Blockchain, IoT and Sidechains

Chinazaekpere Emmanuel Ngubo
Department of Informatics
King's College London
London, UK
chinazaekpere.ngubo@kcl.ac.uk

Mischa Dohler
Department of Informatics
King's College London
London, UK
Mischa.Dohler@kcl.ac.uk

Peter McBurney
Department of Informatics
King's College London
London, UK
Peter.McBurney@kcl.ac.uk

***Abstract*—Two of the most interesting fields of research today is Blockchain and the Internet of Things (IoT). The workings and promises of both technologies have led to research into a joint application in the near future. A true joint application of these technologies would involve the IoT having an external connection and not being limited to a local network or Blockchain. Making IoT devices participate in the Blockchain while making their data available across other Blockchain platforms is a challenge still being explored. We intend to approach this problem using sidechains, creating an inter-Blockchain network.**

***Keywords*-IoT; Blockchain; Distributed ledgers; Sidechains.**

I. INTRODUCTION

One of the most talked about applications of the Blockchain is in the field of the Internet of Things(IoT). It is believed that the distributed nature of the Blockchain as well as its cryptographic structure can introduce an element of data ownership and increase the speed of communication between devices. In most designs, the IoT is seen to have a more centralised structure, centred around a server and as such the IoT is a system designed on the server-client model. A centralised structure suggests the presence of a bottleneck of which in this case would be the server. However, the distributed structure of the Blockchain has no such bottleneck limitation and therefore would an excellent structure for a Big Data technology such as the IoT.

The Internet of Things as the name suggest is a means of taking everyday objects and machinery, embedding them with sensors, actuators, RFIDs, NFC and enabling these embedded technologies to not only communicate with their environment but also be able to communicate via the Internet. For example, we have transitioned from regular human-operated on-site washing machines to mobile app operated washing machines and are now moving towards autonomous washing machines. Energy and gas companies since 2017 have been deploying smart meters in the UK, replacing old archaic pay-point ways of monitoring and paying. There are other examples of autonomous devices being introduced into western society. As old, archaic ways of doing things are being replaced by modern, digitised methods; there seems to be a growing list of the application of IoT. This success of the IoT has led to an almost 30% yearly increase in the number of connected IoT devices according to Gartner. Though there has been a decline in the 2020 projections, from 50 to 20 (at the writing of this paper), the number remains in the billions. This increase can be noticeably seen in the number of smart home devices being sold such as (Google Home, Nest thermostat, Phillips Hue smart light and Amazon Alexa in Amazon Echo [1]).

The most obvious advantage of the Blockchain technology is that it can connect a large number of nodes using its distributed network and still carry out the same operations, achieving the same results [2], if not better, and with the advantage of a cryptographic identification for the devices. A cryptographic ID for the IoT means anonymity on the network as well as an added layer of security and authentication. These devices, having a cryptographic ID can communicate in a trustless network absent of central dependencies, which in turn means faster communication or better latency between communicating IoT devices. But it is also important for IoT devices operational on local Blockchains to be able to communicate with other devices if needed, in real-time or close to real-time.

The goal of this paper is to show how sidechains can be deployed in IoT for inter-chain communications. The rest of the paper is sectioned as follows: Section II is a description of technologies, a brief introduction and overview of both the Internet of Things and the Blockchain. Section III renders the Blockchain tailored specifically for the IoT and its resource-constrained nature. In section IV, we present our proposal for inter-Blockchain communication using sidechains in an IoT case scenario and section V Conclusion.

II. DESCRIPTION OF TECHNOLOGIES

In this section, we provide a brief description of both technologies.

A. Internet of Things (IoT)

The Internet of Things as described earlier in the introduction, is a network of connected devices, specifically devices which connect with their surroundings. In most cases, these devices refer to the sensors and actuators and not the devices in which they are contained. For example, a watch which measures heart rate is not an IoT device, the heart rate sensor and the mechanism by which the sensor relays its gathered data via the internet is the IoT device. This technology gathers and responds to data submitted or received from the application layer [3] of the cloud technology.

Given the above description of the IoT, they are not to be likened to a traditional PC. Their limited or singular line of use restricts them from having un-needed resources. Therefore, they are resource-constrained devices. For example, a heart

rate sensor need only sense pulse, record it and pass the data along. There is no need for complex operating systems and software. These devices are classified based on data dependency: devices which depend on data collected by other devices to operate efficiently (for example, light bulb needs data from the motion sensor to determine when to turn on or off) and non-data dependent devices such as the motion sensor.

As the IoT devices need to communicate, the most accepted communication scheme for the IoT is the server-client model, where the cloud is the server and the device the client or in cases where the devices are grouped into clusters [4], the cluster head(CH) is the direct client. As efficient as this model has proved to be, there is an obvious bottleneck involved such as centralisation. This bottleneck has been identified to be central point of failure if a server is to be taken down, delay in operational services of the number of on-going requests from IoT devices is over-bearing on the remaining online servers. Another challenge with this communication structure includes the round-trip communication involved, i.e. devices geographically next to each other have to communicate via servers which might be located halfway around the world. Below we use an example of a smart home to illustrate the server-client communication model.

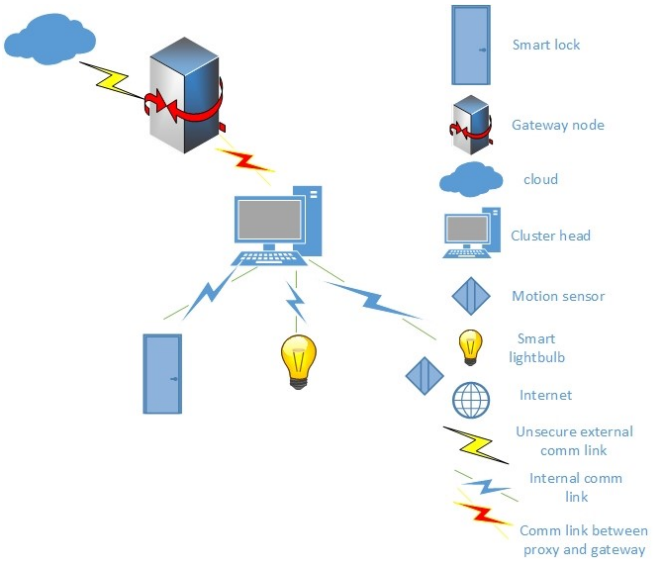

Fig. 1: IoT Smart Home Communication

B. Blockchain Technology

The Blockchain technology is a type of Distributed Ledger Technology (DLT). Distributed Ledger Technology (DLT) has in the past few years, relatively since 2009 (around the start-up of Bitcoin) [5] [6], attracted deserved attention from the research community, commercial organisations [7] and individuals. DLT, being a data structure [8], introduced a way of recording information on financial transactions without the need for an intermediary presence, while at the same time ensuring integrity. As the Blockchain is a distributed ledger technology, it goes to reason that it operates as some heterogeneous distributed database. It is heterogeneous [5] because it allows for all manner of system specification and operating system - from miner systems requiring high amounts of GPU (graphics processing unit) to resource constraint devices which can house a limited amount of Blockchain data and yet carry out operations. Being a distributed ledger, it operates via a distributed structure, running on a peer-to-peer network. This network design is unlike the server-client model of the IoT. It is void of centralisation as each peer communicates with its neighbouring peers and there is by default no central authority or data house. The strength and security of the Blockchain are dependent on the capacity of the nodes that make up the Blockchain as the nodes have to come to a consensus before data is put into blocks.

There are numerous consensus mechanisms in use and proposed for the Blockchain, some of which are Proof of Work (PoW) [9] used by Bitcoin, Ethereum and many others. Proof of Stake (PoS) [10], Proof of Authority (PoA), Proof of Exercise [11], Byzantine Fault Tolerance [12] by HyperLedger Fabric, Proof of Elapsed Time [13] Intel SawtoothLake [14]. How a Blockchain achieves consensus is critical to how the Blockchain would operate and the integrity of the data on the Blockchain as well as the authentication of the blocks. There are mainly two types of Blockchain; the public and private Blockchain.

The popular cryptocurrency, Bitcoin is an example of a public Blockchain. A public Blockchain is a Blockchain that is open to the public; there are no restrictions as to who can join the Blockchain. If a person is joining the Blockchain for malicious intents, he/she would still be allowed access to the Blockchain and to become a full node if he meets the system requirements. A full node is a node which has an internal up-to-date copy of the Blockchain and is also able to verify operations on the Blockchain. Whereas the private Blockchain has certain restrictions, like an access-list, admitting new nodes only by invitation [15], ensuring only permitted nodes can be on the Blockchain. This type of Blockchain exchanges anonymity for security, i.e. to ensure there are no unknown participants or nodes with unclear intentions, the identity of all nodes is widely known. Both the public and the private are identical in every way except in respect to admittance, considering that both Blockchains run on the same factors such as consensus algorithms and hashing protocols. There is another type of Blockchain which is an off-shoot from the private Blockchain, it is known as the consortium Blockchain. The consortium Blockchain is as such a private Blockchain with the exception that it relegates block creation control and other managerial control to a singular node or a select few. An example of this would be Parity [8].

The Blockchain has become a distributed ledger that performs far more than record-keeping, with the Bitcoin Blockchain we see transactions taking place on the Blockchain and details of these transactions recorded on the Blockchain. With Ethereum being a Turing complete Blockchain, smart contracts can be run on the Blockchain to involve participating

nodes. Contracts which follow strict rules and do not need human intervention to operate efficiently. We have also witnessed the success of the Decentralised Autonomous Organisation [16](DAO) launched on the Ethereum Blockchain.

III. Blockchain for the Internet of Things

The worldwide success of cryptocurrencies such as Bitcoin and Ether have proved beyond a doubt the usefulness of Blockchains. There is now growing research in non-financial fields such as e-health [17], smart cities [18], data management and analytics [19], smart green-house farming [20], industrial sector [8], smart supply chain [21] etc. However, the application of Blockchain to the IoT holds quite promising and rather soon implementations. The transition from a centralised model to a distributed model might not be easy, but it seems like the best given the IoT devices growing nature.

Although what has been marketed as a key point for the Blockchain has turned out to be incompatible for the IoT. The memory space needed by each node to contain a full copy of the operations on the Blockchain, can as operations increase be quite much. Over the past few years, the Bitcoin Blockchain has seen a considerable increase in memory space requirements: 26gb in December 2014, 51gb, the following year, 93gb in December 2016 and 145gb December 2017. This doesnt prove too much of a problem for traditional PCs as the cost of memory space is reducing but for the memory-constrained IoT devices, which once deployed are expected to have a life-span of at least ten years before servicing, this large requirement would not hold. Our solution to this problem comes down to access. Which device has access to what and which devices can carry-out certain operation?

Firstly, we propose that for the IoT, a private Blockchain, more specifically, a consortium Blockchain be used instead of a public Blockchain. As explained earlier, a private differs from public purely on the basis of an access-list. The security of IoT devices are not as resilient as that of the traditional PC, therefore, an additional layer of screening (regarding the Blockchain) would be a welcomed layer of security. Also, IoT devices that interact with consumers and gather information have serious privacy implications. Scenarios such as a smart door lock that records what times of the day the door is open and closed or a data collected by a pacemaker and sent to a hospital. Such information should not be available to the public, regardless of the fact that they are all cryptographically hidden with the signees private key [5]. A consortium Blockchain being a private Blockchain would be suitable for the IoT, given it is built around an access-list and all participants are known.

Secondly, given our definition of a full node, we go further on to say that in our design of a Blockchain and IoT scenario, not all IoT devices would be full nodes. Being a consortium Blockchain, certain IoT devices which have been identified to have a little more resource than others in the cluster would be made signers on the Blockchain. This would be our proposed method of consensus; an implementation of the Proof of Authority (PoA). PoA is consensus mechanism which assigns some nodes to be authorities, having the joint ability to create new blocks and secure the Blockchain. A majority decision among the authorising nodes is critical in authorising blocks and permanently adding them to the Blockchain. As the chain needs to be approved by a majority of the authorities, such a Blockchain would be void of forks (split decision in which chain is the main chain. PoA also proves better against PoW which requires arbitrary mathematical problems and is computationally intensive, and PoS which involves the use of tokens. A key value of the Blockchain rests on its ability to ensure the integrity of its data. If an attacker were to somehow get on the Blockchain network, he/she cannot add or remove blocks without a majority decision.

Besides introducing a distributed platform, the Blockchain is also capable of carrying out smart contracts or self-executing scripts. A smart contract is a self-automated logic operation. When a smart contract is initialised, the set rules stated during its build cannot be changed. For example, if A was to send funds to B after B submitted a legal document on a particular date. The smart contract would hold the funds from A ensuring A doesnt spend them upon receiving the document and also B would receive the fund upon rendering the document. The smart contract needs no human intervention as it is its own regulatory body. Using smart contracts and Ethereums programming language, Solidity, developers are building distributed apps (Dapps) on the Ethereum virtual machine (EVM). There are currently 977 recorded dapps created and operational on EVM [22]. Such a contract would be powerful for exchanges and transactions between IoT devices. Slock.it [23] is based on Ethereums smart contracts. They offer smart locks which respond to data received from a smart contract. The merits of smart contracts go far beyond financial purposes, entering into the space of alerting the police if certain conditions are not met upon entering the house or supplying data from non-dependent devices to data-dependent devices. The IoT devices which are scarce of onboard computational resources outsource heavy computations to the data centres through cloud computing infrastructure [24].The EVM is able to handle complex code which the IoT resource constrained nature limits it from processing but in all regard, it would simply be replacing one cloud technology for another.

IV. sidechain proposal

The collaboration between the IoT and the Blockchain as stipulated above is real and is happening [21]. The goal of this paper as state in the introduction is to show how sidechains can be deployed in IoT for inter-chain communications. A sidechain, regardless of the word side, is a full-Blockchain but one tailored specifically to validate and facilitate the transfer of local validated assets to and from the main chain. The bitcoin sidechain communication is achieved through two-way pegging. In two-way pegging, the token of value is sent to a set output on the main chain that can only be unlocked using an SPV proof (Simplified Payment Verfication) of possession on the sidechain. This process involves the use of a confirmation period and a contest period as means to ensure integrity and

security. As the name implies, this process can take place in two ways, the token can be made available on the sidechain from the main chain and vice-versa.

To achieve our goal, we have chosen to adopt a variant of two-way pegging [25]. A typical contest and confirmation period would last a day or two individually, rounding up to about four days. This time delay is excessively too long for the IoT system, which is based around almost real-time actions based on almost real-time data. Therefore, we have chosen in our model to remove both the confirmation and contest period. This raises the question of how to deal with the security and integrity assured by both time periods. As the IoT would most-definitely be transferring data and not cryptocurrencies, the need for both time periods is gone, as they are to ensure that sufficient PoW has been carried out on the Blockchain.

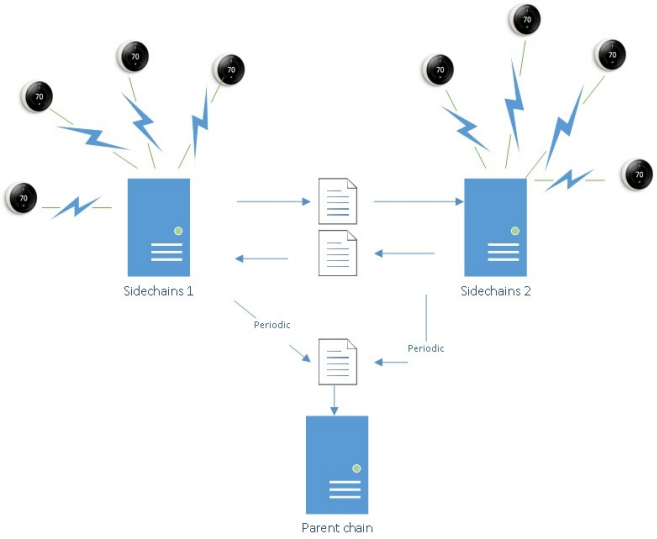

Fig. 2: Design on inter-blockchain communication using sidechains

A typical scenario for our design would be thus: Suppose there are fixed smart temperature sensors on each floor of a building and these sensors on each floor are configured to a different side chain, which is a full Blockchain in its own right. These devices, being configured to be nodes on the Blockchain, would be able to submit the data gathered on to the Blockchain. A smart contract could be initiated anytime these sensors submit data. this contract would find the mode of all the temperature readings rendered and by this deliver one number as the final temperature reading. Then the nodes chosen to the authorisers would sign off and place the reading in a new block. This operation is local and works almost like a regular LAN (Local Area Network), but in the world of IoT, data gathered by one device might be useful to another device or just for a service check-up. There has to be a means for such data to move from one Blockchain to another, efficiently and securely. To achieve communication or synchronisation across multiple floors, we have to introduce a router of some sort into the network.

The SPV proof is very essential to the communication between sidechain and mainchain of the Bitcoin Blockchain. SPV is be a list of block headers and cryptographic proof that the asset was the result of an output which can be located in one of blocks associated with the aforementioned block headers presented. But since we are using PoA and not PoW, we do not have to be burdened with an SPV, a smart contract between chains would be sufficient. This external smart contract would act as a link between chains. Authorities on chains can initiate a smart contract to request or to send data blocks to a device on another chain. The smart contract would require inputs from at least two of the registered signatory nodes before the process can be started. Note, each node on the side chain needs only its own public key to publish onto the Blockchain, but for inter-Blockchain or inter-sidechain communication, a minimum of two authorised nodes has been specified. Preferably, the authorised nodes would be more resource available nodes compared to the rest of the devices present.

V. CONCLUSION

IoT devices are designed to be small but efficient devices. Unlike the traditional PC, which can perform a number of tasks concurrently, they are designed to perform one core service. A smart light bulb is designed to solely turn on and turn off the light as well as transmit data of its actions to a designated address. Said light bulb is not designed to play a movie, run complex code or even house other applications. This is simply a case of designing a system to achieve a specific task. For efficiency, this design has constrained the system to certain limits, such as storage capacity, processor capabilities, connection type such as BLE (Bluetooth low energy, 6LoWPan [4]). The Blockchain being a growing record requires a substantial amount of space and this storage hosting has been a key challenge in this field of research.

As IoT devices are increasingly deployed there will be increasing numbers of applications which use them and which require communication between devices. Applications and inter-device communications, however, will face the challenge of only limited processing and memory capacity at the device level, and sidechains may provide a solution to this challenge. Sidechains allow between-device communication to be mediated by the sidechain, and processing to occur through smart contracts sitting on the chain (or sitting on another blockchain).

The IoT offers the possibility of making real-time data and processing available. The combination of blockchains with the IoT goes beyond mere financial recording and authorisation. We believe the use of sidechains will enable greater communication between devices and greater sophistication of processing of the data collected.

ACKNOWLEDGEMENT

This study is a part of an extensive research into the blockchain and its possible use-cases for the IoT at King's College London, UK.

REFERENCES

[1] Y. N. Aung and T. Tantidham, "Review of Ethereum: Smart home case study," in *2017 2nd International Conference on Information Technology (INCIT)*. IEEE, nov 2017, pp. 1–4. [Online]. Available: http://ieeexplore.ieee.org/document/8257877/

[2] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7467408/

[3] J. Rui and S. Danpeng, "Architecture Design of the Internet of Things Based on Cloud Computing," in *2015 Seventh International Conference on Measuring Technology and Mechatronics Automation*. IEEE, jun 2015, pp. 206–209. [Online]. Available: http://ieeexplore.ieee.org/document/7263548/

[4] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017.

[5] A. Kuzmin, "Blockchain-based structures for a secure and operate IoT," in *2017 Internet of Things Business Models, Users, and Networks*. IEEE, nov 2017, pp. 1–7. [Online]. Available: http://ieeexplore.ieee.org/document/8260937/

[6] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *International Conference on Advanced Communication Technology, ICACT*, 2017.

[7] P. L. Seijas, S. Thompson, and D. Mcadams, "Scripting smart contracts for distributed ledger technology," 2017. [Online]. Available: https://eprint.iacr.org/2016/1156.pdf

[8] D. T. T. Anh, M. Zhang, B. C. Ooi, and G. Chen, "Untangling Blockchain: A Data Processing View of Blockchain Systems," *IEEE Transactions on Knowledge and Data Engineering*, pp. 1–1, 2018. [Online]. Available: http://ieeexplore.ieee.org/document/8246573/

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[10] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol," 2017. [Online]. Available: https://eprint.iacr.org/2016/889.pdf

[11] A. Shoker, "Sustainable blockchain through proof of exercise," in *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)*. IEEE, oct 2017, pp. 1–9. [Online]. Available: http://ieeexplore.ieee.org/document/8171383/

[12] J. Sousa, A. Bessani, and M. Vukolić, "A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform," sep 2017. [Online]. Available: http://arxiv.org/abs/1709.06921

[13] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (poet)," in *International Symposium on Stabilization, Safety, and Security of Distributed Systems*. Springer, 2017, pp. 282–297.

[14] A. Baliga, "Understanding Blockchain Consensus Models," 2017. [Online]. Available: https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf

[15] "The difference between public and private blockchain - Blockchain Unleashed: IBM Blockchain Blog." [Online]. Available: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

[16] C. Jentzsch, "Decentralized Autonomous Organization to Automate Governance," *SlockIt*, pp. 1–30, 2016. [Online]. Available: slock.it/dao.html

[17] M. MediChain, "MediChain ICO Whitepaper 1.03 - Google Docs," 2017. [Online]. Available: https://docs.google.com/document/d/1M4j-ertE4Couj0tdVzNQeE_y3YgXZbJXAafiPO_v5C8/edit

[18] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," in *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, dec 2016, pp. 1392–1393. [Online]. Available: http://ieeexplore.ieee.org/document/7828539/

[19] H. T. Vo, L. Mehedy, M. Mohania, and E. Abebe, "Blockchain-based Data Management and Analytics for Micro-insurance Applications," in *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management - CIKM '17*. New York, New York, USA: ACM Press, 2017, pp. 2539–2542. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3132847.3133172

[20] A. S. Patil, B. A. Tama, Y. Park, and K.-H. Rhee, "A Framework for Blockchain Based Secure Smart Green House Farming." Springer, Singapore, dec 2018, pp. 1162–1167. [Online]. Available: http://link.springer.com/10.1007/978-981-10-7605-3_185

[21] IBM, "THE SMARTER SUPPLY CHAIN OF THE FUTURE." [Online]. Available: https://www-935.ibm.com/services/uk/gbs/pdf/gbe03167-usen-02.pdf

[22] "State of the Apps 977 Projects Built on Ethereum." [Online]. Available: https://www.stateofthedapps.com/

[23] "Slock.it - Blockchain + IoT." [Online]. Available: https://slock.it/index.html

[24] J. Chen, C. Touati, and Q. Zhu, "Heterogeneous Multi-Layer Adversarial Network Design for the IoT-Enabled Infrastructures," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*. IEEE, dec 2017, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/8254620/

[25] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, "Enabling Blockchain Innovations with Pegged Sidechains," 2014.