WHITEPAPER 1.0

Powered by Dona Mara

HAPI

HAPI is a set of cross chain smart contracts that are embedded into DeFI products that allow them to reach a new security level. Also, HAPI's Oraclizing and DAO system delivers SaaS in the DeFi environment that prevents hack attempts.

Table of Contents

Table of Contents 1

Cybersecurity Transgressions in the Current DeFi Ecosystem 2

The Problem 3

HAPI Protocol 5

Community Aspect of HAPI 6

Confidentiality Aspect of HAPI 7

Integrity Aspect of HAPI 11

Availability Aspect of HAPI 12

Smart Contract Integration and Oracle Utilization 13

Concept and Outline of The Main Framework of HAPI 15

HAPI Token Model and Utility Cases 18

Roadmap and Plans for The Future 19

Risks 21

Cybersecurity Transgressions in the Current DeFi Ecosystem

From its inception, DeFi has been a vulnerable target for a wide array of malicious exploitations. The growing concern over this easily exploitable nature of DeFi projects has been a reliant repellent for enterprises and companies to start adopting crypto. Grotesque headlines, and the harsh reality of the victims of unfortunate happenstances, have played a huge negative role in rallying mass adoption and attracting a new stratum of people in the crypto sphere.

It’s patently visible even in today’s more matured cryptomarket how prevalent this kind of occurrence can be. Simple inquiry in the Google Search will yield an insurmountable number of examples, and even rankings of the most notorious hacking contrivances that had happened in the recent days, months, and years. Fairly unnoticed has been this omission in crypto, summoning even more doubts about the validity and future of the whole conceptual idea.

Despite the most egregious hacks, to this day we don’t see a fairly reliable failsafe mechanism that sets out to rectify the most notable loopholes. This warrentedly raises even more dubious outcry from the Media Outlets, orthodox Financial Institutions, and people still on the fence about the cryptocurrency market.

The Problem

The problem is here, and it needs to be resolved in order to bridge the cleft of unreliability that is currently rampant and ongoing. To exemplify it warrants to take under scrutiny an eerily recent hack that transpired in the digital currency space. The infamous attack on one of the most influential South Korea's exchanges - Bithumb. Perpetrators villainously took control of $30 million worth of digital tokens. Ostentatiously flaunting the exploitability of CEX (Central Exchanges) and showcasing the Achilles' Weakness of the current modus operandi of exchanges in general. This case presents one of the most recent and largest hacks/exploits of the contemporary digital currency market. Unfortunately, this is only a globule of sand in the seabed of countless hacks. To better illustrate the magnitude and resonance of these examples, it will be better to list them in the order of gradual decrease of the loss that was incurred upon particular DeFi, DEX, CEX.
We shall inquire first in the recent CEX hacks and the scope of the damages done:

Coincheck: $534 Million
BitGrail: $195 Million
Bitfinex: $72 Million
Coinrail: $37.2 Million
Bithumb: $30 Million

The Problem

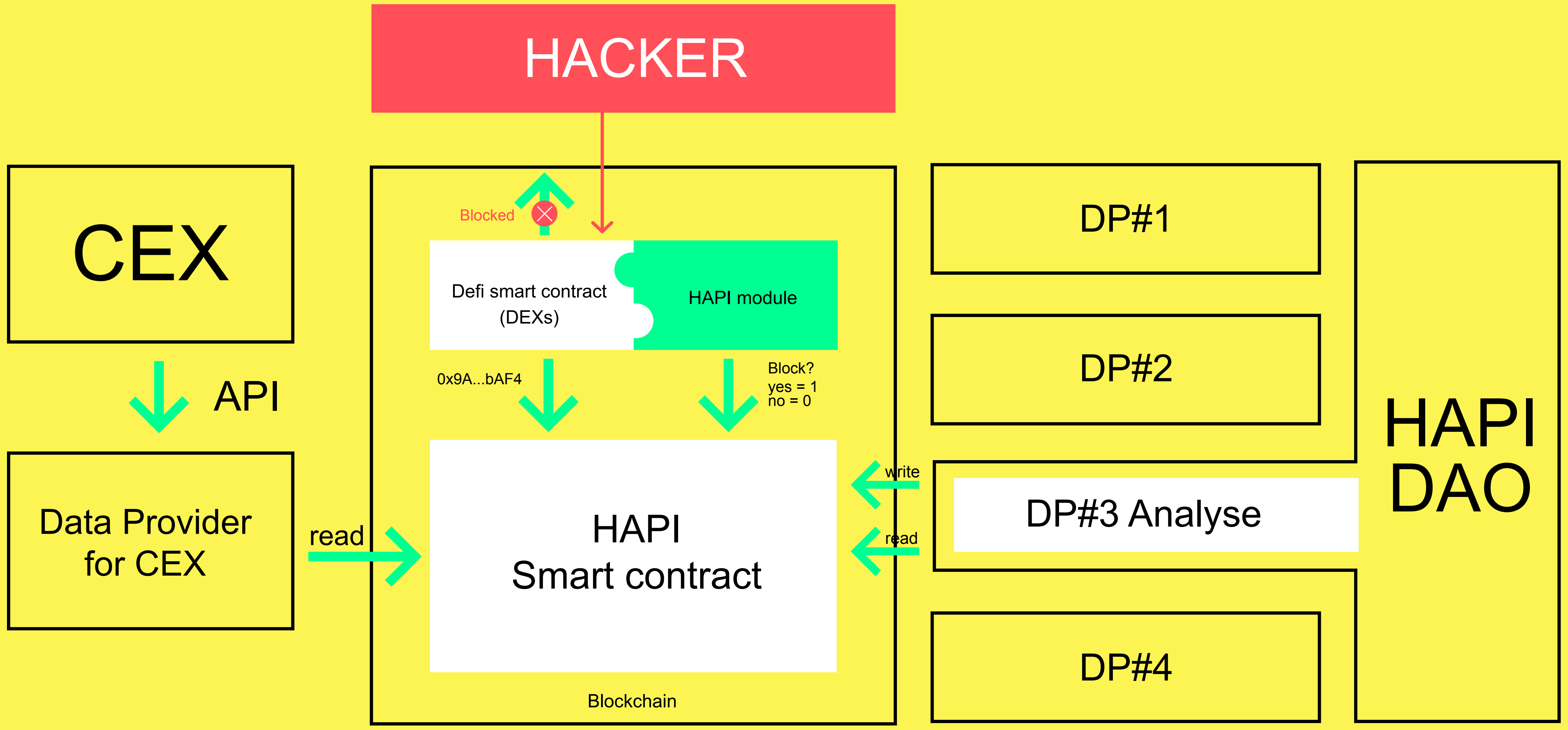
It would be close to impossible to list every DeFi hack that has happened in the last decade. Therefore, to keep up with the times and ensure that the data presented is the most recent one (May 19 2021) we will be condensing the list into only 2021 exploits.

DeFi:
EasyFi Hack **$80 Million**
Uranium Finance Migration Exploit **$50 Million**
Alpha Homora Iron Bank Exploit **$37 Million**
Meerkat Finance Exploit **$13 Million**
PAID Network Infinite Mint Attack **$3 Million**

From the DeFi vulnerability, it is painfully obvious that similar hacks and exploits are exposing novice retail investors to unnecessary risks and unpredictable losses that stem solely from the fact of neglected security implementation. It is also evident that retail investors that got “burned” in the event of them not being responsible for the loss will then exude far less enthusiasm in investing in crypto-based projects further down the line. This is the proverbial manifestation of unneeded risk exposure that CAN be remedied if and when the right functionality and toolset are implemented.

HAPI Protocol

The mission of HAPI is to rectify a cornucopia of issues that are entrenched in the current DeFi space. The approach HAPI takes does differ from the current solutions on the market. The differentiating points are both visible from the technical standpoint and community side of things. From the technical standpoint, HAPI incorporates a slew of preventative solutions that will inhibit exploits from transpiring beforehand. That also involves the utilization of the cybersecurity audit database by virtue of which malfeasance and maliciousness can be impeded in a timely manner. It is better illustrated in the following example: A particular DeFi is about to be a subject of a malicious exploitative attack. To aid in preventing the above-mentioned invasion, HAPI utilizes the combination of smart contract integration (SC) and Oraclization (oracles that are used on-chain). Before the attack has even been engendered, HAPI, with the help of off-chain dataprovider, can detect, mark, and delineate the potential threat of a particular address, by incorporating oracles specifically engineered, or programmed if you will, to preemptively act on the danger that a particular address poses. In this vein, a nascent calamity can be eluded against the clock. A more in-depth explanation will be provided in the paragraph below (number of the paragraph).



Community Aspect of HAPI

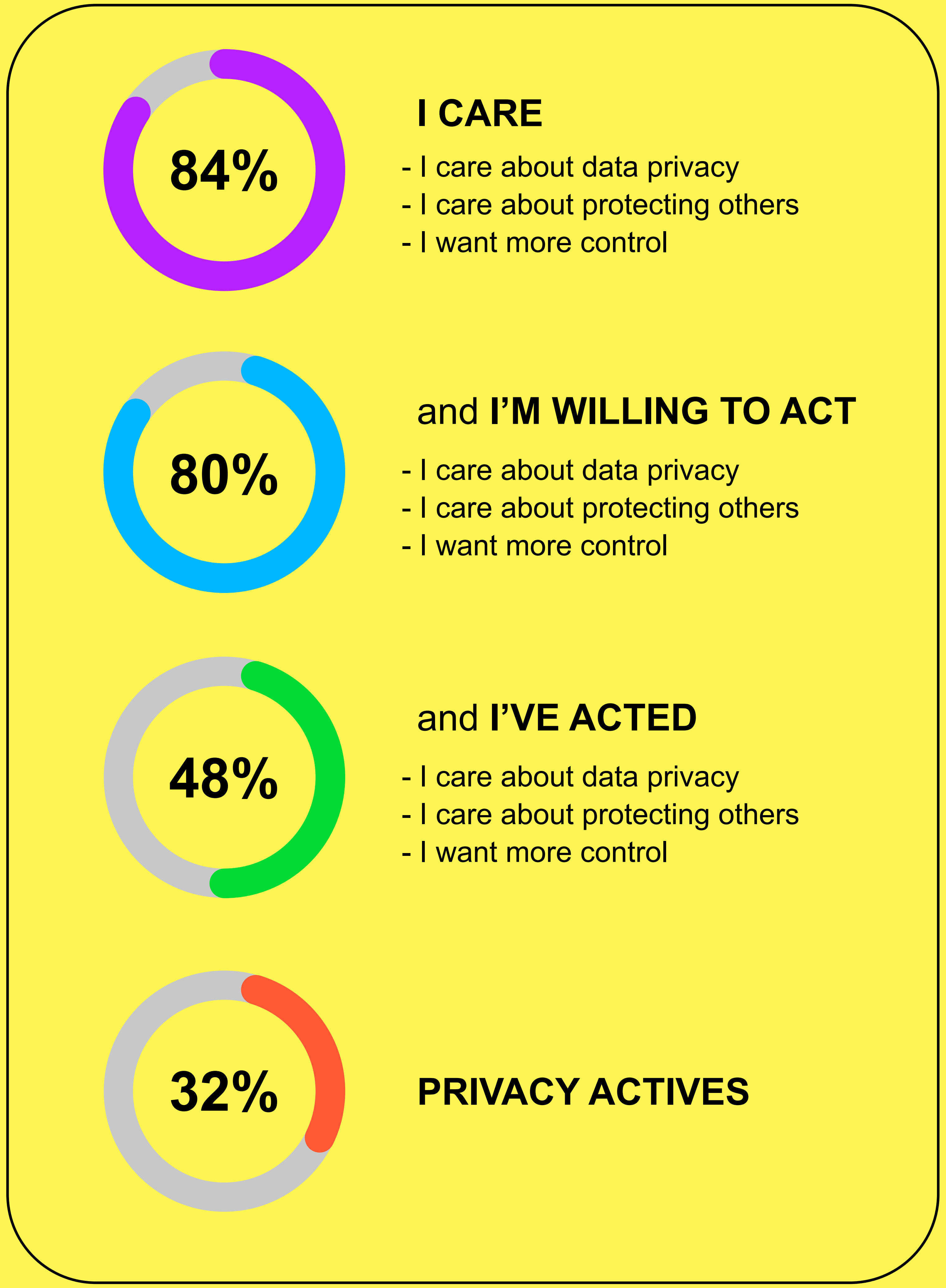
The community aspect of HAPI is also a crucial distinguishing part of the protocol. The community has direct involvement in the address database and can import data (wallet address as an example) of an arbitrary unlawful player to the Blockchain analysis database of HAPI. An enrolled address will be thoroughly scrutinized and a respective verdict placed. With this type of communal incorporation, HAPI aims at creating a prolific database of an ever-increasing set of constituents that will assist in blacklisting and, eventually, ridding the system off of “unconstitutional” participants. We will be expounding on the community aspect more in-depth in the coming paragraphs.

Most of the issues HAPI tackles are directed towards resolving and propounding the common triad in cybersecurity: Confidentiality, Integrity, and Availability. To better cognize the aspects of each and how HAPI intertwines them into the protocol, we will need to deconstruct and singularize them one by one.

Confidentiality Aspect of HAPI

Confidentiality is the term mostly used to refer to the sensitive data that is privately or corporately owned and is not designed or designated to be propagated, publicised, promoted, or shared. Confidential nature also imparts a general notion of privacy and even decentralization - more so if we are talking about cryptography. Unauthorized access or misuse of confidential data most of the time also entails judiciary repercussions that discourage individuals from engaging in these sorts of errands.

The very bedrock of crypto has been built with confidentiality in mind. Protecting personal finance-related transactional interactions from third parties and ensuring total privacy. Bitcoin being the pioneer in this regard has successfully showcased to people of all social layers that privacy, and confidentiality ought to constitute the most basic human right. With the fear of sounding pretentious and being called “crypto maximalist”, let’s look at the statistics of individual privacy value.



84%

I CARE

- I care about data privacy
- I care about protecting others
- I want more control

80%

and **I’M WILLING TO ACT**

- I care about data privacy
- I care about protecting others
- I want more control

48%

and **I’VE ACTED**

- I care about data privacy
- I care about protecting others
- I want more control

32%

PRIVACY ACTIVES

Confidentiality Aspect of HAPI

Though it might be highly correlative data, it clearly shows that:

a) More individuals place value on privacy

b) Privacy is becoming a measure of individual deliberation

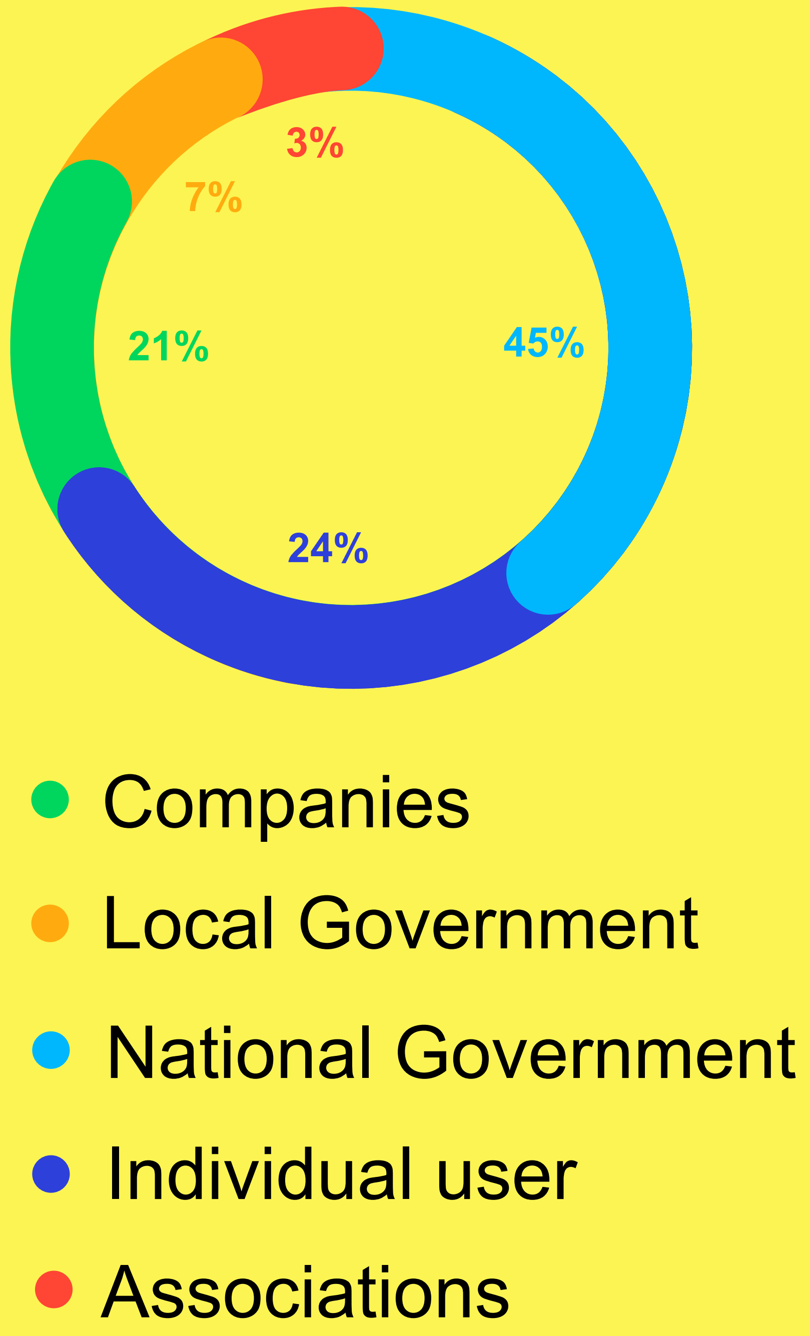
With the growing popularity of cryptocurrency, we can make a reasonable deduction that privacy has also become more prolific and “popular”

Cybersecurity solutions always teeter on the verge of not being truthful to the bounds of their reach. Many are also prone to overstepping the boundaries of confidentiality which is quite problematic in and of itself. HAPI enshrines the fundamentals of Bitcoin and the overall mission of blockchain. This is the reason why decentralized quality is crucial to the methods and approaches HAPI takes as to not to impinge on confidentiality and, at the same time, secure the efficiency of the protocol.

HAPI doesn’t store any sensitive data and exclusively utilizes oracles and smart contract functionality as the basis to provide security solutions. HAPI also operates on the public niveau with governance being partially delegated to the community. People can freely contribute to the database, making the system in place public, expandable, and self-sustainable.

Who is primarily responsible for protecting data privacy

N = 2601



Integrity Aspect of HAPI

Integrity and the crucial role that it plays in oraclization can't be understated. The value of integrity in oracles has been sufficiently elaborated on Chainlink (ref). The data extracted from the database and the dataprovider itself should not be a subject of negligence. The link between oracle and dataprovider mandates uninterrupted and untampered quality simply on the basis of projecting up-to-date, reliable, and trustworthy data feed to HAPI SC.

HAPI designs its oracles in a way that ensures that "adapters" (the link between oracle and smart contract) remain in the untampered state. This is achieved by employing Transport Layer Security (TLS). The TLS protocol focuses on providing integrity first and foremost (ref). It's the crucial link between integrity and privacy that allows for communication between two computer applications. TLS enables data integrity to be consistent, prevents data tampering, and eavesdropping. TLS is normally composed of two layers: TLS handshake protocol, and TLS record.

TLS employs a coordinated flow of operative functions before the connection can be considered secure. The initial execution is commenced by using a handshaking procedure. There are two basic ciphers that are introduced during handshaking: asymmetric cipher, and symmetric cipher. In basic terms, symmetric cipher consolidates encryption of the connection and asymmetric cipher vouches for session-specific intercommunicated key and general cipher settings. Handshake protocol thus represents a secure way of encrypting data transmission, making data integrity of paramount importance is integral for HAPI protocol.

Availability Aspect of HAPI

Availability for Oracle-based projects like HAPI means putting a substantial amount of trust into a third-party provider to deliver up-to-date, timely, and consistent data for oracles to transfer to the Mainchain. Off-chain dataprovider thus empowers the core mechanism of the protocol. Therefore there is a considerable degree of trust that gets translated to the dataprovider and its ability to delegate trustworthy and timely datafeed. In the first stages of the working protocol and first iteration of integration, HAPI will utilize third-party solutions. The requirements we set and the investigative work that we have done in order to ensure that the dataprovider chosen is qualified, is commensurate with the degree of trust our community puts on us. Our basic set of requirements for dataprovider are as follows: efficient data transfer, robust, and voluminous database, low response time, and immaculate track record. Off-chain dataprovider supplies SC with datafeed that then sends a response to the Mainchain. Depending on the state of the response and whether the data, in our case wallet address, is considered to be fraudulent - the verdict is enacted. HAPI reserves the right to report the potentiality of the threat to the operator. In that case, the operator, for instance, CEX, can then act upon this data at their own liberty.

Smart Contract Integration and Oracle Utilization

HAPI incorporates a system of specifically designed pleiades of decentralized Security Oracles that enable a consistent, and up-to-date relay of datafeed to the Mainchain. These security oracles tether to the outside world (off-chain) via API to the given database. This database consists of a myriad of data that oracles can extract. Consequently, with the help of the data extracted oracles then record this data onto the blockchain.

Despite the relative simplicity of the process, it does require stout reliability of all the elements working conjointly in a harmonious way. On top of that, there is also a hidden complexity of “oracle-engineering”. Oracles in the system ought to have a gamut of mandatory characteristics in order not to be exploited, mishandled, and tampered with. HAPI designs its oracle with the utmost security in mind. In order to achieve the coveted level of security for oracles, there is a need to lay in a supplemental layer of “assurance”. This is the raison d'etre of using TLS as a mediator of a secure connection between an oracle and a server.

Smart Contract Integration and Oracle Utilization

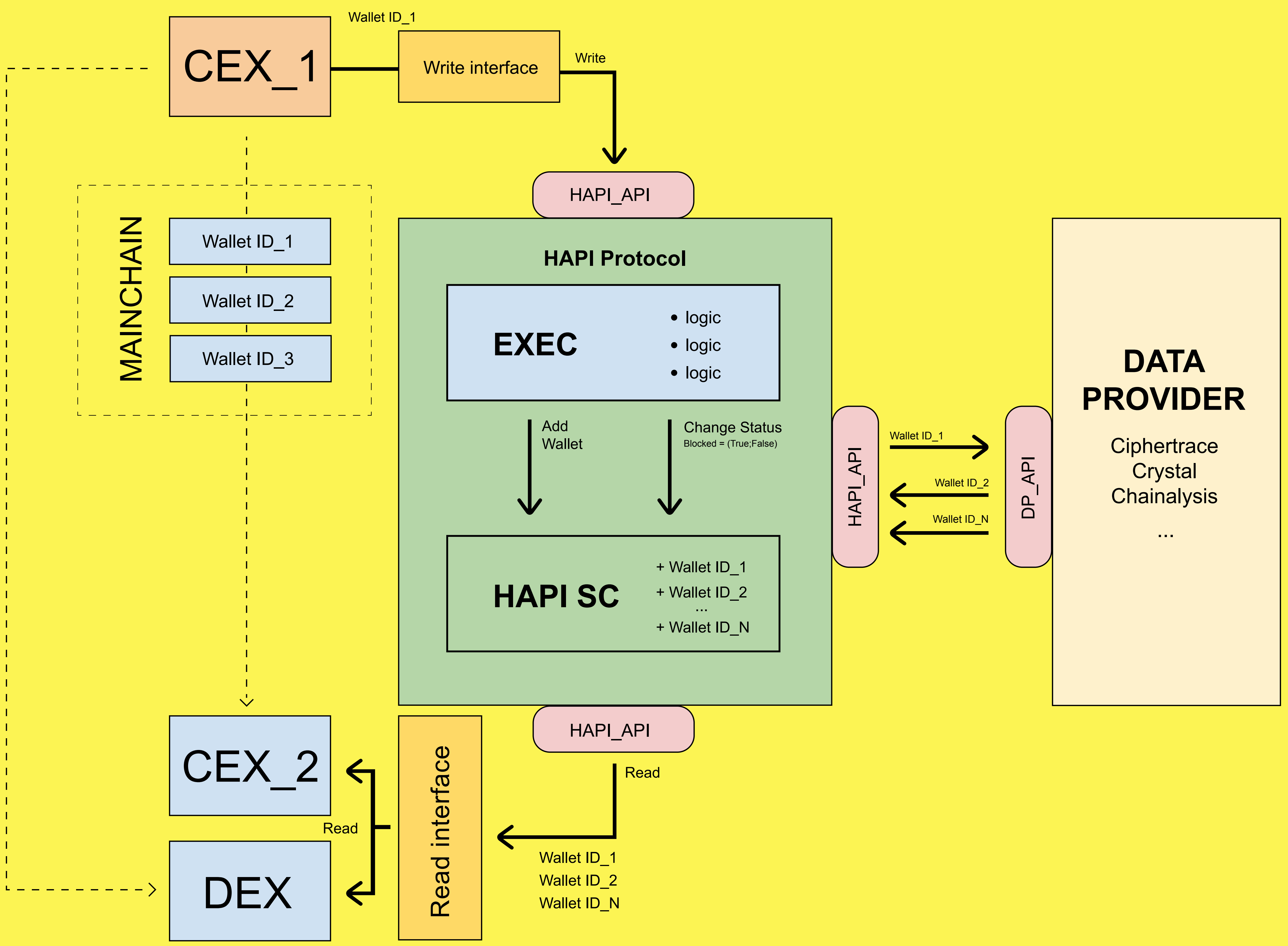
On the topic of smart contracts that are specific to the use case of HAPI namely cybersecurity facet. The smart contract will store a list of compromised blockchain addresses that customers can access to lock and/or refund transactions from such addresses for AML and CFT purposes. HAPI makes it possible to freeze the siphoning of the funds from a CEX (as an example) to a fraudulent wallet. This can be executed either on the side of CEX or, with a given consent from the operator, directly by HAPI protocol. The addresses will be reported by a set of trusted entities through oracles. These entities can be exchanges (they'll report known hacks), AML data providers (like Crystal or Ciphertrace; services that collect data on illicit addresses), approved tracers (services that track previously reported addresses for funds movement). HAPI customers are people who want to check their incoming (or outgoing) transactions for compromised addresses and can access this data via smart contract directly (DEXes, DeFi, etc) or through an API gateway (CEXes or other off-chain services).

Smart contracts will be managed by a governance subsystem, changes will be implemented by a committee (i.e. signed by a multisig). Some reporter methods can be called by the committee itself to report community-generated incidents.

Concept and Outline of The Main Framework of HAPI

For the convenience of exposition, we will order the operational sequence in the following way:

1. CEX 1 detects fraudulent transactions - hack that speedily turns into outflow of funds to the unknown wallet.
2. CEX_1 reports the even into HAPI Protocol that writes into the HAPI SC WalletID_1 to which the funds have been transferred.
3. HAPI Protocol analyses (based on the given metrics) a transaction and categorizes it in: Approved address WalletID_1 on the HAPI SC; Rejected inquiry of WalletID_1 on the HAPI SC
4. If the address is on the HAPI SC - HAPI Protocol sends WalletID_1 to DATAprovider in order to track and trace the upcoming transactional dealings from the same wallet.
5. DATAprovider via Oracles relays to the HAPI Protocol all of the nascent wallets on which the transactions are being transferred from the source wallet WalletID_1
6. HAPI Protocol analyses (based on metrics) wallet addresses Approved address WalletID_1 on the HAPI SC; Rejected inquiry of WalletID_1 on the HAPI SC
7. HAPI Protocol sends CEX_2 and DEX identificators of wallets from HAPI SC



Concept and Outline of The Main Framework of HAPI

An unlawful actor makes an attempt to send fraudulent funds on CEX 2. CEX 2 knowing the threat from the aforementioned wallet can expose it to the potential risk - blocks the transfer.
Unlawful actor makes an attempt to connect the address to DEX, DEX declines this attempt and/or completely blocks the wallet from making a transaction within DEX.

HAPI allows for CEX to promptly notify its users about fraudulence taking place via Write Public Interface. CEX receives data about fraudulent activity described above, with this data available CEX may not only deftly freeze the siphon of funds but also reactively respond and announce to the users to abstain from using the CEX functionality for the time being. In this quite simple yet convenient fashion, CEX garners not only additional “points” for trustworthiness but also guards its users against the potentiality of being exploited further.

The second aspect and further layer of security are security audits. HAPI lays the foundation of security solutions incrementally and security audits database plays a crucial role in building the edifice of the combined system of guarantee. The irrefutable benefit of creating a robust database of audited smart contracts is helping DEXes to categorize and segregate audited and unaudited smart contracts mitigating the risks of hacking.
The combination of the two above-mentioned approaches aids in creating a stout, secure, and safe environment that if not completely eliminates hacking invasion but drastically reduces and mitigates damages incurred from the attack while also blacklisting, learning from it with the help of machine learning, and preventing it from happening again.

Concept and Outline of The Main Framework of HAPI

Machine Learning implementation distinguishes HAPI from the current propositions on the market of security solutions. By utilizing a swath of machine learning algorithms, HAPI protocol will be able to acquire data, process it efficiently each time, and learn to detect the potential data-invasive, transaction-malfeasant emergence of an attack. In this vein, HAPI will operate not only as an act-on protocol but also as a preventive and preemptive operating one. Machine learning integration into blockchain-based solutions is quite a hurdle. In and of itself Machine Learning does benefit significantly from the centralization in so far as it is easier to accrue needed data and digest it more effectively. In the realm of decentralized cosmos, there is a visible roadblock on how to approach machine learning integration into cybersecurity solutions, namely HAPI protocol. Notwithstanding this aspect, we are currently tightly working with Machine Learning experts and have already gathered enough conceptual ideas and will be releasing a separate article dedicated to Machine Learning and its Role in HAPI Protocol.

HAPI Token Model and Utility Cases

HAPI token is the native digital token of the HAPI Protocol. HAPI token presents a transferable token of value that serves a subset of specific functions, utilities, and general intercommunication between the users of the Protocol. In essence, HAPI at the current stage of development is aimed at B2B solutions which by its nature exclude the general participants of the crypto market. The purpose of the HAPI token in part is thus to introduce community members uninitiated in the business scope to partake in the growth and fostering of the project. This is achieved by incentivization of “players” inside the communal milieu to take part in the so-called staking and farming initiatives and other activities directed towards expanding the community aspect and encouraging players to facilitate the
The main utility cases for HAPI token comprise the backbone of its validity.

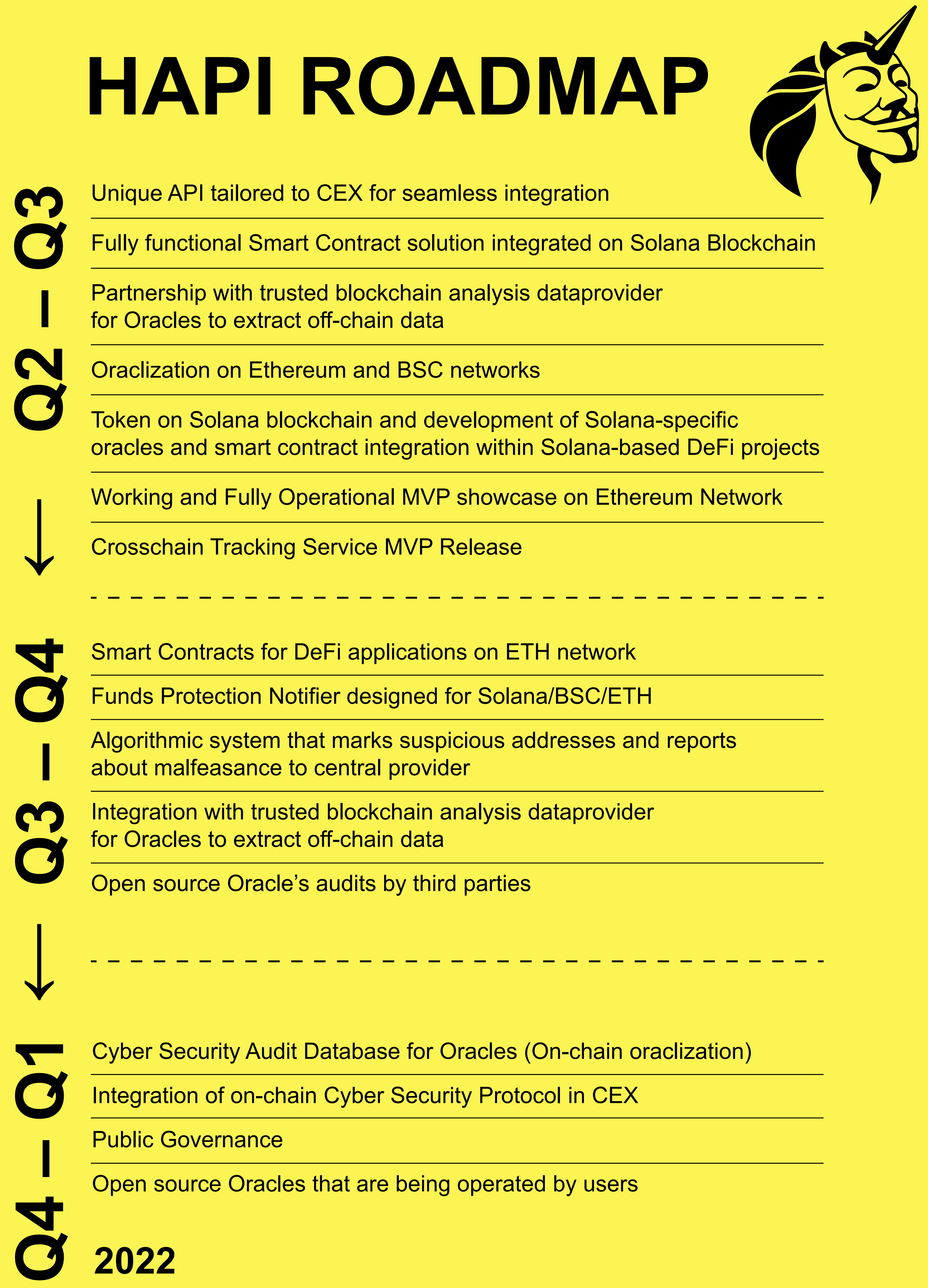
Token Utility：

- Data submission fee. Provides rights for the customer to submit any information connected with the hack or suspicious wallet.
- Governance. Provides governance rights for the Users (DP election by DAO). Each HAPI token stakeholder can participate in governance conducted by a voting procedure. The voting involves staking HAPI tokens to support or reject voting proposals.
- Oracle rewards. Serves as a payment method to Oracles for the review and audit work done on the submitted data.
- DeFi projects audit report submission. DeFi projects will legitimize their code by submitting it to a unified audit reports data center.

HAPI token doesn’t represent a share in the company or immediate involvement in the governance of the project’s endeavors. Instead, the HAPI token is a mode of payment within the Protocol that allows for seamless transfer of value, and exchange.

Roadmap and Plans for The Future

Current Roadmap reflects both already achieved milestones as well as what HAPI team is looking to deploy in the next quarter. Long term goals include: Public governance, security audit database, proprietary database of wallet addresses, machine learning implementation. The ongoing work and tight collaborative efforts with Solana has forced us to concentrate more on the Solana Blockchain integration. It also includes deployment of smart contract functionality on Solana and transfer of HAPI token on Sol.



HAPI ROADMAP

Q2 – Q3

- Unique API tailored to CEX for seamless integration
- Fully functional Smart Contract solution integrated on Solana Blockchain
- Partnership with trusted blockchain analysis dataprovider for Oracles to extract off-chain data
- Oraclization on Ethereum and BSC networks
- Token on Solana blockchain and development of Solana-specific oracles and smart contract integration within Solana-based DeFi projects
- Working and Fully Operational MVP showcase on Ethereum Network
- Crosschain Tracking Service MVP Release

↓

Q3 – Q4

- Smart Contracts for DeFi applications on ETH network
- Funds Protection Notifier designed for Solana/BSC/ETH
- Algorithmic system that marks suspicious addresses and reports about malfeasance to central provider
- Integration with trusted blockchain analysis dataprovider for Oracles to extract off-chain data
- Open source Oracle's audits by third parties

↓

Q4 – Q1

- Cyber Security Audit Database for Oracles (On-chain oraclization)
- Integration of on-chain Cyber Security Protocol in CEX
- Public Governance
- Open source Oracles that are being operated by users

2022

Risks

Participating in the sale of HAPI Token, purchasing HAPI Token and using any services offered by HAPI is fraught with significant risks and potential financial losses, including but not limited to:

- Features, functions, parameters and other qualities of HAPI Token («HAPI Token Qualities"),, as well as software, networks, protocols, systems and other technologies (including, if applicable, any blockchain) ("Base Technology") used for administration, creation, issuance, transfer, cancellation, utilization or processing of operations involving HAPI Token, may be technologically complex or difficult to comprehend or assess.

- HAPI Token and its Base Technology may be vulnerable to attacks targeting the security, wholeness or functionality of HAPI Token or its Base Technology ("Attack"), which may include Attacks employing computing power sufficient to suppress normal operation of the blockchain or another Base Technology.

- HAPI Token, HAPI Token Qualities or Base Technology may change or in one way or something cease functioning according to expectations due to changes made to the Base Technology, changes made using the features or functions embedded in the Base Technology, or changes brought on by an Attack. These changes may include, without limitation, "changes to the source code" or a "rollback" of HAPI Token or the blockchain.

Risks

- HAPI Token may be nullified, lost or spent, or lose most or all of its value in some other way as a result of changes to the source code, rollbacks, Attacks, changes to HAPI Token Qualities or inability of HAPI Token to function as intended.

- HAPI may pause or revoke access to services in the interest of complying with applicable laws and regulations, or if instructed by law enforcement or other governmental agencies, as well as other reasons, at the discretion of HAPI.

- HAPI Token may change in price or lose all of its value due to various factors, including discovery of unlawful behavior, market manipulation, changes to HAPI Token qualities or presumed value of Token Qualities, Attacks, as well as other factors, including, among other things, factors independent of HAPI.

- HAPI Token may decrease in price or lose all of its value due to legal or regulatory activity, or other actions made by law enforcement or other governmental bodies.

- Equally applicable to any other crypto asset, the risks outlined above may result in the loss of HAPI Token, a drop in or total loss of value of HAPI Token, inability to gain access or transfer HAPI Token, inability to trade HAPI Token, inability to gain financial benefits granted to holders of HAPI Token, and other financial losses.