



WITCOIN
move the knowledge

WHITEPAPER

Witcoin – Part II: Technical Description



Witcoin – Part II: Technical Description

Víctor Torres-Padrosa, Xavier Tarrés, Víctor Muñoz
Draft ver. 0.7; Oct 10, 2017

Abstract — As it was introduced in the Part I of this whitepaper, witcoin is a currency backed by knowledge that enables anyone and everyone to participate or contribute if they possess the requisite knowledge. A new overlaid decentralized platform of several actors that consult with each other across corporations and organizations is conceived for connecting and developing individuals, their ideas, and their projects so that the individuals collaborate with each other, getting and providing the best of their digital selves: their knowledge. The more knowledge that is put into action, the more wealth and the more witcoins represent and share this benefit among the actors. Some of them will do it professionally for themselves or on behalf of a company, others as a safe complement of their experience.

In this Part II, we are describing the chosen Ethereum implementation of wits as smart contracts and the witcoins as ERC223 tokens and superior versions, the business models of the several roles, and the technical roadmap.

I. INTRODUCTION

In today's networked age, competition is increasingly over platforms. Already many cooperation platforms play in the market. On the one hand, the successful set up and operation of an OI-platform (Open Innovation) or virtual currency platform could not be taken for granted. Simple databases where partners cooperate are proved often to be inflexible and eventually unsuccessful. What is the online values that makes a difference? Platforms also rely on the power of network effects — as they attract more users, they become more valuable to the users.

On the other hand, there is blockchain technologies that will happen everywhere. It first came to light in the late 2000's as the architecture underpinning bitcoin, the best known and most widely held digital currency. But, as with the Internet, the Web and other major technologies, the blockchain has now transcended its original objective, being Ethereum a great upgrade. It has the potential to revolutionize the finance industry and transform many aspects of the digital economy [1], and the most interesting aspects for us here is their transformation power of the innovation processes [3].

Distributed ledger systems, i.e. the blockchain technology, today are being built in a variety of industries but to realize the promise of this emerging technology, an open source and collaborative development strategy that supports multiple players in multiple industries is required. This development can enable the adoption of blockchain technology and even more with Ethereum at a pace and depth not achievable by any one company or industry. This type of shared or external Research & Development (R&D) has proven today to deliver billions in economic value. These values will be adopted by witcoin.

Using Ethereum technology can be a step closer to a radical re-think of the way we conduct business and engage in competition [2], that is precisely one of the matching goals of witcoin.

Indeed, an increasing number of industries organize their activities along the structure of central platforms surrounded and/or complemented by networks/constellations of other organizations, which technologically and strategically depend upon the core platform [4]. In today's context, increased pervasiveness of digital technologies and connectivity, combined with a global worldwide and distributed supply of

¹ This is the 2nd part of the whitepaper, which is composed of two parts: the first is for witcoins and the roadmap, and the second one presents a detailed platform description.





WITCOIN

move the knowledge

ICT skills [5], has made the platformization trend even stronger.

This is happening for OI and for Blockchain and Ethereum at the time, and these platforms concepts must converge with Witcoin, as we state in [6].

As said in the Part I of the whitepaper, witcoin is a currency backed by knowledge and wits are useful knowledge.

The witcoin platform will be deployed on top of Ethereum, which means that witcoins will be Ethereum tokens and wits will be smart contracts enabling wit owners to be rewarded for their usefulness.

This technical document describes how the implementation of the witcoin will be done and how the corresponding knowledge or wit will be represented.

Section II will show the architecture, section III the description of the witcoin tokens, section IV the implementation of the wits as smart contracts, to go on in sections V, VI, and VII with several roadmap and biz for sustainability aspects.

II. THE WITCOIN ARCHITECTURE

The witcoin architecture relies on three different contracts, namely the witcoin platform, the witcoin supply, and the witcoin token.

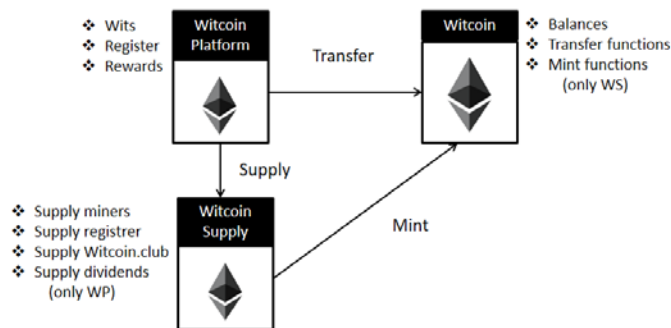


Fig. 1. The witcoin contracts

The witcoin platform contract is in charge of receiving and registering wits. Please note that the wit itself is a separate smart contract that is created at the time of registration (see section IV for further details), registering a wit is receiving the address of such contract. The witcoin platform contract also distributes the rewards among the corresponding cited wits and the witcoin.club by generating the corresponding transfers according to the rules specified in Part I.

The witcoin supply contract is in charge of supplying witcoins to the miners, witcoin club and registrars and distribute dividends, according to the rules specified in Part I. The witcoin supply contract can be only executed from the witcoin platform contract when new wits are registered.

Finally, the witcoin token contract is in charge of witcoin balances, transfers, and minting new witcoins whenever required by the witcoin supply.

In the future, it is foreseen to enable the creation of branded witcoins or witcoin biz tokens.

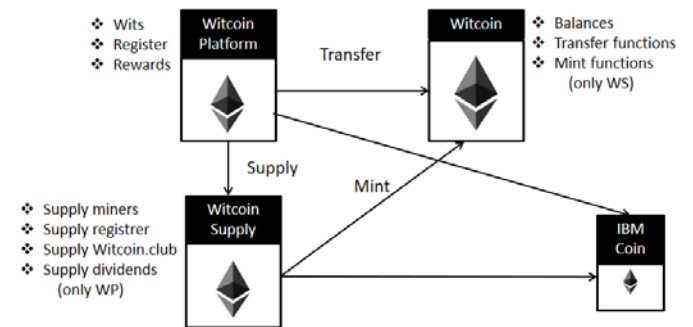


Fig. 2. Branded witcoins

Witcoin biz tokens will enable different companies or platforms to adopt the witcoin principles rewarding their users or employees for the usefulness of their knowledge. Witcoin biz tokens will be a way to differentiate communities and to measure the knowledge created by them, while enabling a different market quotation. Moreover, the exchange among witcoin tokens and witcoin biz tokens will be fully compatible. Witcoin biz tokens require the witcoin platform contract to use new branded contracts for keeping separate balances, transfer functions and minting. The witcoin platform and witcoin supply contracts will remain the same, thus ensuring that miners, registrars, the witcoin.club and dividend receivers are properly supplied with the new biz token whenever a wit is cited.

The creation of the witcoin biz token will ruled by the witcoin.club to regulate their growth and reduce the impact on the witcoin platform memory consumption and thus, the operating costs.



III. THE WITCOIN TOKEN

A. The Witcoin Token

The witcoin token relies on the ERC223 token standard, which enables all the functions from previous ERC20Basic and ERC20 tokens. Thus, the witcoin token enables account to account transfers, transfer from with approval, and the new ERC223 functions for transfers from accounts to contracts without the need to *approve* and *transferFrom* at receiver contract, among other² functions.

B. The Knowledge Token

Our aim is to define a new standard as an evolution of the ERC223 token standard to be used as the knowledge token, which will include all the functions and structure defined in section I.A.

The initial version of the knowledge token will include the mint function to mint and distribute new tokens whenever new wits are registered.

Thus, the witcoin token will extend the knowledge token, which will, on its turn, extend the ERC223 token.

```
pragma solidity ^0.4.15;
import './ERC223.sol';

contract KnowledgeTokenInterface is ERC223{
    address public minter;
    event Mint(address indexed to, uint256 amount);
    function changeMinter(address newAddress)
    returns (bool);
    function mint(address _to, uint256 _amount)
    returns (bool);
}
```

Fig. 4. The knowledge token interface

```
pragma solidity ^0.4.15;
import "../dependencies/ownership/Ownable.sol";
import "./ERC223Token.sol";
import "./KnowledgeTokenInterface.sol";

contract KnowledgeToken is KnowledgeTokenInterface, Ownable, ERC223Token {

    address public minter;
    mapping(address => uint) balances;
    uint256 public totalSupply;

    modifier onlyMinter() {
        // Only minter is allowed to proceed.
        require (msg.sender == minter);
    }

    function mint(address _to, uint256 _amount)
    onlyMinter public returns (bool) {
        totalSupply = totalSupply.add(_amount);
        balances[_to] = balances[_to].add(_amount);
        Transfer(0x0, _to, _amount);
        Mint(_to, _amount);
        return true;
    }

    function changeMinter(address newAddress)
    public onlyOwner returns (bool){
        minter = newAddress;
    }
}
```

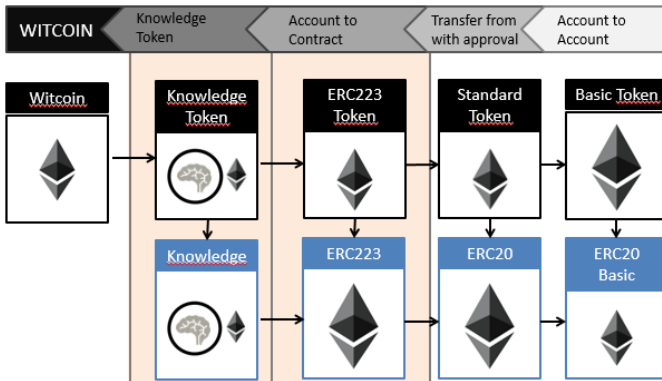


Fig. 3. The witcoin and knowledge token

Figures 4 to 6 include the first implementation of the knowledge token interface, knowledge token and witcoin. The full development resources can be found at witcoin-io on GitHub³.

² <https://github.com/Dexaran/ERC223-token-standard>

³ <https://github.com/Witcoin-io/witcoin/>





WITCOIN

move the knowledge

Fig. 5. The first knowledge token implementation

```
pragma solidity ^0.4.15;
import "../KnowledgeToken.sol";

contract WitCoin is KnowledgeToken{
    function WitCoin() {
        totalSupply = 0;
        name = "Witcoin";
        symbol = "WIT";
        decimals = 8;
    }
}
```

Fig. 6. The first witcoin implementation

IV. THE WIT IMPLEMENTATION

Although the wit is implemented as a smart contract, we have worked out several options for the WIT implementation. Next, we describe them as a progressive evolution in terms of capabilities.

The first option would be to implement the wit as a proof of existence. This means that given a content and its hash, the hash is inserted in the blockchain through a transaction. In this case, provided a wit and the mechanism to obtain the hash from it, anyone would be able to search and find such wit throughout the Ethereum blockchain and prove it was registered. This option is nothing new when compared with the state of the art, since there are already some existing initiatives that implement the proof of existence⁴.

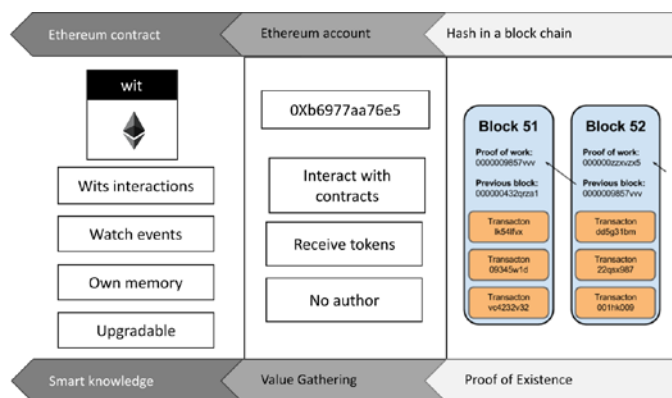


Fig. 7. The wit implementation alternatives

The second option would be to implement the wit as an Ethereum account. In this case, each wit would have a corresponding Ethereum account that would be used to interact with contracts and receive rewarding tokens. Each account would be monitored from the wit owner's Ethereum wallet and the link among the account and the corresponding wit contents will not be transparent, which means that it should be kept within the witcoin platform contract.

The third option, i.e. the one being adopted, assumes that a wit is an Ethereum contract. As a contract, a wit can have its own intelligence, memory, the possibility to watch events and interact with other wits. The citations to other wits are already implemented in the smart contract. It can be upgradable as well, enabling the wit contents or owner to be changed under specific conditions. In practical terms, since it is a smart contract, any user would be able to interact with their wits from their wallet to consult or modify its status.

Our vision is that the wit, in a similar way to the knowledge token, will become a standard, a knowledge standard in the form of a smart contract that can evolve over time with different successive versions extending the previous ones.

Figure 8 shows the first interface of the wit contract containing the minimum information to be stored in it:

- Author
- Citations: the list of wits cited from the current wit

```
pragma solidity ^0.4.15;

contract WitKnowledgeInterface {

    address author;
    address[] citations;

    function withdrawWitcoins() onlyOwner;
    function getAuthorAddress() returns(address);
}
```

Fig. 8. The minimum wit contract interface

Again, all the development resource can be found at witcoin-io on GitHub⁵. The additional information that the wit might contain would be:

- Title: the title of the wit
- Description: a summary or overview of the wit contents

⁴ For example, <https://app.originstamp.org/home>

⁵ <https://github.com/Witcoin-io/witcoin/>



- Registration Date: the date when the registration has been completed, which is only known when the registration transaction is validated.
- Owner, %Ownership: the list of owners (1..N) and the percentage of ownership of the wit.
- ResourceHash, ResourceKeeperAddress (opt): a list of related resources such as any type of multimedia files or documents identified by their SHA-256 hash and optionally an address where to find them on IPFS.

In order to reduce the transaction costs, the additional information in the wit will not be provided in the moment of registration. However, the wit owner will be entitled to call the wit contract to set such extra information, which means that the cost of transaction to enhance the wit with additional information will be fully covered by the wit owner.

Thus, any registrar willing to register wits would need to follow two very simple steps:

- 1) Create a new wit contract. Depending on the amount of information to be stored in the wit, this contract creation will be more or less gas expensive.
- 2) Call the witcoin platform to register the wit providing the wit contract address.

V. CONTRACT UPGRADES

The wit smart contract opens the door to a wide range of potential applications beyond those that have been initially foreseen in the preliminary implementations and use cases described in the Part I of this whitepaper. That's why it is mandatory to enable since its conception the possibility to increase their functionality. Therefore, the knowledge token and wit are designed to be upgradable since they make use of a versioning system consisting of a contract dispatcher, which can be upgraded to call new contract upgrades.

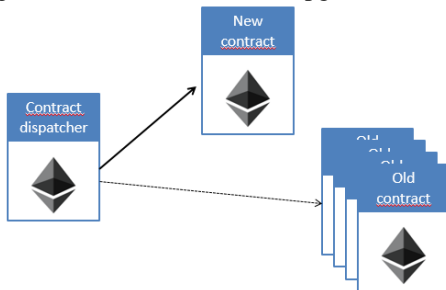


Fig. 9. How contracts can be upgraded

However, this mechanism requires the contracts storage to be migrated as well. In order to avoid this huge effort in terms of

transactions and resources, the wit and witcoin contracts will be designed to keep the logic and the data separated in different contracts. Thus, whenever a contract upgrade is needed, the new contract will use the same storage as the old contract, without the need for a data migration. These features will impact in future developments of digital preservation, that is one of the potential usages of the wits that will be worth exploring after the full development of the main use cases.

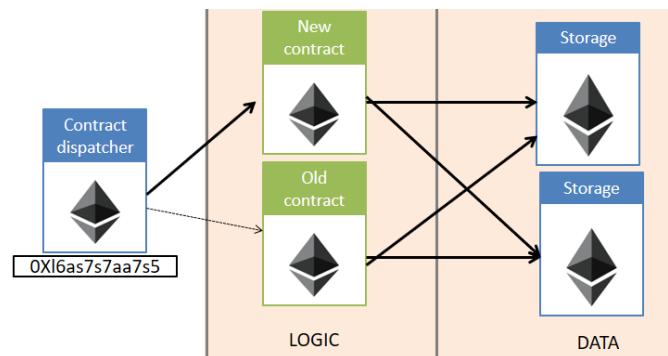


Fig. 10. How contracts can be upgraded

VI. WIT REGISTRATION COST

Several cases are analysed to estimate the cost of registration of a wit: basic, advance, and cost rationalization registration.

C. Basic Registration

In this case, we consider the cost of registering 1 wit that includes one single citation. In this case, the following costs would apply:

Type	Gas
Transaction	21000
Save witcoin	40000
Citation reward	33812
Coin creation	67625

Table 1. The cost of registering 1 wit (the basic one)

It is important to note that, provided that the wit will be a smart contract, this requires a contract deployment for each wit registration, which would increase the bill by 60.000 additional gas. Then, the total cost would be of 222.437 gas. To ensure the ethereum transaction to be processed, if we take a SafeLow (<20m) price for the gas of 3 gwei, the total cost for the registration would be of 0,000667 ETH.





WITCOIN

move the knowledge

D. Advanced Registration

In this case, we consider the cost of registering 1 wit that includes 3 citations and 4 rewarding levels, i.e. citations of citations. In this case, the following costs would apply:

Type	Gas
Transaction	21000
Save witcoin	40000
Citation reward	2615563
Coin creation	67625

Table 2. The cost of registering 1 wit (the worst one)

The total cost would be of 2.838.801 gas, including 60.000 gas related to the wit contract. To ensure the ethereum transaction to be processed, if we take a SafeLow (<20m) price for the gas of 3 gwei, the total cost for the registration would be of 0,008336 ETH.

It is important to note the great influence on the cost of the citations rewards, which increases exponentially according to the citations and levels of citations involved in the registered wit. This could put the overall system stability into risk. Thus, next section explains to overcome this problem.

E. Cost Rationalisation

As we have seen, the number and levels of citations have very high impact on the cost of registration, mainly due to the costs related to the transfers to cited wits triggered by the wit registration.

In order to keep the witcoin system stable, we propose two possible measures to be adopted to reduce drastically the transfer costs.

The first measure relies on the accumulation of received witcoins until a threshold is reached. Once the threshold is exceeded, then the witcoin platform executes the corresponding transfers. This threshold will be determined so that the mean extra cost due to transactions per wit registration does not exceed the cost of 3 citations, i.e. 101.436 gas.

Although this measure keeps transfer costs controlled, it still has some implications in the sense of liquidity, since a registration might imply the exceedance of the thresholds in several accounts and thus unleash an important number of transfers with the corresponding costs, which might result in some liquidity peaks concerns.

The second measure also relies on the accumulation of received witcoins, but gives the control to the users to ask for their accumulated funds whenever they want. In this case it will be the users the ones to afford the transfer cost.

The analysis on section VII relies on the first alternative, for which we estimate the mean cost of registering a wit by 323.873 gas or 0,00972 ETH, making the same assumption of 3 gwei per gas to ensure a SafeLow transaction (transactions confirmations in less than 20 minutes).

VII. REGISTRARS BIZ CASES

In this section, we present five different business cases for registrars corresponding to five possible values of the witcoin with respect to the ether. Case 1 is the starting point, where the witcoin initially value is of 880 witcoin (WIT) per 1 ETH.

Case	ETH	WIT
1	1	880
2	1	222
3	1	88
4	1	20
5	1	1
6	1	0,1

Table 3. Witcoin conversion rates in the business cases

We consider that the baseline registration fee in WIT is fixed by the witcoin.club and that it will be adapted proportionally to the increase of value of the WIT. The 80% of the registration fee will go for the citations, while the remaining 20% will be given to the registrar.

Table 4 shows the cases 2 to 6 deployed along several number of wits registered per month, from 1 to 100.000.

In order to make the conversion from ETH into EUR, we have assumed a conversion rate 1 ETH = 250 EUR.

As it can be seen, the benefit for registrars will range from 920k to 28k EUR in the case of 100k wits registered per month.





WITCOIN

move the knowledge

Num. of wits/month for Case 2	Costs (ETH)	Income (WIT)	Cost (WIT)	Benefit (WIT)	Benefit (ETH)	Benefit (EUR)
1	0,0009716	0,3692774	0,2156994	0,1535780	0,0621214	0,09
100	0,0971619	36,9277407	21,5699418	15,3577989	6,2121429	9,15
1.000	0,9716190	369,2774069	215,6994180	153,5779889	62,1214291	91,46
10.000	9,7161900	3.692,7740694	2.156,9941800	1.535,7798894	621,2142906	914,57
100.000	97,1619000	36.927,7406943	21.569,9418000	15.357,7988943	6.212,1429057	9.145,66

Num. of wits/month for Case 3	Costs (ETH)	Income (WIT)	Cost (WIT)	Benefit (WIT)	Benefit (ETH)	Benefit (EUR)
1	0,0009716	0,1559565	0,0855025	0,0704540	0,0008006	0,20 €
100	0,0971619	15,5956510	8,5502472	7,0454038	0,0800614	20,02 €
1.000	0,9716190	155,9565103	85,5024720	70,4540383	0,8006141	200,15 €
10.000	9,7161900	1.559,5651033	855,0247200	704,5403833	8,0061407	2.001,54 €
100.000	97,1619000	15.595,6510333	8.550,2472000	7.045,4038333	80,0614072	20.015,35 €

Num. of wits/month for Case 4	Costs (ETH)	Income (WIT)	Cost (WIT)	Benefit (WIT)	Benefit (ETH)	Benefit (EUR)
1	0,0009716	0,0376211	0,0194324	0,0181887	0,0009094	0,23 €
100	0,0971619	3,7621088	1,9432380	1,8188708	0,0909435	22,74 €
1.000	0,9716190	37,6210880	19,4323800	18,1887080	0,9094354	227,36 €
10.000	9,7161900	376,2108802	194,3238000	181,8870802	9,0943540	2.273,59 €
100.000	97,1619000	3.762,1088019	1.943,2380000	1.818,8708019	90,9435401	22.735,89 €

Num. of wits/month for Case 5	Costs (ETH)	Income (WIT)	Cost (WIT)	Benefit (WIT)	Benefit (ETH)	Benefit (EUR)
1	0,0009716	0,0019899	0,0009716	0,0010183	0,0010183	0,25 €
100	0,0971619	0,1989876	0,0971619	0,1018257	0,1018257	25,46 €
1.000	0,9716190	1,9898757	0,9716190	1,0182567	1,0182567	254,56 €
10.000	9,7161900	19,8987573	9,7161900	10,1825673	10,1825673	2.545,64 €
100.000	97,1619000	198,9875730	97,1619000	101,8256730	101,8256730	25.456,42 €

Num. of wits/month for Case 6	Costs (ETH)	Income (WIT)	Cost (WIT)	Benefit (WIT)	Benefit (ETH)	Benefit (EUR)
1	0,0009716	0,0002099	0,0000972	0,0001127	0,0011271	0,28 €
100	0,0971619	0,0209870	0,0097162	0,0112708	0,1127078	28,18 €
1.000	0,9716190	0,2098697	0,0971619	0,1127078	1,1270781	281,77 €
10.000	9,7161900	2,0986971	0,9716190	1,1270781	11,2707806	2.817,70 €
100.000	97,1619000	20,9869706	9,7161900	11,2707806	112,7078059	28.176,95 €

Table 4. Income, cost and benefit in cases 2 to 6





WITCOIN

move the knowledge

VIII. TECHNOLOGICAL ROADMAP

The foreseen technological roadmap involves several steps to reach a full operational witcoin system. We plan to have the witcoin system available in three months and the first relevant use case integrated in 5 months. Next follow the dates foreseen, assuming the crowdsale provides the needed resources for development.

1. October 10, 2017: the full whitepaper is published, both the Part I – concept and Part II – Technical description, the web is online and the pre-sale information available in the website.
2. October 16, 2017: the protocol, token definitions and first wits are available on Github as well as the NIR-VANA use case is defined and the crowdsale is launched.
3. December 1, 2017: the witcoin supply and witcoin platform contracts are created and deployed on a testnet for alpha versions.
4. February 1, 2017: the witcoin supply and witcoin platform contracts are deployed on the Ethereum network for beta versions and launch. The witcoin vault (WV), a specific witcoin wallet, is released. An API for registrars offering a high-level interface to interact with the witcoin system through an RPC client is released.
5. March 15, 2018: the first integration of the witcoin system is fully provided for the NIR-VANA platform Open Innovation use case, which is based on HumHub⁶.
6. From April 2018 to March 2019: integration in additional online social networks, enterprise social networks and online collaboration tools. Adoption of witcoin in IM, CRM and ERP platforms.

And between the main milestones there the following remarkable moments:

7. April 15, 2018: the wit registration through email is finished and released.
8. May 15, 2018: the retweet use case is finished and released.
9. September 2018: a first fully workable implementation of a bot making use of witcoin, including the use and exploitation of different data sources through big data.

GLOSSARY

Wit – Knowledge that makes sense

Witcoin – Currency used to acknowledge that a wit has made sense to someone else.

Citation – whenever a peer acknowledges a wit because of having found it useful.

ACKNOWLEDGEMENTS

To the useful insights and contributions of Josep Lluís de la Rosa, Andrés el-Fakdi, Adrià Llorens, David Bruguera, and more.

REFERENCES

- [1] <http://www.archive.annenberglab.com/blogs/iberger/2016/01/blockchain-and-open-innovation>
- [2] <http://tabbforum.com/opinions/cryptoeconomics-the-opportunities-and-challenges-of-blockchain>
- [3] Johansen, SK (2017) A Comprehensive Literature Review on the Blockchain Technology as an Technological Enabler for Innovation, working paper https://www.researchgate.net/publication/312592741_A_Comprehensive_Literature_Review_on_the_Blockchain_Technology_as_an_Technological_Enabler_for_Innovation
- [4] Gawer, A., and Cusumano, M. A. (2013). Industry. Platforms and Ecosystem Innovation. *J Prod Innov Manag* 31, no. 3 (September 4, 2013): 417–433.
- [5] Chesbrough, H., & Bogers, M. (2014). Explicating Open Innovation: Clarifying an Emerging Paradigm for Understanding Innovation Keywords. In H. Chesbrough, W. Vanhaverbeke, & J. West (Eds.), *New Frontiers in Open Innovation* (pp. 1–37). Oxford University Press. <http://doi.org/10.1093/acprof>
- [6] de la Rosa, J. L., Maicher L., Torres, V., El-Fakdi, A., Miralles, F., & Gibovic D., (2017). A SURVEY OF BLOCKCHAIN TECHNOLOGIES FOR OPEN INNOVATION. 4th ANNUAL World Open Innovation Conf. WOIC 2017, San Francisco (CA, USA), December 14-15, 2017.

⁶ <https://www.humhub.org>





WITCOIN

move the knowledge

