Blockchain 4 Prosumers Project

WP 1: Privacy and security mechanisms

Miguel van de Laar

Jan Beumers

Dominique Nijssen

Research Centre for Data Intelligence

Zuyd University of Applied Sciences, Heerlen, The Netherlands

Interreg
Euregio Maas-Rijn
EUROPESE UNIE

Zuyd
Research
ZUYD

Report Outline:

1. Blockchain Technology for Prosumers

A blockchain is a system for storing data in data blocks where each new block is added to the chain in such a way that it cannot be changed. There are various variations and applications for Blockchain technology (Edriouch, Bemelmans, Zoet, & Beumers, 2018). For instance we can distinguish public, private and hybrid blockchain systems. A public blockchain can be accessed by anybody; there is no need for trust between users and a specific (third) party. On the opposite side of the spectrum is the private blockchain which is accessible by invitation only and permissions have to be given to perform actions in the blockchain. Finally, as the name implies, the hybrid blockchain is a bit of both worlds where parts of public and private blockchain technologies are combined to create new solutions.

It is expected for blockchain technology to have a disruptive impact in various fields (Weller, 2015). The energy sector for example is one such field (Alladi, Chamola, Rodrigues, & Kozlov, 2019) (Samuel, et al., 2019). This report explores ways to implement blockchain within the INTERREG Blockchain 4 Prosumers project (BC4P). A number of options are evaluated by comparing consensus mechanisms, privacy guards and a number of practical concerns.

1.1. Consensus mechanisms

Consensus within a blockchain is reached by applying an algorithm (consensus mechanism) that ensures that all participating nodes come to an agreement about the true and valid state of the blockchain network and therefore controls the way decisions are made within the network. For example the consensus mechanism when used in the context of crypto currency solves the so called 'double spending' problem (ictrecht, 2017) which would occur when a user tries to use their balance in currency in two places. Figure 1 shows how the various consensus mechanisms are categorized according to Ismail and Materwala (2019).

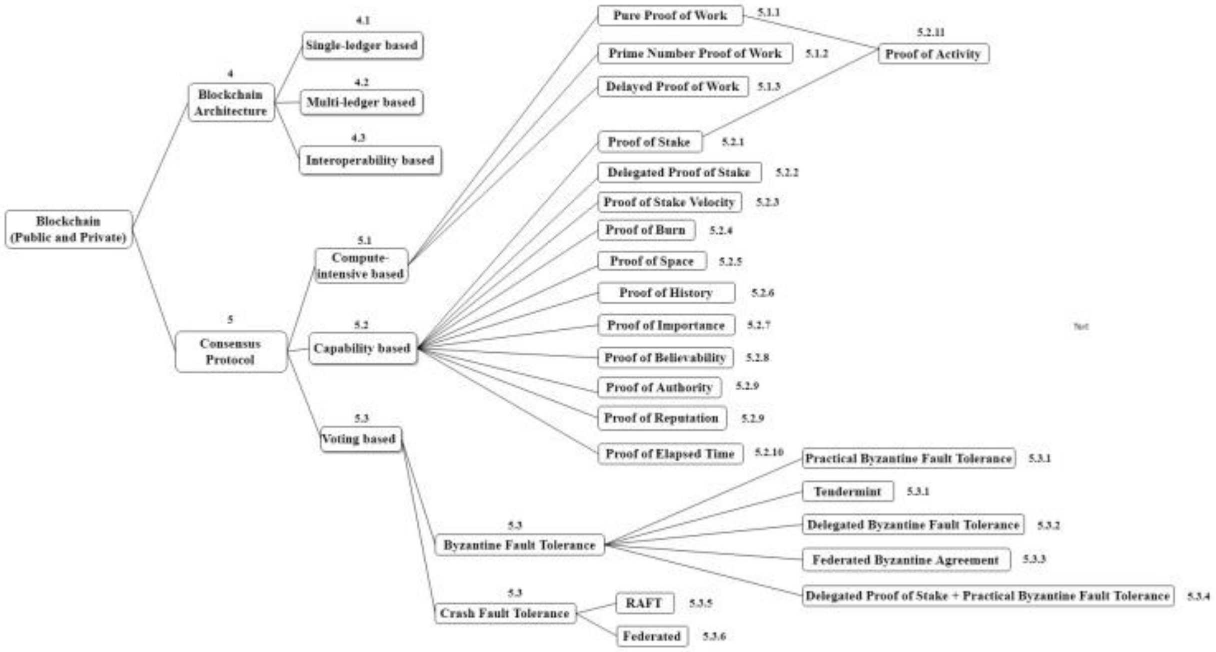

Figure 1: Possible consensus mechanisms according to Ismail and Materwala (2019).

1.2 Privacy control

In addition to consensus mechanisms that secure the network there are algorithms in place that guard the privacy of users. Information privacy in this context is the right for a user to choose which personal information is visible and to whom. There are a number of methods to guard a user's privacy, like using a mixing service, ring signature, and zero-knowledge proof (Feng, He, Zeadally, Khan, & Kumar, 2018).

Using a mixing service prevents an analysis of the network to see which entities have performed which transactions together by combining multiple transactions into one. The ring signature technique enables users to sign a transaction without disclosing which party actually performed the transaction. Another method to guard privacy is using non-interactive zero-knowledge proof where the interaction between the user that gives the proof for a transaction and the user that verifies the transaction is performed in an anonymised and distributed way (Feng, He, Zeadally, Khan, & Kumar, 2018).

1.3. Evaluation method

A number of scenarios were defined by combining a type of blockchain (public, private, or hybrid) with a consensus mechanism and type of privacy control to form a possible blockchain environment. Based on the requirements a number of scenarios have been analysed. The scenarios were chosen based on the following criteria:

- Community size
- Energy consumption
- Security
- Privacy friendliness
- Implementation complexity
- Measure of decentralisation
- Smart contract support
- Transaction costs

2. Public blockchain

2.1. Consensus mechanisms in the public blockchain

Public blockchains can use a number of different consensus mechanisms. These consensus mechanisms can be grouped into compute-intensive based and capability based (See figure 1).
Compute-intensive based consensus mechanisms use a method where the validators with the most computing power have the highest chance of validating a block.
Capability based consensus mechanisms were developed to counter the high energy consumption of computer-intensive based consensus mechanisms and use a non-computation based property of validators such as the amount of currency owned or available storage space to decide who can validate a block.

The main disadvantages to operating a public blockchain are high energy consumption and low transaction speeds. When using a public blockchain with the Proof-of-Work consensus mechanism a single transaction may cost as much as ten euros in energy (Lai, Chuen, & Lee, 2018).

Proof-of-Work

Proof-of-Work (PoW) is a type of compute-intensive based consensus mechanism where validators (miners) are rewarded with tokens that they may trade for value-accepted currency. In addition all actors are discouraged from undermining the network because the cost in power consumption will be higher than potential gains that can be had from doing so (Lai, Chuen, & Lee, 2018). Using PoW increases energy consumption significantly over other available consensus mechanisms (Johannes Sedlmeir, 2020). Bitcoin (Anderson, 2021) (Standford Edu, sd), Ethereum (Coininfobe, 2017) and Polkadot (Thoma, 2021) are blockchain-based cryptocurrency that use PoW.

Proof-of-stake

Proof-of-Stake (PoS) is a capability based consensus mechanism where validators are selected based on the number of tokens that they own or pledge (stake) when performing a validation. If the validation turns out to be incorrect they can be penalized. Contrary to PoW, PoS does not stimulate high energy consumption. Cardano (Ross, 2021), Algorand (Schoeman, 2021) and Tezos (Knight, 2020) are examples of blockchain-based cryptocurrencies that use PoS.

Proof-of-Burn

Proof-of-Burn (PoB) is another capability based consensus mechanism meant to combat the energy consumption of PoW (Ismail & Materwala, 2019). For PoB validators have to 'burn' tokens by sending them to a so-called 'eater address'. An eater address has a public key, but no corresponding private key making it impossible to recover these coins. Coins sent to such an address are removed from the network and cannot be reused. Like PoW, PoB uses the concept of validators investing computing power to enhance the chance of validating the next block in the blockchain. The winning validator is chosen by calculating the burn hash for each validated block and choosing the lowest burn hash. As of this writing Slimcoin is the only cryptocurrency to implement PoB.

Zero-Knowledge Proof

Zero-Knowledge Proof (ZKP) is yet another capability based consensus mechanism where a 'prover' can convince a 'verifier' in a number of ways that an action on the blockchain is legitimate without sharing the contents of that action. This keeps the information in the transaction private (Yang & Wenjie, 2020). Each ZKP has the properties completeness (if a statement is true the verifier can confirm that the correct input has been given), solidity (a statement cannot be approved falsely and the prover cannot convince the verifier that the correct input is present if it is not), and zero knowledge (the verifier receives no details about the transaction apart from information whether the transaction is valid or not. Personal information and other details about the transaction stay hidden) (Enwood, 2021).

2.2. A public blockchain for prosumers?

The suggested scenario for a public blockchain application for BC4P is one that uses the PoW consensus mechanism and ensures privacy by implementing a mixing service. This scenario has been chosen mainly because it is feasible in practice (Zheng, Xie, Dai, Chen, & Wang, 2017). Figure 2 gives a schematic view of this scenario. This scenario has been scored as explained in paragraph 1.3 (see table 1).

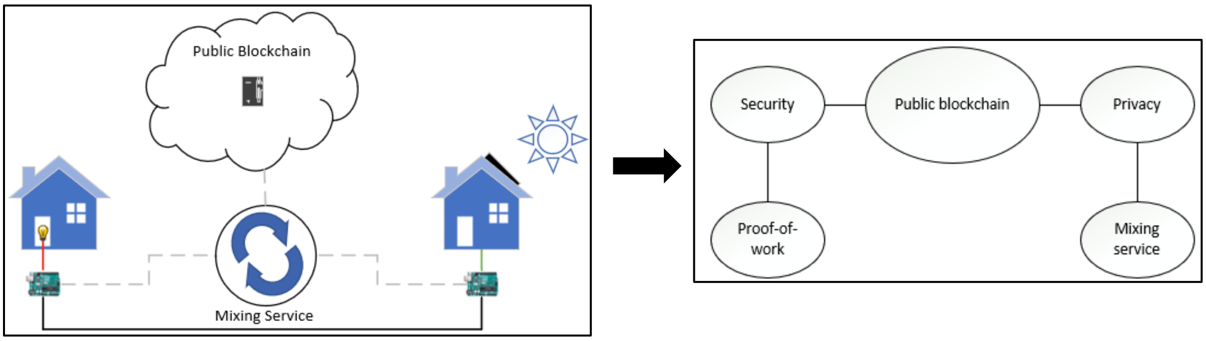

Figure 2: the Public blockchain scenario for the BC4P project

Criterium	Score	Explanation
Community size	5	A public blockchain is accessible for anybody without having to request access from a third party. Anyone can perform transactions and read data stored on the blockchain. Also the developer community is reasonably large (Bitcoinist, 2020).
Energy consumption	1	A transaction in a public blockchain using PoW costs a lot of energy and money (Johannes Sedlmeir, 2020) (Business Insider, 2021).
Security	5	Using a public blockchain is secure when a large number of nodes make up the network. Only when a single party controls at least 51% of the nodes is there a real risk to the network (Lai, Chuen, & Lee, 2018) (Congcong Ye, 2018).
Privacy friendliness	4	By using a mixing service it becomes virtually impossible to trace a transaction back to who initiated it. One possible drawback is possible delays when too few transactions use the service (Feng, He, Zeadally, Khan, & Kumar, 2018).
Implementation complexity	4	Since public blockchains are already up and running it is possible to build new applications within existing infrastructure.
Measure of decentralisation	5	The public blockchain is fully decentralised.
Smart contract support	5	Ethereum blockchain supports Smart Contracts
Transaction costs	1	Transaction costs on Ethereum are high (about $ 18 per transaction).
Overall score	**30**	**This solution scores very well on security, privacy and scalability. The costs however (in terms of energy consumption, transactions, and overhead) are very high.**

Table 1: Scores for the Public Blockchain scenario

3. Private blockchain

When using a private blockchain members are pre-selected to take part in the network. This means that a community can be constructed by the administrators of the blockchain. Since a network is controlled by one or more people (as nodes) there is little to no decentralisation (Zigurat, sd). A number of consensus mechanisms can be used when building a private blockchain usually variations on Byzantine Fault Tolerance and Crash Fault Tolerance methods (Pahlanjani, Kshirsagar, & Pachghare, 2019).

3.1. Consensus mechanisms in the private blockchain

Within a private blockchain in the area of consensus mechanisms a preference is given to voting algorithms (see figure 1) since the nodes in the network are known (Ismail & Materwala, 2019). Using a private blockchain does not require the use of a cryptocurrency, allows for fast transaction speeds, and possibly does not incur transaction costs.

Byzantine Fault Tolerance

The Byzantine Fault Tolerance (BFT) mechanism is a way to create order and to perform checks when multiple persons or systems are involved in a decision. The protocol is executed by two categories of 'peers':

1. validating peers that ensure that the consensus algorithm is put in place and can validate different types of transactions (Pahlanjani, Kshirsagar, & Pachghare, 2019).
2. Non-validating peers that enable the connection between clients and validating peers.

Hyperledger Fabric for instance is a blockchain framework that is used to execute smart contracts in combination with a modular infrastructure that provides a plug-and-play implementation. A possible drawback of using Hyperledger Fabric is that there currently is no tool or mechanism that identifies possible risks in the code of a smart contract. To help mitigate this drawback it is suggested to use a programming language like Go (Yamashita, Nomura, Zhou, Pi, & Jun, 2019) which makes it harder to write code that is non-deterministic (Murphy et al., 2018).

Ripple uses a so-called Practical Byzantine Fault Tolerance mechanism which should eliminate the risk of centralisation. It also has a lower energy consumption (since the algorithm needs no electricity to generate the next block), is supposed to be more scalable and should have lower transaction costs (EuroSys, 2018). The trade-off is that Ripple is very complex to implement which may lead to security issues when implementing and practical limitations on scalability.

The Stellar Consensus Protocol (SCP) is based on a new model, the so-called Federated Byzantine Agreement (FBA). This model functions with a chainlike structure where each node knows a set of nodes that have been classified as important. The protocol waits for a majority of these important nodes to agree to a transaction before it is allowed. SCP is an asynchronous protocol that guarantees consensus even when a node malfunctions. SCP is characterised by centralised control, low latency, trust and asynchronous security (Pahlanjani, Kshirsagar, & Pachghare, 2019).

Crash Fault Tolerance

In general a system that implements Crash Fault Tolerance (CFT) has a degree of resiliency in the protocol so that the network can complete its task and reach consensus even if a number of components fail.

The main differences between BFT and CFT is that BFT can withstand malicious actors (CFT cannot) but needs more nodes to reach a consensus (BFT can still function when up to a third of the nodes fail (including malicious actors), while CFT can function even if up to half the nodes have failed).

In short: if all actors can be trusted to act benignantly CFT will be tolerant of more (system) failures but if not all actors can be trusted to do so BFT should be used. When malignant actors are present when using CFT they can prevent consensus from being reached and thus in essence perform a Denial-of-Service attack.

Raft Consensus is a type of CFT that can be used when there will be no malicious actors and fast block creation and block finalization are required. It allows for block creation on demand and to manage the process with logging. (Ongaro & Ousterhout, 2014). In Raft there is a single elected leader and it is responsible for managing the data flow. When it fails or disconnects the network votes on a new leader. This process is shown in Figure 3.

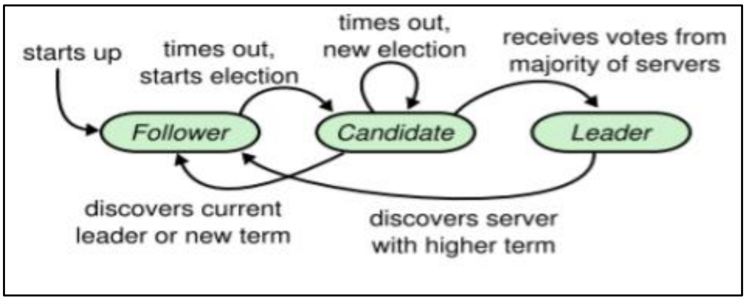
starts up
times out, starts election
times out, new election
receives votes from majority of servers
Follower
Candidate
Leader
discovers current leader or new term
discovers server with higher term

Figure 3: Lifecycle of peers in Raft Consensus (Pahlanjani, Kshirsagar, & Pachghare, 2019)

Another variant on CFT is the Federated Consensus Protocol which is implemented by Chain Protocol for Consensus. In this model blocks are only accepted if they have been signed by a specific number signers. The protocol checks if a block has been signed a required number of times which depends on requirements of security and the demand for transaction speed (Ismail & Materwala, 2019).

3.2. A private blockchain for prosumers?

The suggested private blockchain application consists of a private blockchain that uses the Raft consensus mechanism and a ring signature (Feng, He, Zeadally, Khan, & Kumar, 2018) to ensure privacy (See figure 4). Table 2 shows the evaluation for this scenario.

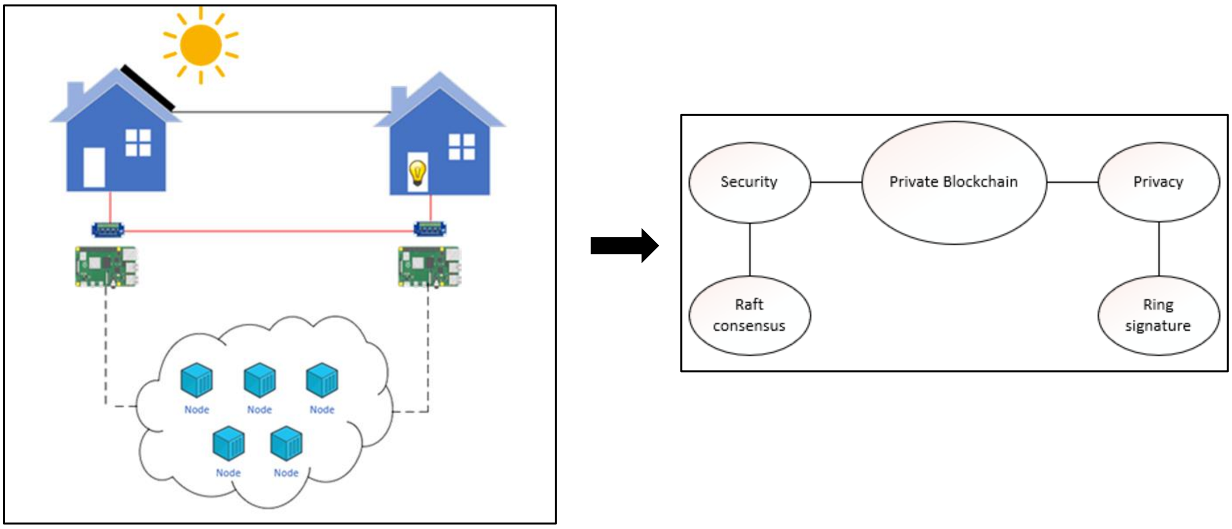

Figure 4: the Private blockchain scenario for the BC4P project

Criterium	Score	Explanation
Community size	3	It will depend on the size of the community whether this scenario can be used. Having a higher number of nodes will further decentralise the private blockchain and therefore make it more secure (Cyberheroes, 2017).
Energy consumption	5	Energy consumption of a private blockchain solution is relatively low. By using a consensus mechanism that does not use a lot of energy the private blockchain's energy consumption can be limited.
Security	4	Since a limited number of nodes would be used to operate a private blockchain it would be easier for a malicious actor to employ a larger number of nodes and take control of the blockchain. Using Raft consensus would block that actor from making changes to the blockchain since no consensus would be reached.
Privacy friendliness	5	A Private Blockchain is very privacy friendly because users have to be given permissions to perform actions on the blockchain. In addition in the proposed private blockchain privacy is increased by using Ring Signature (Feng, He, Zeadally, Khan, & Kumar, 2018).
Implementation complexity	4	Implementing Raft Consensus is considered to be plug-and-play (Ongaro & Ousterhout, 2014).
Measure of decentralisation	1	Private blockchains tend to be less decentralised since fewer nodes are necessary to host a blockchain (Li, Yang, He, Chen, & Wang, 2019).
Smart contract support	5	Smart Contracts can be implemented on a Private Blockchain (for instance using Hyperledger Fabric).
Transaction costs	5	A Private Blockchain has very low transaction costs, if any.
Overall score	**32**	**This scenario scores well across the board and has also been proven to be feasible in practice.**

Table 2: Scores for the Private Blockchain scenario

4. Hybrid blockchain

The idea behind Hybrid Blockchain is to have the best of both worlds to reduces weaknesses inherent in each approach. There are different approaches to building a hybrid blockchain:

1. Combining a private network and a public network;
2. Combining two different consensus mechanisms in a single network;
3. Combining a blockchain with a more traditional solution.

Combining networks

A Hybrid Blockchain is built by combining two networks: a public blockchain and a private blockchain. The public network can be viewed and used by anyone and contains only the hashes of transactions performed on the private blockchain. The private network has the content of the transactions, provides the hashes to be stored in the public blockchain and can only be used and viewed by selected users (Li, et al., 2018).

A combined hybrid blockchain has the following the properties (Kim, Park, & Ryou, 2018):

1. The code of the blockchain supports public and private blockchains. This requires a certain level of support in terms of APIs, tools, and even programmers.
2. The organisation supports data connectivity at a number of levels, like supporting storing hashes from the private blockchain in the private network, a sufficient level of availability, and verifiability.
3. The organisation supports collaboration between heterogeneous networks with different protocols which is done often through offering APIs.

Combining consensus mechanisms in a single network

By combining consensus mechanisms in a single network (which could be public or private) an improved solution can be created.

Combining blockchain and traditional solutions

Combining blockchain and more traditional approaches is often referred to as “on-chain off-chain” hybrid. A blockchain (which could be public or private) is combined with a more traditional solution (like a centralised database or cloud solution). There are many possible structures and architectures to create a hybrid chain. Different problems will call for a different division between public and private information, which accounts for the many different structures (Cui, et al., 2020).

4.1. Consensus mechanisms in the Hybrid Blockchain.

Proof of activity.

For solutions where networks are combined there currently exists only one recognised consensus mechanism: Proof-of-Activity (PoA) which is a combination of PoW and PoS. (Cui, et al., 2020).
There are a number of different implementations available for PoA that employ both PoW and PoS. In general combining these two mechanisms increases security of the network because the stakeholders first have to verify a block before it is added to the blockchain which reduces the chances of a hostile takeover (Sharma, sd).

Decred

Decred for instance works as follows: first PoW-miners create new blocks; once these are mined the PoS-miners decide whether that block is confirmed. The PoS-miners buy votes by staking tokens of the currency used within that blockchain. The hybrid mechanism chooses five random votes to decide on the effectiveness of the created block. If at least three of the randomly chosen five votes are in favour the block is added to the blockchain. The rewards are divided between the PoW-miners (60%), the PoS-miners (30%), and towards further development of the system (10%).

Fork-free hybrid consensus

Fork-free is like Decred but differs in that there is a small verification group that randomly changes every ‘round’. The difficulty of the block to be mined (the so-called nonce) that is received by the PoW-miners is verified by this group through a democratic system where each member has a single vote.

Flexible proof-of-activity

The Flexible PoA mechanism works similarly to Fork-free except that Flexible PoA does not choose the verification group members randomly since random selection does not give a motivation to build up extra capacity to mine blocks. Flexible PoA uses a chance for each node to become a verification group member which is weighted based on the capacity for mining blocks thereby rewarding nodes for increasing the capacity to mine blocks (Liu, Tang, Chow, Liu, & Long, 2019).

On-chain off-chain hybrid

Another way to create a hybrid blockchain is by building up the network partly on a blockchain and partly off the blockchain. This is not a recognised consensus mechanism but is a solution that has been used in practice.

An example is the Ethereum & Checking Contractual Compliance (CCC) hybrid blockchain. This was developed because no centralised or decentralised blockchain solution was found that combined the required scalability, performance, service quality, security, and reliability. CCC is an algorithm that checks whether parties keep to contractual agreements that have been encoded digitally. It is a way to develop clauses in contracts in such a way that these can be checked automatically (Molina-Jimenez, Shrivastava, & Strano, 2012).

4.2. A Hybrid blockchain for prosumers?

The proposed hybrid blockchain solution is the on-chain off-chain Checking Contractual Compliance (CCC). By employing a public blockchain the solution stays transparent and all transactions can be viewed on a public blockchain. To ensure that the contents of messages (that may contain privacy sensitive information) are secure Zero-Knowledge Proof is applied. As described before, this type of algorithm ensures that private information is not shared. Figure 5 shows a model for this scenario and table 3 shows the scores for this hybrid blockchain solution.

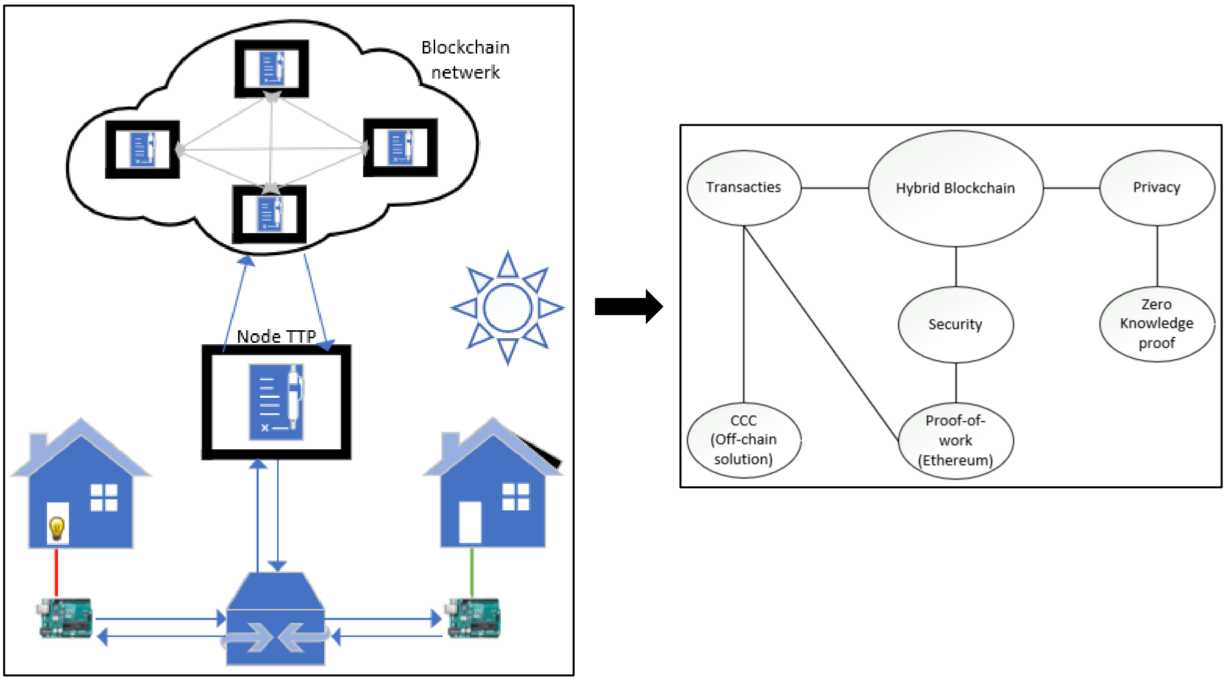

Figure 5: the Hybrid blockchain scenario for the BC4P project

Criterium	Score	Explanation
Community size	4	By combining a Public blockchain and off-chain application this solution is scalable. This means that it will work for any size community.
Energy consumption	1	Since the public Blockchain (by default Ethereum because of the need for Smart Contracts) employs Proof-of-Work there is a high energy consumption for each transaction.
Security	4	Using a Public blockchain increases security because of the high number of nodes. In contrast the CCC is controlled by a Trusted Third Party which might reduce the security.
Privacy friendliness	4	By using Zero-Knowledge Proof the contents of the transaction are not publicly visible which guarantees privacy.
Implementation complexity	2	Because on-chain and off-chain systems have to be combined the complexity of implementation increases.
Measure of decentralisation	3	Transactions are stored on the blockchain but processed by a centralised party.
Smart contract support	5	Ethereum blockchain supports the use of Smart Contracts. CCC also supports these, albeit off-chain.
Transaction costs	2	Transaction costs on Ethereum are high; Using CCC lowers the effective costs.
Overall score	**25**	**This scenario scores high for scalability but the various costs make it unrealistic.**

Table 3: Scores for the Hybrid Blockchain scenario

Concluding remarks

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).

References

Alladi, T., Chamola, V., Rodrigues, J. J., & Kozlov, S. A. (2019). Blockchain in smart grids: A review on different use cases. *Sensors, 19*(22), 48-62.

Anderson, S. (2021, August 02). *What Are the Advantages of Paying with Bitcoin?* Retrieved from Investopedia: https://www.investopedia.com/ask/answers/100314/what-are-advantages-paying-bitcoin.asp

bernd Teufel, A. S. (2019, Dec). *Blockchain energy: Blockchain in future energy systems*. Retrieved from sciencedirect: https://www.sciencedirect.com/science/article/pii/S1674862X20300057

Beumers, J., & Laar, V. d. (2021, September). Blockchain4Prosumers. (Snijders, Rutten, & Lelieveld, Interviewers)

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

Coininfobe. (2017). *Ethereum voor- en nadelen. Ontdek het hier!* Retrieved from Steemit: https://steemit.com/cryptocurrency/@coininfobe/ethereum-voor-en-nadelen

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

Dappsforbeginners. (2018, Oktober 10). *Two party contract*. Retrieved from Dappsforbeginners: https://dappsforbeginners.wordpress.com/tutorials/two-party-contracts

Dorri, A., Luo, F., Kanhere, S. S., Jurdak, R., & Dong, Z. Y. (2019, Juli 19). *SPB: A Secure Private Blockchain-Based Solution for Distributed Energy Trading*. Retrieved from IEEE: https://ieeexplore.ieee.org/abstract/document/8767089

Dorri, A., Luo, F., Kanhere, S. S., Jurdal, R., & Dong, Z. Y. (2018, juli 28). *SPB: A Secure Private Blockchain-based Solution for Energy Trading.* Retrieved from https://arxiv.org/abs/1807.10897

Edriouch, J., Bemelmans, R., Zoet, M., & Beumers, J. (2018). *Blockchain voor het hbo.*

Enwood, D. (2021, Juni 1). *Zero-knowledge proofs – a powerful addition to blockchain*. Retrieved from Blockhead: https://blockheadtechnologies.com/zero-knowledge-proofs-a-powerful-addition-to-blockchain/

EuroSys. (2018, April 23). *Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains*. Retrieved from EuroSys: https://arxiv.org/abs/1801.10228

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

Gramoli, V. (2016). *On the Danger of Private Blockchains*. Retrieved from Zurich IBM: https://www.zurich.ibm.com/dccl/papers/gramoli_dccl.pdf

Guegan, D. (2017, May 18). *Public Blockchain versus Private blockhain*. Retrieved from CCSID: https://halshs.archives-ouvertes.fr/halshs-01524440/document

Herlihy, M. (2018, July). *Atomic Cross-Chain Swaps*. Retrieved from PODC: https://dl.acm.org/doi/pdf/10.1145/3212734.3212736

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

Kim, G., Park, J., & Ryou, J. (2018). *A Study on Utilization of Blockchain for Electricity Trading in Microgrid*. Retrieved from IEEE: https://ieeexplore.ieee.org/abstract/document/8367221

Knight, R. (2020, December 15). *CORE Report: Tezos (Abridged)*. Retrieved from Cryptoeq: https://www.cryptoeq.io/corereports/tezos-abridged

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

Lazka, A., Dubey, A., Walker, M. A., & Schmidt, D. (2017, Oktober). *Providing Privacy, Safety, and Security in IoT-Based Transactive Energy Systems using Distributed Ledgers*. Retrieved from Research gate: https://www.researchgate.net/publication/318875755_Providing_Privacy_Safety_and_Security_in_IoT-Based_Transactive_Energy_Systems_using_Distributed_Ledgers

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

Li, Z., Kang, J., Yu, R., Deng, Q., & Zhang, Y. (2017, december 22). *Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things*. Retrieved from IEEE: https://ieeexplore.ieee.org/document/8234700

Li, Z., Wu, H., King, B., Ben Miled, Z., Wassick, J., & Tazelaar, J. (2018, Juni). *A Hybrid Blockchain Ledger for Supply Chain Visibility*. Retrieved from IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/8452028/authors#authors

Liu, Z., Tang, S., Chow, S., Liu, Z., & Long, Y. (2019, Juli). *Fork-free hybrid consensus with flexible Proof-of-Activity*. Retrieved from ScienceDirect: https://www.sciencedirect.com/science/article/abs/pii/S0167739X18326256

Molina-Jimenez, C., Shrivastava, S., & Strano, M. (2012, juni). *A Model for Checking Contractual Compliance of Business Interactions*. Retrieved from IEEEXplore: https://ieeexplore.ieee.org/abstract/document/5928317/

Murphy et al. (2018, April 28). *Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains*. Retrieved from ACM: https://dl.acm.org/doi/pdf/10.1145/3190508.3190538

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

Rijksdienst voor Ondernemend Nederland. (2021, Januari 8). *Smart grids en slimme energiesystemen*. Retrieved from rvo: https://www.rvo.nl/onderwerpen/duurzaam-ondernemen/energie-en-milieu-innovaties/smart-grids

Rosenfeld, M. (2014, February 12). *Analysis of hashrate-based double-spending*. Retrieved from arxiv: https://arxiv.org/pdf/1402.2009.pdf

Ross, L. (2021, September 13). *IS CARDANO A GOOD INVESTMENT?* Retrieved from Benzinga: https://www.benzinga.com/money/is-cardano-a-good-investment/#pros-for-cardano

Samuel, O., Javaid, N., Awais, M., Ahmed, Z., Imran, M., & Guizani, M. (2019). A blockchain for fair data sharing in deregulated smart grids. *IEEE Global Communications Conference*, 1-7.

Schoeman, L. (2021, September 9). *Algorand Reviewed*. Retrieved from SaShared: https://sashares.co.za/algorand-review/#Pros_and_Cons

Sharma, T. (n.d.). *A BRIEF INTRODUCTION TO HYBRID POW+POS CONSENSUS MECHANISM*. Retrieved from Blockchian Council: https://www.blockchain-council.org/blockchain/a-brief-introduction-to-hybrid-powpos-consensus-mechanism/

Shi, R. P. (n.d.). *Hybrid Consensus: Scalable Permissionless Consesnsus* . Retrieved from zurich: https://www.zurich.ibm.com/dccl/papers/pass_dccl.pdf

Snijders, Rutten, & Lelieveld. (2021). *Onderzoeksrapport.* Heerlen: Zuyd Hogeschool.

Snijders, Rutten, & Lelieveld. (2021). *Plan van Eisen.* Heerlen: Zuyd Hogeschool.

Solaiman, E., Wike, T., & Sfyrakis, I. (2020, Mei 13). *Implementation and evaluation of smart contracts using a hybrid on- and off-blockchain architecture*. Retrieved from Wiley Online Library: https://onlinelibrary.wiley.com/doi/full/10.1002/cpe.5811

Standford Edu. (n.d.). *Bitcoin decentralized, peer-to-peer, Cryptocurrency*. Retrieved from Stanford Edu: https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/DigitalCurrencies/disadvantages/index.html

Thoma, M. (2021, July 4). *CORE Report: Polkadot (Abridged)*. Retrieved from Cryptpeq: https://www.cryptoeq.io/corereports/polkadot-abridged

Timmermans, M. (2021, Januari 25). *Wat is Proof of Burn*. Retrieved from AllesOverCrypto: https://allesovercrypto.nl/blog/proof-burn#De+voordelen+van+Proof+of+Burn

Weller, D. (2015, August 11). *Beyond Bitcoin: How the Blockchain Could Disrupt Our Financial System*. Retrieved from Forbes: https://www.forbes.com/sites/sap/2015/08/11/beyond-bitcoin-how-the-blockchain-could-disrupt-our-financial-system/?sh=6b62e5d42da5

Yamashita, K., Nomura, Y., Zhou, E., Pi, B., & Jun, S. (2019). *Potential Risks of Hyperledger Fabric Smart Contracts*. Retrieved from IEEE: https://ieeexplore.ieee.org/abstract/document/8666486

Yang, X., & Wenjie, L. (2020, maart 30). *A zero-knowledge-proof-based digital*. Retrieved from ScienceDirect: https://www.sciencedirect.com/science/article/pii/S0167404820303230

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, sonsensus and future trends. *IEEE international congress on big data*, 557-564.

Zigurat. (n.d.). *Zigurat*. Retrieved from Public vs Private Blockchain: What’s the difference?: https://www.e-zigurat.com/innovation-school/blog/public-vs-private-blockchain-whats-the-difference/