Holochain and Privacy

Oliver Burmeister[1] Paul d'Aoust[2] Anwaar Ulhaq[3] Kirsten Wahlstrom[4]

[1]School of Computing and Mathematics

Bathurst Campus

Charles Sturt University

[2]Holo.Host

British Columbia

Canada

[3]School of Computing and Mathematics

Port Macquarie Campus

Charles Sturt University

[4]UniSA: STEM

Mawson Lakes Campus

University of South Australia

Abstract

Holochain is an open-source framework for building scalable, distributed, peer-to-peer applications (called hApps). By doing so, it addresses some inherent limitations of a traditional blockchain by proposing an efficient and resilient solution. However, how holochain introduces the implementation of privacy into its design remains an open question. This paper extends prior work on Holochain and privacy by design. As privacy has a broad spectrum, we consider only a special case of the right to be forgotten, a form of privacy which is a human right established by the European Court of Justice. In an exemplary

implementation of the right to be forgotten, people would be able to erase the data on holochain related to them as required. In this paper, we explore and discuss how holochain can embed the right to be forgotten while implementing hApps. We discuss six important considerations for a programmer to ensure privacy by design in hApp's implementation. It will extend the capabilities of a holochain system by embedding the notion of privacy into its design.

Keywords Blockchain, Holochain, privacy, informed consent.

1 Introduction

Questions regarding privacy have proven fertile for centuries: Aristotle differentiated the *Oikos* from the *Polis* (Molitorisz, 2020) and more recently Wahlstrom, Ulhaq, and Burmeister (2020) considered a type of privacy known as 'the right to be forgotten' (European Union, 2016) within the context of blockchains.

Wahlstrom et al. (2020) were motivated by the observation that blockchains are immutable by design and therefore, inconsistent with the right to be forgotten. However, the work on privacy with respect to blockchain contexts is ongoing. For example, Zyskind and Nathan (2015) demonstrate that it is possible to use a blockchain as an automated access-control manager, which implements Tavani and Moor's (2001) restricted access account of data privacy. However, there are other accounts of privacy which may be discussed with respect to the blockchain. For example, Nissenbaum (2009) argued that privacy is contextually dependent; Floridi's Information Ethics (2008) conceptualises data privacy as a function of friction in the infosphere and suggests that data is constitutive of selfhood, noting the difference between *my data* (which describes *me* directly) and *my car* (which describes much less about *me* indirectly); elsewhere, privacy is described as personal property (Schwartz, 2004) that may be transacted. These accounts of privacy are not mutually exclusive. For example, it is clear that Floridi is placing data privacy within a specific context when he

describes it a feature of the infosphere and in any given social context, it may be the norm to restrict or control access to data.

In Wahlstrom et al. (2020) the following understanding of privacy was central to our considerations, “People exercise privacy through personal information preferences and practices which are specific to social contexts and changing over time” (p2). This understanding acknowledges that privacy is an intrinsic and pliant feature of any social context and that it therefore plays a role in the shaping of social contexts (Burmeister, 2016; Burmeister & Kreps, 2018; Wahlstrom, Fairweather, & Ashman, 2017). As blockchain applications extend beyond the fiduciary to other social contexts, it is timely to provide further consideration of the right to be forgotten and privacy more broadly. Therefore, this paper extends the consideration of the right to be forgotten in Wahlstrom et al. (2020) through the description of some of the technical features of the Holochain platform.

2 Holochain

There have been various suggestions for supporting privacy (for example, those listed in Wahlstrom, Roddick, Sarre, Estivill-Castro, & deVries, 2006) including, as noted above, attempts to leverage blockchain platforms to implement the restricted access account of privacy (Zyskind & Nathan, 2015). Similarly to the approach described by Zyskind and Nathan (2015), Holochain provides, “Individual authority over data sharing, access, and storage” (Holochain, 2020).

Holochain is a platform for which apps (called hApps) are developed (Holochain, 2020). hApps provide for distributed and transparent ledgers of transactions which are not always fiduciary. Examples include energy trading, farm produce trading, village resource-sharing, agile project management, publishing, heterogeneous IoT, social media, and event and disaster management (these and other examples are listed at https://forum.holochain.org/c/projects/new-projects/109). The Holochain platform supports

distributed, server-less apps running on devices with localised data storage and management. For this reason, Holochain is disruptive of client/server and cloud platforms.

A hApp "… consists of a network of agents maintaining a unique source chain of their transactions, paired with a shared space implemented as a validating, monotonic, sharded, distributed hash table (DHT) where every node enforces validation rules on that data in the DHT as well as providing provenance of data from the source chains where it originated" (Harris-Brown, Luck, & Brock, 2018, p4). In less compact terms, nodes in a hApp create their own (small) blockchains for holding verified data which are journaled in a DHT (Frahat, Monowar, & Buhari, 2019). The DHT is sharded and distributed back to the nodes in the hApp (Holotescu & Vasiu, 2020), which validate the shards against their source blockchains (Harris-Brown et al., 2018).

An inherent limitation of a traditional blockchain is its computation and communication cost, which makes a blockchain less efficient (ie slower) as it gets bigger. Whereas a hApp is more scalable than a traditional blockchain because validating shards of the DHT at nodes is a more efficient process than validating an entire blockchain. As a traditional blockchain gets bigger, it gets *less* efficient and more resilient; but as a hApp gets bigger, it gets *more* efficient and more resilient.

3 Holochain privacy

In an ideal implementation of the right to be forgotten, people would be able to erase the data describing them as needs arise. With respect to Holochain, there is a trade-off: data that people want to hold privately on their own chain still needs to be verified from the DHT on the network, and as yet this trade-off is not resolved. Nonetheless, constructing an understanding of how Holochain contributes to the privacy landscape is an interesting challenge, calling for some reflection.

In a hApp's network space, there is a piece of code that implements the 'rules of the game' that all participants in that space consent to. Therefore, the availability of the right to be forgotten and privacy more broadly ultimately comes down to a programmer's understanding of privacy and the implementation choices they make. From a technical perspective, a contextual view of privacy is constructive because contexts are easy to create, configure, and build secure membranes around. However, the extent to which contexts in the software are as flexible and reconfigurable as social contexts remain unknown. That said, when designing and implementing an hApp, there are six things a programmer can consider.

First, when defining the data schema, a given data type can be *private*, *public*, or *public but encrypted*. Private data stays on the participant's own device, while public data gets published to the DHT. This access model is granular in that all participants in the space have access to all public data and importantly, journal headers are always available, so even with private data, there's a public record that data was written, even if the data itself isn't visible.

Second, given that all public data is visible to all participants in a hApp's network space, participants' access to that space can be specified in code. Some hApps may be totally open, while others may require an invite code, proof of subscription, signed vouches from existing members, etc.

Third, there are two sorts of sharding in Holochain. One is that each individual has their own journal. The other is that, for each individual entry and header in a participant's journal, only a small portion of their peers are able to validate and store it. The maintenance of data integrity in the case of non-consensus is beyond the scope of this paper.

Fourth, access to private entries on one's journal can be granted through a version of capability tokens in which a taken may be non-transferable. That is, it can only be used by the instantiation the grantor gives the token to.

Fifth, only public data gets validated or rejected by the network, and what constitutes valid data is really up to the developer and the context of their user base. For example, in one hApp, financial transactions might require public audibility, in which case removal of a piece of data might indeed render a journal un-verifiable for future entries; another context might elect trusted notaries to witness all transactions, in which case all entries could be private and only the notary's signature would be public; a third context could employ zero-knowledge proofs and hide the data in plain sight; and contexts in which one data item is unlikely to have a hard dependency on another, data may be safely erased at will.

Sixth, the issue of how to scrub data has been addressed in Holochain's designs but not yet implemented. Holochain intends to introduce two new DHT operations: *withdraw* (which will enable users to redact data formerly published) and *purge* (which will allow other user's data to be marked for deletion, e.g., illegal or dangerous material). However, because Holochain is inherently a Peer-to-Peer (P2P) implementation of blockchain, a purge is a request to delete the offending data rather than a deletion of it, so nodes owned by malicious actors may not comply. In this way, Holochain aims to support the right to be forgotten.

4 P2P privacy

GDPR frames the right to be forgotten as a matter of fiduciary relationships, whereas P2P platforms are about peers of roughly equal (or at least undetermined) power consenting to engage with each other. So it appears that the right to be forgotten may not be relevant with respect to P2P platforms.

P2P platforms can be compared to real-world relationships except that in a P2P context, computational power is applied to the spread of data, a phenomenon described by Moor (1997). However, in P2P contexts, participants are knowingly and mutually consenting. Consent is a theme that surfaces in the privacy literature (Whitley, 2009) yet the extent to which consent is fully informed cannot readily be ascertained because 'fully informed' means

something different for each person. For example, can a 12-year-old schoolchild be informed to the extent that a 45-year-old seasoned programmer can be informed? Thus, there is scope for providing diverse re-presentations of requests for informed consent.

5 Conclusion

This paper extended prior work on Holochain and privacy. Technical details and consideration of informed consent have been contributed. Some indications for future consideration and possible development have been identified.

6 References

Burmeister, O. K. (2016). The development of assistive dementia technology that accounts for the values of those affected by its use. *Ethics and Information Technology, 18*(3), 185-198.

Burmeister, O. K., & Kreps, D. (2018). Power influences upon technology design for age-related cognitive decline using the VSD framework. *Ethics and Information Technology*, 1-4.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016).

Floridi, L. (2008). Information ethics: a reappraisal. *Ethics and Information Technology, 10*(2-3), 189-204. doi:10.1007/s10676-008-9176-4

Frahat, R. T., Monowar, M. M., & Buhari, S. M. (2019). *Secure and Scalable Trust Management Model for IoT P2P Network.* Paper presented at the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS).

Harris-Brown, E., Luck, N., & Brock, A. (2018). Holochain: scalable agent-centric distributed computing. *GitHub. URL: https://github.com/holochain/holochain-proto/blob/whitepaper/holochain.pdf*.

Holotescu, V., & Vasiu, R. (2020). Challenges and Emerging Solutions for Public Blockchains. *BRAIN. Broad Research in Artificial Intelligence and Neuroscience, 11*(1), 58-83.

Molitorisz, S. (2020). *Net Privacy: How we can be free in an age of surveillance*: NewSouth.

Moor, J. (1997). Towards a theory of privacy in the information age. *SIGCAS Comput. Soc., 27*(3), 27-32. doi:doi.org/10.1145/270858.270866

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, US: Stanford Law Books.

Schwartz, P. (2004). Property, Privacy, and Personal Data. *Harvard Law Review, 117*(7), 2056-2128.

Tavani, H., & Moor, J. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *SIGCAS Comput. Soc., 31*(1), 6-11. doi:doi.org/10.1145/572277.572278

Wahlstrom, K., Fairweather, N. B., & Ashman, H. (2017). *Brain-Computer Interfaces and Privacy: Method and interim findings.* Paper presented at the ETHICOMP 2017, Turin, Italy.

Wahlstrom, K., Roddick, J. F., Sarre, R., Estivill-Castro, V., & deVries, D. (2006). *On the ethical and legal implications of data mining*. Retrieved from

Wahlstrom, K., Ulhaq, A., & Burmeister, O. (2020). Privacy by design. *Australasian Journal of Information Systems, 24*.

Whitley, E. (2009). Informational privacy, consent and the “control” of personal data. *Information Security Technical Report, 14*(3), 154-159. doi:http://dx.doi.org/10.1016/j.istr.2009.10.001

Zyskind, G., & Nathan, O. (2015). *Decentralising privacy: Using blockchain to protect personal data.* Paper presented at the 2015 IEEE Security and Privacy Workshops.