WhatsHalal

Technical Paper

VERSION 2.01 – JULY 2018

Table of Contents

EXECUTIVE SUMMARY

WhatsHalal started as a food delivery mobile application. With numerous other delivery services available, WhatsHalal truly shines in its handling of Halal food. Far too often, we see other delivery services pack Halal and non-Halal food into the same delivery food bag. This poses a large issue for the Muslim community. WhatsHalal aims to solve this problem by providing a Halal food delivery operation.

However, that was only in the beginning. We realized that the industry is bogged down with too many differing standards and too many certification bodies. This becomes a problem for suppliers and consumers. *Suppliers* trying to enter a new market will have to seek new certificates in place and may have to tweak, or even overhaul, their supply operations. For *consumers*, they need to verify the authenticity of the Halal certification, as well as the parameters on which the certificate was issued. This causes large inefficiencies in the Halal food-supply industry.

WhatsHalal now aims to be a unifying certification system which embraces all the ideals and requirements of the different Muslim sects. We will provide a platform where suppliers can obtain certifications, and consumers can verify these certifications. This is when we realized that with blockchain technology, we can create a global ecosystem for the Muslim population:

- Frequent travellers, they commonly face issues finding Halal food in a foreign country. We intend to expand our delivery services globally to solve this problem. By onboarding F&B outlets across the world, Muslims travelling to a new place can effortlessly order Halal food and have it delivered right to their doorstep.
- Payments inside the application will support paying using the user's home currency. This reduces the cost per transaction for the user as the exchange administration charge is reduced (as compared to paying via credit card with banks' administration fees levied).
- Using WhatsHalal crypto-payment system will have discounts off the menu prices to incentivise usage as well as a reward system. This will provide data points for Halal compliance and data gathering.

All in all, we are striving to create a robust and vibrant community in which Muslims and non-Muslims alike can partake in excellent food that is traced end-to-end. I would like to thank you for your interest in our project.

Azman Ivan Tan
Chief Executive Officer
WhatsHalal

PROBLEM STATEMENT

The primary issue with food delivery for Muslim consumers in South-East Asia, where the WhatsHalal project started, is poor handling of Halal food. Delivery personnel need to meet delivery time-frames and are sometimes assigned by the system to pick-up food from multiple food joints before delivering them. It is not uncommon for Halal food and non-Halal food to be packed into the same carrier bag. This is an issue for the Muslim community.

Additionally, for Muslim travellers, seeking Halal food is not an easy task. This is further complicated by multiple certification bodies in the world, with each adhering to differing standards. The travellers will need to verify the if the standards used in the certificate meets the minimum requirements of their own. There is also the uncertainty of whether off-the-shelf products conform to multiple standards, or to only the country it is sold in.

Suppliers within the Halal food community who are looking to expand their reach overseas are often required to change their processes to comply with the new standards in order to enter the new market. There is no unifying standard for suppliers to conform to. It is also difficult for foreign certification bodies to do checks, or if they do, the cost might be prohibitive to a supplier of smaller scale.

OUR SOLUTION

WhatsHalal was founded to address the main issue of food delivery. By employing our own delivery couriers and having strict guidelines on food handling, we ensure that our clients receive food that are still Halal and uncontaminated. We intend to expand this service regionally and globally. We envision a future where Muslim travellers can, with a simple to use mobile application, order food and have it delivered through a trustworthy service provider.

When dealing with regional expansion, the team found that the situation in the Halal food industry is highly inefficient. As such we found that blockchain technology is perfect for our situation. With large occurrence rates relating to fake Halal certification, or incompatible certificates, the blockchain public visibility is an invaluable tool for solving this problem.

Our system also aims to create a reward system for users to submit information of new products to test for Halal compliance. The system will provide details in time on whether the food is Halal, as well as to which standards does it adhere to. This information will become publicly available and can solve the uncertainties regarding Halal certified foods in foreign countries. It will also attract new participants into the ecosystem, while incentivising everyone to assist in locating and certifying new products and building our database.

WhatsHalal aims to create a team of inspectors and certifying agents that can conduct global checks on suppliers. The inspection and certification processes can be paid for using our cryptocurrency (WHT). This adds a revenue stream for existing certification bodies and would incentivise them to participate and embrace this ecosystem.

PUBLIC BLOCKCHAINS

The primary purpose of public blockchains is to store and allow access to a public anonymised ledger. This was first conceptualised and implemented on Bitcoin Core protocol. The idea was to create a permissionless, publicly accessible and decentralised ledger system on which Bitcoin would be transacted. This eliminates the traditional need for a centralised entity to monitor and verify transactions. Without a central system to verify transactions, the system is vulnerable to double-spend events, where a transaction is sent twice within a short time span. This can be due to transmission errors or an attempt to defraud the system.

Blockchain technology was implemented to prevent this via a consensus-based decision making protocol. The idea was that every transaction will have its verification randomised be embedded into the blockchain by a "miner" that guessed the correct solution through an algorithmic problem. The randomisation process for verification will prevent transaction verifications from being spoofed. Furthermore, the two or more transactions are likely to be embedded into different versions of the blockchain due to competition between "miners" to be the first to guess correctly and write the next block. If there are different versions of the blockchain, the copy with the largest distribution across the network is taken to be the valid version. This makes any attempt to execute a double-spend attack extremely costly. This adds a "self-healing" capability to the data, allowing the network to recover from corrupted data and external attacks.

However, this presents an issue for practical uses in business scenarios: due to the decentralised and anonymous nature of the system, any transactions made erroneously or due to a successful cracking attempt, transactions cannot be reversed. Private key security, handling and storage becomes paramount. Exposure can mean permanent loss of assets via cyber theft, and key data loss or corruption means permanent loss of assets. This becomes a problem for SMEs that deal with the public. The vast majority of people are not sufficiently knowledgeable in understanding the system, or may become frustrated in their endeavour into the cryptocurrency space.

PRIVATE BLOCKCHAINS

Private blockchains maintain the ability for the data to withstand corruption and attacks by being able to "self-heal" through consensus and elimination of incorrect blockchain versions. Most importantly, private blockchains allow for control of the data in certain situations. This solves the problem of being unable to assist in situations when users erroneously transfer their digital assets. The biggest advantage that private blockchains have is the reduced cost for maintenance. As of June 2018, Bitcoin's network consumes more than 70 TWh[1] (terawatt hour). This is highly inefficient given that the vast majority

[1] Source: https://digiconomist.net/bitcoin-energy-consumption

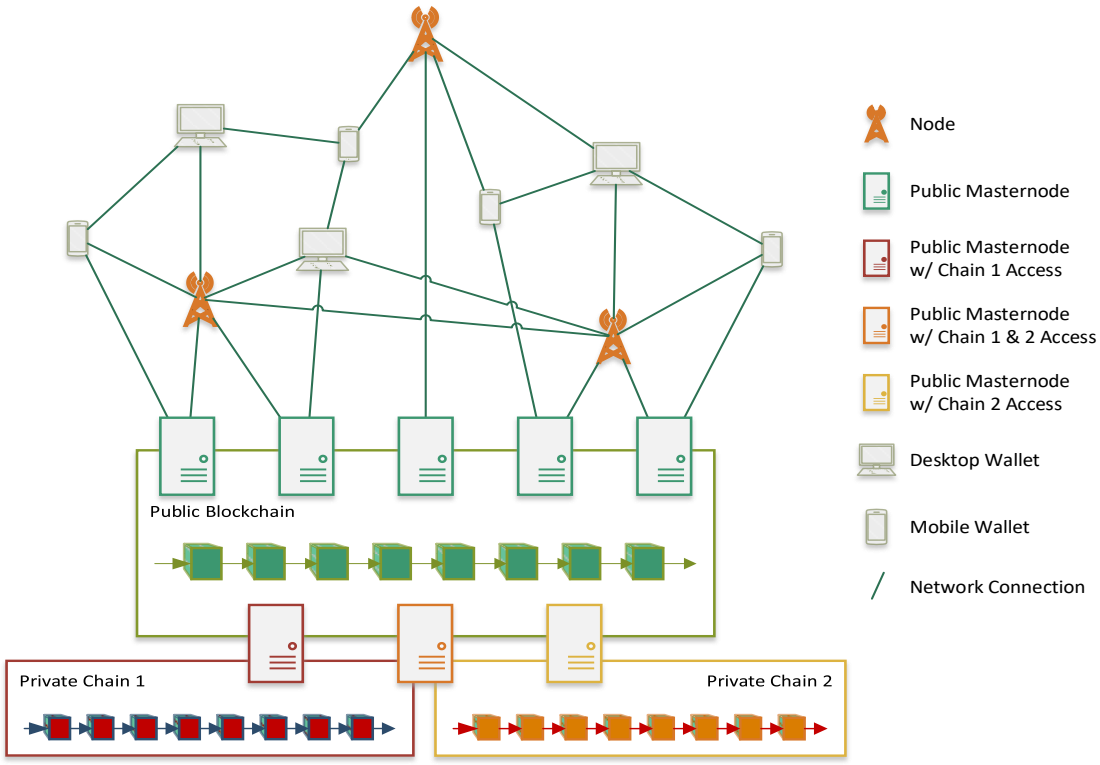
of the energy is consumed by miners who race to be the one to solve the cryptographic puzzle.

Private blockchains consumes a tiny fraction of this due to the difference in the consensus algorithm, i.e. consensus protocol operates differently and a master-node is chosen at random after every round to write data to a new block on the chain. This reduces the energy consumption required by cryptographic hashing functions to only the master-node that is chosen. This is similar to “Proof-of-Stake” consensus, but the master-nodes to be allowed to access to the blockchain is permissioned.

However, this is not a fully publicly visible blockchain. It lacks the accountability and verifiability of public blockchains. While access can be granted, this takes time and effort for users, and may even be beyond their capability to implement.

HYBRID BLOCKCHAINS

Hybrid blockchains provides a middle ground between two with a public layer and private layer. All master-nodes are granted permission to join the blockchain and help with data propagation to sub-nodes and user devices. Master-nodes have the ability to spawn additional private chains accessible to themselves and any other master-nodes that are permissioned to join the private network. In the diagram below, we have the public master-nodes allowing access to the public chain. This is where the public ledger resides as well as public facing information datasets.



Two of the master-nodes in the diagram have private chains spawned under them. They have also both permissioned one master-node to access both of their private chains. In this environment, public devices can access data in the private chains via the permissioned master-nodes, while being able to see the public layer transparently. The “red” master-node can only access Private Chain 1, and the “yellow” master-node can only access Private Chain 2, while the “orange” master-node can access both private chains. If the two private chains need to interact with each other, they can only do so through the public shared layer. Datasets can be hashed and pushed to the public layer for storage. This system keeps the proprietary information private, yet allowing for validation of the datasets in the private blockchains.

HYBRID BLOCKCHAIN IN WHATSHALAL

As we aim to be a global solution for tracking of Halal certification, as well as a payment layer for transaction of goods and services, the hybrid blockchain is perfectly in line with our requirements. Business-to-business data will require privacy (logistical data, business contracts, etc.) while end-user transactions with retailers require decentralised publicly visible verification. The multi-layer system that is provided by hybrid blockchain systems allow us the flexibility to implement this to the fullest extent and create a secure and flexible ecosystem for all users in our system.

We expect a high rate of adoption of our suite of technologies and services due to this, as there is yet a global, yet unified system made for the Muslim community worldwide. There are blockchains created to track Halal certification but none are as extensive in coverage and applicability as what we envision the WhatsHalal system to be.

THE HYPERLEDGER INITIATIVE

Hyperledger is a global collaborative effort to bring about new blockchain technologies. As an initiative of The Linux Foundation, all codes and resources are open-source. The aim of Hyperledger is to create enterprise-class distributed blockchain ledgers that are applicable to businesses. Currently, Hyperledger includes Sawtooth, Fabric, Indy, Iroha and Burrow blockchains.

The primary goal is to create technologies, built upon distributed ledger technology (DLT), that are secure, fast and modular. This allows businesses to tap into blockchain technology without adding a large amount of cost to maintain the network, as compared to public blockchains where transaction fees are levied. It allows for selective permissioned access to private data when required, yet have a layer that is public facing for everything else.

The Hyperledger mandate rules out the use of cryptocurrency within the system for now. As such, it is perfectly suitable for our hybrid blockchain system, with a separate implementation of the public transaction layer.

HYPERLEDGER FABRIC

Hyperledger Fabric is one blockchain technology within the Hyperledger initiative created by IBM. It provides relatively fast finality (consensus on block data) thus resulting in good transaction speeds as compared to Bitcoin and even Ethereum. However, Fabric is weaker at dealing with Byzantine faults as compared to the other DLTs in Hyperledger. Byzantine Fault Tolerance[2] (BFT) is the system's capability in dealing with faulty or malicious components in the network. This is not necessarily a security issue given that master-nodes require permission to join the network. There is also work-in-progress by IBM to improve upon Fabric's BFT capabilities. Given the modular architecture of Fabric, improved modules are pluggable without interference to other systems.

Fabric has an installable Smart Contract capability. This allows for public visibility layer for Halal certification and traceability. Fabric already has a good track record in supply chain management. The ability for multi-signature activation of contracts allow for WhatsHalal and a regional/local authority to enable a Halal certificate for a business. The subsequent movement of goods or provision of services through the contract holder will have the ledger's unique signature added to the tracking of the product. This allows for end-to-end traceability.

---

[2] See: Byzantine Generals' Problem