BLOCKCHAIN 4 PROSUMERS

a comparison of alternatives

Interreg Euregio Maas-Rijn EUROPESE UNIE

ZUYD

Lectoraat Data Intelligence
Nieuw Eyckholt 300
6419 DJ Heerlen

BLOCKCHAIN TECHNOLOGY.

Blockchain4Prosumers

The Blockchain4Prosumers project links Blockchain technology with prosumers (households that consume and produce energy at the very same time) and explores the ways in which blockchain technology can increase the possibility to make locally generated energy available via trading platforms or directly to other consumers and users.

Using this technology, participants can perform transactions without the need for a central certifying authority.

What is it?

As a technology, a blockchain is a distributed ledger of all transactions across a peer-to-peer network. Using this technology, participants can perform transactions without the need for a central certifying authority (Yaga et al., 2019). Potential applications include fund transfers, settling trades, voting systems etc. Also in the energy sector it can establish a secure, transparent, automated an decentralized handling of small-scale energy transactions allowing for the development of prosumer business models (Hwang, et al., 2017).

What are we using it for?

Blockchain4Prosumers links two core elements:

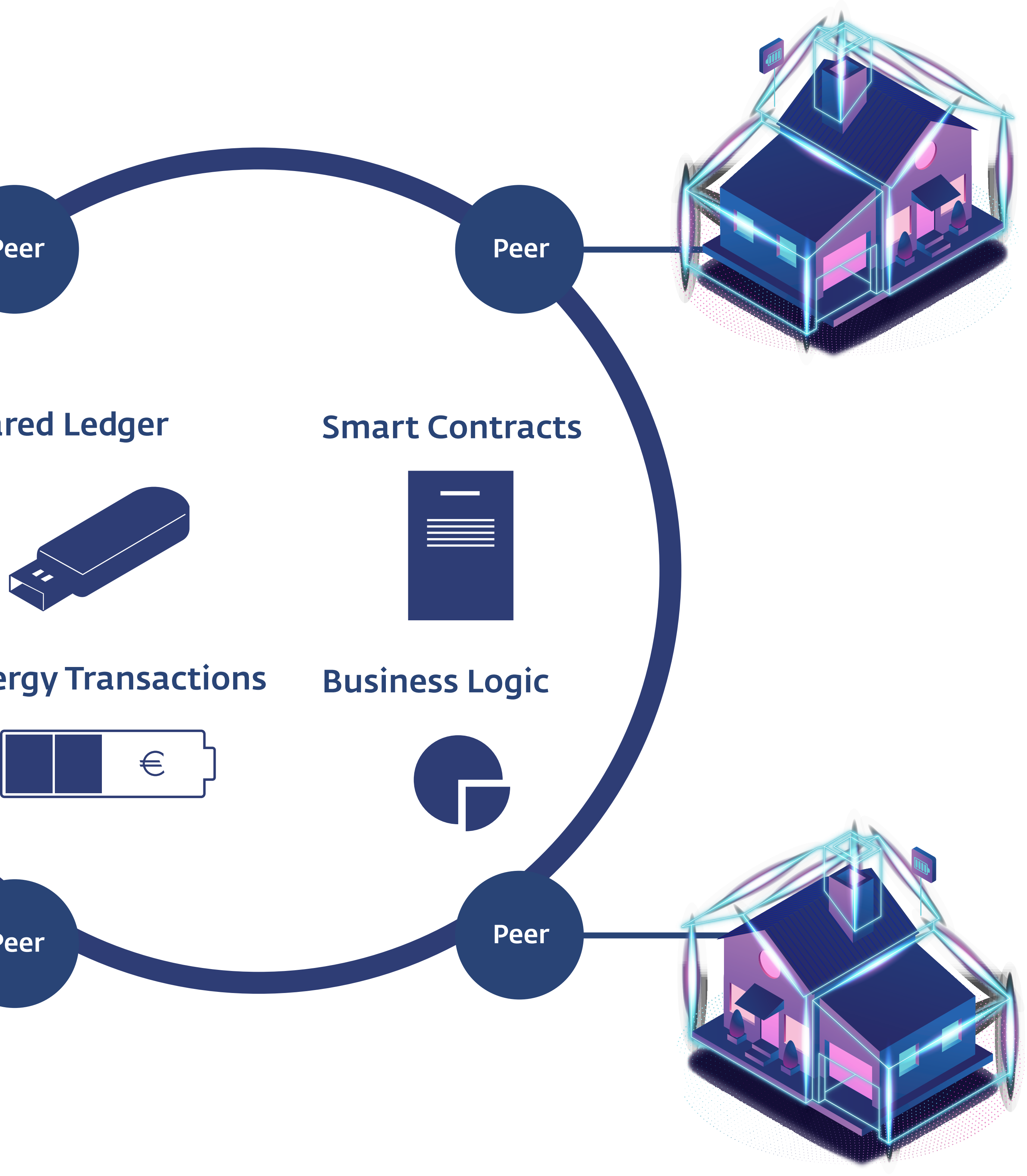
The blockchain technology 🔗 The prosumer

In order to make locally generated energy available via trading platforms or directly to other users (Peer-2Peer trade).

THE WAY IT OPERATES.

The increasing amount of renewable energy sources in the energy system calls for new market approaches to price and distribute the volatile and decentralized generation. Local energy markets, on which consumers and prosumers can trade locally produced renewable generation directly within their community, balance generation and consumption locally in a decentralized approach (Mengelkamp et al., 2018; Saxena et al., 2019).

Our approach is based on a distributed information and communication technology in the form of a blockchain. The peer-2-peer network of households within the community can place energy bids for its available distributed energy sources and an action mechanism is used to clear the market and compute the market clearing price. The marketplace is implemented in a blockchain infrastructure where the bids are stored and smart contracts are used to implement the calculation of the market clearing price. The question to be answered is what is the most promising blockchain implementation for this scenario is. This study aims to assess potential blockchain alternatives (type, security, privacy).



Peer

Peer

red Ledger

Smart Contracts

ergy Transactions

Business Logic

Peer

Peer

Saxena, S., Farag, H., Brookson, A., Turesson, H., & Kim, H. (2019, November). Design and field implementation of blockchain based renewable energy trading in residential communities. In 2019 2nd International Conference on Smart Grid and Renewable Energy (SGRE) (pp. 1-6). IEEE.

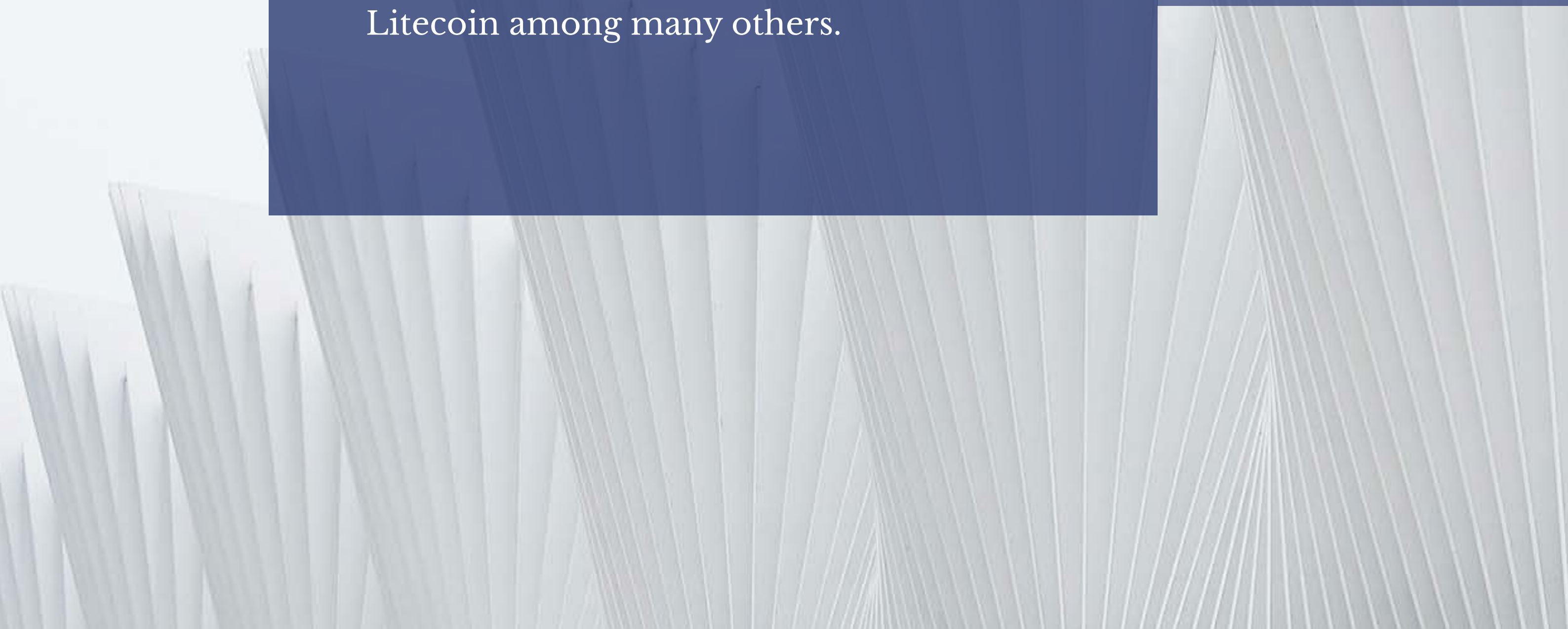
TYPES OF BLOCKCHAIN TECHNOLOGY.

PUBLIC BLOCKCHAIN

A public blockchain allows anyone to join without any permission. It is assumed that every node in the network will be rewarded monetarily by being honest and performing its duty impartially (Pilkington, 2016). Public blockchains use various types of consensus mechanisms such as compute-intensive based and capability based. Compute-intensive mechanisms have been very popular but they bring high energy consumption and low transaction speed (Lai et al., 2020). Examples of public blockchains are Bitcoin, Ethereum and Litecoin among many others.

PRIVATE BLO

In a private block
pre-selected and t
by administrato
network, the pa
not necessarily
In most cases
are implemente
of business col
Different consen
used to construct
notably are the
method and
(Pahlanjani et al.,
blockchains are
Fabric, and Quor



CKCHAIN

kchain the participants are
the community is managed
rs. Since it is a trusted
articipating nodes might
be rewarded monetarily.
the participating nodes
ed compulsory because
laboration requirements.
sus methodologies can be
a private blockchain, most
Byzantine Fault Tolerance
Crash Fault Tolerance
2019). Examples of private
Hyperledger, Hyperledger
rum.

HYBRID BLOCKCHAIN

In order to solve systemic vulnerabilities in both public and private blockchain solutions, the best of both worlds can be combined in so-called hybrid blockchains. Within a hybrid blockchain there is only one recognized consensus method in the form of proof-of-activity. Various combinations are possible within this proof-of-activity mechanism, which ultimately leads to a lower energy consumption compared to a public blockchain (Cui, et al., 2020).

PRIVACY MECHANISMS.

Ring signature.

A ring signature is a type of digital signature that can be performed by any member of a set of users that each have keys. Therefore, a message signed with a ring signature is endorsed by someone in a particular set of people.

Mixing service.

A mixing service allows to mix potentially identifiable information in order to obscure the trail back to the fund’s original source.

Zero-knowledge proof

Zero-knowledge proof is a method by which one party can prove to another party that the given statement is true, without conveying any information apart from the fact that the statement is true.

SCORING METHODOLOGY.

Analyzing the possible combinations of blockchain type, consensus mechanism and privacy algorithm resulted in a set of three alternatives (public, private and hybrid).

The scoring of these three blockchain alternatives was created by using a predefined ranking methodology (Rankin & Grube, 1980). A panel of researchers ranked the three suggested alternatives on a Likert scale (Joshi, Kale, Chandel, & Pal, 2015) in which the lowest rank (1) was a labeled as a total disagree and the highest rank (5) was labeled as a fully agree.

PUBLIC BLOCKCHAIN

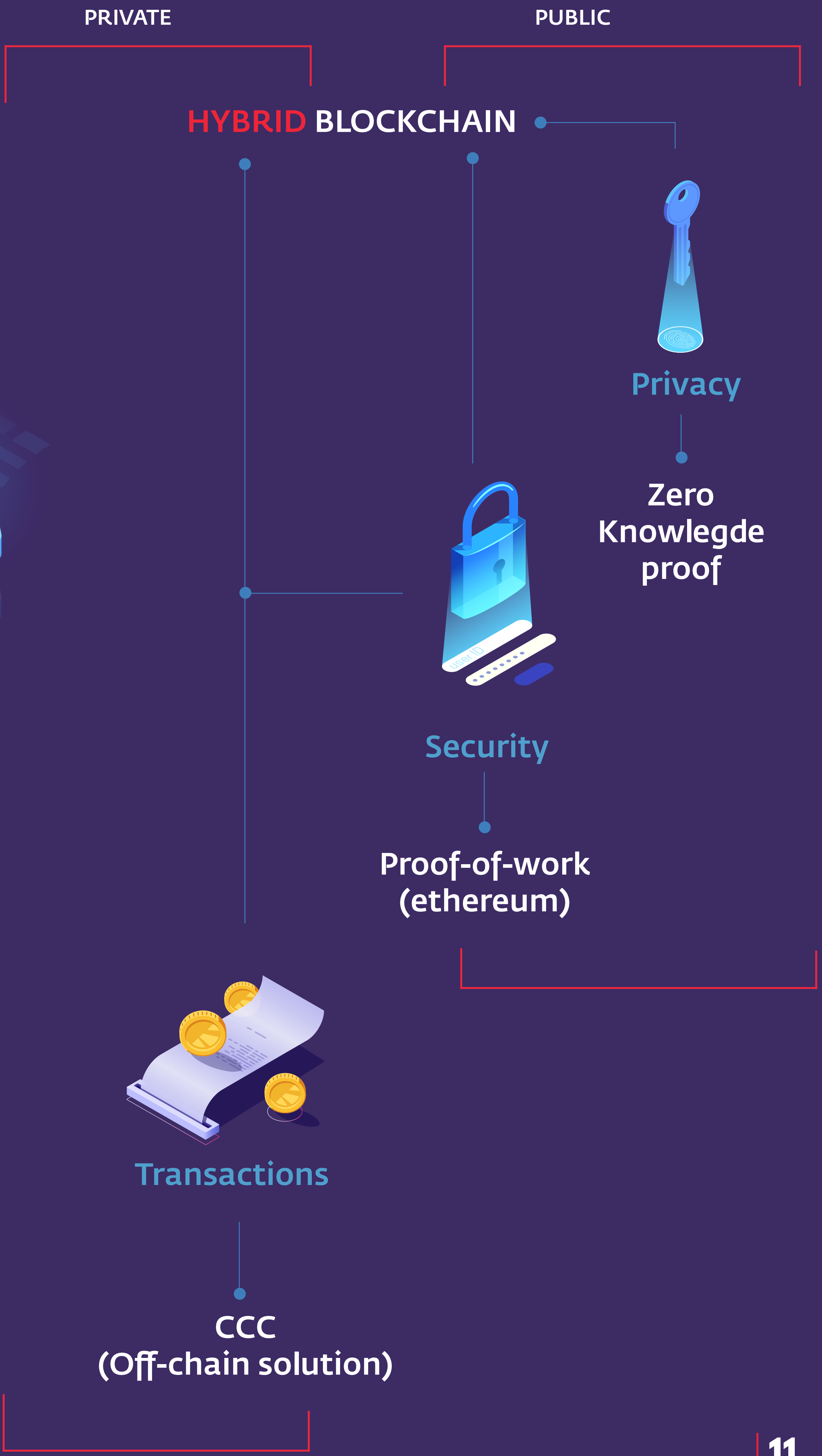
Security — Proof-of-work

Privacy — Mixing service

PRIVATE BLOCKCHAIN

Security — Raft consensus

Privacy — Ring Signature



PRIVATE

PUBLIC

HYBRID BLOCKCHAIN

Privacy

Zero Knowlegde proof

Security

Proof-of-work (ethereum)

Transactions

CCC (Off-chain solution)

SCORECARDS.

COMMUNITY SIZE

SCORE 5

PUBLIC.

Owing to its public character, the community around public blockchains can easily grow. Anyone can become part of the community without prior permission and anyone can execute transactions and read the data stored on the blockchain (Bitcoinist, 2020).

ENERGY CONSUMPTION

SCORE 1

PUBLIC.

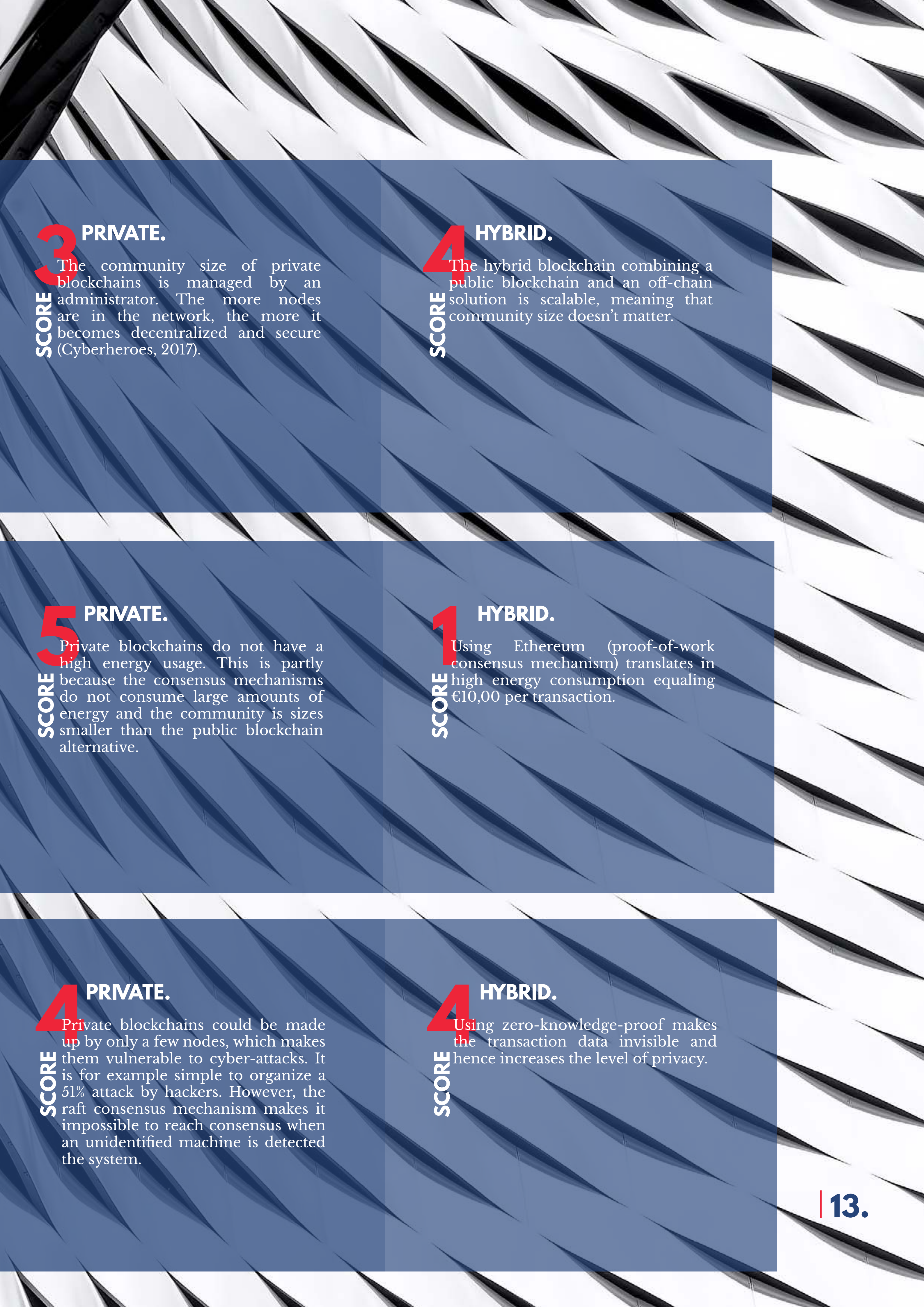
Using a proof-of-work consensus mechanism, the transaction costs are estimated around €10,00 for the energy needed to make that transaction (Johannes et al., 2020). For Bitcoin the costs of one single transaction are even estimated at €420,69 for one transaction (Business Insider, 2021).

SECURITY

SCORE 5

PUBLIC.

Public blockchains run the risk of a 51% attack on its network meaning that if one party has a 51% or more possession of the total calculation power it can transform the data stored in the blocks (Lai et al., 2018; Congcong Ye, 2018).



PRIVATE.

SCORE 3

The community size of private blockchains is managed by an administrator. The more nodes are in the network, the more it becomes decentralized and secure (Cyberheroes, 2017).

HYBRID.

SCORE 4

The hybrid blockchain combining a public blockchain and an off-chain solution is scalable, meaning that community size doesn’t matter.

PRIVATE.

SCORE 5

Private blockchains do not have a high energy usage. This is partly because the consensus mechanisms do not consume large amounts of energy and the community is sizes smaller than the public blockchain alternative.

HYBRID.

SCORE 1

Using Ethereum (proof-of-work consensus mechanism) translates in high energy consumption equaling €10,00 per transaction.

PRIVATE.

SCORE 4

Private blockchains could be made up by only a few nodes, which makes them vulnerable to cyber-attacks. It is for example simple to organize a 51% attack by hackers. However, the raft consensus mechanism makes it impossible to reach consensus when an unidentified machine is detected the system.

HYBRID.

SCORE 4

Using zero-knowledge-proof makes the transaction data invisible and hence increases the level of privacy.

SCORECARDS.

PRIVACY

SCORE 4

PUBLIC.

The usage of a mixing service privacy algorithm it is almost impossible to trace back the individual who is behind a certain transaction (Feng et al., 2018). However, one of the disadvantages is the delay it could cause in the system.

COMPLEXITY OF IMPLEMENTATION

SCORE 4

PUBLIC.

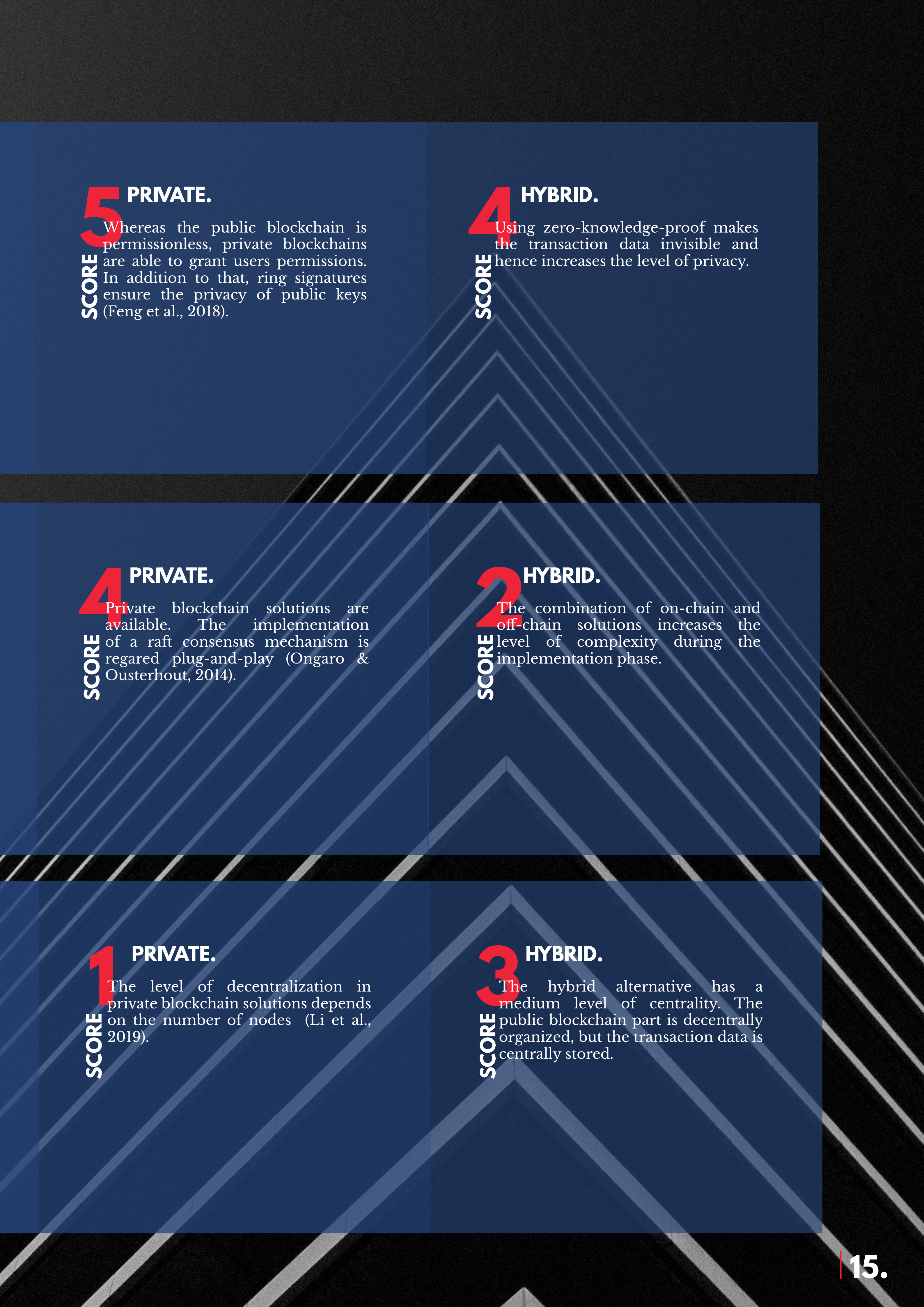
Public blockchains are already widely available, hence the implementation of a future BC4P application is assumed to be practically doable.

LEVEL OF DECENTRALIZATION

SCORE 5

PUBLIC.

Full decentralization.



SCORE 5

PRIVATE.

Whereas the public blockchain is permissionless, private blockchains are able to grant users permissions. In addition to that, ring signatures ensure the privacy of public keys (Feng et al., 2018).

SCORE 4

HYBRID.

Using zero-knowledge-proof makes the transaction data invisible and hence increases the level of privacy.

SCORE 4

PRIVATE.

Private blockchain solutions are available. The implementation of a raft consensus mechanism is regared plug-and-play (Ongaro & Ousterhout, 2014).

SCORE 2

HYBRID.

The combination of on-chain and off-chain solutions increases the level of complexity during the implementation phase.

SCORE 1

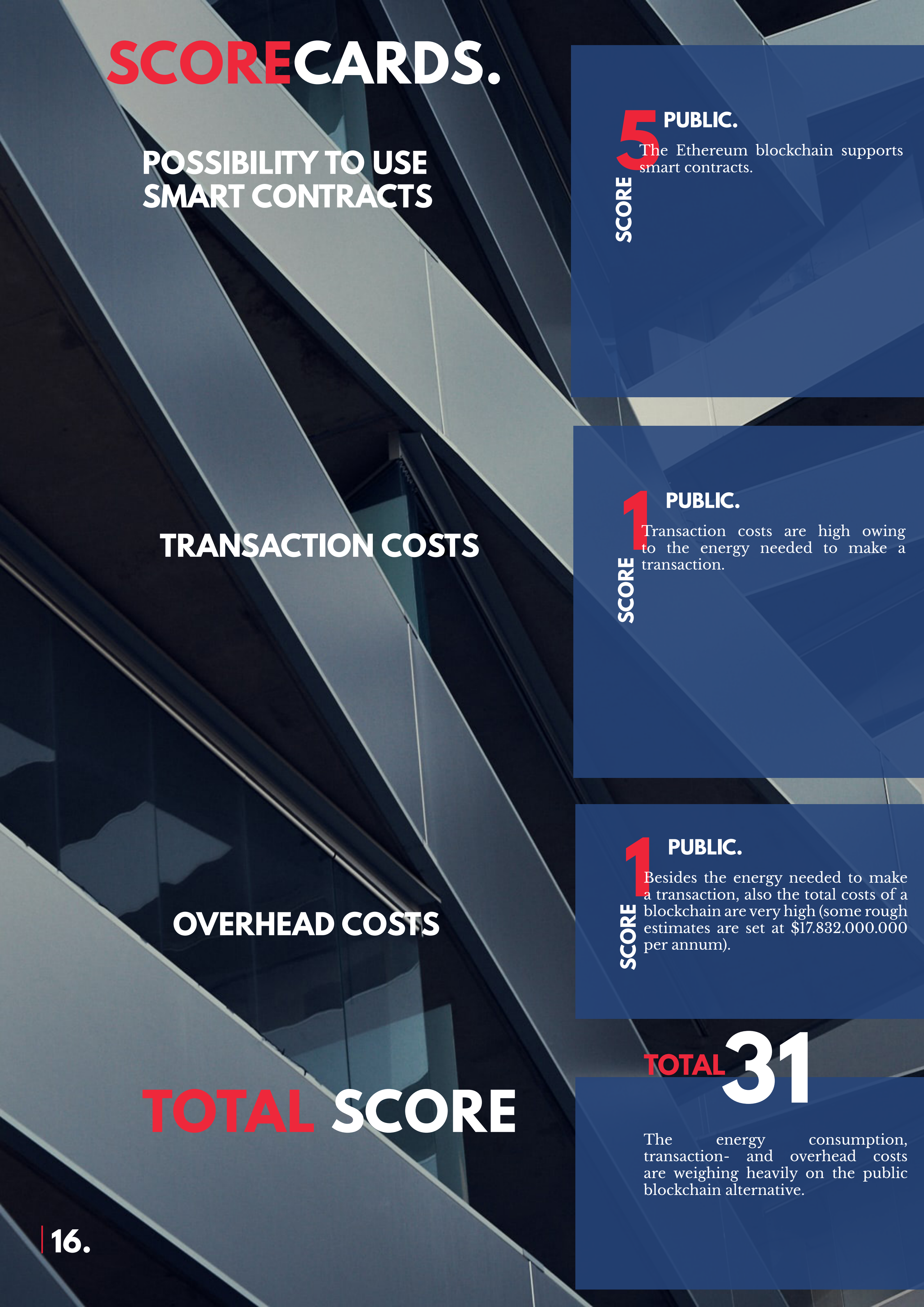
PRIVATE.

The level of decentralization in private blockchain solutions depends on the number of nodes (Li et al., 2019).

SCORE 3

HYBRID.

The hybrid alternative has a medium level of centrality. The public blockchain part is decentrally organized, but the transaction data is centrally stored.



SCORECARDS.

POSSIBILITY TO USE SMART CONTRACTS

SCORE 5

PUBLIC.

The Ethereum blockchain supports smart contracts.

TRANSACTION COSTS

SCORE 1

PUBLIC.

Transaction costs are high owing to the energy needed to make a transaction.

OVERHEAD COSTS

SCORE 1

PUBLIC.

Besides the energy needed to make a transaction, also the total costs of a blockchain are very high (some rough estimates are set at $17.832.000.000 per annum).

TOTAL SCORE

TOTAL 31

The energy consumption, transaction- and overhead costs are weighing heavily on the public blockchain alternative.

SCORE 5

PRIVATE.

Hyperledger Fabric is an example of a private blockchain solution which supports the usage of smart contracts.

SCORE 5

HYBRID.

Both Ethereum and CCC support the usage of smart contracts.

SCORE 5

PRIVATE.

Compared to the high transaction costs of the public blockchain alternative, the estimated transaction costs for a private blockchain are €0,0000067 (Business Insider, 2021).

SCORE 2

HYBRID.

Compared to the private blockchain alternative, the transaction costs are high.

SCORE 3

PRIVATE.

Owing to the size, overhead costs are way less than the public blockchain alternative.

SCORE 1

HYBRID.

Overhead costs for the public blockchain part are high.

TOTAL 35

The private blockchain (Hyperledger Fabric combined with a raft consensus mechanism and ring signature privacy algorithm) scores high an most of the criteria.

In order to test the practical implementation, a Proof-of-Concept is piloted.

TOTAL 26

The scalable alternative is not interesting for the BC4P project owing to high transaction costs and high energy usage.

CONCLUSION & DISCUSSION

This study aimed to analyze potential blockchain alternatives for the Blockchain4Prosumers project based on type, consensus mechanism (security) and privacy algorithms.

Three alternatives have been identified:

1. A public blockchain using a proof-of-work consensus mechanism and a mixing service algorithm to cover privacy concerns.
2. A private blockchain using a raft consensus mechanism and a ring signature algorithm to cover privacy concerns.
3. A hybrid blockchain using a proof-of-work consensus mechanism and a zero-knowledge-proof algorithm to cover privacy concerns combined with an off-chain solution (CCC) for the transaction data.

A panel of researchers has critically ranked these alternatives based on predefined criteria resulting in the recommendation of a private blockchain solution.

Alternatively, a traditional transaction method in the form of Online Transaction Processing (OLTP) which has been piloted In various smart energy management projects (Nagesh et al., 2010; Nur Asyik et al. , 2011).

4 ALTERNATIVES.

SCORECARDS.

PRIVATE BLOCKCHAIN.

35

PUBLIC BLOCKCHAIN.

31

HYBRID BLOCKCHAIN.

26

TRADITIONAL SOLUTION.

31

REFERENCES.

Bitcoinist. (2020). Bitcoin's Github Community Now Boasts of 3000+ Members. Retrieved from Bitcoinist: Cryptocurrency News & Technology: https://bitcoinist.com/bitcoins-github-community-now-boasts-of-3000-members/

Business Insider. (2021, Jul 13). A single Bitcoin transaction has a bigger carbon footprint than 100,000 hours of YouTube videos — here's how the crypto industry wants to fix that. Retrieved from Business Insider India: https://www.businessinsider.in/cryptocurrency/news/a-single-bitcoin-transaction-has-a-bigger-carbon-footprint-than-100000-hours-of-youtube-videos/articleshow/84373569.cms

Congcong Ye, G. L. (2018, Sept 23). Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting. Retrieved from ieeexplore: https://ieeexplore.ieee.org/abstract/document/8563187/authors#authors

Cui, Z., XUE, F., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020, Januari 7). A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN. Retrieved from IEEEXplore: https://ieeexplore.ieee.org/abstract/document/8951253

Cyberheroes. (2017, December 28). Private vs Public Blockchain. Retrieved from Cyberheroes: https://www.cyberheroes.be/blog/private-vs-public-blockchain

Feng, Q., He, B., Zeadally, S., Khan, M. K., & Kumar, N. (2018, Oktober 29). A survey on privacy protection in blockchain system. Retrieved from Journal of Network and Computer Applications: https://www.sciencedirect.com/science/article/abs/pii/S1084804518303485

Hwang, J., Choi, M. I., Lee, T., JEon, S., Kim, S., Park, S., & Park, S. (2017). Energy Prosumer Business Model Using Blockchain System to Ensure Transparency and Safety. Energy Procedia, 141, 194-198.

ictrecht. (2017, April 12). ICTrecht. Retrieved from Coinrecht #3 - Het belang van consensus in de blockchain: https://www.ictrecht.nl/blog/coinrecht-3-het-belang-van-consensus-in-de-blockchain

Ismail, L., & Materwala, H. (2019, August 29). A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions. Retrieved from Preprints: https://www.preprints.org/manuscript/201908.0311/v1/download

Johannes Sedlmeir, H. U. (2020, June 19). The Energy Consumption of Blockchain Technology: Beyond Myth. Retrieved from Springer Link: https://link.springer.com/article/10.1007/s12599-020-00656-x#Sec2

Joshi, A., Kale, S., Chandel, S., & Pal, D. K. (2015). Likert scale: Explored and explained. British journal of Applied Science & Technology, 7(4), 396.

Lai, R., Chuen, K., & Lee, D. (2018). Blockchain – From Public to Private. Retrieved from ScienceDirect: https://www.sciencedirect.com/science/article/pii/B9780128122822000073

Li, Y., Yang, W., He, P., Chen, C., & Wang, X. (2019). Design and management of a distributed hybrid energy system through smart contract and blockchain. Retrieved from Science Direct: https://www.sciencedirect.com/science/article/abs/pii/S0306261919307755

Mengelkamp, E., Norteisen, B. B., Dauer, D., & Weinhart, C. (2018). A blockchain-based smart grid: towards sustainable local energy markets. Computer Science-Research and Decelopment, 33(1), 207-214.

Nagesh, D. R., Krishna, J. V., & Tulasiram, S. S. (2010). A real-time architecture for smart energy management. 2010 Innovative Smart Grid Technologies (ISGT) (pp. 1-4). IEEE.

Nur Asyik, H., Blagoje, S., & Akthar, K. (2011). Analysis of distributed generation systems, smart grid technologies and future motivators influencing change in the electricity sector. Smart Grid and Renewable Energy 2011, (pp. 1-4).

Onderzoekdoen. (n.d.). Likert Schaal. Retrieved from Onderzoekdoen: https://www.onderzoekdoen.nl/enquete-onderzoek/likert-schaal/

Ongaro,]. D., & Ousterhout, J. K. (2014). In search of an understandable Concensus Algorithm. Retrieved from USENIX: https://www.usenix.org/node/184041.

Pahlanjani, S., Kshirsagar, A., & Pachghare, V. (2019). Survey on Private Blockchain Consensus Algorithms. Retrieved from https://ieeexplore.ieee.org/abstract/document/8741353

Pilkington, M. (2016). Blockchain technology: principles and applications. In F. Xavier Olleros, & M. Zhegu, Research handbook on digital transformations. Edward Elgar Publishing.

Rankin, W. L., & Grube, J. W. (1980). A comparison of ranking and rating procedures for value system measurement. European Journal of Social Psychology, 10(3), 233-246.

Saxena, S., Farag, H., Brookson, A., Turesson, H., & Kim, H. (2019). Design and field implementation of blockchain based renewable energy trading in residential communities. 2019 2nd International Conference on Smart Grid and Renewable Energy (SGRE) (pp. 1-6). IEEE.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. Gaithersburg: National Institute of Standards and Technology.