

Copyrights © 2015 Tarique A Bhuiyan

W3C Blockchain and the Web

Position Statement



Prepared by
Tarique A Bhuiyan
Founder, Chairman & CTO
Hashcloud pty ltd
June 9, 2016

Internet of Services

What do I mean by “Internet of Services”?

My view is that the digital disruption of Services will happen when we have internet of services, which is essentially internet of things for services, be it financial services or government services, or any other services. A service is typically manufactured by processing a number of ‘service documents’ and / or ‘service attributes’ or simply ‘service data’. For example: to register a banking client for, say, internet banking, a bank will need the service applicant to provide some authentication / verification data about the applicant, proof that the client is already banking with that bank, potentially filling out a form, etc. The bank then verifies the document /data by some mechanisms and then processes the registration.

Another example: to process a tourist visa application, an embassy will require the service applicant to provide some authentication / verification data about the applicant, some identity documents of the applicant, invitation letter, filling out of a form (which are essentially service data for application for a visa service), fees, etc. The embassy then verifies the document /data by some mechanisms and then processes the application.

The issue is: when the same applicant is going to apply for another bank internet banking registration or for another tourist visa application, s/he will be required to provide the same document(s) and data again which the bank / embassy would then require to validate again. Then again and again and so on! The point is that Mr X is Mr X, no matter which service he is applying for and ‘Data Y’ related to Mr X is ‘Data Y’, no matter where it is required!

The question we need to ask ourselves is that if it is possible to create service document and data standards and then an individual would then create his own data and document repository on the web which is then verified by some authority (preferably by the issuing authority that issued the document and the data or by a 3rd party trusted organizations like banks, government agencies, etc.) after which the document and data are then cryptographically hashed and recorded on a blockchain. Finally the blockchain receipt is issued for all such hashes recorded on a blockchain.

This way, whenever the individual needs to apply for a service, all s/he will need to do is to just share only those document(s) or data along with their respective blockchain receipts that are required by the service provider, e.g. a bank, an insurance company, an embassy, a membership organization, a hospital, a real estate agency, etc. These services provider could then use these data / documents and their respective blockchain receipts to prove the integrity, irrefutability, authenticity / verifiability and existence of these data.

However, the problem is that there is no such standard of service documents and especially for Service Data, let alone for the data that are required for the verification of IDs of the service applicants. Such a standard for ID data will help verifying a person’s authenticity by any company via any blockchain as the slightest difference in data of a particular service would result in a totally different cryptographic hash which won’t be found on the blockchain and would fail in the verification and authentication process explained earlier.

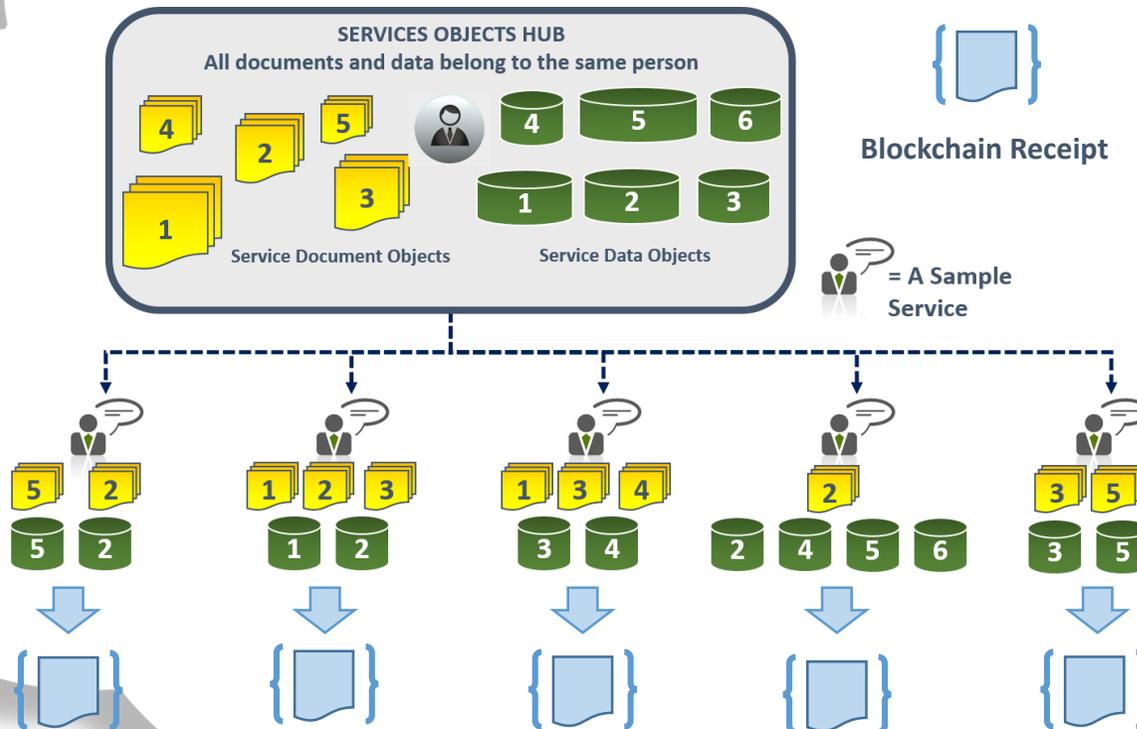
Internet of Services

continued...

So, what am I trying to achieve through W3C?

There is a need to have standardized data & document objects along with their hashing mechanisms (e.g. SHA256 or SHA512, etc.) and then put the cryptographic hashes of these objects on a blockchain to enable internet of services allowing any service seeker and service provider to seamlessly provide services being sought by the service seeker, thus giving the best web based digital services experiences to the services seekers.

However, **more importantly**, there is also a need to standardize the 'Blockchain Receipt' across a plethora of blockchains or distributed ledgers that will eventually come into existence. Having a standard receipt means it will become easier for any company or individual to prove the irrefutability that one or more services data and / or document(s) was recorded on a particular blockchain.



So, what is my proposal to W3C?

Like the web saw the proliferations of many browsers, on the distributed ledger space, there will be many blockchains and this is bound to happen. That's alright!

However, like we have the HTML standards for the web, we need to have a standard for the Blockchain Receipts. If there is a standard for blockchain receipts, no matter which blockchain is used, it will enable various organizations or even individuals to validate services data or documents (for which the Blockchain receipts will be issued) during a service delivery process via the web. This will be the precursor to creating an 'internet of services' ecosystem on the web.

My proposal to W3C is to create standards for blockchain receipts based on REST API based JSON (JavaScript Object Notations) standards.

An example of a Blockchain receipts is provided in the next page.

Blockchain Receipt: Example

This is a sample Receipt (on the right) issued by Tierion as explained in a whitepaper titled 'Chainpoint' (source: <https://tierion.com/features> and <https://github.com/chainpoint/chainpointc>)

This is an example of a receipt issued by Tierion (www.tierion.com) when Tierion records the cryptographic hash of some data or a document onto the Bitcoin Blockchain.

However, the problem will be when another 3rd party vendor similar to Tierion issues a blockchain receipt differently even when that company records the cryptographic hash of some data or a document onto the same Bitcoin Blockchain.

The problem becomes bigger when there are other blockchains involved and there are also many such 3rd party vendors who record cryptographic hashes on one or more blockchains.

This will create problems for the blockchain focussed applications that are being and will be developed and there will be many such applications.

As such, it is important that we realize this potential issue now and standardize it!

```
{
  "header": {
    "chainpoint_version": "1.0",
    "hash_type": "SHA-256",
    "merkle_root": "6a9a3c86d47f1fe12648c86368ecd9723ff12e3fc34f6ae219d4d9d3e0d60667",
    "tx_id": "012fdc0eb5ebae181e1197b4e9307731473118b0634d3ede749a562e9d11809e",
    "local_timestamp": "1436172703"
  },
  "target": {
    "target_hash": "2f7f9092b2d6c5c17cfe2bcf33fc38a41f2e4d4485b198c2b1074bba067e7168",
    "target_URI": "http://example.org/target_name",
    "target_proof": [
      {
        "left": "e1566f09e0deea437826514431be6e4bdb4fe10aa54d75aecf0b4cdc1bc4320c",
        "parent": "0fdd6b6895e15115c262f6acb9a6ae0c73248568b740454ab21591f8a533dd7f",
        "right": "2f7f9092b2d6c5c17cfe2bcf33fc38a41f2e4d4485b198c2b1074bba067e7168"
      },
      {
        "left": "0fdd6b6895e15115c262f6acb9a6ae0c73248568b740454ab21591f8a533dd7f",
        "parent": "6a9a3c86d47f1fe12648c86368ecd9723ff12e3fc34f6ae219d4d9d3e0d60667",
        "right": "3b7546ed79e3e5a7907381b093c5a182cbf364c5dd0443dfa956c8cca271cc33"
      }
    ]
  },
  "extra": [
    { "custom_key_1": "value_1" },
    { "custom_key_2": "value_2" }
  ]
}
```

Appendix – My backgrounds in Blockchain

I am the Founder, Chairman & CTO of Hashcloud Pty Ltd, a Sydney, Australia based Blockchain Technology focussed start up. I along with my team are now developing a Blockchain integrated Digital KYC (Know Your Customer) and Digital Verification of ID (VoI) Platform at our lab based in KL, Malaysia. The platform is now at beta stage of development, ready for piloting.

My passion for Blockchain has led me to pursue a research doctoral degree (Doctor of Business Administration) at the University of Southern Queensland under the Australian Research Training Scheme in part time. A very passionate person in the Blockchain Technology, my research interest is how various industry verticals will be impacted by Cryptocurrency and Blockchain technologies. Before I founded Hashcloud, I was a Principal Consultant with Infosys Consulting based in Sydney and was also a Senior Manager at Accenture Australia prior to joining Infosys. During 2008-2010, I returned to Bangladesh to work as the Chief Information Officer (CIO) at BRAC Bank in Bangladesh. While at BRAC Bank, I also initiated a mobile payments project that eventually led to the creation of start-up called bKash where I was later appointed as the Founding CEO. I also has a Master of Commerce in Information Systems and Technology from Macquarie University in Sydney, Australia as well as an MBA from IBA, University of Dhaka, Bangladesh.

Listed below are my blockchain related credentials:

- Delivered a teaching workshop on 'Blockchain Technology' at Institute of Systems Science (ISS), National University of Singapore to the senior ISS academics in Jan 2016.
- Delivered a research seminar presentation on the topic 'Bitcoin & Blockchain – a look under the hood' at USQ in Brisbane to USQ academics and students in June 2016.
- Attended Blockchain University 'Cohort 5' in October 2015 in San Francisco, USA.
- Currently doing a Research DBA (Doctor of Business Administration) Program at University of Southern Queensland (www.USQ.edu.au), the research topic being: "Understanding the 'Blockchain' Technology – its value, its future and how the Blockchain technology could revolutionize the services industries using Blockchain & Web technologies".