior within the bloxberg network. The bloxberg governance model regulates the three pillars of the bloxberg consortium:

1. *Decision rights* - all rules concerning rights governing control over certain assets. Can be divided into decision management rights - which allow generating decision proposals, executing or implementing decisions - and decision control rights - allowing for the ratification of decisions, monitoring of decisions and their performance.
2. *Accountability* - the mechanisms by which members can be held accountable for their actions and decisions. This also includes enforcement mechanisms.
3. *Incentives* - all reasons and mechanisms that motivate members to act in alignment with bloxberg.

Decision rights
To become a member, you need to be a research institute which has been voted in by a majority of existing members, and ANY research institute (see definition of research institute below) can become a member of the bloxberg consortium. All consortium members have the right to trigger on-chain and off-chain events.

bloxberg decision algorithm:
The bloxberg decision algorithm is established to incentivize consortium members to execute their duties in the bloxberg network as stated in the governance model. All bloxberg founding members start with a voting power of 25%, new consortium members will start with a voting power of 0%.
Voting 3 times in a row increases the voting power of an organization by 25%, the maximum possible voting power of one organization is 100%. On the other side, non-voting three times in a row will decrease the voting power of an organization by 25%, the minimum possible voting power is 0%.

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

Voting for new bloxberg consortium members:
1. Applicant fills out a form on the official (bloxberg.org) website
2. Once every **4 weeks** members vote for **4 weeks** on new applicants
3. The voting is executed on-chain after an off-chain discussion
4. The voting is executed according to the bloxberg decision algorithm
5. The bloxberg consortium needs a quorum of **>50%** to execute a valid voting, but a minimum of **3 voting** organizations.
6. If **> 50%** of the valid votes is yes, the new member is accepted. If not the new member is rejected and can reapply at a later time.

7. The Iron Throne is instructed to add the new member as a validator node to the bloxberg network.
8. The new member has to run one authority-node, but can have n non-authority nodes. The authority-node must be available in the network all the time.

The Iron Throne:
One consortium member has the iron throne for **1 year**, starting with the annual bloxberg summit. During this year the iron throne has the duty to execute the consortium votes for adding and removing members to/from the bloxberg network.

The iron throne also commits to organize the annual bloxberg summit for all bloxberg consortium members.
For the first year after the genesis of bloxberg the initiating research organization 'Max Planck Society' will have the iron throne. The next iron throne will always be voted on the annual bloxberg summit. The acting iron throne can reapply for the next period; a maximum of succeeding periods is not defined by the consortium.

Voting for the iron throne:
1. The voting is executed according to the bloxberg decision algorithm
2. The bloxberg consortium needs a quorum of **>75%** of the participating organizations at the annual bloxberg summit to execute a valid voting, but a minimum of **3 voting** organizations.
3. The voting is executed off-chain
4. If **> 50%** of the valid votes is yes, the organization is appointed as the iron throne for **1 year**

Accountability
Sanctions (revoke membership) can be taken if a member misbehaves. The exclusion of an authority-node in the bloxberg network has to be approved by a voting of the bloxberg consortium members.

Events which will trigger a sanctions voting:
1. An authority-node is offline for **> month**
2. The authority-node spams the network
3. The member acts in a non-compliant manner according to the governance model
4. The entity is not aligned with the manifesto

Voting for the exclusion of a bloxberg consortium member:
1. A voting for exclusion will be triggered if one of the above mentioned events occur
2. The voting is executed off-chain
3. The voting is executed according to the bloxberg decision algorithm
4. The bloxberg consortium needs a quorum of **>75%** to execute a valid voting, but a minimum of **7 voting** organizations.
5. If **> 75%** of the valid votes is yes, the member is excluded
6. The Iron Throne is instructed to exclude the member from the bloxberg network
7. The excluded organization can reapply for a bloxberg consortium membership

Forking of the Blockchain:
The bloxberg consortium members take all possible precautions to avoid forking of bloxberg. Nevertheless if the iron throne refuses to fulfil his 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.

All members are known and identified by their authority-node address in the bloxberg network.

Incentives
Joining the bloxberg consortium:

1. Members of the bloxberg consortium can shape the bloxberg infrastructure by proposing and voting on rules for the governance model
2. Members of the bloxberg consortium can vote on new members
3. By engaging on the bloxberg consortium a research organization gives a strong statement towards and decentralized and autonomous services to advance science and the global scientific community.
4. Utilization of the bloxberg blockchain as the underlying infrastructure for existing blockchain applications as it is free of charge and much faster compared to other public blockchains.

Usage of the bloxberg network:

1. Transactions in the bloxberg core infrastructure are free of charge
2. The bloxberg network is maintained by research organizations only
3. The bloxberg consortium is truly global and democratic
4. Due to the bloxberg consortium all dApps and Apps on the infrastructure have an excellent visibility within the global scientific community.

Governance Model

Changing the governance model:

1. Changes of the governance model are discussed off-chain at the annual bloxberg summit
2. The voting is executed according to the bloxberg decision algorithm
3. The bloxberg consortium needs a quorum of **>75%** to execute a valid voting, but a minimum of **7 voting** organizations.
4. The voting is executed off-chain discussion
5. For changing the governance model the proposal needs **>75%** of acceptance

Definition of a science organization:

Institutions can apply as a bloxberg consortium member, if it is a '*Science organization, specifically academic, higher education and primarily publically funded research institutions.'*

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 (see appendix 3), 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.

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. The initial applications on the bloxberg network (minimum viable product MVP) include a research data certificate service along with a blockchain explorer to monitor the network. 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.

Website

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. Via the bloxberg website it is also possible to utilize the Apps developed as a MVP for the bloxberg genesis.

Apps/dAPPs

Apps or dApps running on top of bloxberg can be developed by third parties, consortium members, and scientists, amongst others. The aim of the bloxberg consortium is to encourage development of apps that benefit the scientific ecosystem. The bloxberg network provides three basic Apps for the time of the genesis on the network, representing the MVP for the bloxberg infrastructure.

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.

bloxberg Faucet

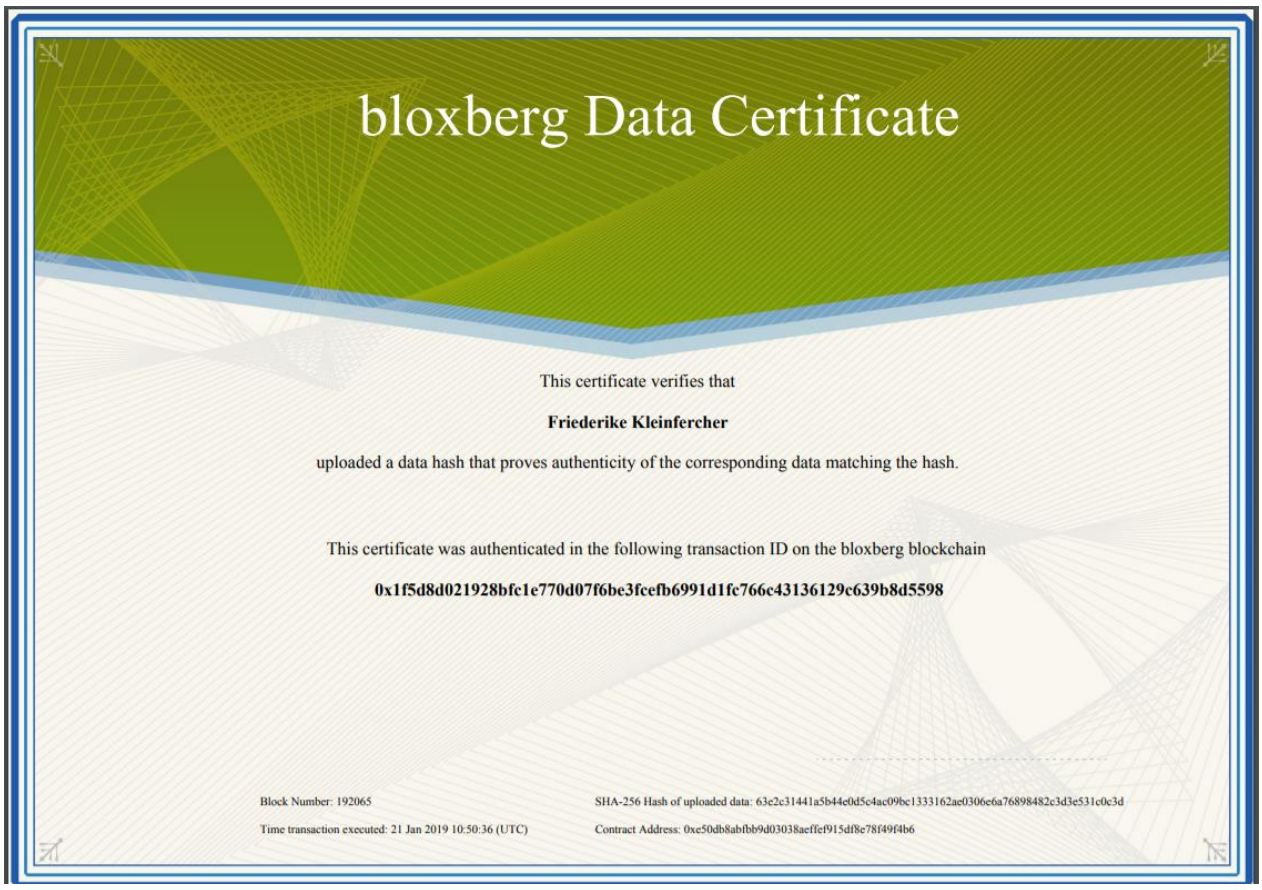
The faucet dApp is primarily for providing bergs (the bloxberg currency) to users of the blockchain. In order to interact with blockchain applications or deploy smart contracts, bergs are utilized for this interaction. The faucet guarantees that people who wish to build on bloxberg or utilize the functionality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

Appendix

1. **bloxberg certificate – example**



2. **bloxberg summit;** the constitution of the bloxberg founders