HABITS TECHNICAL WHITEPAPER

Habits Team

December 26, 2019

Habits is a fashion e-commerce where customers will be able to *try-on* their favorite products thanks to Augmented Reality, in real-time. At the same time, brands will be guaranteed to have visibility and advertising space, thanks to a mechanism which will be propelled by its own Token Economy. Blockchain and elements of Decentralization will be used to ensure brands that tokens they own are consumed if and only if a customer *actually* tries on their product. Habits Technical Whitepaper explains in a concise manner what the Habits network is, sets the requirements for such an ecosystem and finally introduces adopted implementation.

Key Concepts

AR Augmented Reality. 1

GDPR General Data Protection Regulation. 1, 9

HAP Habits Admin Panel. 1, 3, 6

HBX Habits Token. , 1, 2, 3, 4, 5, 6

HM Habits Mirror. 1

IPFS Inter-Planetary File System. 3, 8, 9

PoT Proof of Try-On. 1, 2, 3

zk-STARK zero-knowledge Succinct Transparent ARguments of Knowledge. 8

zk-SNARK zero-knowledge Succinct Non-interactive Argument of Knowledge. 8

ZKP Zero Knowledge Proof. 2, 8

1 **Habits Network**

Habits Nodes, Customers, Brands

2 **Key Requirements**

Why Decentralization, Stability, Confidentiality, Usability

3 **Proof of TryOn**

PoT Creation, Decentralized Messaging and Payments

4 **Token Economy**

HBX Token, Gas and Fee Management

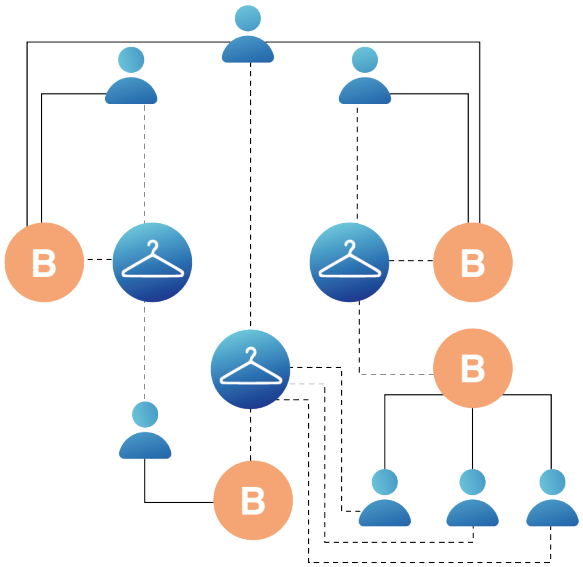
5 **Brand Marketing Campaigns**

Product and Marketing Campaign Management

6 **Architecture**

Decentralized Logic and Off-Chain Trusted Execution

1 Habits Network



CUSTOMERS

Within the Habits ecosystem, thanks to **Augmented Reality**, customers will be able to try-on products whether using Habits Mirror or their own smartphones directly. When trying on products, both the Habits Mirror and smartphones will interact with the Ethereum Blockchain Protocol in order to produce a **Proof of Try-On** (PoT). Despite elements of decentralization (e.g. having an unique Ethereum account that will be used to log in) customers won't be required to store private keys, and neither Habits will do that for them. This will lead to a rapid and **smooth registration** process just like for any other app.

FASHION BRANDS

By acquiring **Habits Tokens** (HBX) through the Habits Admin Panel (HAP), Brands will be able to upload 3D Models of their own products, create and manage related **marketing campaigns** and reach customers directly in a manner that old business models aren't capable to offer. A simple formula equates one HBX to a single customer TryOn. The main **purpose of a Proof of Try-On** indeed, is to ensure Brands that only real and unique customers are trying on their products through Habits. Once they verify authenticity, an HBX token is transferred back to Habits. In other words, Brands will always know what they are paying for, and by doing so will pay much less than with traditional Customer Acquisition Processes.

HABITS

Habits Business Model will be implemented as Decentralized Logic through a set of Smart Contracts, and no usage of Distributed Ledger Technologies is expected both in short and long term development. The Habits Decentralized Logic will orchestrate verifiable off-chain code execution and decentralized data access in a confidential and compliant to the General Data Protection Regulation (GDPR) manner. Usage of these technologies will allow near instant horizontal **scalability** due to business expansion in more geographical areas.

2 Key Requirements

2.1 DECENTRALIZATION

The user of a decentralized system is able to successfully complete a **critical operation** without necessarily relying upon the correct behavior of other users or any kind of third party. In the case of Habits, decentralization is used to ensure the Brand that:

- **D1** the HBX payment occurs if and only if the buyer *actually* tries-on its product (Proof of Try-On);
- **D2** the payment triggering is **automatic** and **unstoppable**, therefore Habits can't interfere with the process;
- **D3** there is an **authentic** customer base upon which marketing campaigns are launched, at the same time without revealing any data about Habits customers themselves.

2.2 STABILITY

Due to their open, permissionless setting, Blockchain Protocols can experience unpredictable network loads which can negatively impact both performance and transaction fee. On the other hand, a Brand must be able to always safely interact with the system and be charged a clear and **predictable** amount for each marketing campaign. Therefore, the technical solution designed at Habits will be able to:

- **S1** guarantee operativity and **quality of service** to customers and brands, i.e. guarantee that the Brand will always be able to operate on the platform despite Ethereum's network load and scalability issues.

2.3 CONFIDENTIALITY

Confidentiality is the ability to keep data undisclosed despite decentralization and therefore public availability of that data. By combining Ethereum with an additional layer of cryptographic tools, including Zero Knowledge Proof (ZKP) technologies, the system will allow:

- **C1** **access** for users only to selected data within the system, and to no one outside the platform;
- **C2** **obfuscation** of data and user generated operations while still enabling public ledger traceability;
- **C3** to guarantee **C1** and **C2**, while being able to prove that confidential data is correct without revealing it (linked to **D1-3**).

2.4 USABILITY

Adopting a Blockchain solution also means dealing with private keys which unfortunately would still require today a learning curve from new Habits users. In order to easily acquire new users the system should appear easy-to-use:

- **U1** Customers and Brands shouldn't be forced to register by creating a wallet by themselves or to store private keys, they can do that only if they want to;
- **U2** Habits nor any other third party will store user private keys, and will still guarantee powerful forms of data recovery in case that someone loses the ability to log in;
- **U3** Brands should perceive token usage as clear and transparent as possible.

3 Proof of Try-On

The main goal of the try-on mechanism in this case is to ensure that once the buyer views a 3D Model, the HBX token transfer must occur without Habits being able to interfere or to control it somehow, which also implies that the buyer should be authentic. A **solution** which satisfies D1, D2 and D3 would be the following protocol:

TryOn Genesys

- Customer **views** the product through the Dapp
- Customer Dapp **instantly signs** newly created TryOn data (*who*, *when*, *what*) with Customer Ethereum Account derived key pair

Direct Communication

- Customer Dapp **sends** Proof of Try-On to both the Brand and to Habits
- Proof of Try-On is sent preferentially through a **Decentralized Messaging Protocol**, although typical channels might also be used

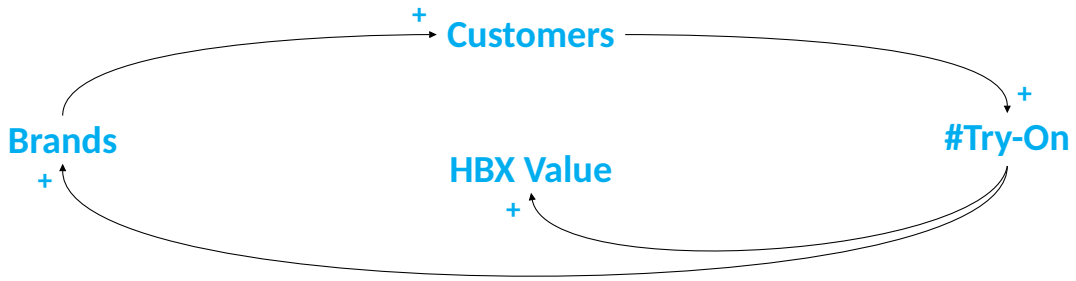
Verify and Pay

- when the new PoT arrives, a Smart Contract is used by the Brand to check if the signed TryOn belongs to a **unique and registered customer**, and unnecessary for the verification details about the customer aren't revealed to anyone
- the Brand **pays** an HBX for each received PoT

Enabling customers to have an Ethereum account is *essential* for the Proof of Try-On mechanism, while having them to necessarily manage private keys is bad if we want a frictionless and effective user registration process. In order to be decentralized without sacrificing anything (i.e. not storing their login data while simultaneously letting users to easily log in), non-custodial *Authentication Providers* will be used. By doing so, requirements U1 and U2 (see Section 2) are met. Habits Tokens can be quickly and intuitively bought by Brands prior to launching a new Marketing Campaign, directly through the Habits Admin Panel (requirement U3). Brands don't have to always be logged in or to run a node in order to perform real-time operation approvals. Each new Proof of Try-On indeed, concatenates to the TryOn history of that particular 3D Model. A history which is an Inter-Planetary File System (IPFS) asset, and is pointed to by Habits and Brand Smart Contracts.

4 Tokenomics

A Habits Token represents the **right to expose** a product 3D Model to a customer Try-On, one single time. It has been previously established that an easy customer registration is crucial. The more customers there are on Habits, the more Brands will want to expose their clothes. And the more they will want to expose their products, the more **value** an HBX token will gain. Cyclically, more Brands and products will attract more customers.



4.1 GAS

Everytime a transaction upon the Ethereum Blockchain is generated, its sender should pay a fraction of `ETH` as incentive for miners to compute that transaction and include the newly generated state into a block. This requires the Ethereum user to create in the first place its own wallet and fill it with some `ETH`. Since Habits will be a decentralized application, owning a wallet with `ETH` won't be enough for brands in order to use its functionalities. In order to transact upon Habits infrastructure indeed, a brand would be required also to install extensions such as `Metamask`. After automatically detecting newly generated transaction by the *Habits Admin Panel* during its usage, `Metamask` would then ask the brand within its browser to confirm and pay for it. Imposing to a customer of the dapp, in this case a brand or an independent designer, to independently perform previously described steps might be an unnecessary learning curve and risk. Habits customers shouldn't be forced to buy `ETH` on an external to the Admin Panel exchange in order to operate upon.

4.2 TRY-ON FEE

Currently, the main open problem of Ethereum is **scalability**. That is, the ability of a Blockchain protocol to maintain an acceptable transaction throughput (tx/s) at a growing number of users. Lacking scalability in a public decentralized environment means that when the network is overloaded by too many transactions to be processed, transaction validation waiting queue quickly grows. Ethereum miners tend to include into the next block those transactions which have the highest fee. Given this fact, users will soon start to rush at rising their offer to miners in order to skip the congestion. Despite ongoing active research and development to improve Ethereum as a protocol, there is no guarantee that network overloads won't happen again. On the other hand, Habits is solving one of the biggest problems of today's fashion industry, that is **lowering** *Customer Acquisition Cost* for Brands. In order to achieve that, the Token Economy must be *insensitive* to the underlying Blockchain Protocol **fee fluctuation**. In other words, the requirement **S1** must be meet.

4.3 HOW

NO GAS

- ERC-865 Token Standard is adopted in order to **abstract** gas usage to the eyes of users
- when creating their own marketing campaigns, Brands will **pay with HBX** instead of ETH
- HBX tokens will return to Habits, which in turn will pay miners with the equivalent in ETH

- given the network fee unpredictability, it still must be avoided the scenario where an arbitrary number of tokens are being scaled from a Brand balance, each time a try-on occurs

NO FEE

- Layer 2 Scaling Solution will be used in order to allow to charge a Brand for predictable amounts of HBX, a feature which is facilitated by
  - the gradual launch of **Ethereum 2.0** with improved scalability features and off-chain compute
  - constant developments which are being made within the **Ethereum Decentralized Finance** ecosystem
  - and emerging powerful scaling techniques such as *Optimistic* or *Zero Knowledge Rollup*
- network fees are applied only to rare operations such as creating a marketing campaign

5 Marketing Campaigns

Buy HBX

- Brand simply **buys** Habits Tokens through Habits Admin Panel with Fiat currency;
- tokens are sent directly to the **wallet**, no external crypto-currency exchanges required;

Upload 3D Model

- Brand **uploads** its product 3D Model on the platform by using HBX, which later can be **updated**;
- product upload and updates are **recorded** on the Blockchain, certifying product evolution;
- Habits will also provide a service for product 3D Model creation;

Start Campaign

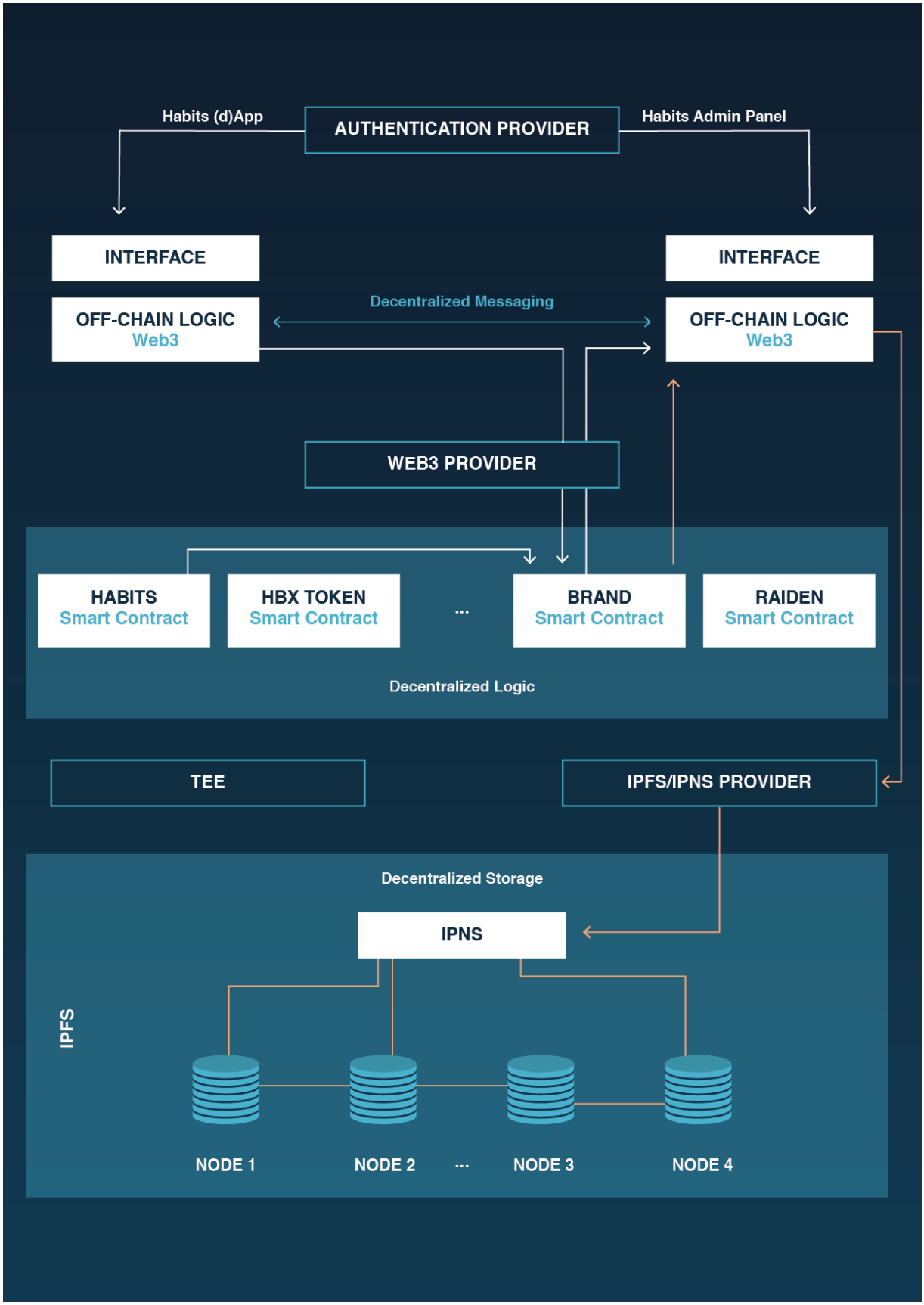
- the Brand selects its budget, **target** and additional parameters at will;
- the product is launched through a Market Campaign and is ready to receive Try-Ons from customers;
- a new State-Channel is created each time a marketing campaign is open;

Modify Campaign

- once the marketing campaign is started, HBX tokens that are its budget are locked until Try-Ons are consumed;
- if the Brand interrupts the marketing campaign earlier, unspent tokens are released and free to be used in any other manner;

When a Brand inserts the 3D model and wants to make it visible on the platform, Habits executes an algorithm which targets the user base that is considered by the Brand to be the most fit for that product. Any other types of computations might be executed as well.

6 Architecture



6.1 OFF-CHAIN EXECUTION

It has been mentioned (Section 5) that Brands will have the ability to target more or less specific customer groups when starting a Marketing Campaign. That means that there will be more or less complex **algorithms** which can't be executed on-chain due to gas cost and scalability. On the other side, in a configuration which executes code purely within a typical, closed source back-end, it is very difficult to demonstrate execution fairness and authenticity of provided output to Brands. For Habits this is a crucial aspect though, since it must be proved that there is an authentic customer base upon which marketing campaigns are launched (requirement D3 in Section 2).

Algorithms will be executed as *private transactions* between Habits and Brands as if both of them were mutually untrusting parties, without (a) disclosing transaction content to other parties using mainnet Ethereum and (b) without disclosing sensitive data about customers to Brands, while being able to provide proof of authenticity of input data, output data and source code integrity. Algorithms are removed from the main Blockchain Protocol and shifted towards off-chain Trusted Computation. At first, hardware Trusted Execution Environments [4] will be used to complete this task, by using *oracles* to guarantee interoperability. However, Habits is aiming to use purely software based Zero Knowledge Proof solutions involving additional mechanisms such as `ZoKrates` [1] and further Ethereum improvements as a protocol regarding its integration with zk-SNARKs [2] and zk-STARKs [3]. The abstract platform architecture is represented in the Figure above, off-chain logic is executed client-side and through trusted off-chain computing.

6.2 PROVIDERS

Inter-Planetary File System (IPFS) will be used as a protocol for decentralized storage. IPFS and `web3` Habits providers will easily allow to horizontally scale when needed, provide fast and secure access while strengthening the overall Ethereum network. It's worth mentioning that another advantage of `IPFS` over conventional databases is that synchronization between nodes is preferable but not strictly required in order to access content. An external provider might be used for non-custodial user authentication. A customer registers to the Habits platform by downloading and starting to use the dapp. First, a non custodial wallet for the buyer is being generated according to a mechanism like the one developed by Portis [5]. It is required indeed for the buyer to also be identified by an Ethereum account in this schema, although it's not required to make them generate transactions unless Habits will decide so, somewhere in the future. The user might never notice that it is using an Ethereum account. Despite decentralization indeed, required information for login might be just an e-mail (or phone number) and password. Customers and brands might have two methods of access management, they can choose whether to use the already mentioned e-mail and password method, or, to manage by their own a pass-phrase/private key through hardware or software wallets.

6.3 DATA

It has been seen that business logic will be at least partially executed by leveraging off-chain execution environments, but how about input data for those executions? It must remain confidential while being able to guarantee authenticity for Brands. Files posted on IPFS are public, copyable and accessible by any other IPFS node in the network, similarly to a subset of Blockchain principles. In order to keep data accessible only by owners upon IPFS, each new file ϕ will be encrypted using the same cryptographic key pair underlying the respective owner Ethereum account. Only then, the encrypted file can be published to IPFS obtaining the its *multihash* which can be saved into a Smart Contract and act like a **storage pointer**.

If some file ϕ needs to be accessible by multiple parties, then multi-key encryption can be used upon ϕ, using multiple public keys derived from respective Ethereum addresses.

IPFS implements a popularity based mechanism for files. It means that when a node adds some file ϕ to the network, other nodes can copy it and store it locally too. But other nodes would do that only if ϕ is requested globally, because they want to hold important and most wanted files. Since ϕ is unusable without a specific Ethereum account, no one other than Habits itself (which provides the service for them) has the incentive to store it locally. In this worst case scenario Habits can just *forget* about the file, by eliminating pointers to it from the Smart Contract. Within the European Union, this mechanism also allow to be compliant with General Data Protection Regulation (GDPR) by providing to Habits users the

- right to withdraw, the data subject have the right to withdraw consent at any time, (Art. 7 GDPR);
- right to be forgotten, the platform should comply with the right to erase personal data wherever they are (Art. 17 GDPR);
- right to rectify, it is the right to obtain rectification of inaccurate personal data without delay (Art. 16 GDPR).

References

[1] Jacob Eberhardt and Stefan Tai. *ZoKrates – Scalable Privacy-Preserving Off-Chain Computations*. Information Systems Engineering (ISE), TU Berlin, Berlin, Germany.

[2] Christian Reitwießner. *zkSNARKs in a Nutshell*.

[3] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh and Michael Riabzev. *Scalable, transparent, and post-quantum secure computational integrity.* March 6, 2018.

[4] Bakshi et al. *Enterprise Ethereum Alliance Off-Chain Trusted Compute Specification v1.1* 8 October 2019.

[5] Itay Radotzki and Tom Teman. *Portis: key management and smart contract interaction using end-to-end encryption* June 11, 2019.