



**AVARTA**



# **AVARTA** **WHITEPAPER**

Version 1.2

# CONTENTS

<b>Forward Statement</b>	<b>3</b>	NFT storage	16
<b>Abstract</b>	<b>4</b>	Third-party integration	17
<b>Background</b>	<b>6</b>	Recovery in case of emergency	17
Logging in: if only it were that easy	6	<b>Token Utility</b>	<b>18</b>
Overcollateralization: draining DeFi appeal	7	Staking	19
Increased Regulation	8	Avarta Token Sale & Distribution	20
Opportunity	8	<b>Roadmap</b>	<b>21</b>
<b>Trust Score</b>	<b>10</b>	<b>Team &amp; Advisors</b>	<b>22</b>
Detailed use case: Peer-to-peer Blockchain lending	11	Advisors	24
<b>Avarta Network</b>	<b>13</b>	<b>Disclaimers</b>	<b>25</b>
Best in class security	14	The Tokens	25
Single sign-on	16	Avarta Platform	28
Cross-chain yield optimization	16	Definitive Documentation	28
DeFi integration	16	Indemnity and Limitation of Liability	29
		Future Statements	29
		Risk Disclosures	30



# FORWARD STATEMENT FROM THE CHAIRMAN

To all valued members of the blockchain community,

The blockchain world has seen an exponential growth in participation and its users since 2017. As an ecosystem, it has provided cutting edge technology and user cases that can help the wider public. Recent innovations such as Decentralized Finance (“DeFi”) and Automated Market Makers (“AMMs”), if adopted in the right manner, can provide great utility and positive change to traditional banking and capital markets.



The growth of blockchain and its associated technologies must be augmented by better security to protect both blockchain’s users and its communities. To achieve critical mass adoption amongst the wider public, there must be a balance between regulators, privacy preservation and the ease of use to achieve such security. As of the end of June’21, the total market capitalization of the cryptocurrency market stands at close to US\$ 1 Trillion; this is 10 times the size of the market compared to 4 years ago which stands at close to US\$100 Billion. With so much more capital and liquidity in the market, authentication in a decentralized manner takes on increasing importance for all participants.

This is one of our main motivations for launching the Avara blockchain project. We aim to create a leading project that serves to help improve current issues around whitelisting, collateralization on DeFi lending and authentication for major blockchain participants. As such, our project can provide a fundamental security layer for Level 1 (“L1”) infrastructure protocol layers, DeFi lending platforms and Centralized Exchanges. By working with end consumers and blockchain’s major players, I am of the firm belief that we can make the blockchain world a better place.

All successful projects start with a strong purpose to solve problems for society, and it takes an equally strong team to bring the vision to life. With Avara, we hope to add significant value on the security and authentication front, especially so in the blockchain world.

Yours Sincerely,

A handwritten signature in black ink, appearing to read 'Prince Abdul Qawi'.

**Prince Abdul Qawi**

Office of His Royal Highness Pengiran Muda Abdul Qawi of Brunei Darussalam



# ABSTRACT

Avarta addresses authentication and identification challenges that pervade both traditional and blockchain applications. As blockchain matures and cryptocurrency projects are looking for identity solutions, they find themselves stuck with either pseudonymous solutions or centralized customer identification programs. Powered by patents, Avarta is a 4-in-1 solution for DeFi and blockchain whereby your face is your private key to multiple blockchains.



## OUR CORE FEATURES ARE:

1. Biometrically-secured, multi-chain blockchain wallet
2. Anti-bot mechanism for public DEX listing
3. Multi-signature wallet for corporations and legacy planning
4. Multi-chain, decentralized identity management with risk based scoring mechanism

Avarta provides crypto companies and the blockchain industry established standards of authentication and proof of identity that serve the industry, rather than adopting outdated standards from centralized institutions.

Avarta provides a military-grade security enabled identity wallet that allows people to control their private keys conveniently. Avarta's cross-chain support means that cryptocurrency users can consolidate all of their cryptographic keys in one wallet that requires no passwords, no seed phrases and no need to write down the keys in a safe (or not-so-safe) location. Using a combination of biometrics and device data, Avarta is able to create a trust score with a military-grade level of authentication assurance, creating a completely secure wallet for users.



The Avarta system is designed to be used for Decentralized Finance (DeFi) applications. One of the drawbacks of blockchain's trustless nature is that a person doesn't retain a reputation or credit rating. On top of that, the fluctuations in the price of cryptocurrency represent a risk when it comes to lending or investing against a cryptoasset. As a result, DeFi applications often need to overcollateralize to compensate for fluctuations and for the fact that there is no identification of the investor or borrower.

By creating a unique, secure identity, as well as a way to store a person's full transaction history, Avarta allows an individual to prove they are a reliable investor, lender, or borrower, giving them access to services based on trust—similar to a credit rating. Unlike centralized credit ratings, however, Avarta gives full control to the user. The user can determine when and how to expose their information, and they can remain anonymous if that is allowed by the platforms they use.

Avarta's mission is to create a secure, private and user-controlled authentication layer that puts the full power of the web into users' hands.



**WITH AVARTA, YOUR BIOMETRICS ARE YOUR OWN PRIVATE KEYS.**

# BACKGROUND

## LOGGING IN: IF ONLY IT WERE THAT EASY

Password fatigue has been an issue for years, but in the crypto world, the problem is compounded by complex private keys, seed phrases, and non-custodial wallets that put 100% of the responsibility for remembering those phrases on the user. While this takes control from banks and puts it in the hands of users, the downside is the loss of funds. It is estimated that approximately 20% of Bitcoin, or approximately \$140 billion, is inaccessible due to the loss of cryptographic keys by users. [1]

Privacy and control are some of the main advantages of using cryptocurrency, so people don't want to use centralized exchanges or custodial wallets. But even non-custodial wallets are susceptible to attacks such as reverse proxy phishing, cryptojacking, dusting, and clipping. [2] As cryptocurrency gains momentum, the need for user-friendly and highly-secure authentication methods is growing. Blockchain wallets are poorly protected. Metamask, the most common Ethereum wallet in DeFi, uses a simple password login and is vulnerable to a variety of attack. [3]

Cybercrime accounted for more than \$3 billion in losses in the crypto market, with the most lucrative target being cryptocurrency wallets, with an average of \$112 million per wallet hacking event compared to about \$10 million per attack on Ethereum apps or exchanges. [4] With the amount of money at stake growing rapidly, making wallets safe is a huge priority for the industry.

Passwords have long been a security risk and inconvenience. For increased security and better user experience, the industry is moving to biometrically-powered authentication. Gartner predicts that by 2022, 60% of large and global enterprises and 90% of midsize enterprises will implement biometrically-powered methods in more than 50% of use cases. [5]

1. 20% of All Bitcoin Is Lost, Unrecoverable, Study Shows, Nathan Reiff, Investopedia, June 2019. Cryptocurrency
2. Attacks to Be Aware of in 2021, Photon Research Team, digital shadows.
3. 6 Ways a Site Can Attack Your Metamask, Shannon Wu, Bloom, February 2018.
4. Cryptocurrency Hackers Steal \$3.8 Billion in 2020, Will Neal, Organized Crime and Corruption Reporting Project, January 2021.
5. Embrace a Passwordless Approach to Improve Security, Gloria Omale, Gartner Group, January 2019.



Truly biometrically-powered authentication does not require the user to remember any type of password. Keys can be stored on people's mobile devices and unlocked with biometrics. The most commonly used biometrics are facial scans, retina scans, and fingerprint scans, but today's technologies can also record people's unique heart rate patterns, gait, and other types of biometrics identified by wearables. Interactive Voice Recognition (IVR) and call recording systems have been using voice recognition for years so that as someone is giving their identifying information over the phone, the systems simultaneously match their voice patterns and flag suspicious activity. Mass adoption of biometrics and the almost complete disappearance of security concerns among consumers have eliminated the barriers to implementation. [6]

Avarta provides the solution to this with our military-grade solution that is patented both in the USA (United States Patent: No.10,277,603) and in South East Asia (Malaysia Patent: No. MY-176069-A) covering the ability to authenticate a transaction in a multi-faceted manner.

## OVERCOLLATERALIZATION: DRAINING DEFI APPEAL

DeFi lending has been one of the exciting applications of blockchain technology. The ability to take out middlemen such as bankers has provided opportunities for borrowers and lenders alike. However, using cryptocurrency to collateralize these loans exposes the lenders to the risk associated with cryptocurrency volatility. As a result, lenders require additional collateralization. For example, MakerDAO requires 150% collateralization and Compound also requires extra collateralization. In many platforms, if the collateral loses value too quickly, the loan can automatically be called by the smart contract.

Overcollateralization creates inefficiency, with cryptocurrency being tied up in these loans when it could be invested elsewhere. One of the potential solutions would be to create some kind of credit score for the participants in DeFi vehicles. However, investors who prefer anonymity or use pseudonymous cryptographic addresses simply have no way to build up a credit score or reputation as reliable traders. Traditional credit ratings don't have direct applications in the crypto and blockchain world, and there are yet to be any established standards or best practices for crypto assets.

6. Login Preferences Among Older Adults, Hypr.





## INCREASED REGULATION

In an attempt to limit the pervasiveness of cryptocurrency use to launder money, the Financial Action Task Force (FATF) extended its definition of the Travel Rule to cover Virtual Asset Service Providers (VASPs) <sup>[7]</sup>, which include cryptocurrency exchanges and other financial cryptoasset service providers. The Travel Rule is a product of FinCEN, the U.S. regulatory agency responsible for enforcing the Bank Secrecy Act. It was created in 1995 and requires that financial institutions transmit certain information on certain funds transfers and transmittals to other institutions. In 2019, FATF, a global money laundering and terrorist financing watchdog, extended the mandate to cover cryptocurrency transactions – the implications of which have yet to be fully understood. It is possible that platforms that were thought to be previously exempt are now being recognized as potential violators of this rule, including decentralized exchanges (DEXs) and DeFi projects.

Because of the way such protocols and programs interact with individuals, they are unable to record the information necessary to fulfill the language of the Travel Rule. Without substantial changes to the way they do business, they may find themselves operating in violation of international laws. Thus, a wallet solution that can help solve this issue could have added significant value and pave the way for decentralized financial service providers to continue to operate in compliance with international money laundering laws.

## OPPORTUNITY

The DeFi industry is growing rapidly and as it matures, solutions are required for developing trusted systems for authentication and reputation. While the “trustless” slogan has been touted for blockchain, the idea behind it is that trust is designed into the system so that people don’t have to know the person on the other end of the transaction.

7. FATF: Most countries have yet to implement anti-terrorism crypto ‘travel rule’, M Lim, June 2021, Forkast,



To build that trust, the following elements will become fundamental in DeFi:

### **RELIABLE AND SECURE AUTHENTICATION.**

*Trusted wallets need to secure people's information and identities. Users need seamless and biometrically-powered authentication that reaches the same security levels as banking and other financial systems. Without a centralized banker that insures funds, the security needs to be even better.*

### **TWO-WAY AUTHENTICATION AND TRANSACTION VERIFICATION.**

*In today's blockchain systems, people simply send money from one wallet to another. There's no way to send a confirmation signal to accept funds or other type of handshake between people to make sure they are really sending to the right person and the right wallet.*



### **CRYPTO CREDIT RATINGS OR BACKGROUND CHECKS.**

*Unlike centralized credit ratings authorities, the DeFi model of credit scoring will be based more on transparency of interactions, the ability of individuals to check one another's credit worthiness, and certifying bodies. Creating aggregate wallets that allow users to store transactions over multiple chains can enable this kind of decentralized credit ratings. [8]*

### **KYC FOR NON-PERFORMING LOSS (NPL).**

*Asset tracking and appropriate measures for tax and compliance purposes need to be implemented so that people can maintain their accountability to their jurisdictions. Financial institutions will increasingly be picking up on the DeFi trend and requiring additional services in order to secure their transactions.*

Security is key for this industry. Blockchain is rapidly expanding beyond the \$2 Trillion mark, and many predict that DeFi will overtake traditional banking. Tooling for the industry must include security and data privacy solutions.

The combination of biometrically-powered technology, blockchain, and regulations protecting investors is enabling a new wave of applications that provide the security and infrastructure for a new financial system.

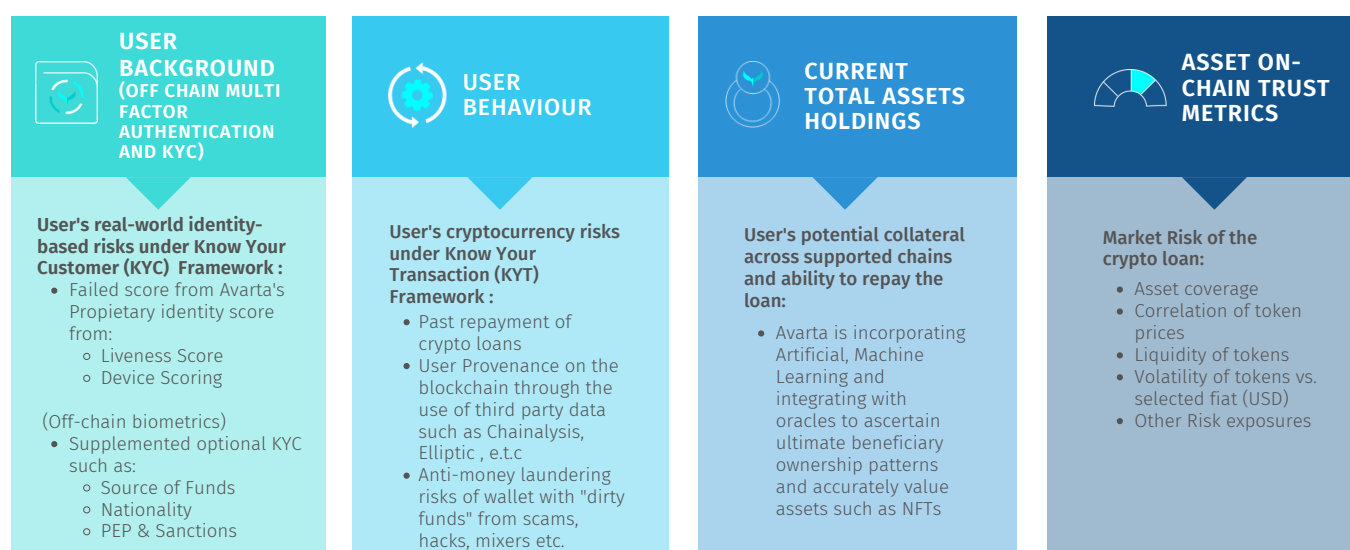
8. DeFi's Critical Missing Piece: Credit Scores, Rafael Cosman, CoinTelegraph, April 2021.

# TRUST SCORE

## AVARTA TRUST SCORE

Avarta leverages data collected by people's mobile devices to create the Avarta Trust Score for a safer and more equitable world. The storage and control of transactions by the user enables cryptocurrency traders and investors to develop credit histories that increase efficiencies across the DeFi space.

Avarta uses an amalgamation of on-chain and off-chain risk parameters to obtain a Avarta Trust Score for the user. The Avarta score which is bucketed into quality ranges (A,B,C,D etc) can be used by the user for any DeFi lender/ counterpart for credit assessment purpose. The Avarta Score can also be driven by the needs of certain DeFi/ non-DeFi lenders based on their own risk based parameters. The non-exhaustive list of risk parameters (not exhaustive and constantly being refined) that will feed into the score are:



As Avarta creates the data layer to allow the risk-based scoring to be performed, the wallet enables the users to preserve their transaction history and to send it to any third party. In a decentralized environment, different independent certification agencies can emerge, creating different types of credit ratings or ranking on people's reliability as lenders, borrowers and traders. The Avarta system will provide ways for people to export their trading history to other authorities, either in part or whole. For example, if someone wants to prove their holdings in just one currency, or show all of the collateralization current on the portfolio, they could expose just that information. Credit rating agencies could require full or partial history, depending on the types of transactions.



## **DETAILED USE CASE: PEER-TO-PEER BLOCKCHAIN LENDING**

Peer-to-peer loans have been one of the longest-standing use cases discussed in the cryptocurrency industry. Peer-to-peer loans can take a number of formats: collateralized and non-collateralized loans. To date, only collateralized loans have been possible because of the lack of credit ratings and true identities in the blockchain DeFi applications. Following is a case for a collateralized crypto loan.

A crypto-backed loan is a collateralized loan that a user receives through a crypto exchange or other crypto lending platform. DeFi collateralized loans have been extremely popular, allowing people to make investments and increase their income.

Lending in DeFi most often uses tokenized pools to aggregate liquidity, which streamlines the business process for borrowing. One does not have to source potential lenders or negotiate the interest rate since there is a single entry point for all loans, and the interest rate is determined algorithmically from market conditions. Some of the largest protocols include Compound, Aave, dydx and MakerDAO.

Key characteristics of DeFi loans are as follow:

### **PERMISSIONLESS**

Anyone can borrow cryptocurrencies without having to undergo KYC or get permission from a third party.

### **AUTOMATED**

Loans are automatically dispersed through smart contracts, with positions being liquidated if a collateralization ratio falls below the predefined threshold.

### **NON-CUSTODIAL**

With DeFi loans, there is no need to transfer ownership of the underlying collateral. All funds are secured by smart contracts, with the borrower being responsible for maintaining that position.

### **SECURE**

Major borrowing protocols have been rigorously audited, meaning that funds supplied to loans are backed by the most robust code in the world.

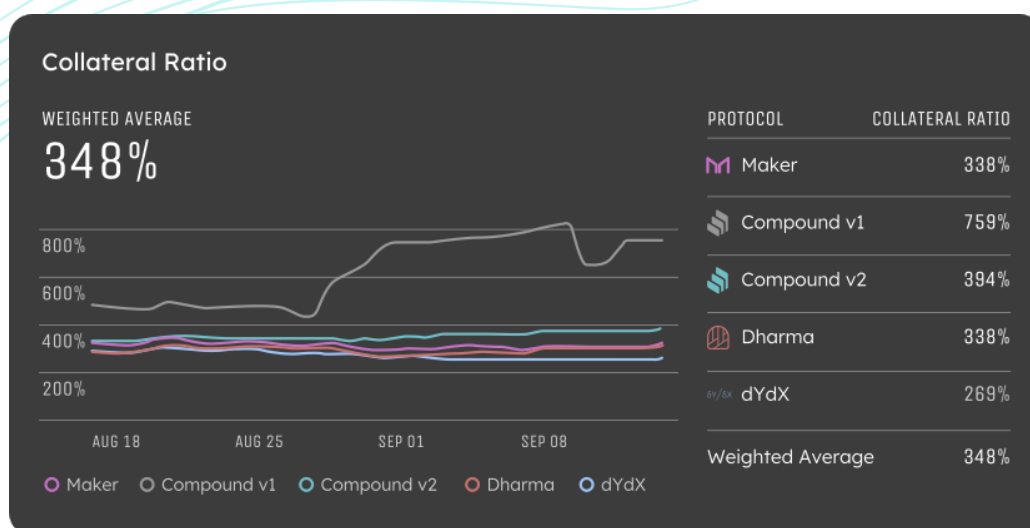
## DYNAMIC

The vast majority of borrowing in DeFi leverages variable interest rates which shift relative to the utilization ratio of any given asset.

## PERPETUAL

DeFi loans can be opened for any amount of time, so long as the debt is paid back and the position is sufficiently collateralized

However, one unique feature for Defi is that it is usually overcollateralized which reduces the lenders' risk. However, this overcollateralization reduces the attractiveness of borrowing assets.



Source: Loanscan

One of the reasons for over-collateralization is that the borrower's identity, credit history, and other assets are hidden to the lender. However, with Avarta, a lender could ask for additional information. For example, if the lender sees that the borrower has a valuable collection of NFTs, they could make a loan based on basic collateral, and monitor the wallet on a regular basis, just to make sure that the borrower still has a liquid position. The lender knows that the borrower is "good for the money" even if there is a decrease in the value of the collateral. In case the cryptocurrency rates drop and the borrower needs to put in more collateral, the lender can make a request to the borrower and they can settle or have the loan cash out automatically. If the borrower has a good borrowing history, this increases the lenders' assurance that they are taking a reasonable risk.

The use case above discusses collateralized loans, but Avarta envisions that over time, with the use of the Avarta scores and third-party applications, it will be possible to create decentralized financial institutions that are able to take risks based on credit history, providing peer-to-peer loans without collateral.

# AVARTA NETWORK

With our mission in mind, the Avarta Solution also consists of a seamless, biometrically-powered, multi-chain wallet that stores people's cryptographic keys and transaction histories, eliminating cryptocurrency loss due to security breaches, cryptographic key loss, or forgetting of seed phrases. The wallet acts as the secured gateway into the blockchain and crypto world with an unparalleled intuitive user experience feeding in data into the Avarta Protocol.

Avarta is based on a decentralized blockchain devoted to identity and privacy solutions. The Avarta Network includes:

## **PATENTED BIOMETRICALLY-POWERED MULTI-FACTOR AUTHENTICATION**

Avarta combines biometrics and device data to create an authentication score that ensures that only the actual wallet holder can access their information.

## **ADVANCED SECURITY**

The security provided is strong enough to be trusted with financial accounts and personal data.

## **MULTI-CHAIN PROFILING**

Single-sign-on (SSO) capabilities enable users to hold one wallet and be able to manage their cryptographic keys across multiple blockchains and dApps. The ability to facilitate transactions over multiple blockchains will allow the consolidation of transaction history to a cohesive credit score that can be ported across different DeFi apps.

## **LOCAL AND AVARTA STORAGE**

Keys and data are stored locally with the user and with Avarta storage. Only a successful authentication can allow a transaction by the authenticated Avarta user.

## **PASSWORD MANAGEMENT**

Multiple cryptographic keys are seamlessly and securely stored in one place.



## TRANSACTION HISTORY

Maintaining the transaction history of the user is core to the future of DeFi capabilities to work across applications and blockchains. By understanding a user's total net worth, trading income, lending and borrowing history, and trust history, DeFi applications can compose trust assessments and provide services to individuals tailored for their capacity for making trades, taking loans, lending to others, etc.

Avarta holds all of the person's blockchain private keys for a single-sign-on (SSO) experience for all cryptocurrency applications. Because it can only be unlocked through recognizing the specific person, device and behaviors, the Avarta wallet is completely secure and the user never has to remember complicated passwords or answer security questions.



### KEY FEATURES OF THE AVARTA WALLET:

- Decentralized multi-chain user-controlled wallet
- Free to use
- Earn rewards and yields for use
- Biometrically accessible
- Multi-factor authentication
- Military-grade security
- Passwordless sign-in
- Single sign on
- Safekeeping of cryptoassets
- Tracking of all DeFi applications
- DeFi Integration
- Cross-chain yield optimization
- NFT storage
- Enterprise-grade
- Insurance coverage
- Compliance-ready
- Anti-bot mechanism for IDOs
- Multi-signature capability
- Risk- based scoring

## BEST IN CLASS SECURITY

The patented biometrics solution is at the core of the Avarta technology. Avarta has developed technology that identifies people as well as—or better than—humans identifying one another. By combining a multitude of factors that are collected through an individual's device, Avarta provides authentication that simply cannot be reproduced by anyone but the individual who owns the wallet.

Mobile devices carry a tremendous amount of information on everyone including voice patterns, gait, the way someone holds the phone, taps and swipes, etc. In addition to the personal information, the device itself is unique in terms of the model, battery life patterns, location, storage, etc. Combining information on the phone plus the individual is enough to create an extremely high level of confirmation that a person is who they say they are. Not only that, but a facial scan or fingerprint set can be compared to databases of other biometrics and confirm that the person is unique and not using anyone else's data. Such databases are now used regularly for border control. People's privacy is preserved because biometric scans are not stored as raw data but rather as hashed patterns, called templates, that represent a unique person's print. Because the hash is always performed the same way, matching hashes indicate a print is the same person.

The Avarta Score generated is a unique composite score calculated by the AI-powered synthesis of authenticating each user by multiple means. Avarta can also be used to create a unique user template based on industry standards for biometric templates and compare identities to make sure that someone does not have duplicate identities.



#### **AVARTA USES A COMBINATION OF BIOMETRIC AND DEVICE SPECIFIC DATA, INCLUDING:**

- Facial Recognition
- Device analytics, such as the specific device model, internal components, installed apps, speed, etc.
- Device usage behaviors, such as the number of contacts, the regular movement patterns of the particular user, battery life, geolocation, etc.
- Sudden or multiple changes in the devices attributed to a particular user.
- User-device behaviors, such as speed of swipe, weight of tap, usage patterns of the applications etc.

Through the Avarta Platform, users create an "Avarta" of themselves with their wallet address and can choose which information forms part of their digital identity. Users are required to choose a minimum amount of data for a secure score, and some information is built into the device itself. For obvious reasons, this whitepaper does not reveal the exact combination of inputs that Avarta uses to authenticate.

## SINGLE SIGN-ON

As described within the previous features, Avarta knows who the user is at any given time. The Avarta app operates as an agent to log in to any dApp or exchange where the user is registered. Avarta maintains a secure registry of the keys, provides the authentication, and logs in on their behalf.

Single sign-on (SSO) means that users do not need to spend any time finding their passwords—they can work seamlessly with no interruption and Avarta makes sure everything simply works.

## CROSS-CHAIN YIELD OPTIMIZATION

By providing a single wallet with multiple chain logins, Avarta enables cross-chain asset optimization through DeFi exchanges. Investors can leverage the cross-chain capabilities of Avarta to assess and optimize cross-chain yield farming, staking, and other investment opportunities. Third parties can create a variety of apps to leverage these cross-exchange and cross-chain visibility capabilities.

## DEFI INTEGRATION

In addition to the Avarta wallet, Avarta's authentication service is available as an SDK for integration with blockchain, DeFi and other types of applications that require single-sign-on, identity, or biometrically-powered authentication. Avarta provides tools for developers to integrate this technology into their dApps to replace less secure or difficult-to-use login capabilities.

## NFT STORAGE

The Avarta wallet allows the holding and tracking of NFTs being held by the user. Avarta holds the private keys and the logins to marketplaces for NFTs, allowing the Avarta users to access, display, trade and prove ownership of their NFTs, artworks, collectibles and assets.

Non-fungible tokens are growing in importance in terms of their value, not just as art objects but also as proof of ownership of real-life objects. <sup>[9]</sup> NFT holdings indicate the value of people's portfolios, and therefore are a key part of creating credit ratings and investor profiles.

9. Mattereum: Enabling NFTs for Physical Assets.



## THIRD-PARTY INTEGRATION

Through integration with various third-party information, Avarta can provide a range of DeFi services that can leverage the information that users collect on their own transactions to give them a crypto-based identity and reputation.



### SERVICES THAT COULD BE PROVIDED BASED ON THE INTEGRATION INCLUDE:

- Unique identity services (based on templates that can be compared to other individuals in a database)
- Know Your Customer integrations to other services
- Integration with Web 2 and other services
- Wallet risk scores and counterparty transaction risk assessment
- Trader rankings and success scores

Users can choose the information they release to trusted parties, gaining access to specific services, whitelisting, and acquiring favorable interest rates.

## RECOVERY IN CASE OF EMERGENCY

Because the Avarta system is heavily dependent on biometrics and there is no custodial operation to recover data or keys held under Avarta wallets, it's necessary to implement a recovery methodology that is verifiable in the case that someone has incurred an injury that would prevent them from opening the wallet. The person can designate up to seven other people who have Avarta profiles and who would be able to open the wallet, either as individuals or by agreement (a minimum of 3 of five people for example) in case of the person's death or injury. The person could set a minimum amount of time between their final login with their own credentials and the release of the keys to custodians. For example, if someone suffers a stroke and is unable to log in because their facial, voice and physical attributes were significantly altered, there could be a 30 or 60 day minimum wait time before the people they designated as custodians would be able to open the wallet.



# TOKEN UTILITY

AVARTA is the cryptographic token on the Avarta ecosystem. The token serves as a pay for use for all services and transaction, as well as rewards tiering and governance within the full Avarta ecosystem and its associated solutions.

As the central tenet to the Avarta ecosystem, the AVARTA token serves multiple purposes within the ecosystem. The key pillars on supporting the Avarta ecosystem is detailed in the diagram below:

## AVARTA TOKEN USE CASES

### AVARTA TRUST SCORING

- Borrow and save digital assets at special rates unlocked by Avarta's Trust Score technology
- Gain priority access and secure larger investment allocations for new projects with a higher Trust Score

### WHITELISTING

- Allows for streamlined access to DeFi projects on pre-whitelisted wallet addresses through the Avarta layer
- Priority of access through Avarta KYC'ed Wallet layer

### GOVERNANCE

- Tokens confer voting rights to make decisions on decentralised governance processes
- Allows users to continue to have a voice and guide the future direction of the project

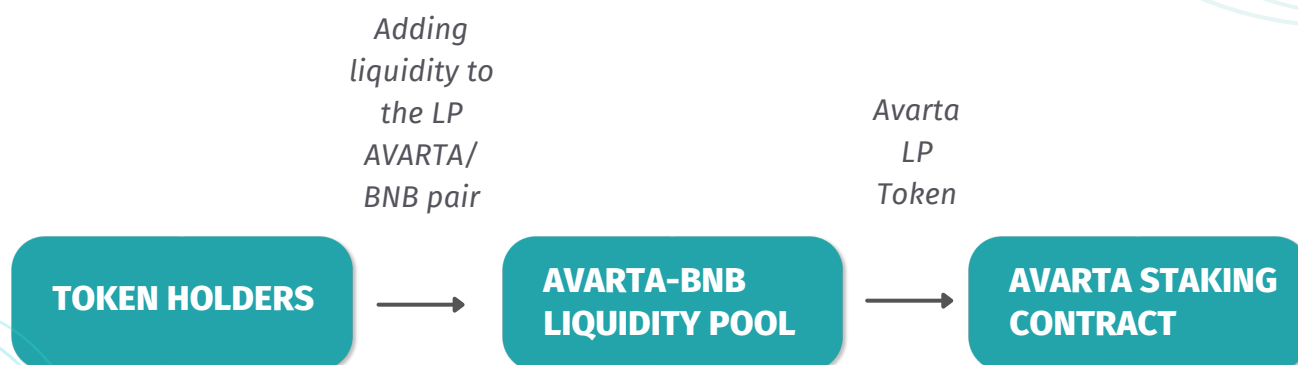
### BIOMETRICS WALLET

- Bring together multiple wallets from multiple chains into a single, non-custodial wallet service
- Swap digital assets with each other
- Stake digital assets on DeFi protocols



Based on the model above, applications and users can interact with the Avarta ecosystem through the use of Avarta's tokens. With a limited supply of tokens and the increasing utility of the suite of solutions, we expect a constant and upward demand for AVARTA tokens. Please refer to the Avarta Token Utility Paper for a deeper understanding of Avarta Token Use Cases.

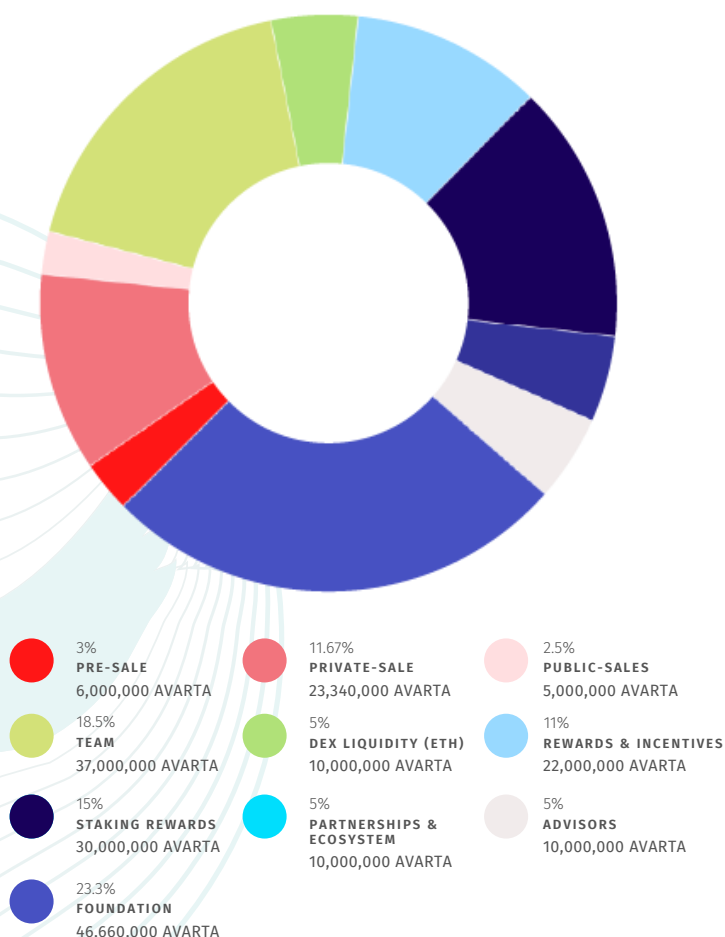
## STAKING



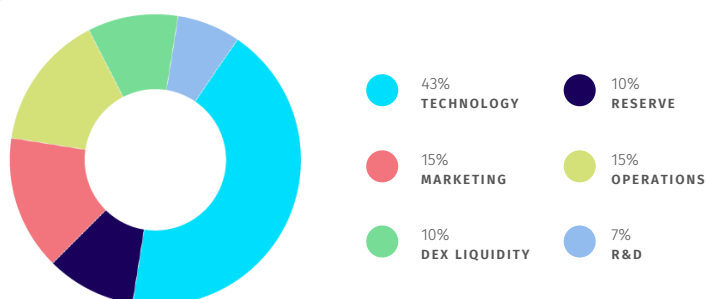
AVARTA can be earned when participants add liquidity to Avarta's DEX liquidity pool. Avarta will create a staking contract that is activated when LP shares generated from liquidity providers are deposited into the AVARTA staking contract. AVARTA is paid into the staking pool and earned by LP miners based on their pro-rata share in the staking pool.

## AVARTA TOKEN SALE & DISTRIBUTION

Tokens created by the contract will be distributed based on the following:



### USE OF PROCEEDS



Contributions received from the token sale will be used according to the above breakdown. These percentages are subject to change at any moment and provided as an approximation.

VESTING	
Pre-Sale	7% at listing. Linear vesting over 12 mo. thereafter (Weekly Vesting)
Private Sale	10% at listing Linear vesting over 9 mo. thereafter (Weekly Vesting)
Public Sale	40% at TGE Linear vesting over 1 mo. thereafter (Weekly Vesting)
Team	6 mo. cliff Linear vesting over 18 mo thereafter
DEX Liquidity	6 month lockup
Incentives and Rewards	Released as per actual incentives given
Staking Rewards	Release as per actual staking APRs
Partnerships and Ecosystem	2 mo. cliff Released as per actual incentives given
Advisors	6 mo. cliff Linear vesting over 18 mo thereafter
Foundation Reserve	1 mo. cliff Equal vesting over 24 mo. thereafter





# ROADMAP



## 2021' Q2

*Pre-sales Round Completed. Biometrics layer validation*

## 2021' Q3

*Start build of Avarta Wallet. Release of Whitepaper*

## 2021' Q4

*Launch of IDO. Proof of Concept and Technical Solutioning for Production Wallet*

## 2022' Q2

*Working with Tier 1 protocol layers. Testnet Avarta Wallet with 5 chains.*

## 2022' Q3

*Mainnet Avarta Wallet with 5 chains. First version of Avarta Trust Score Methodology.*

## 2023'Q2

*Testnet implementation of Trust Score Methodologies, Avarta Wallet to include new features such as Cross Chain Token Swaps etc*

## 2023' Q4

*Development of more Avarta Wallet features, Trust Score to be implemented in Wallet under limited release*

# AVARTA TEAM



**PRINCE ABDUL QAWI  
OF BRUNEI**

*Chairman  
Technologist and Angel investor*

*Prince Abdul Qawi is the chairman of the National Insurance Co Bhd of Brunei. He has invested in multiple projects previously in high profile listed and non-listed companies.*



**MATTHEW  
AINSCOW**

*Chief Executive Officer  
Serial Tech Entrepreneur*

*As an investor and experienced investment professional, Matthew has had successful tech exits. He also holds patents in biometric platforms and authentication.*



**HONG LOON  
GAN**

*Chief Operation Officer  
Experienced Entrepreneur*

*Hong Loon, CFA certified, is a serial entrepreneur with a strong financial background. He has experience in Deutsche Bank, MUFG and a leading family office advising governments and central banks.*



**JORDEN  
SEET**

*Chief Technology Officer*

*Jorden was previously from Standard Chartered's Digital Assets team, BMW Group's Blockchain Engineering team and J.P. Morgan's Software Engineering team. He has won several global hackathons and was the lead author for a peer-reviewed technical paper on enhancing consensus mechanisms via quantum computing techniques.*



**MICHAEL  
TAN**

*Chief Security Officer*

*Michael has over 15 years of experience in both private and public sectors, providing assurance and advisory services particularly on ethical hacking and has helped his clients improve their cybersecurity defences*



**BELINDA  
LIM**

*Chief Marketing Officer  
Blockchain Author*

*Belinda is the highly acclaimed Author of "Blocklass". A five year veteran, she had advised several blockchain startups. She is also a Certified Anti-Money Laundering Specialist (CAMS).*



**PAVLOS  
JOSEPH**

*Head of Partnerships*

*Pavlos has an extensive network in the world of blockchain and cryptocurrency. He is the leading advisor to Lydia-capital, a blockchain VC that takes early stage positions.*



**ARTUR  
NIKI**

*Security Engineer*

*Arthur is an experienced cyber security specialist. He has previously worked with several blockchain projects; achieving compliance with local laws and developing secure approaches for business processes.*



**DANIEL  
TEWELDE**

*Head of Community*

*Daniel is a veteran blockchain advocate. He has been instrumental in community roles for projects including RSK and Fantom.*



**ROSS  
GRUBI**

*Business Development Manager*

*Ross has over 10 years of experience in creator economy and gaming, primarily focused on marketing and partnerships. He has previously worked with several blockchain projects and leading esports brands.*



**VANESSA  
TANG**

*Director of Marketing  
(Asia)*

*Vanessa has extensive experience in differing sectors in crypto, finance and tech. She specialises in creating strategic solutions and leading dynamic digital and social campaigns based on consumer insight and data.*



**ZACH  
SOILEAU**

*Director of Marketing  
(North America)*

*Former global social media manager and product marketing manager for Cardano founding company, Emurgo. Growth marketing consultant for several DeFi and NFT launches, and community manager with CipherTrace.*

## ADVISORS



**HOCK LAI  
CHIA**

*CEO of Switchnovate*

*Hock Lai is the CEO of Switchnovate, co-chairman of the Blockchain Association Singapore. He is the former (founding) president of the Singapore Fintech Association.*



**BARRY  
HERBST**

*Blockchain Aficionado & Investor*

*Barry brings significant relationship-building across a diverse and holistic global network. His experience as both a Blockchain Aficionado & Investor allows him to understand projects intimately from both a strategic and technology standpoint.*



**VINSON  
LEOW**

*Founder of CRT Capital*

*Vinson is a veteran of advising blockchain projects. He brings a rich history of successful listings and community building as founder of Crypto Round Table as well as his own entrepreneurial achievements.*



**LESTER  
LIM**

*Founder of X21 Digital*

*Lester incubates and supports promising projects via his immense resources & connections in the blockchain ecosystem. He is also Advisor to Pinknode, Blank wallet, Polkafoundry, MahaDao, and many more.*



**RODERICK  
MCKINLEY**

*CFA Tokenomics Advisor*

*Roderick is a CFA Charterholder with 10 years' experience spanning infrastructure finance; start-up funding; and operational finance. He has advised 20 blockchain projects by sharing his tokenomic design services and strategic guidance.*





# DISCLAIMER(S)

---

This Whitepaper provides a summary of the main features of Avarta, the tokens to be issued by Avarta (the “Tokens”) and the Avarta platform. It contains general advice only and has been prepared without taking into account any participant’s objectives, financial situation or needs. Prospective participants should read the Whitepaper carefully and assess whether the information is appropriate for them in respect of their objectives, financial situation and needs. Any and all information as well as material provided in this Whitepaper are for informational and discussion purposes only, and should not be relied upon, either wholly or partially, when making any decision. Prospective participants should independently verify the information and/or material contained in this Whitepaper and seek the professional advice of their respective solicitor, professional accountant or other professional adviser.

This Whitepaper is distributed on a confidential basis to a limited number of recipients and may therefore not be for use by or reproduced for any person other than the person to whom it is distributed. The recipient, by its acceptance of this Whitepaper, agrees to keep permanently confidential all information contained in the Whitepaper (and all accompanying documents), and the recipient agrees not to disclose, distribute or permit to be communicated verbally, directly or indirectly or otherwise, or to otherwise reproduce this Whitepaper or the contents herein except with the prior written consent of Avarta. For the purposes of this acknowledgement “recipient” includes, without limitation, any principal, director, shareholder, employee or agent of the recipient.

## **The Tokens**

Neither Avarta nor any Tokens have been approved or disapproved by any securities regulatory authority anywhere in the world nor has any such securities regulatory authority passed upon or endorsed the merits of the offering of the Tokens or the accuracy or adequacy of the Whitepaper. Any representation to the contrary is a criminal offence.

The invitation contemplated in this Whitepaper is not, and shall not under any circumstances be construed as, a public offering of the Tokens described in this Whitepaper. Neither does anything in this Whitepaper constitute a recommendation or solicitation to use any Tokens, the Avarta platform or any related products, services or technologies. This Whitepaper does not constitute and may not be used as a prospectus or offering document, or is an offer or invitation to buy Tokens, subscribe for securities or any other asset. This Whitepaper will not be registered as a prospectus under any applicable securities legislation in any jurisdiction.

The distribution of this Whitepaper in certain jurisdictions may be restricted and accordingly, persons into whose possession this Whitepaper come are required to inform themselves about and observe such restrictions including obtaining any requisite governmental or other consent and observing any other formality prescribed in such territory. No action has been taken or will be taken in any jurisdiction that would permit a public offering of the interests or possession or distribution of the information set out in this Whitepaper in any jurisdiction where action for that purpose is required.

FOR THE AVOIDANCE OF DOUBT,

(A) THIS WHITEPAPER AND THE TOKENS DESCRIBED IN THIS WHITEPAPER HAVE NOT BEEN AND WILL NOT BE REGISTERED UNDER THE US SECURITIES ACT OF 1933, AS AMENDED (THE “SECURITIES ACT”), AND MAY NOT BE OFFERED OR SOLD WITHIN THE UNITED STATES OR TO, OR FOR THE ACCOUNT OR BENEFIT OF, U.S. PERSONS (AS DEFINED IN REGULATION S UNDER THE SECURITIES ACT); AND

(B) THIS WHITEPAPER AND ANY OTHER DOCUMENT OR MATERIAL ISSUED IN CONNECTION WITH THE TOKENS DESCRIBED IN THIS WHITEPAPER HAVE NOT BEEN AND WILL NOT BE REGISTERED AS A PROSPECTUS WITH THE MONETARY AUTHORITY OF SINGAPORE.

Unless expressly permitted, Tokens cannot be received, used, or held by, transferred or sold to, a person which is (a) the subject of economic or financial sanctions or trade embargoes administered or enforced by any country or government, including, but not limited to, those administered by the United Nations Security Council, the European Union, Her Majesty’s Treasury of the United Kingdom or Office of Foreign Assets Control of the United States or any other applicable jurisdictions, (b) located, organised or resident in any country or territory that is the subject of country-wide or territory-wide sanctions, (c) listed in any sanctions-related list of sanctioned persons, including, but not limited to, those maintained by the United Nations Security Council, the European Union, Her Majesty’s Treasury of the United Kingdom or Office of Foreign Assets Control of the United States, (d) located, organised or resident in Canada, Cuba, the Democratic People’s Republic of North Korea, Hong Kong SAR, the Islamic Republic of Iran, Libya, the People’s Republic of China, South Sudan, Sudan (North), Syria, the Crimea, United States of America, any jurisdiction in which the acquisition and/or ownership of Tokens is prohibited by applicable law, or (e) directly or indirectly owned or controlled by any person or persons described above.

No warranties or representations of any kind are made with respect to the Tokens and all warranties and/or representations, whether express or implied, relating to the Tokens are disclaimed (including but without limitation any implied warranties as to merchantability, fitness for a particular purpose, title and non-infringement).

The Tokens shall be provided on an “as is” and “as available” basis. There is no guarantee that the Tokens will perform as expected or hold any particular value or price. The Tokens may lose some or all of their value. No promises, guarantees or undertakings are made with respect to the Tokens, their price, value, supply amount, performance, etc. Avarta shall not influence the price of such tokens or its performance, and assume no liability to any person for the Tokens, their performance, value or loss in value, the use or inability to use the Tokens.

Any Token is not an investment, security, share or equity interest, debt or loan nor a derivative instrument of any of the foregoing.

Unless otherwise specified, the Tokens do not have any rights, uses, purpose, attributes, functionalities or features, express or implied, including, without limitation, any uses, purpose, attributes, functionalities or features on the Avarta platform (including but not limited to any voting, distribution, redemption, liquidation, proprietary or other financial or legal rights).

Participation in a token sale carries high risk; it is highly speculative and prospective participants are strongly advised to seek professional advice. Please read the Risk Disclosures below. The recipient, by its acceptance of this Whitepaper, accepts all the listed risks and agrees that Avarta shall not be in any way liable for any losses, damages or costs incurred due to or in connection with such risks. The Avarta reserves the right to issue and/or risk disclosure statements.

Prospective participants should also note that the Whitepaper does not purport to identify, and does not necessarily identify, all of the risk factors associated with the proposed participation with the token sale. Accordingly, each prospective participant, prior to participating in the token sale, must conduct and rely upon its own investigation of risk factors associated with the proposed participation in the token sale.

The Whitepaper contains material provided to Avarta from various sources and any references thereof do not imply our endorsement of the same. No representation or warranty is made or should be implied as to the accuracy or completeness of the material contained herein and no responsibility or liability will be accepted by Avarta for any loss or damage, howsoever arising, which results from an action or reliance in whole or in part on such material. The information in this Whitepaper is not complete and may be changed. Prospective participants should independently verify the material contained in the Whitepaper. No person has been authorised to give any information or to make any representations other than as contained in the Whitepaper and any representation or information not contained herein must not be relied upon as having been authorised by Avarta.

The information contained in this Whitepaper about the Tokens and the proposed business opportunity is not intended to be the only information on which a decision is to be made and

is not a substitute for a disclosure document, or any other notice that may be required under law. Detailed information may be needed to make a token participation decision. In particular, prospective participants should be aware that no established market exists for the trading of any Tokens that may be offered.

This Whitepaper does not purport to be complete and does not necessarily contain all information which a prospective participant would consider material. Accordingly, this Whitepaper should not form the basis of any decision to participate in the proposed token sale. In making any decision to participate in the the proposed token sale, prospective participants should inform themselves as to (a) any possible tax consequences, (b) any legal requirements, (c) any financial and other consequences of participating in the proposed token sale; and (d) any foreign exchange restrictions or exchange control requirements which they might encounter under the laws of the countries of their citizenship, residence, incorporation or domicile and which might be relevant to the purchase, holding, or disposal of the Tokens. No representation or warranty is made or implied as to the availability of taxation deductions or any other taxation implications in relation to Avarta and the Tokens.

If you are in any doubt about the contents of this Whitepaper, you should consult your solicitor, professional accountant or other professional adviser.

## **Avarta Platform**

The Avarta platform is in beta stage and all related software is experimental. The Avarta platform is provided on an “as is” and “as available” basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the Avarta platform is free of defects, vulnerabilities, merchantable, fit for a particular purpose or non-infringing. Any use of the Avarta platform shall be at your own risk. In no event shall we be held liable in connection with or for any claims, losses, damages or other liabilities, whether in contract, tort or otherwise, arising out of or in connection with the Avarta platform or its operation or use.

## **Definitive Documentation**

Prospective participants should obtain copies of the relevant definitive documentation (the “Definitive Documentation”) before making any binding commitments in respect of their proposed participation in the token sale. Information in the Whitepaper is qualified in its entirety by reference to the detailed information in the Definitive Documentation. Only the particular representations and warranties contained in such Definitive Documentation will have any legal effect. To the extent that statements made in the Whitepaper summarise provisions of any agreement, they are qualified in their entirety by such provisions.



Although every effort has been taken to ensure the accuracy of the facts and matters stated in the Whitepaper, in the event of any inconsistency between the information contained in the Whitepaper and any Definitive Documentation, the relevant Definitive Documentation shall prevail to the extent of such inconsistency. Prospective participants and their advisers should carefully review and evaluate the Definitive Documentation.

## **Indemnity and Limitation of Liability**

The recipient, by its acceptance of this Whitepaper, agrees, to the fullest extent permitted by applicable laws and regulations, to indemnify, defend and hold Avarta, its directors, officers, shareholders, employees, directors, consultants, representatives, agents and/or contractors harmless from and against any and all loss, penalty, claim, damage, liability or expense whatsoever (including reasonable legal fees and costs) due to or arising out of or based upon (a) any inaccurate representation or warranty made by the recipient, or breach or failure by the recipient to comply with any covenant or agreement made by the recipient or in any other document furnished by the recipient to any of the foregoing persons in connection with the Tokens or the Avarta platform, or (b) any action instituted by or on the recipient's behalf against any of the foregoing persons.

To the maximum extent permitted by applicable laws and regulations, in no event shall Avarta, its directors, officers, shareholders, employees, directors, consultants, representatives, agents and/or contractors be liable or responsible for any direct, indirect, special, punitive, exemplary, incidental, or consequential damages or losses of any kind, nor shall they be liable for the loss of goodwill, loss of profits (including expected), loss of data, diminution of value, and/or business interruption arising out of or in connection with the use of the Tokens, the Avarta platform or this Whitepaper or reliance thereon, any inaccuracy or omission in this Whitepaper, whether based upon breach of warranty or contract, negligence, strict liability, tort, or any other legal theory, regardless of whether Avarta or any of the foregoing persons have been advised of the possibility of such damages or losses.

## **Future Statements**

Except for historical information, there may be matters in this Whitepaper that are forward-looking information. Such information are only predictions and are subject to inherent risks and uncertainty. Forward-looking statements, which are based on qualifications, assumptions and estimates (in each case whether or not identified herein) and are generally identifiable by the use of the words 'may', 'project', 'intend', 'should', 'continue', 'target', 'anticipate', 'will', 'believe', 'estimate', 'plan', 'expect', 'intend', 'seek', the negatives thereof or similar expressions. Participants are cautioned not to place undue reliance on forward-looking information. By its nature, forward-looking information involves numerous assumptions, inherent risks and uncertainties both general and specific that contribute to the possibility those predictions,

forecasts, projections and other forward-looking statements will not occur. Those risks and uncertainties include factors and risks specific to the industry in which Avarta operates as well as general economic conditions. Forward-looking Information is provided for illustrative purposes only and is not intended to serve as and must not be relied on by any participant as a guarantee, an assurance, a prediction or a definitive statement of fact or probability. Actual performance, events, results or outcomes may be materially different from those expressed or implied in those statements.

All forward-looking information attributable to Avarta or persons acting on behalf of Avarta are expressly qualified in their entirety by the cautionary statements in this section. Except as expressly required by law, Avarta undertakes no obligation to publicly update or revise any forward-looking information provided in this Whitepaper whether as a result of new information, future events or otherwise, or the risks affecting this information.

None of Avarta, its officers or any person named in this Whitepaper with their consent, or any person involved in the preparation of this Whitepaper, makes any representation or warranty (express or implied) as to the accuracy or likelihood of fulfilment of any forward-looking information except to the extent required by law. The forward-looking information reflect the views held only as at the date of this Whitepaper.

## **Risk Disclosures**

### **Risk of Software Weaknesses**

Although Avarta shall make reasonable efforts to ensure that the Tokens, the Avarta platform and related software adopt high-security standards, Avarta does not warrant or represent that the Tokens, the Avarta platform or any such related software are secure or safe, or protected from fishing, malware or other malicious attacks. Further, the Tokens, the Avarta platform and related software may contain weaknesses, bugs, vulnerabilities, viruses or other defects which may have a material adverse effect on the operation of the tokens to be issued by Avarta, the Avarta platform or any such related software or may lead to losses and damages for users of the tokens to be issued by Avarta, the Avarta platform or any such related software or third persons.

### **Risk Inherent in the Blockchain**

The Tokens, the Avarta platform and related software are or will be deployed on blockchain related networks. As a result, any malfunction, breakdown or abandonment of such blockchain(s) may have a material adverse effect on the Tokens, the Avarta platform or such related software. Moreover, advances in cryptography, or technical advances such as the development of quantum computing, could present risks to the Tokens, Avarta platform, related software, and related blockchain software by rendering ineffective the cryptographic consensus mechanism that underpins the relevant blockchain network. The smart-contract concept, the underlying software application and software platform are still in an early

development stage and unproven. The blockchain, as well as any other blockchain, can be attacked which may result in downtime, consensus split, long reorganization of the chain, 51 percent attack, or other adverse outcomes each of which may lead to complete loss of the participant's digital assets.

### **Risk of Flawed Logic of the Tokens, the Avarta Platform or Related Software**

The underlying logic of the Tokens, the Avarta platform and their related software may be flawed, defective or impaired, which can result in smart-contracts operating incorrectly or not as expected, or transactions being executed in violation of logic which underpins the smart-contracts, which can lead to partial or complete loss of digital assets used in the transaction.

### **Risk of Confusing User Interface**

Certain user interface elements or design decisions may be confusing or mislead participants, which may result in the execution of a different action or transaction than intended or desired, or connection of a wrong wallet, account or network.

### **Risk of Legal Uncertainty**

The intended activities of the Avarta platform are subject to various laws and regulations in the countries where Avarta operates or intends to operate. Avarta may be obliged to obtain different licenses or other permissive documents in some or all jurisdictions where it intends to operate its business, therefore, its business in such jurisdictions shall always be subject to obtaining such licenses or permissive documents, if so directed by applicable laws. There is a risk that certain activities may be deemed in violation of any such law or regulation. Penalties for any such potential violation may be unknown. Additionally, changes in applicable laws or regulations or evolving interpretations of existing law could, in certain circumstances, result in increased compliance costs or capital expenditures, which could affect Avarta's ability to carry on its business model.

### **Risk of Theft**

There is no assurance that there will be no theft of the participant's digital assets as a result of hacks, sophisticated cyber-attacks, distributed denials of service or errors, double-spent attacks, flash-loan attacks, vulnerabilities or defects of the Tokens, the Avarta platform, any related software or otherwise. Such events may include, for example, flaws in programming or source code leading to exploitation or abuse thereof. Any of the above may lead to partial or complete theft or loss of digital assets used in transactions carried out in connection with the Tokens, the Avarta platform or any related software.

## Value Risks

Tokens may drop substantially in value, or may remain illiquid for long periods of time or indefinitely. Avarta cannot guarantee an active secondary market for the exchange of Tokens purchased in the token sale. Not all disclosures or statements are being made in this disclaimer section. Participants should review the Definitive Documentation in their entirety and seek the professional advice of their respective solicitor, professional accountant or other professional adviser.

The Tokens may change in value based on a number of factors that are outside Avarta's control. There is no guarantee or expectation that the Tokens will increase in value, provide a return, or have sufficient adoption and liquidity on exchanges. Owning these Tokens does not constitute a share of equity or ownership in Avarta. The token economy is new and exciting. Regulatory circumstances may require that token mechanics be changed or altered.







**AVARTA**