COMP842 Research Proposal - Beauty and the Blockchain

I. Background

The beauty industry is enormous, with a retail value (RSP) of USD$535.6 billion in 2022 (Passport, n.d.). Market trends in the Asia-Pacific region are driving consumers towards demanding seamless experiences that are digitally enhanced with the latest technology. The COVID-19 pandemic also heightened health/safety concerns and paved the way for the blend of social media and purchasing channels (Passport, 2021).

II. Problem Definition & Scope

The digitalisation of the beauty world can mean that consumers are more worried and particular about their beauty choices and that there is less transparency and more obfuscation with social media marketing and digital hoaxes (Cole, 2022). Many beauty professionals do not need formal certification and even if so, false certification is a common issue, causing serious repercussions (Rahman et al., 2023). Moreover, a global or national database is often missing or insufficient to verify the service providers consumers hire (More et al., 2021).

Prior to more technical discussion, a definition of certification is provided, being " an official document attesting a certain fact... [and] are seen as certificates that prove attainment of certain levels of academic met of the bearer, which can confer advantages to individuals that hold such a certificate" (Saramago et al., 2021, p. 1). ri

Emerging and established technology in the realm of blockchain can solve legitimacy issues. Even with digital certification providers, there is too much vulnerability to deceptive activities so providers are relying on centralised data authorities that lack the transparency something like a distributed ledger would provide (Saramago et al., 2021). However, blockchain gives consumers an immutable and protected public-facing display of certificates (Saramago et al., 2021), where various parties (in this case, educational beauty organisations) must concede that the submitted document (a qualification) is legitimate and then it would be published to the distributed ledger (More et al., 2021).

III. Research Design & Methodology

The research focuses on Ethereum, specifically Ethereum 2.0 which uses the Proof-of-Stake (PoS) system to comply with the latest developments and ensure security and scalability (Ghorbanzadeh, 2023). Moreover, Ethereum has the most known manifestation of smart contracts (Angelis, 2018). To achieve this idea, research into self-sovereign identities (SSIs), Decentralised Identifiers (DIDs), verifiable credentials (VCs), smart contracts, permissioned blockchains, and the InterPlanet File System (IPFS) is needed. The creation of initial designs would come from this research and inform the development of a minimum viable product (MVP).

A. Key Concepts

DIDs, SSIs and VCs: These elements link together to define the different stakeholders within the proposed framework. These parties are 1) the professional seeking verification, 2) the educational provider of the professional, 3) the governing body of trust certifiers and 4) the consumer. Parties 1-3 will need established DIDs that attribute statements to them (More et al., 2021). Such statements would be known as VCs, which would only be issued to a stakeholder's DID if verified by the issuing body of trust certifiers (Barclay et al., 2020). From there, the governing body issues a unique key to the DID, the record of which is stored on a distributed ledger. In relation to Ethereum's PoS model, if the issuer or governing body is found to be fraudulent, their invested stake within the system can be revoked and the information rendered invalid (Ghorbanzadeh, 2023).

Permissioned Blockchains: This is where the participants in the consensus protocols are known and while read functions are public, writing and committing are limited to predefined entities (Angelis, 2018). In this context, it would be interesting to understand how a proposal like this behaves on a permissioned blockchain. As the goal is to ensure utmost verification and security, it's pertinent to think of ways that only verified issuers can assign VCs to DIDs.

Smart Contracts: The process where the credential transforms from an application to a VC happens through a Solidity smart contract deployed on a distributed ledger on the permissioned blockchain (More et al., 2021). The smart contract acts as the code stored to determine the outcome of the verification and can only run through if all the TCs concede the application meets the criteria to continue.

IPFS: The IPFS is a decentralised storage architecture that provides decentralised cloud storage through peer-to-peer networking and content addressing (Doan et al., 2022). Files added to the IPFS are split into chunks, hashed and given unique content identifiers that validate the permanency of the record (IPFS, n.d.). In this context, IPFS would store the VCs TCs assigned to successful applications. This helps to give

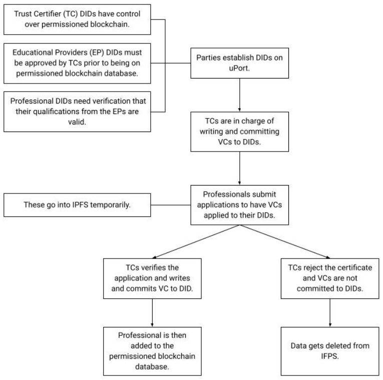
Trust Certifier (TC) DIDs have control over permissioned blockchain.
Educational Providers (EP) DIDs must be approved by TCs prior to being on permissioned blockchain database.
Professional DIDs need verification that their qualifications from the EPs are valid.
Parties establish DIDs on uPort.
TCs are in charge of writing and committing VCs to DIDs.
These go into IPFS temporarily.
Professionals submit applications to have VCs applied to their DIDs.
TCs verifies the application and writes and commits VC to DID.
TCs reject the certificate and VCs are not committed to DIDs.
Professional is then added to the permissioned blockchain database.
Data gets deleted from IFPS.

Fig. 1. The proposed model.

the information that consumers view legitimacy as the IPFS is secure, tamper-resistant, and transparent (Rahman et al., 2023).

B. Proposed Process

Below is the initial proposal of how the elements work together. Further research is expected to refine and redesign this.

IV. Aims & Conclusion

The research aims to not only validate the hypothesis that this would connect together but also to understand the application of the program in the beauty industry. Some beauty brands have explored blockchain already. An example is that NARS cosmetics released non-fungible token (NFT) artwork to celebrate their most famous shade (Hirschmiller, 2023). However, there is a distinct lack of literature connecting verification, beauty and blockchain together. This gives rise to an opportunity to explore something relatively new.

While researching a novel concept like this is exciting, a lack of literature may remove important contextual clues in building this report and product. However, this is to be expected and will be discussed, alongside any pivots and changes, in the final presentation and accompanying documents.

References

Angelis, S. D. (2018, May 9). *Assessing Security and Performances of Consensus algorithms for Permissioned Blockchains*. arXiv.Org. https://arxiv.org/abs/1805.03490

Barclay, I., Radha, S., Preece, A., Taylor, I., & Nabrzyski, J. (2020, April 6). *Certifying provenance of scientific datasets with self-sovereign identity and verifiable credentials*. arXiv.Org. https://arxiv.org/abs/2004.02796

Cole, L. (2022, July 21). Why is there so much fake news on beauty TikTok? *Dazed Digital*. https://www.dazeddigital.com/beauty/article/56553/1/why-is-there-so-much-fake-news-on-beauty-tiktok-influencers-dangerous

Doan, T. V., Psaras, Y., Ott, J., & Bajpai, V. (2022, February 13). *Towards decentralised cloud storage with IPFS: Opportunities, challenges, and future directions*. arXiv.Org. https://arxiv.org/abs/2202.06315

Ghorbanzadeh, M. (2023, July 9). *Proof-of-stake (pos)*. Ethereum. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

Hirschmiller, S. (2023, July 31). How NARS' hybrid NFT/AR orgasm activated campaign is bringing web3 to A wider audience. *Forbes*. https://www.forbes.com/sites/stephaniehirschmiller/2023/07/31/how-nars-hybrid-nft–ar-orgasm-activated-campaign-is-bringing-web3-to-a-wider-audience/?sh=490767070f41

IPFS. (n.d.). *IPFS powers the distributed web*. IPFS. Retrieved August 4, 2023, from https://ipfs.tech/#how

More, S., Grassberger, P., Hörandner, F., Abraham, A., & Klausner, L. D. (2021). Trust Me If You Can: Trusted Transformation Between (JSON) Schemas to Support Global Authentication of Education Credentials. *International Conference on ICT Systems Security and Privacy Protection*, *625*, 19–35. https://doi.org/10.48550/arXiv.2106.12793

Passport. (n.d.). *Beauty and Personal Care: Euromonitor from trade sources/national statistics*. Euromonitor ; Euromonitor. Retrieved August 2, 2023, from https://www-portal-euromonitor-com.ezproxy.aut.ac.nz/statisticsevolution/index

Passport. (2021, August 23). *Current and Future Drivers of Asia Pacific Consumer Markets*. Euromonitor ; Euromonitor International. https://www-portal-euromonitor-com.ezproxy.aut.ac.nz/analysis/tab#

Rahman, T., Mouno, S. I., Raatul, A. M., Azad, A. K. A., & Mansoor, N. (2023, July 11). *Verifi-Chain: A Credentials Verifier using Blockchain and IPFS*. arXiv.Org. https://arxiv.org/abs/2307.05797

Saramago, R. Q., Jehl, L., Meling, H., & Estrada-Galiñanes, V. (2021, September 23). *A tree-based construction for verifiable diplomas with issuer transparency*. arXiv.Org. https://arxiv.org/abs/2109.11590