Uncloak™

Next Generation Cyber Security Threat Management

WHITEPAPER

January 25, 2018

Written By Tayo Dada

Version: 1.6

Summary

Uncloak™ is the world's first blockchain powered cyber threat solution putting businesses one step ahead of hackers

THIS NOTICE IS VERY IMPORTANT AND THEREFORE SHOULD BE READ THOROUGHLY. YOU SHOULD SEEK THE APPROPRIATE PROFESSIONAL ADVICE (E.G. FINANCIAL, TAX, LEGAL OR COMMERCIAL) IF YOU ARE UNCERTAIN OF ANY ACTION TO BE TAKEN WITH REFERENCE TO THIS WHITE PAPER.

This White Paper states the current views of Uncloak Ltd ("Uncloak"), which concerns the proposed next generation cyber security blockchain powered application and bug bounty token reward network named 'Uncloak', the external cryptographic tokens proposed to be used with Uncloak ("UNC") and related matters. This White Paper may, without notice, be updated by Uncloak Platform, although Uncloak is under no obligation to revise any information contained therein. It is your responsibility to ensure that you have read and understood the contents contained within the latest version of the White Paper.

Indicative Information: All information contained within this White Paper, unless expressly specified otherwise, is indicative as Uncloak, and the technologies on which it will be based, are currently under development and therefore unestablished. Several risk factors, including without limitation: defects in technology, legal or regulatory exposure, market volatility, sector volatility, corporate actions, or the unavailability of complete and accurate information may lead to plans, predictions or assumptions within this White Paper being unattained.

Information Purposes Only: This White Paper does not constitute, nor is it intended to be, a prospectus or an offer to sell, a solicitation of an offer to buy, or a recommendation of UNC, Uncloak, an investment in Uncloak or any project or property of Uncloak Platform or Uncloak, or shares or other securities in Uncloak Platform or any affiliated or associated company in any jurisdiction; it is for informational purposes only.

Not a contract: This White Paper is not a contract and does not legally bind Uncloak Platform or any other party. By publishing this White Paper, Uncloak Platform does not intend to solicit, and is not soliciting, any action with respect to UNC or any contractual relationship with Uncloak Platform or any affiliated or associated company. Based on this White Paper, Uncloak Platform will not accept any cryptocurrency or other form of payment in respect of UNC. If Uncloak Platform elects to sell UNC, any sale will only be made on the terms and conditions of a binding legal agreement between Uncloak Platform and the buyer. Uncloak Platform will announce any such details separately from this White Paper.

Not Designed or Intended as an Investment Product or Securities: UNC has been designed to be the sole medium for exchange internally within the Uncloak Platform, and to be converted to be traded externally. UNC has not been designed to have the characteristics of an investment product and is not intended to be a security or any other type of financial or investment instrument in any jurisdiction.

Without limitation, possession of UNC does not entitle holders to a dividend or any financial or other type of return from Uncloak Platform or Uncloak ; UNC does not entitle holders to vote on, or otherwise exercise discretion to govern or influence, any aspect of Uncloak Platform's or any other entity's corporate entity, Uncloak Platform's or any other entity's business, or Uncloak or any other service; and UNC does not confer ownership, equity, or rights, interests, or benefits in the revenues, profits, or other financial aspects of, Uncloak Platform or any other entity, Uncloak, any underlying asset (whether tangible, intangible, or virtual), or any technology or intellectual property developed, acquired, or licensed by Uncloak Platform or any other entity.

Not a Recommendation or Advice: This White Paper has been produced to provide information about the Uncloak Platform and summarises the target market, business model, and technology of Uncloak. This White Paper should not be considered a recommendation for any person to purchase UNC or to use Uncloak. Your requesting a copy, possession, or sharing of this White Paper does not constitute participation in any sale of UNC, if Uncloak Platform elects to conduct such sale. No information in this White Paper should be considered as business, legal, financial, or tax advice regarding the purchase of UNC or the use of Uncloak. No part of this White Paper may be relied on to form the basis of, or in connection with, any decision regarding the purchase of UNC or the use of Uncloak.

Not Reviewed, Examined or Approved by a Regulatory Authority: The information contained in this White Paper has not been reviewed, examined or approved by any regulatory authority. Uncloak Platform has not and will not seek review, examination or approval of any of the information contained in this White Paper under the laws or regulations of any jurisdiction. The publication or distribution of this White Paper does not imply that applicable laws, regulations, or rules have been complied with.

Third Party Sources: The completeness or accuracy of any information extracted from third party sources has not been verified by Uncloak Platform or any Uncloak Related Parties.
Forward-looking Statements: Unless it is indicated that the statement is a statement of fact, all statements in this White Paper, on Uncloak Platform's website, in any communication channels (including but not limited to Steemit, Slack, Medium, Reddit, Telegram, Github, and Twitter), or otherwise made by Uncloak Platform or its authorised representatives in any media including but not limited to statements about Uncloak, UNC, Uncloak Platform's financial position, business strategies, plans and prospects, and industry trends are "forward-looking statements" and should not, in any circumstances, be relied upon. Forward-looking statements should be regarded as aspirational, indicative of what could potentially happen. Influences in the external environment, (including but not limited to changes in political, social, economic, regulatory, and stock or cryptocurrency market conditions) may cause the actual outcome to be very different to what was stated. No representation, warranty, undertaking, promise, or guarantee is given in respect of the forward-looking statements.

Limitation of Liability: To the maximum extent permitted by all applicable laws and regulations within the relevant jurisdiction, Uncloak Platform, its affiliates and any Uncloak Related Parties shall not be liable for any financial, reputational, or liability loss, direct or indirect, or subsequent exposure to other damages or risk arising out of or in connection with any reliance on this White Paper even if Uncloak Platform and Uncloak Related Parties have been advised of the possible errors and the subsequent possibility of such losses or damages.

Disclaimers of Representations, Warranties, Undertakings, and Conditions: The underlying principle behind this White Paper is “Caveat Emptor”. To the maximum extent permitted by all applicable laws and regulations of the relevant jurisdiction, all information provided in this White paper is supplied “as is” with no guarantees of accuracy, relevancy, or completeness., Uncloak Platform and Uncloak Related Parties do not make or purport to make, and hereby disclaim, all representations, warranties undertakings, and conditions (express or implied, whether by statute, common law, custom, usage, or otherwise) regarding Uncloak Platform, Uncloak, UNC, this White Paper, and any forward-looking statements.

Requirement for Reproduction and Distribution: Uncloak Platform’s prior written consent is required to reproduce and distribute in its entirety without change, this White Paper and Notice. No part of this White Paper may be reproduced or used in or, distributed to any jurisdiction where possession or distribution of this White Paper is prohibited or restricted.
English Version Controls: The English language version of this White Paper is the only official version that is currently controlled and therefore if an issue arises between the English version of this White Paper and a translated version, the English version will prevail.

Uncloak™

The future of cyber threat detection

Table of Content

Table of Content

Introduction

Uncloak™ is a unique and fully scalable blockchain powered technology that enables businesses to monitor, protect themselves against and eliminate cyber threats, staying one step ahead of the hacker.

THE PROBLEM

Computer hacking is one of the world's major problems with new breaches of data and releases of ransomware occurring at an alarming rate. Cyber-crime is predicted to cost $6 trillion annually by 2021. There are no boundaries: from some of the world's largest corporations; to critical national infrastructure; to small local enterprises and individuals. They have been hacked and trends suggest this will continue, particularly as evolving programs such as Internet of Things (IoT), smart cities and mass digitisation become the reality of life.

Currently, there is a shortage of cyber security solutions that are proactive in identifying new threats and allowing end users to shut them out or close them down. Whilst some capabilities exist at a Governmental level, Uncloak provides a commercial tool that will close this gap and maintain significant revenues across the many sectors that are susceptible to cyber-crime.

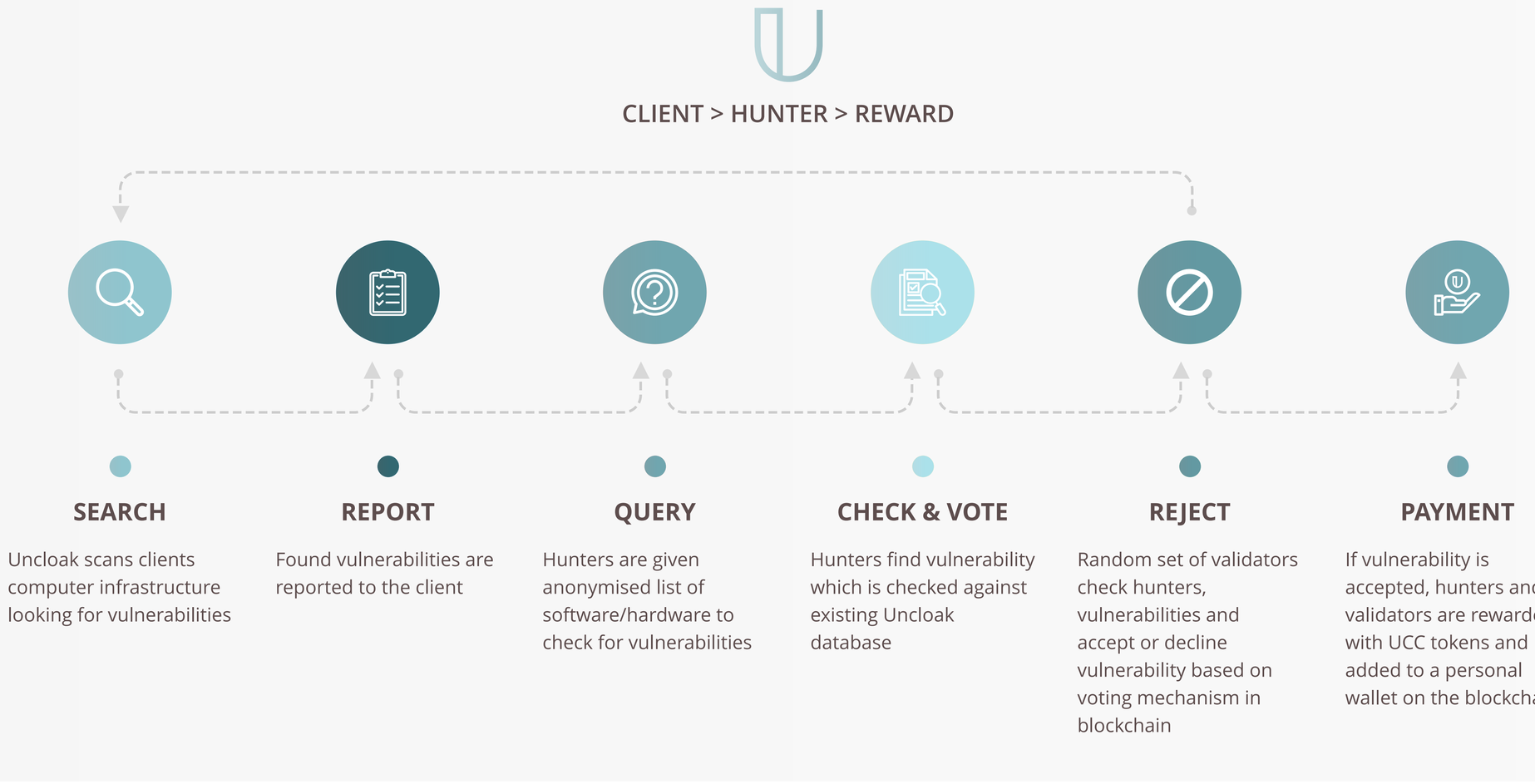
Uncloak is an Artificial Intelligence (AI) based analytical tool for the intuitive, automated and seamless performance of security checks: giving users the ability to cut through the cyber jargon and understand, remediate and resolve cyber security issues. In the absence of innovation tools such as Uncloak, successfully evaluating a company's computers and network infrastructure requires specialised, highly skilled labour, extensive setup time and significant costs. Uncloak seeks to make this level of cyber security available on a mass scale, at a lower cost and with simple end user interaction.

Tackling cyber security threats requires more than antivirus protection, firewalls and intrusion detection systems. Currently cyber security solutions rely on an isolated and custom-made approach to cyber threat management with limited knowledge sharing between competitive security vendors. Most of the patterns and signatures that aid cyber security software in detecting a security vulnerability are freely available on the public internet thus allowing the hacker to have the same knowledge as a security vendor. The result is an endless game of cat and mouse, with a cyclical race to stay one step ahead, until the next breach is surfaced. The status-quo puts the advantage with the hacker.

THE SOLUTION: UNCLOAK™

Our novel approach is to create a decentralised, scalable, blockchain powered cyber security management solution that places an emphasis upon the strength of the wider community to contribute to finding vulnerabilities through a blockchain based mechanism. Uncloak will harness knowledge and expertise, aggregate it into a platform and transform it into a service for end users to purchase. This capability in Uncloak does not currently exist in the commercial market.

Uncloak will build its own threat detection database by using advanced AI technology to crawl the public and private internet looking for the latest cyber security threats, which are converted into security signatures and added to the Uncloak threat detection system to check if the vulnerabilities exist across the subscribed client base networks and infrastructure. Where vulnerabilities exist, the end user will be notified immediately so that corrective action can be taken.



Uncloak™ is in the unique position to becoming a market leader in Cyber security threat detection because, it not only engages an active community of cyber security experts to find undiscovered security threats; but it also constantly updates itself using Artificial Intelligence technology to scan the internet looking for upcoming security vulnerabilities to add to its threat vulnerability database.

"If an end user client can understand their security risk position in real-time, they can place themselves in a strong position to eliminate cyber threats before they occur".

Lena Bhogaita - Operations Lead - Uncloak

THE OPPORTUNITY

The team at Uncloak know that there is a significant opportunity to fill a gap in the cyber security market. That is why we are creating a Token Crowd-sale offering to build on the work completed to date, to allow the development our existing methodologies and to enable the release of the first commercial application for Uncloak.

History of Uncloak

Q4 2016

Development of CSaaS - “Cyber security as a service” application for customers to perform their own security checks.

Q1 2017

Strategic Partnership formed with Adecco, the worlds largest human resources firm to provide cyber security consultancy to public/private sector clients

Q2 2017

Awarded best in class IT consultancy by Wealth and finance magazine.

Q4 2017

CSaaS renamed to Uncloak

Q1 2018

Strategic alliance formed with Krzana™ - artificial intelligence software developers.

Q1 2018

Released whitepaper

Q1 2018

Building community and strategic relationships.

Uncloak is a unique and fully scalable blockchain powered technology that enables businesses to monitor, protect themselves against and eliminate cyber threats, staying one step ahead of the hackers.

Current Cyber Security Threat Landscape

Cyber Security attacks are more frequent than ever before, partly due to the availability of internet connectivity across all types of devices from laptops, desktops, notepads and mobile phones affecting not just businesses but individuals as well. Crypto currencies, crypto exchanges and tokens issuance platforms have also suffered from significant security breaches over the last few years further compounding the issue.

The public sector, internet and telecommunications sectors are highly susceptible to espionage-focused cyber-attacks. The Uncloak team and advisors are experts in these fields.

Businesses need to be aware of the full costs of a cyber-attack, in particular, the “slow-burn” costs (i.e. those associated with the long-term impacts of a cyber-attack, such as the loss of competitive advantage and customer churn). When added to immediate costs (i.e. legal and forensic investigation fees, and extortion pay outs), slow burn costs can dramatically increase the final bill.

Security breaches can cause serious financial and reputational damage. There is no standard model for estimating incident cost, the only data available is that made public by organisations involved. Computer security consulting firms have produced estimates of total worldwide losses: from $13 billion (worms and viruses only) to $226 billion (for all forms of covert attacks) annually.

This has forced companies to diversify products, moving from “detect only” to “detect and respond”, tracking data leaks, hacks, other intrusions and preventing further repercussions from stolen data. For businesses, this mean stopping access to accounts and services subject to data loss or infiltration, tracking the source of intrusion and shoring up cyber defences.

Unfortunately, most companies are highly exposed to cyber threats due to the constantly changing nature of cyber attacks which require security expertise and financial resource to remain secure.

Today and Tomorrow's feature list

There has been a requirement to develop a next generation cyber threat detection application spurred by the demand from firms, who tend to be reactive rather than proactive when it comes to managing their cyber threat issues.

Uncloak™ has already spent one year developing an MVP (a Minimum Viable Product) which is available as a demo due to Uncloak's expertise in the cyber security space working with many small to large enterprise clients who have similar security requirements in protecting their infrastructure and who seek a systematic approach to thwarting would-be hackers. The existing Uncloak application developed in-house that has the current features:

- Automatically identify a client's public internet footprint covering websites, email servers, applications and computers on the internet in readiness for a security scan greatly reducing the timescales around security scanning setup.
- Easy to understand dashboard to check progress of scans and reports, request external IT consultancy and set up schedule scanning jobs
- Black Hat (*) mode – Uncloak Software is able to simulate a live hack attempt against an email server and also check a client's antivirus protection.

(*) A black hat test would simulate what an actual hacker would do to gain access to a corporate computer system.

Uncloak is seeking to meet market requirements through the innovative use of the blockchain and artificial intelligence to ensure it becomes a cyber-security market leader giving companies the best opportunity to proactively secure their computing infrastructure. Some of the features will include the following:

- **On premise software tool**
  Allow users to scan their internal network for threats and vulnerabilities and report back to the central dashboard.
- **Advanced network discovery tool**
  Cloud environments can be scanned with ability to look for vulnerabilities across public/private/hybrid cloud environments ranging from Microsoft™, AWS™ and Google™.
- **Intelligent Security Compliance tool**
  Innovative engine to check against cyber essentials/PCI DSS/ISO27001 compliance requirements.
- **Black hat extreme mode**
  Conversion of online security database into a number of additional tools that can check for vulnerabilities with multiple operating systems issues ranging from the website, workstation and databases.

Uncloak Features

BLOCKCHAIN POWERED BUG BOUNTY

Currently companies are not positioned to be aware of imminent cyber threats that are about to be released into the public domain which can cause not only financial damage but are also damaging to a company's reputation. Oftentimes, current vulnerability scanning applications rely on stale cyber threat security information to diagnose whether a company's website or infrastructure is at risk. Uncloak aims to change this pressing issue.

Uncloak will work using a number of smart contracts (a function allowing a set of predetermined actions to be performed in a secure manner). For example, a smart contract would allow UCC tokens to be issued to the ethical hacker on the basis that a new cyber threat vulnerability has been found and checked by other ethical hackers in the community.

Using a token called UCC on the Uncloak platform a smart contract will be used to create a voting rights system that allows a community of Uncloak registered IT security experts/ software developers (known as 'hunters') to collaborate on finding cyber threats within applications and network devices, whilst also finding the remediation needed to resolve the cyber threat issues.

Any vulnerabilities that have been found within an application by a hunter are immediately checked against an existing public cyber vulnerability database to ensure it is indeed a new cyber threat and not an existing recorded threat. Each hunter has the ability to check another hunter's vulnerability, taking up to 4 validators (ethical hackers) to check that a vulnerability found is genuine and can be recorded to the blockchain as a real cyber threat. The hunter discovering the vulnerability will be given 10,000 UCC tokens unique to the platform, whilst the hunters who checked the validity of the vulnerability will be given 1500 UCC tokens each, which can be converted on our platform to tradeable UNC tokens which can be exchanged for Ethereum on a public exchange.

The use of the block chain and smart contract voting rights system greatly reduces the level of manual administration, costs and time required to advertise a new cyber threat via our Uncloak platform. All subscribers to the Uncloak platform will receive the latest list of cyber threat vulnerabilities against their existing computing infrastructure, allowing them to identify where the potential threats lie and can then take the necessary remediation steps.

The Uncloak platform supports various business goals:

- Vulnerabilities are not allowed to be added to the platform without approval from a pool of verified hunters chosen at random
- End to end visibility of vulnerabilities found and payments to hunters within the Uncloak platform occur automatically without intervention
- Real-time analytics and automated reporting with a locked audit trail of everything
- Tamper-proof vulnerability database
- Securely sharing data with all parties
- Reduce reporting process time and effort for vulnerability checks
- Leaderboard system for all registered hunters/validators with bonus stars given to the most frequent contributors resulting higher in token payouts

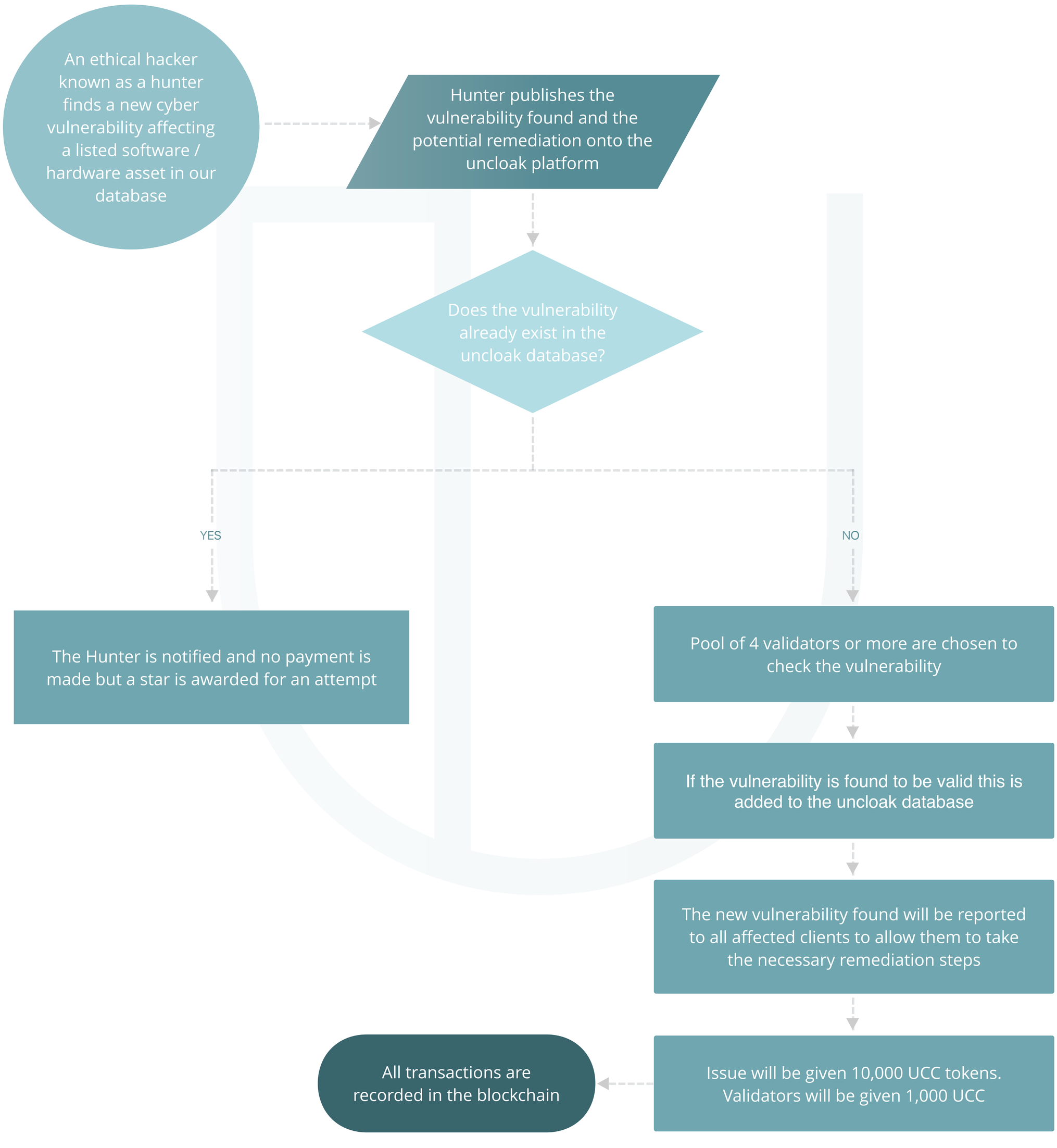
The Uncloak web portal allows companies to purchase ethical hacking testing for their own applications from a pool of verified hunters who have proven to be competent in validating and finding vulnerabilities via a scoring mechanism. Companies can purchase UNC tokens directly on the platform backed by a smart contract which will give them a finite amount of time for the hunters to work on the application to be tested.

Bug Bounty Deliverables

- Transferable UCC tokens governed by Smart Contracts - Provide automated auditing and compliance as a protocol
- Disbursement of funds for hunters/validators
- Real time monitoring of vulnerabilities
- Deploy a Blockchain powered voting rights system
- Automated reporting on funds and balance for hunters
- Real time block chain settlement

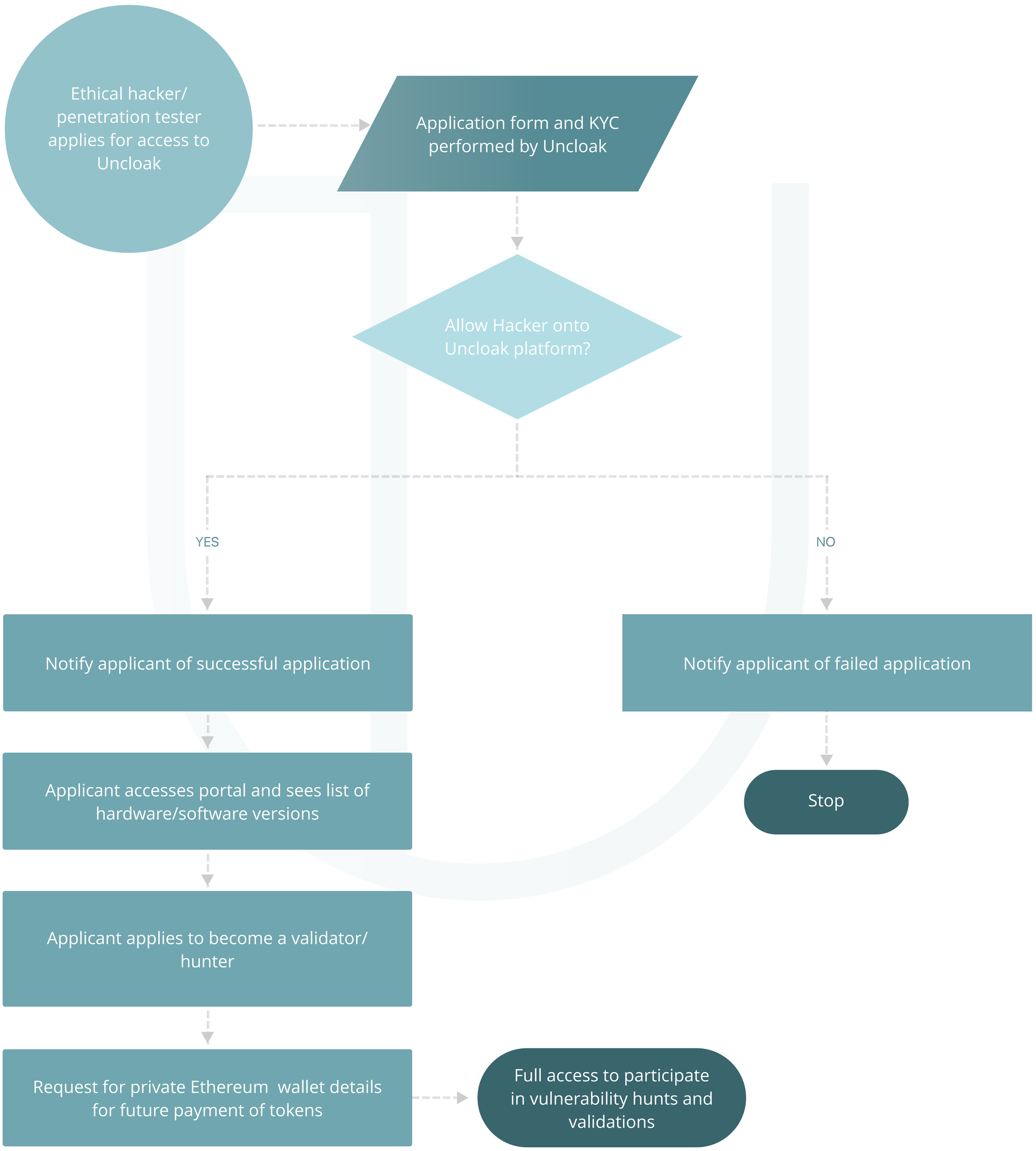
Step 1 – Example of voting rights mechanism in Uncloak

Instead of a costly and timely manual screening/due-diligence process to decide whether a vulnerability should be placed on the Uncloak platform, our solution uses an automated approach to cyber threat management. If a new vulnerability has been raised by a hunter, a number of the following procedures will occur before a new cyber threat is registered, implemented and recorded using Smart Contract invocations. This process is transparent and can be audited by anyone using a blockchain explorer on the Uncloak platform.



Step 2 – Method for allowing ethical hackers to become hunters/validators on Uncloak platform

This process allows the necessary checks to be made before an applicant coming from an ethical hacking/penetration testing environment can access the Uncloak platform. The applicants then select which software/hardware version they believe has an unknown vulnerability with which to post to Uncloak. This process involves two main outcomes: the applicants either receive their UCC tokens into their secure Wallets held on the block chain, or a message recorded on the Uncloak platform is relayed to the applicant to state that the vulnerability is already known therefore payment will not be made.

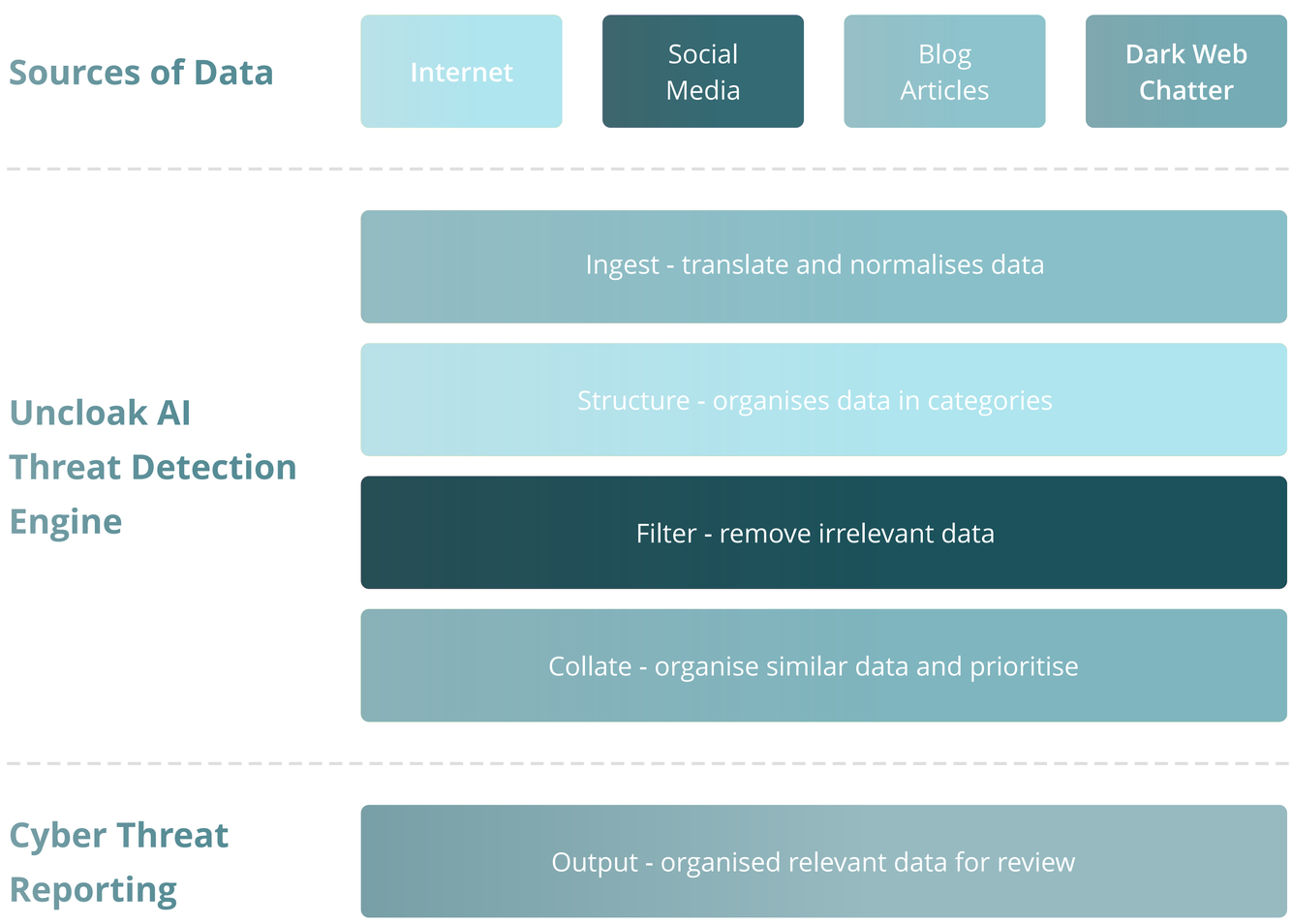


AI THREAT DETECTION ENGINE

A revolutionary step in thwarting hackers' ability to attack a computer network is by performing surveillance on the public internet and also the dark web. The dark web is a secluded part of the internet where black hat (unethical hackers) trade software/hardware vulnerabilities in exchange for untraceable cryptocurrency. The dark web can only be accessed through a special internet browser in order to view content in chatrooms/websites used by black hat hackers.

By working in conjunction with Krzana™, a world leading Artificial Intelligence software development firm specialising in software that is able to read social media content/website posts, Uncloak will be able to provide the most up to date cyber threats database for our clients relevant to their computing infrastructure.

Uncloak AI engine transforms raw unformatted data to relevant cyber threat data



Uncloak will feature a private cloud based real-time cyber threat search engine powered by artificial intelligence, taking vast amounts of unstructured text data and turning it into structured and legible actionable data used for reporting to clients about the current cyber threat landscape.

Our cyber threat detection engine will read streams of published text data from over 7,000 independent/forums/chatrooms/metadata/blogs per minute across the public internet and dark web and tag it appropriately to build up a unique threat landscape report.

Uncloak API Engine System Architecture and Operations

- The core Uncloak API cyber threat engine is a multi-layer data pipeline that runs on AWS. Each layer consists of 1 or more servers working in parallel, and can be scaled independently to handle load.
- Layers communicate using Redis queues that provide backpressure to ensure system stability.
- Deployment is handled by Chef, using Amazon OpsWorks.
- A low-throughput version of the entire system runs on each of our developers' machines, to allow efficient local development and testing.
- The system is primarily written in Python. Both internal and external communication is done in JSON.
- News and user data is stored transiently in Redis and long-term in MySQL on RDS.
- Ontology and knowledge-base information is stored in the graph database Neo4j on TOOK, indexed using Xapian and queried from TOOK over HTTP.

Uncloak is in a unique position to ensure that we are the most relevant source of current and future cyber threat data on the internet, with multiple clients subscribing to the platform just for the use of the AI threat detection engine as a standard due diligence approach to effective cyber threat management.

Use Cases for Uncloak

SMALL CLIENTS (1-250 EMPLOYEES)

Uncloak is designed for companies that wish to perform their own security checks without requiring immediate attention from a certified ethical hacker or security penetration tester. Using Uncloak ensures that all companies have an ability to keep abreast of existing and potential cyber security issues in their infrastructure.

Uncloak performs a number of functions that a professional ethical hacker performs at greatly reduced cost to the company, from the following:

USE CASE 01

- Perform full vulnerability check of all workstations/servers/network hardware/ software on an automated schedule basis without requirement for penetration tester/ethical hackers.
- Check Operating System and application software patch levels are up to date.
- Check for presence of applications / software services with weak configurations and provide suggestions for improving the security of applications and hardware.

LARGE CLIENTS (250+ EMPLOYEES)

Large companies have a differing set of needs that are heavily compliance and IT governance related. IT security requirements related to PCI compliance for debit/credit card systems to ISO27001/NIST/ Cyber Essentials certification place a continuous burden on IT teams. Uncloak software will elevate a number of compliance/certification concerns and provide:

USE CASE 02

- Relevant reporting on upcoming cyber threats and IT security compliance benchmarks.
- Check for presence of vulnerable OS / network available applications / services / weak-deprecated-vulnerable transport layer encryption.
- Check for unneeded applications / services available on workstations/servers.

Marketing Strategy

Uncloak has a clear strategy in regards to attaining global reach through a channel partner model and b2c subscription model. Uncloak will be supported through our relationships with a number of large value-added resellers and end user base who are already accustomed to working with us on a number of cyber security projects. We have two partners in the big 5 consultancies, plus access to over 200 resellers through our current business development staff members.

Uncloak will be pitched at companies that:

01

Need an expert unbiased approach to IT Security solutions, and who know that the current generic market vendors will not work for customers who require support for unique and/or legacy systems in the conduct of their business.

02

The level/capability of the internal IT resource cannot provide the required high quality of service or needs supporting to do so.

03

An in-situ evolved infrastructure needs restructuring to improve IT Security usually as part of IT transformation programme.

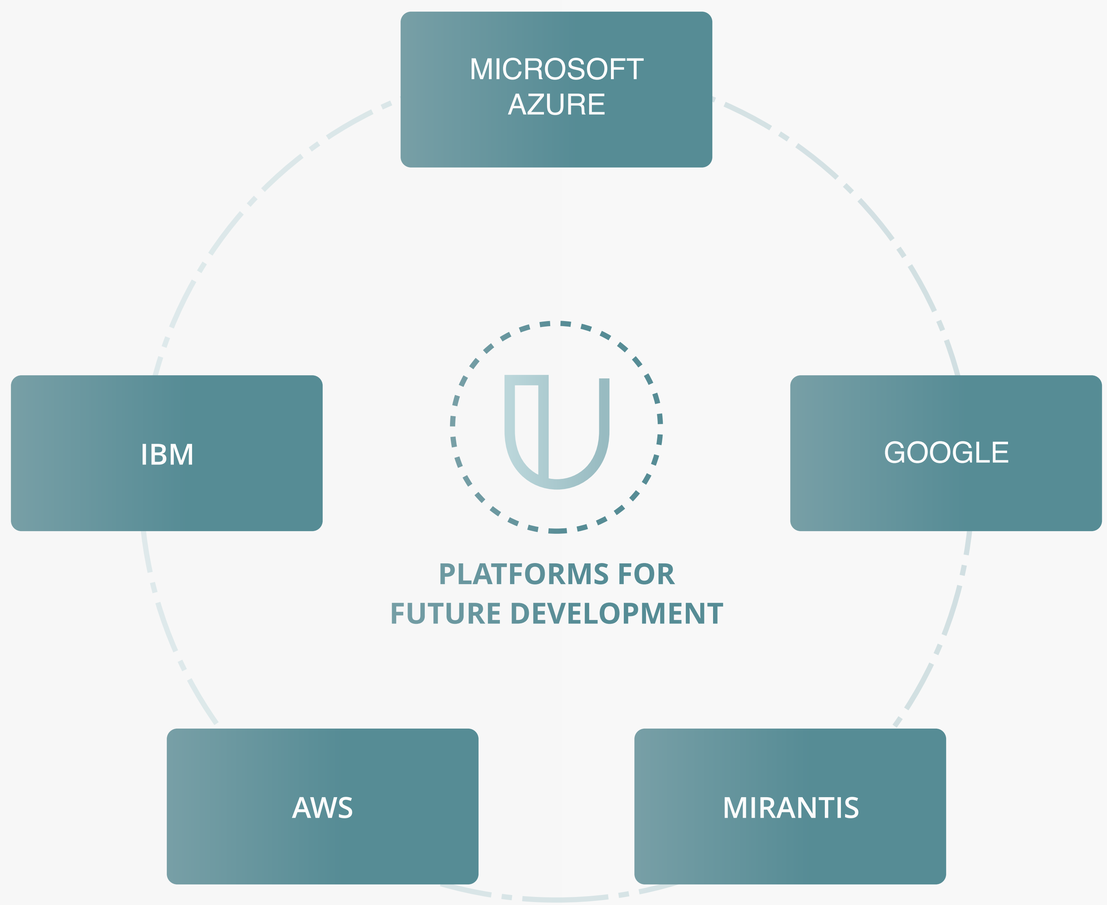
04

The business is at risk and in need of ISO, GDPR, FCA, SRA compliance requirements.

Uncloak's Ecosystem & Partner Program

The ability for Uncloak to be developed by a Cyber Security consultancy and software development house has massive benefits in the understanding of actual consumer demand for particular software features. It is the intent of Uncloak to create a formal framework for how we can support our software development partners who wish to facilitate technology integration and to develop and promote enhanced product solutions to expand the breadth and capability across Uncloak as a global Cyber security solution.

Uncloak aims to provide an interface for leading software development teams to implement our solution into their platforms that would allow end users to quickly power up Uncloak in their private/ public cloud environment:



Development of an open API to allow 3rd party applications to manage remote administration/ reporting and configuration of Uncloak will be key to the success and adoption of the cyber threat application. A comprehensive framework for the API will allow the programmer to get or set variables inside an XML-RPC request that correspond to field values in the configuration database in Uncloak application. This will allow full command and control of an instance of Uncloak from a secure 3rd party software application hosted on premise or in the cloud greatly strengthening the proposition.

The Uncloak Token

Uncloak uses two tokens to power the platform.

TOKEN NAME	UNC	UCC
TYPE OF TOKEN	Ethereum ERC-20 Format	EOS format
USE OF TOKEN	Externally Trade-able	Used internally on platform for rewarding hunters/validators for finding vulnerabilities.
CHARACTERISTICS OF TOKEN	Industry standard format used by majority of tokens. Running on ethereum network. More costly when transacting with slower speeds	Low latency transactions, free usage, multiple threads, turing complete

- UNC tokens can be purchased on a token/crypto exchange using ethereum, neo, BTC dependent on the exchange used.
- UNC tokens purchased on an exchange can be used to purchase and subscribe to Uncloak platform along with fiat currency for subscription services.
- Hunters and validators who have earned UCC tokens on the Uncloak platform for either finding/validating new vulnerabilities can convert tokens into tradeable UNC tokens, which are then sent securely to the hunters/validators registered crypto wallet.
- In the unlikely event that UCC tokens absorb the remaining amount of UNC tokens available an allocation of UCC tokens will be able to be exchanged for payments in Ethereum via the Uncloak platform.

Revenue Model

Uncloak will use a subscription-based model in order to allow both small and large companies to participate in our next generation software application. There are multiple revenues for the application from Uncloak implementation support, access to cyber threat detection Artificial Intelligence engine and API access.

REVENUE STREAM	CHARACTERISTICS
Perpetual Uncloak license	One month annual recurring fee for use of platform-pricing dependent on the number of computers/ websites to be monitored
Monthly subscription	Monthly fee for subscription to Cyber threat
API access	Licence fee payable to allow access for 3rd party applications to interface with Uncloak
Public cloud instance	Compact version of Uncloak within a standalone vm appliance to allow Azure/AWS to deploy to clients on a subscription basis

The base of cyber security-focussed VARs (valued added reseller) is currently very fragmented, with the top 15 players accounting for just one-third of the market, with the remaining two-thirds comprising a ‘long tail’ of other service providers.

While historically these security-focussed VARs have been well placed to serve local needs, the majority have not significantly extended the breadth of their capabilities (i.e. beyond basic product resale and implementation) or coverage (i.e. beyond smaller-sized businesses).

An opportunity exists to fill this demand gap for new entrants with a combination of a software solution such as Uncloak coupled with accompanying IT Security consultancies to further meet client demands, notably by:

- Supplementing security services offerings to include managed security services
- Selling to increasingly large customers with stringent IT security compliance requirements

Uncloak app poses an amazing opportunity to gain a number of additional revenue streams through access to end clients whose requirements for IT security management continually grows.

Overview of Technology

Uncloak™

The future of cyber threat detection

Overview of Technology

Uncloak's technology utilises an EOS proof of stake blockchain for transactions covering the UCC token in order to ensure low latency on transactions, reduced energy use and multiple threading capability.

Here is an overview of the EOS.IO technology.

CONSENSUS ALGORITHM (DPOS)

EOS.IO software utilises the only decentralised consensus algorithm capable of meeting the performance requirements of applications on the blockchain, Delegated Proof of Stake (DPOS). Under this algorithm, those who hold tokens on a blockchain adopting the EOS.IO software may select block producers through a continuous approval voting system. Anyone may choose to participate in block production and will be given an opportunity to produce blocks proportional to the total votes they have received relative to all other producers. For private blockchains the management could use the tokens to add and remove IT staff.

The EOS.IO software enables blocks to be produced exactly every 3 seconds and exactly one producer is authorised to produce a block at any given point in time. If the block is not produced at the scheduled time then the block for that time slot is skipped. When one or more blocks are skipped, there is a 6 or more second gap in the blockchain.

Using the EOS.IO software blocks are produced in rounds of 21. At the start of each round 21 unique block producers are chosen. The top 20 by total approval are automatically chosen every round and the last producer is chosen proportional to their number of votes relative to other producers. The selected producers are shuffled using a pseudorandom number derived from the block time. This shuffling is done to ensure that all producers maintain balanced connectivity to all other producers.

If a producer misses a block, and has not produced any block within the last 24 hours; they are removed from consideration until they notify the blockchain of their intention to start producing blocks again. This ensures the network operates smoothly by minimising the number of blocks missed by not scheduling those who are proven to be unreliable.

Under normal conditions a DPOS blockchain does not experience any forks because the block producers cooperate to produce blocks rather than compete. In the event there is a fork, consensus will automatically switch to the longest chain. This metric works because the rate at which blocks are added to a blockchain chain fork is directly correlated to the percentage of block producers that share the same consensus. In other words, a blockchain fork with more producers on it will grow in length faster than one with fewer producers. Furthermore, no block producer should be producing blocks on two forks at the same time.

If a block producer is caught doing this then such block producer will likely be voted out. Cryptographic evidence of such double-production may also be used to automatically remove abusers.

TRANSACTION CONFIRMATION

Typical DPOS blockchains have 100% block producer participation. A transaction can be considered confirmed with 99.9% certainty after an average of 1.5 seconds from time of broadcast.

There are some extraordinary cases where a software bug, Internet congestion, or a malicious block producer will create two or more forks. For absolute certainty that a transaction is irreversible, a node may choose to wait for confirmation by 15 out of the 21 block producers. Based on a typical configuration of the EOS.IO software, this will take an average of 45 seconds under normal circumstances. By default, all nodes will consider a block confirmed by 15 of 21 producers irreversible and will not switch to a fork that excludes such a block regardless of length.

It is possible for a node to warn users that there is a high probability that they are on a minority fork within 9 seconds of the start of a fork. After 2 consecutive missed blocks there is a 95% probability a node is on a minority fork. With 3 consecutive missed blocks there is a 99% certainty of being on a minority fork. It is possible to generate a robust predictive model that will utilize information about which nodes missed, recent participation rates, and other factors to quickly warn operators that something is wrong.

The response to such a warning depends entirely upon the nature of the business transactions, but the simplest response is to wait for 15/21 confirmations until the warning stops.

TRANSACTION AS PROOF OF STAKE (TAPOS)

The EOS.IO software requires every transaction to include the hash of a recent block header. This hash serves two purposes: it prevents a replay of a transaction on forks that do not include the referenced block; and signals the network that a particular user and their stake are on a specific fork.

Over time all users end up directly confirming the blockchain which makes it difficult to forge counterfeit chains as the counterfeit would not be able to migrate transactions from the legitimate chain.

ACCOUNTS

The EOS.IO software permits all accounts to be referenced by a unique human readable name of 2 to 32 characters in length. The name is chosen by the creator of the account. All accounts must be funded with the minimal account balance at the time they are created to cover the cost of storing account data. Account names also support namespaces such that the owner of account @domain is the only one who can create the account @user.domain.

In a decentralised context, application developers will pay the nominal cost of account creation to sign up a new user. Traditional businesses already spend significant sums of money per customer they acquire in the form of advertising, free services, etc. The cost of funding a new blockchain account should be insignificant in comparison. Fortunately, there is no need to create accounts for users already signed up by another application.

MESSAGES & HANDLERS

Each account can send structured messages to other accounts and may define scripts to handle messages when they are received. The EOS.IO software gives each account its own private database which can only be accessed by its own message handlers. Message handling scripts can also send messages to other accounts. The combination of messages and automated message handlers is how EOS.IO defines smart contracts.

ROLE BASED PERMISSION MANAGEMENT

Permission management involves determining whether or not a message is properly authorised. The simplest form of permission management is checking that a transaction has the required signatures, but this implies that required signatures are already known. Generally, authority is bound to individuals or groups of individuals and is often compartmentalised. The EOS.IO software provides a declarative permission management system that gives accounts fine grained and high level control over who can do what and when.

It is critical that authentication and permission management be standardised and separated from the business logic of the application. This enables tools to be developed to manage permissions in a general purpose manner and also provide significant opportunities for performance optimisation.

Every account may be controlled by any weighted combination of other accounts and private keys. This creates a hierarchical authority structure that reflects how permissions are organised in reality, and makes multi-user control over funds easier than ever. Multi-user control is the single biggest contributor to security, and, when used properly, it can greatly reduce the risk of theft due to hacking.

ACCOUNTS

EOS.IO software allows accounts to define what combination of keys and/or accounts can send a particular message type to another account. For example, it is possible to have one key for a user's social media account and another for access to the exchange. It is even possible to give other accounts permission to act on behalf of a user's account without assigning them keys.

NAMED PERMISSION LEVELS

Using the EOS.IO software, accounts can define named permission levels each of which can be derived from higher level named permissions. Each named permission level defines an authority; an authority is a threshold multi-signature check consisting of keys and/or named permission levels of other accounts. For example, an account's "Friend" permission level can be set for the account to be controlled equally by any of the account's friends.

Another example is the Steem blockchain which has three hard-coded named permission levels: owner, active, and posting. The posting permission can only perform social actions such as voting and posting, while the active permission can do everything except change the owner. The owner permission is meant for cold storage and is able to do everything. The EOS.IO software generalises this concept by allowing each account holder to define their own hierarchy as well as the grouping of actions.

NAMED MESSAGE HANDLER GROUPS

The EOS.IO software allows each account to organise its own message handlers into named and nested groups. These named message handler groups can be referenced by other accounts when they configure their permission levels.

The highest level message handler group is the account name and the lowest level is the individual message type being received by the account. These groups can be referenced like so: @accountname.groupa.subgroupb.MessageType.

Under this model it is possible for an exchange contract to group order creation and cancelling separately from deposit and withdraw. This grouping by the exchange contract is a convenience for users of the exchange.

PERMISSION MAPPING

EOS.IO software allows each account to define a mapping between a Named Message Handler Group of any account and their own Named Permission Level. For example, an account holder could map the account holder's social media application to the account holder's "Friend" permission group. With this mapping, any friend could post as the account holder on the account holder's social media. Even though they would post as the account holder, they would still use their own keys to sign the message. This means it is always possible to identify which friends used the account and in what way.

All EOS.IO information has been kindly provided by
https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

The Company: Structure, Team, Applicants & Advisors

Uncloak™

The future of cyber threat detection

The Team

Uncloak is an Estonia-based company. Estonia has been chosen for it's advanced understanding of block chain technologies and incentive to aid distributed ledger technology companies such as Uncloak to grow unhindered. Estonia is first of its kind to formally recognise the use of blockchain records as an accepted mechanism for transmitting payments, paving the way for broader adoption of the technology.

Tayo Dada

CO-FOUNDER, CEO & CYBER SECURITY EXPERT

Based in London's Tech city, Tayo has Over 30 years of experience working in IT from software development to IT management. Tayo manages an award-winning InfoSec team of experts in IT security and Cyber Threat management who are furnished with industry recognised qualifications/certifications including SC clearance, CISSP, ISO27001, Cyber Essentials, CEH and CREST. Actively involved in working with Start-ups and organisations who aim to accelerate their growth through innovative IT Solutions. Industry expert on IT Security with a background in hacking. Help set up Big 4 consultancy's first ethical hacking division in the UK.

Phil Jackson

CTO & CYBER SECURITY EXPERT

Industry renowned cyber security expert. Over 22 years of IT security and software development experience working with a myriad of organisations and cyber security applications. Strong understanding of the OWASP top 10 vulnerabilities. Contributing to the security test framework. Writing code to add to the security features within the application. Understanding global security threats and understanding impact on our applications. Ability to demonstrate vulnerabilities and advise teams on best practices to close these down. . Commercially skilled in Java, Spring 3 & 4, VB, VB.NET, C#, C++ and Python and scripting languages JavaScript and VBScript.

Nicholas Topham

COO & CO-FOUNDER

Nicholas has worked at the forefront of the TMT sector for 30 years, operating as a CEO, COO, partner level consultant and Investor. His experience spans the decades from computerisation, through liberalisation, mobile, the Internet, Datacentres, the growth of Asia and Developing markets, the Cloud and Applications and the processes necessary to run a business.

Nick Banks

COMMERCIAL DIRECTOR & CYBER SECURITY EXPERT

A senior commercial advisor to innovative technology companies for over thirty years. Building businesses that are sustainable and profitable has been a passion and achievement throughout a long and rewarding career. Successfully taken a number of different innovative technology companies to market globally and driven them to profitability and successful IPO or private sale. Achievements have included starting WatchGuard in Europe prior to a successful IPO, Managing Director of Webroot as it transitioned from a consumer to enterprise focused company, Global VP Sales of IronKey, a brand eventually sold to Kingston Technologies and VP Sales of emerging markets for CyberGuard.

Toby Abel

AI EXPERT

Toby is a technology entrepreneur creating product development teams, overseeing tech builds and crafting funding and BI strategies for startups, MVPs, business transformation and exits. Combining AI- driven search and recommendation engines with industry relevant tools and deep linguistic analysis. Working across business sectors including: events, technology, education, recruitment, security, fashion and news. Toby uses outstanding consultancy skills to take world class teams with proven prototypes to a global stage.

Brendan Sturm

BLOCKCHAIN DEVELOPER

Brendan is an engineer, entrepreneur, and blockchain enthusiast. Brendan's background is in computer science with experience in Solidity, token development, Dapp development, and Python. Previously, he worked at Capital One where he designed and implemented many fraud defenses.

Jae Chung

SENIOR EOS DEVELOPER

Jae Chung is a Systems Engineering major from the University of Pennsylvania. An aspiring entrepreneur, he has been involved in a number of blockchain projects. Sungjae is a firm believer in growing a decentralized network where no one large entity can control and manipulate data. Jae is also a member of the famed HKEOS, an Hong Kong based EOS block producer candidate. Skillsets cover EOS development, C, C++ and Java.

Dean Jackson

SENIOR SOFTWARE DEVELOPER

Dean is an accomplished full-stack developer, one of the original developers of the Uncloak prototype. 15 years of experience working with some of the fastest growing FinTech companies within the UK. Advanced knowledge in private/public cloud infrastructure, PHP, MVC frameworks, REST API, Javascript & Linux OS.

Vincent O'Neill MBE

SENIOR CYBER SECURITY CONSULTANT

A security expert with over 30 years experience of security operations across government, intelligence and commercial sectors. Designer and leader of integrated security solutions for the physical and digital domains. Cyber security advisor and business leader for energy security, financial services risk management and global sports events.

Claire Mclaughlin

HEAD OF COMMUNICATIONS

A commercially astute innovator and strategist with a proven track record of success in driving product development and entry to market. A pioneer of new technology and consumer engagement. Head of Marketing and Content leveraging blockchain technology in partnership with cross-functional teams. Former Global Head of Interactive Technology at the BBC. Key strategist for the UK Women in Technology Network.

Lena Bhogaita

HEAD OF OPERATIONS

An operational specialist in cyber threat analytics and reporting. PMO and product consultant she is responsible for the product launch, communications and business operations of Uncloak. Prior to joining our team, she was Operations Manager for the workplace strategy team at Sky, leading European broadcaster, with +20,000 employees and +23 million subscribers across its media platforms.

Ola Dada

COMMUNITY MANAGER

Actively involved in a number of successful start-ups across EMEA since the emergence of social media. Experienced in facilitating media and business conferences, panels, press and social media. An avid block chain investor with a deep knowledge of security, governance and privacy technologies. An expert of online strategy for 15,000 users+, identifying key messaging for development teams and b2b and b2c communities. Delivers targeted campaign management with measurable outcomes.

Advisors

Uncloak is underpinned by industry experts. Each person is a technology heavyweight contributing to some of the largest and most technically advanced companies in the world. These include the following:

Hugh Chambers

STRATEGIC ADVISOR

Hugh is the CEO of The Cyber Authority, headquartered in London. The Cyber Authority specializes in cyber threat detection, mitigation and remediation. Hugh is an accomplished international business pioneer in the development of innovative and progressive companies across a wide range of disciplines. Hugh has been a senior executive in 40 worldwide companies and a Fellow of the Institute of Directors. Career highlights include being one of the key innovators for the international courier industry, then helping to turn Hong Kong Telecom into a $100m/year EBITDA business over the course of just six months. He then went on to establish a telecommunications company for MIM BV that brought in revenues of $80m/year with operations in 23 time zones. Hugh co-founded Interoute, which stands as the largest telecommunications group in Europe today, recently sold to GTT Communications for $2.3 billion cash (March 2018).

Asad Mahmood

AI AND BLOCKCHAIN ADVISOR

Asad Mahmood, M.D. is a Watson AI and Blockchain Engineer at IBM, Cryptocurrency Investor and ICO Advisor. He is also a Biomedical Engineer, a Computer Scientist and a Medical Doctor. As a developer of decentralized applications (DApps) on the Graphene (Steemit, Bitshares, EOS), Ethereum and Hyperledger Fabric blockchains, Asad leverages his deep technical understanding of blockchain technology to conduct technical code and MVP reviews for new Initial Coin Offerings (ICOs). As an accomplished Blockchain and AI Engineer, Asad brings a hands-on technical approach by advising developers on the architecture and development of the AI engine for the Uncloak application.

Steve Godman
STRATEGIC ADVISOR

Steve is an experienced, commercially-driven entrepreneur who has has been involved in early-stage, disruptive technology businesses for nearly 20 years, following an early career in global logistics. He has led sales and marketing teams across MarTech, messaging, mobile and social platforms. In 2011 Steve served as Commercial Director of Skinkers, driving their acquisition by IMImobile PLC. He continued to orchestrate the successful merging of the two companies and the sale of their mobile and social media aggregation and curation tool to over 80% of UK media companies including the BBC. In 2014, Steve launched Soundmite, the world's first social audio service across mobile and web.

Mitchell Scherr
ADVISOR

Mitchell Scherr is a Digital Data Pioneer with 23 years' experience in the IT industry. He is a market driven CEO, successfully leading businesses and helping organisations and governments to protect, find and make sense of their complex data structures. Mitchell has an acute understanding of every aspect of the corporate lifecycle - from product development to marketing and sales strategy to the development of global alliances and joint ventures and domestic and international fund raising initiatives. He has an extensive experience in the USA, UK, Australia and the GCC. Mitchell is an inventor of two US Patents, relating to 'Relevance Ranked Faceted Meta Data Search' presently used within product offerings provided by Bloomberg/BNA. He was a key note speaker at several major global industry conferences and interviewed and published by NBC and Fox TV, Wall Street Journal, Internet World and Business 2.0.

Charles Nolan
ADVISOR

Charles Nolan is a dynamic individual who specializes in transformation, change and consolidation across a wide range of industries in the Information Technology and Communications field. Charles is adaptable, entrepreneurial and fast acting on assignments delivered to get results. He specializes in execution and delivery within the organisation from Plan through Design, Build & Run. In touch with ever-changing modern technology, Charles can deliver results including the sought after areas of transformation, Operations, Consolidation, Analytics, Cloud Computing and High Density computing. Bringing his international and cultural experience with global organisations, Charles can operate and interact across the globe, and achieve the optimal results within the respective cultural and national environments. Charles' broad industry experience brings a hybrid vigour to his assignments, and he is a known leader in various industry forums, from Strategy, Governance and Innovation, to Cloud Computing, new Technologies and Education.

Corporate Governance, Compliance, Legal

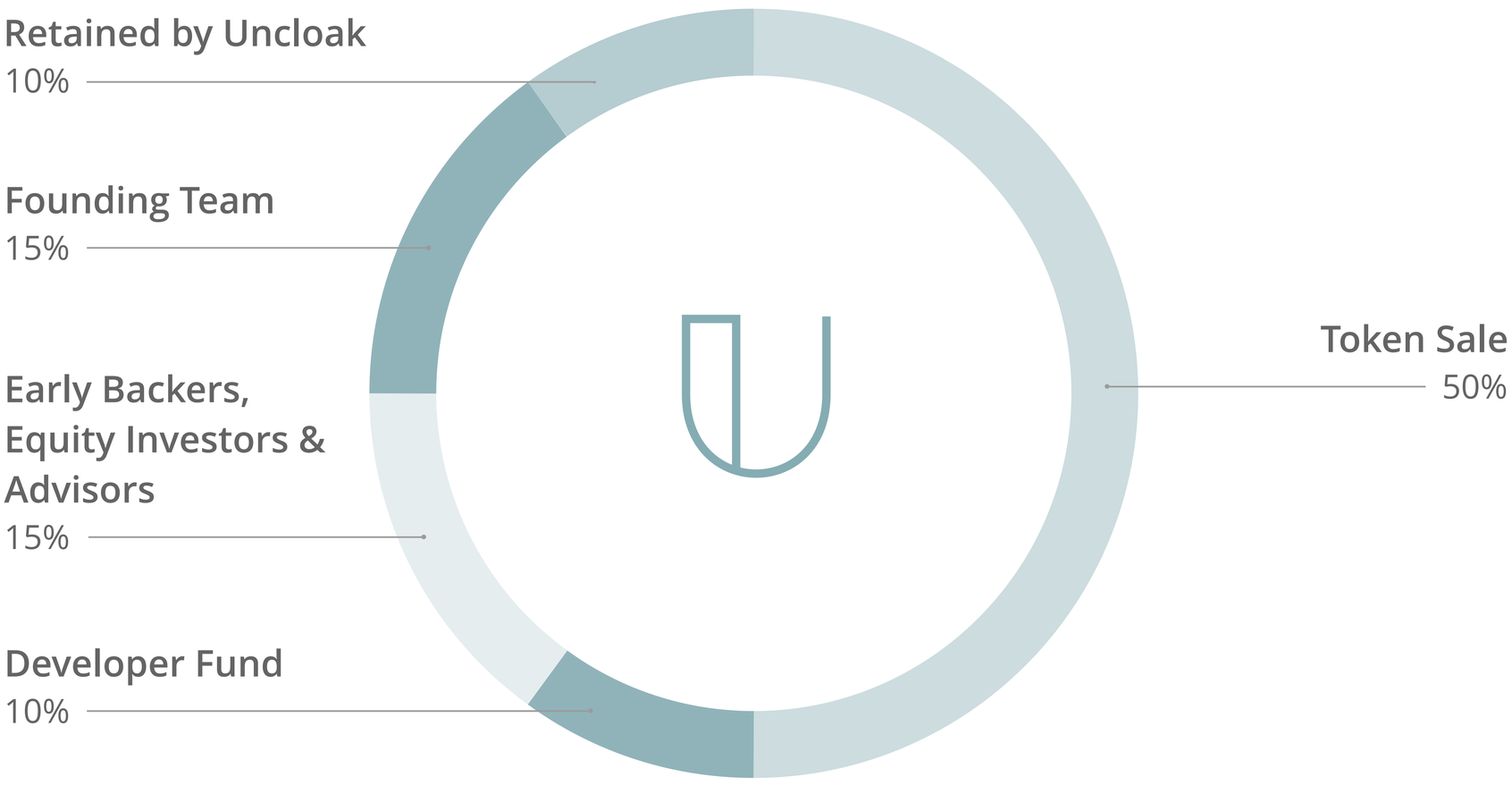
Uncloak™ insists on maintaining high standards for operating a transparent business. We utilise the services of a group of top professional firms in legal & accounting to ensure these standards are met.

We have engaged one of the Big 4 professional services firms to assist us on accounting, tax and governance advisory services

> **Evelyn Warner**
> LEGAL COUNSEL (WARNER ASSOCIATES)
> SRA ID: 325185SRA

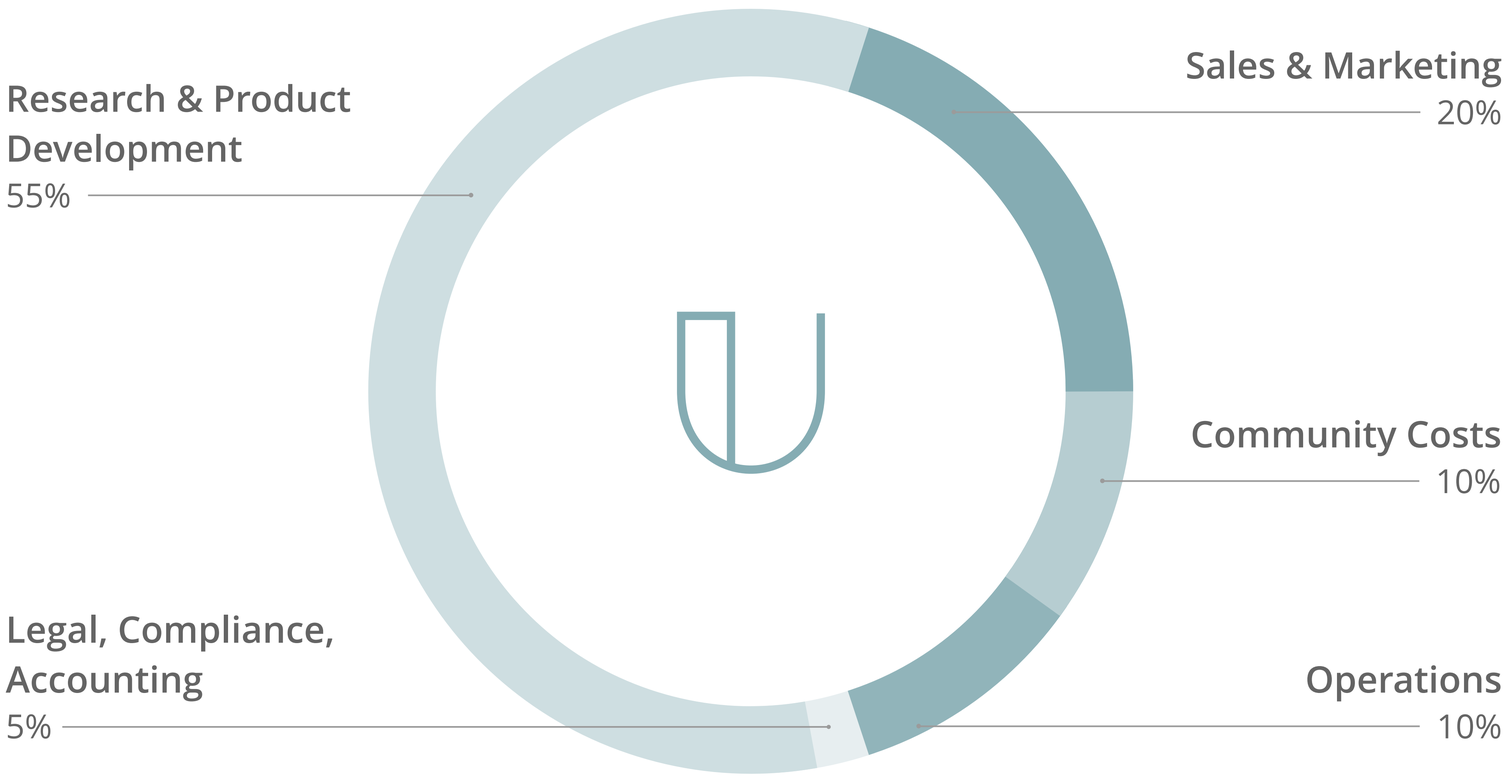
Token Sale

Uncloak will be executing a token sale to raise funds for development and commercialisation of its next generation of cyber threat management. The maximum amount we will accept is a value of $21,000,000 USD. The only accepted currency will be ETH. Exact pricing of ETH to UNC will be determined at a later date prior to the official token sale.



TOKEN SALE	50%	UNC token will be offered for sale to be used for the Uncloak platform.
RETAINED BY UNCLOAK	10%	The retained tokens will be used for converting between UNC and UCC tokens for hunters and can also be used in additional offerings to further development and staff incentives.
DEVELOPER FUND	10%	Used to incentivise, reward and attract outside developers to build projects, integrations, partnerships, hackathons and community involvement. Growing the ecosystem is important.
FOUNDING TEAM	15%	Uncloak's founders have been working on the business for over three years. Allocation of their UNC tokens will vest over 18 months.
EARLY BACKERS, EQUITY INVESTORS AND ADVISORS	15%	Uncloak have early investors and advisors to help with the development of the technology. Part of the equity investments have been converted into tokens.

Use of Funds



RESEARCH & PRODUCT DEVELOPMENT:	55%	Use to continuously develop the product, grow the team globally.
COMMUNITY COSTS	10%	Initial capital needed to incentivise the community and drive membership for bug bounty.
SALES AND MARKETING	20%	Grass-roots marketing to start and expand to webinars, conferences, sponsorships, advertising and PR.
OPERATIONS	10%	General overhead and administrative costs for running the business on a global scale.
LEGAL, COMPLIANCE, ACCOUNTING	5%	

Project Roadmap

Uncloak™

The future of cyber threat detection

Roadmap

Q4 2016

Q1 2017

Development of CSaaS - “Cyber security as a service” application for customers to perform their own security checks

Q2 2017

Strategic Partnership formed with the worlds largest human resources firm to provide cyber security consultancy to public/private sector clients

Q4 2017

Awarded best in class IT consultancy by Wealth and finance magazine

Q1 2018

CSaaS renamed to Uncloak

Q1 2018

Strategic alliance formed with world leading artificial intelligence software developers

Q1 2018

Released whitepaper

Q2 2018

Building community and strategic relationships.

Q2 2018

Uncloak™ UNC token crowd sale

Q3 2018

Development of cyber threat detection AI engine (beta)

Q3 2018

Development of bug bounty alpha based on EOS™

Q3 2018

Launch of Uncloak channel partner model

Q4 2018

Launch of Bug Bounty community

Q4 2018

Launch of Uncloak bug bounty alpha on EOS testnet

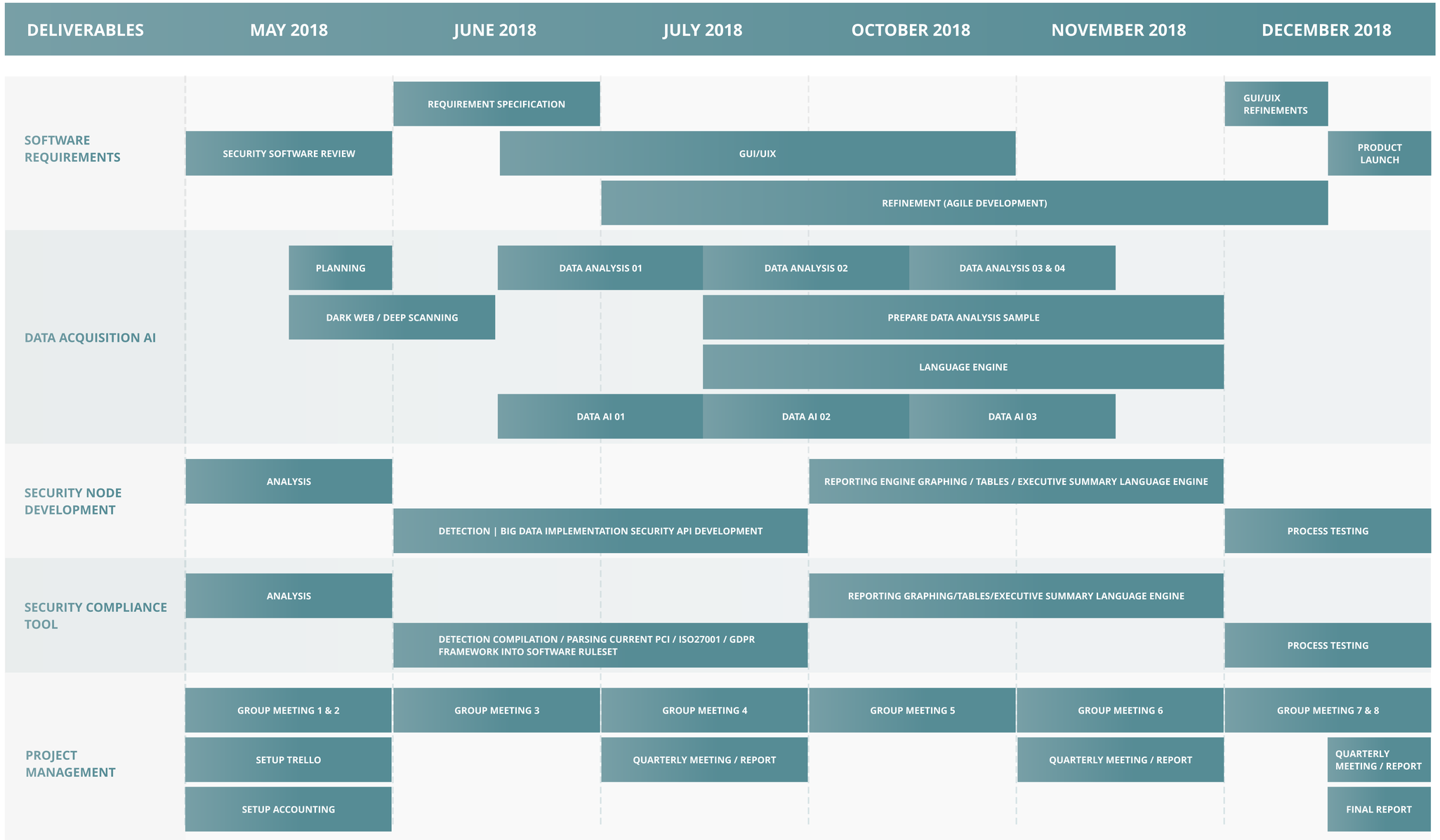
Q4 2018

Alpha launch of Uncloak AI engine

Q4 2018

Uncloak™ general public platform release

Project Gantt Chart



Work Package Descriptions

WORK PACKAGE 1	SOFTWARE REQUIREMENTS – GUI/UIX
OVERVIEW	Scoping of the Uncloak solution/software requirements/APIs/competitor analysis/ gap analysis.
DURATION	9 months
DESCRIPTION OF WORK	The project employs an Agile approach to Tasks - Timeline analysis and agreement on target solutions for software coding team. Continued cyber app software developments and refinements based on end user feedback and support from industry advisors steering committee. The requirements will be updated accordingly with software development. The final delivered software will be tested against Industrial guidance steering committee requirements.
DELIVERABLES	• Initial gathered requirement • Refinement / updates of requirements • GUI Design • GUI / UIX refinements design • Final Uncloak UIX requirement specification • Test report results • Peer-reviewed research, ongoing client management

WORK PACKAGE 2	DATA ANALYSIS - DATA ACQUISITION MACHINE LEARNING
OVERVIEW	Uncloak will be able to pull articles/posts/blogs data directly from deep web/dark web/public internet sources and create a set of live reports based upon the patterns found.
DURATION	4 months
DESCRIPTION OF WORK	This work package includes review of existing internet data scanning internet/dark web/deep for security vulnerabilities spoken in chat rooms/forums/blogs. The acquisition of web data will serve as a component for creating the premium security threat landscape reporting feature.
DELIVERABLES	• Data Acquisitions for Test report • TEST Capture 1 of Dark web/deep web data • TEST Capture 2 • TEST Capture 3 • Disseminate Via WP5

WORK PACKAGE 3	SECURITY NODE DEVELOPMENT - BIG DATA ELEMENT
OVERVIEW	Uncloak™ will pull anonymised vulnerability data from all client Uncloak scans to create a threat landscape report which highlights the most prevalent issues affecting workstations/servers/routers/firewall. The benefits of the report will allow a client to see that the most common attacks/vulnerabilities in real-time and help to mitigate against cyber security risks.
DURATION	9 months
DESCRIPTION OF WORK	The work package will initially utilise and evaluate methods and implementations of detecting Security patterns in Stage 1. Next, we will address collecting security information from multiple Uncloak-app implementations. The most effective, efficient and robust analytics will then be implemented, optimised, and tested for the final build based on three or four Uncloak nodes per WP 2.
DELIVERABLES	• Initial Analysis • Stage 1 Detection • Stage 2 filtering and cleanup of data • Refinements: • GUI Integration • Final Report

WORK PACKAGE 4	SECURITY COMPLIANCE TOOL
OVERVIEW	This development will allow Uncloak to check against compliance standards covering the IT elements of ISO27001, GDPR and PCI DSS such as password strength on workstations/servers, encryption used, poor security policy on computers.
DURATION	9 months
DESCRIPTION OF WORK	This work package focuses on creating tools that are able to pull security IT compliance data from workstations/servers/routers/firewalls/network which is then used to analyse/benchmark data against it standards such as cyber essentials, ISO 27001, using deep learning technologies (techniques. Inherently tied to WP 3 and using Data from WP 2. Initial R&D of existing pipeline. Framework devised for program advancement.
DELIVERABLES	• Process R&D Requirements • Framework COMP • Composite • Refinements • Prototype • Final Report

WORK PACKAGE 5	PROJECT MANAGEMENT
OVERVIEW	Effective and experienced project management will ensure the Uncloak project is delivered on time and to specification.
DURATION	9 months
DESCRIPTION OF WORK	A series of scheduled in-person monthly meetings will occur at DEV for monitoring and continued QA of developments. Using TRELLO for virtual tasking organisation. This work package includes managing the project by making the decisions at established milestones, ensuring that the project's result will contribute to the benefits, supporting the project management in terms of advice, purchase needs and resource needs, staying continuously informed about the project's status by means of steering group meetings, status reports, budget, risk and project analyses.
DELIVERABLES	• Project plan • Industrial Guidance Steering Group Data analysis • Risk register • Contracts and Legal • Status reports • Stakeholder reports • Project report (final)

Risk Assessment

RISK	IMPACT	LIKELIHOOD	MITIGATION APPROACH
Competition Competition emerges for Uncloak-degree data analysis software.	**M**	**M**	• Seek patent protection for foreground intellectual property emerging in the project. • Develop hard-to-replicate software assets
Slow Market Adoption The willingness of customers to adopt Uncloak security software over traditional formats may be slower than expected; e.g. the market for cyber security threat detection is relatively new, rapidly evolving and somewhat unproven.	**M**	**L**	• Target sales efforts in domains where early market adoption has already started in IT security firms/IT consultancies • Work with established channel market to to push the adoption of Uncloak™
Technical challenges Some of the technical approaches in the project to perform dark web/deep web research require algorithms and have never been automatically implemented in IT security applications	**H**	**L**	• Utilise Uncloak/DEV staff with the significant expertise in both IT security applications, Big data processing, and data analysis production. • Adopt an Agile approach to include stakeholders in the development cycle to specify software features and use a MoSCoW (Must, Should Could, Would) requirements prioritisation.
Implementation Delays Software projects can face implementation delays	**M**	**M**	• Using the Agile approach, establish software requirements early into the project, and refine software requirements with the development. Avoid the temptation to add features (feature creep) and focus on high priority requirements. • Use a professional project task tracking tool like Jira to avoid overloading individuals with tasks. • Project management to have monthly reviews of project to ensure the project stays on schedule and meets deadlines.

Risk Disclosures

Please study, understand and evaluate the risks that Uncloak Platform describes below.

The realisation of any one or more risks, either described in this White Paper, or any unforeseen or unforeseeable risks, could significantly reduce or eliminate the utility or value of UNC and any participant (each, a "Participant") in a proposed sale of UNC (the "Token Sale") could lose their entire investment in UNC. Uncloak Platform does not state that this White Paper discloses all risks and other significant aspects of the Token Sale, including risks which may be specific to a particular Participant and thereby unknown to Uncloak Platform.

All proposed Participants should fully understand and be comfortable with the risks described in this White Paper and they should consult their legal, commercial, financial, tax, or other professional advisers; otherwise, they should not participate in the Token Sale.

To the maximum extent permitted by all applicable laws and regulations, Uncloak Platform (and Uncloak Related Parties shall not be liable for any direct or indirect loss or adverse effect on revenue, income, profits, business, business opportunity, anticipated saving, data, reputation, or goodwill; or any other losses or damages of any kind, including but not limited to indirect, special, incidental, reliance, consequential or punitive, in tort, contract, strict liability, or otherwise, arising out of or in connection with any loss or damage of a Participant (or a proposed Participant) relating to the information supplied within this White paper.

Company Risks

Company Failure: The failure of Uncloak Platform's business and its subsequent dissolution or winding up could be as a consequence of the realisation of one or more of the other risks in this White Paper or of risks not known at the time of publication.

Should Uncloak Platform's business fail and Uncloak or the software platform on which it operates (the "Application") is not transferred to and operated by another company, Uncloak would terminate and any UNC would have no utility or value. Uncloak Platform cannot commit to the transfer of the Application or Uncloak to another company if its business fails. If Uncloak Platform does transfer the Application or Uncloak to another company, Uncloak Platform cannot commit that the other company will operate Uncloak and\or UNC to a Participant's satisfaction or at all.

Management Failures: Uncloak could be adversely affected by Uncloak Platform's management's failure to manage its corporate and other resources effectively and efficiently to develop, operate, maintain, support, improve, market, and sell the Application and Uncloak, or to manage the growth of Uncloak or its business, or to adapt the Application or its business to technological or market changes, or to identify and effectively respond to the risks described in this White Paper or otherwise.

No Governance Rights: Ownership of, investment in or participation with UNC does not confer any governance or similar rights with respect to Uncloak Platform, the Application, or Uncloak. Uncloak Platform will make all decisions concerning its business, the Application, and Uncloak. These decisions need not be referred to investors in and owners of UNC and may be at variance with their expectations.

Business Model Risks: The Business Model to which Uncloak Platform designed Uncloak (including the Application and UNC) depends on several factors, including:

- Uncloak Platform's ability to hire top engineers to develop the Application and Uncloak
- The number of users providing resources to support the functions of Uncloak
- The availability of UNC to Uncloak users after the Token Sale
- The number of users perceiving UNC to be valuable and thus willing to use Uncloak as either providers of resources or consumers of Uncloak.

If this business model or its underlying assumptions are flawed or incorrect Uncloak may underperform or fail. Uncloak Platform may at its discretion elect to amend or optimise the business model of Uncloak to address any flaws or in response to competition or market requirements or otherwise. In turn any such changes may fail to achieve their purpose and could adversely affect Uncloak.

Insufficient Funding: Operational funding for Uncloak Platform will initially depend on the proceeds of the Token Sale until such time, if ever, that Uncloak Platform earns sufficient revenue from Uncloak or other activities. The proceeds of the Token Sale are cryptocurrencies that may fluctuate in value. Uncloak Platform may, at its discretion, engage in hedging or similar activities to manage these fluctuations, but these activities themselves may adversely affect the value of the proceeds. In addition, any cryptocurrencies held by Uncloak Platform may not be convertible to fiat currencies or other cryptocurrencies at a favourable rate, if at all...Should Uncloak Platform's funds not be sufficient to sustain its operations, Uncloak Platform may reduce or suspend its operations, adversely affecting Uncloak Platform's ability to develop and operate Platform at the intended level or at all.

Unanticipated Risks: Uncloak will be launched and will evolve in environments that are uncertain and subject to rapid, unpredictable, and potentially adverse change This will create future risks which are unknown and unknowable but which could adversely affect the viability or existence of Uncloak.

Product Risks

Delay: Uncloak Platform may not develop and deploy the Application according to its intended schedule, which could delay the deployment of the Application, adversely affecting the acceptance of Uncloak.

Inability to Use UNC: Holders of UNC will not be able to use them with Uncloak until the Launch. Launch may be delayed or may not occur at all. Even after Launch, the availability of certain services will be limited.

Failure to Develop and Support the Service: Uncloak (including UNC) may not have the utility or functionality described in this White Paper or expected by a Participant. This may be because of the realisation of one or more of the risks outlined in this White Paper, the realisation of risks not described in this White Paper, business or technical decisions taken by Uncloak Platform in good faith, failure to launch Uncloak with a full set of intended features and functions, discontinuation of certain features and functions of Uncloak, failure to support or enhance Uncloak

Service Issues: Uncloak performance may be adversely affected, because of infrastructure failures, security events, including but not limited to breaches, hacking, viruses, malware or other malicious code, and other causes. Uncloak Platform may be unable to restore Uncloak to normal operations.

Service Updates: Uncloak Platform may not update Uncloak to fix bugs, address incompatibilities, respond to user feedback, or react to competitive threats adversely affecting Uncloak.
Failure to Meet Expectations: The initial and future versions of Uncloak may not meet a Participant's expectations regarding items such as features, functions, performance, availability, quality, security, scale, price.

Reliance on Third Parties and Third-Party Systems: Uncloak Platform relies on third parties and third-party systems it does not control to operate and provide services for the Application and Uncloak. The failure of those third parties or third-party systems to perform according to Uncloak Platform's needs and expectations could adversely affect Uncloak.

Privacy Risks: Uncloak will rely in part on Ethereum and other public, decentralised platforms. Any information about or belonging to a Participant that is processed by or stored in these platforms in connection with a Participant's use of Uncloak, may be inspected by the public, via the Internet. Certain information may, even if encrypted, be associated with a Participant by Combining this information with other public or non-public information may allow information to be inferred.

Technology Risks

Core Technology Risks: The Ethereum blockchain platform and various open source software applications and libraries are core technologies for Uncloak but are immature and not fully proven. If these core technologies do not meet Uncloak Platform's expectations, are not fully supported and updated in all aspects of system performance, security, integrity and availability, are developed in a way that is incompatible with Uncloak, or do not meet future requirements of Uncloak, Uncloak Platform may change the features, functions and specifications of Uncloak or to discontinue Uncloak.

Integration Risks: Uncloak will be integrated using third party services. Should these services fail, or not meet Uncloaks expectations and requirements in any way, Uncloak will be adversely affected.

Smart Contract Risks: Certain key features of Uncloak will be implemented in smart contracts on the Application and on the Ethereum blockchain platform. These contracts can be difficult to change or amend for whatever reason. Uncloak Platform may therefore not correct defects or improve Uncloak in a timely manner to meet changing requirements, which could adversely affect the utility or viability of Uncloak.

Hacking: All software systems, not just the Application and the Ethereum blockchain platform, are subject to attack with the intent to. disrupt, corrupt, or interfere with the system, defraud or steal currency or other valuable data stored in the system. Participants or UNC holders: may be affected by this.

Mining Attacks: Ethereum is a decentralised service comprising a global peer-to-peer network of many independent node operators. Coordination or collusion among node operators could compromise the integrity of Uncloak, cause loss, theft, or corruption of UNC and other valuable data stored in Uncloak,, or increase the cost of using the platform to levels that make operation of Uncloak uneconomic and unsustainable.

Security Risks: Advances in techniques or computing power, and exploitation of known current weaknesses to compromise the cryptographic algorithms underpinning the security and integrity of Uncloak, may cause the loss, theft, or corruption of UNC and other valuable data stored in Uncloak, and require the suspension or discontinuation of Uncloak. The development of stronger cryptographic algorithms and their implementation in Uncloak and its underlying core technologies is uncertain.

Prohibitively High Transaction Costs: All transactions on the Ethereum blockchain platform have a cost in Ether ("Gas") which at the date of this White Paper, are nominal. However, Gas prices may increase and make the trading of UNC on the Ethereum blockchain platform commercially unfeasible.

Ethereum May be Superseded: In Uncloak Platform's view, the Ethereum blockchain platform is currently the optimum blockchain platform from which to issue UNC. However, it is not known whether the Ethereum blockchain platform will remain the predominant platform for token issuances. Should Ethereum be superseded, UNC could be adversely affected as usage and adoption declines.

Regulatory Risks

Regulatory Status: Regulators in many jurisdictions have announced their intention to consider the adoption and tightening of regulations to cover cryptographic tokens and their markets for them. It is not known how or when different jurisdictions will interpret existing laws and regulations or adopt new laws and regulations, or whether those laws or regulations would be applied retroactively. The affect these changes would have on the Application, Uncloak, UNC and the Token Sale are not known but the direct or indirect effects could cause Uncloak Platform to modify or discontinue certain features or functions of Uncloak and\or the Application, or cause Uncloak Platform to discontinue the Application or Uncloak in specific, or all jurisdictions.

Excluded Jurisdictions: It is a Participant's sole responsibility to determine if they are prohibited or restricted from participating in the Token Sale, or if such participation constitutes a breach of the laws or regulations of their jurisdiction, whether by virtue of their citizenship, residency, or other association with a jurisdiction which prohibits or otherwise restricts the conduct of the Token The Participant will be solely responsible for any criminal and/or other penalties being imposed Compliance Risks: The failure to comply with laws and regulations that apply to Uncloak Platform, the Application and/or Uncloak would restrict or prevent Uncloak Platform from operating Uncloak in that jurisdiction and may be costly and divert a significant portion of Uncloak Platform's attention and resources. There is no guarantee that Uncloak Platform will qualify for or be granted the necessary licence, registration, or approval, required to operate. Failures to comply with applicable laws or regulations could leave Uncloak Platform subject to significant legal liability and financial and reputational losses adversely affecting the Application, Uncloak, and/or UNC.

Tax: The tax status of the Application, Uncloak, UNC, and the Token Sale is unclear or unsettled in many jurisdictions. Interpretation of existing or adoption of new tax laws and regulations could result in unanticipated and potentially retroactive tax liability for Uncloak Platform and other stakeholders in Uncloak, including Participants and UNC holders. In these circumstances, Uncloak Platform could modify or discontinue certain features or functions of Uncloak or the Application, or increase prices for Uncloak and the Application. In addition, dealing in UNC may become subject to tax in certain jurisdictions.

Regulatory Risks

Lack of Market Penetration: Failure to attract users and/or third parties providing services to Uncloak at a required level could negatively affect the development of Uncloak and/or the utility or value of Uncloak and/or UNC.

Competition: Other organisations developing services that compete with Uncloak or cryptographic tokens similar to Uncloak may adversely affect the adoption and use of Uncloak and/or the adoption, utility, and/or value of UNC, and ultimately the viability and continued existence of Uncloak and/or UNC.

Secondary Markets for UNC: As at the date of this White Paper, there is no public market, virtual currency exchange, or other secondary markets for UNC. Should any of these environments exist, there is no assurance that an active or liquid trading market for UNC will develop be sustainable.

Unless Uncloak Platform publicly states otherwise, Uncloak Platform has no financial or other relationship with, and does not endorse, any such exchange or secondary market that elects to transact in UNC. Any Participant wishing to use virtual exchanges and\or secondary markets should seek professional advice as their use could result in Participants' or UNC holders' loss of UNC or other losses.

Price Volatility: The price of UNC in the Token Sale may not be indicative of the price of UNC on public markets. UNC have no intrinsic value at the time they are created. The price of UNC on public markets may be extremely volatile, in response to various factors, some of which are outside Uncloak Platform's control, including, but not limited to, the following:

- The volatility of the prices of cryptographic tokens generally
- General economic conditions and macroeconomic changes
- Changes and innovations in blockchain technology, the industry sectors in which Uncloak Platform operates, and other technologies and markets
- Uncloak Platform's announcements pertaining to strategic direction, key personnel, financial and operational results, partnerships, significant transactions, new products, and other events
- Activities and announcements of Uncloak Platform's competitors
- Third-party reports, recommendations, and statements regarding UNC, the Application, Uncloak, or Uncloak Platform

Regulatory Risks

Risk of Dilution: In addition to the Token Sale, Uncloak Platform will create and distribute UNC as described in pages 31 and 32 of this White Paper. In many cases these UNC will be distributed for less consideration per UNC than in the Token Sale. The distribution of such UNC will increase the overall supply of UNC in the market and may result in downward pressure on the market price of UNC. In addition, Uncloak Platform reserves the right to create and distribute new UNC in one or more other token sales.

Market Perception: The market price of UNC could be adversely affected by negative publicity, social media commentary, rumours, and other information, whether or not true, about Uncloak Platform, the Application, Uncloak, UNC, the technology on which Uncloak is based (including Ethereum), and/or the legal or regulatory environment in which the Application or Uncloak operates.

General Economic and Market Risks: Like all businesses, Uncloak Platform and its suppliers and third parties are susceptible to adverse changes in general global and regional economic and market conditions which may adversely affect the availability, reliability, performance, adoption, and the success of Uncloak.

Participant Risks

Private Key Risks: Each Participant is solely responsible for securing the private key that controls their UNC. If a Participant loses or is unable to recover their key or credentials for whatever reason, they will permanently lose their UNC.

Token Sale Process Risks: The process for participating in the Token Sale will be described in the Token Sale Terms If this process is not followed, a Participant may not be able to participate in the Token Sale or purchase UNC, they may permanently lose the funds which they intend to submit as payment for UNC, or they may permanently lose UNC which they have purchased. The Payment Address, like all software systems, has security vulnerabilities and is subject to attack and attempts to steal funds Each Participant accepts all risk and is responsible for all loss or theft of their payments from the Payment Address.

Incompatible Wallet: The technical requirements for the Payment Address will be described in the Token Sale Terms. Use of a wallet, service or other technology that does not conform to these technical requirements, their UNC may be permanently lost.

Uninsured Losses: UNC are not insured by Uncloak Platform or by any public agency and Uncloak Platform cannot issue new or substitute UNC to replace lost or stolen UNC. If a Participant wishes to insure their UNC they must do so at their own expense.

Defined Terms

Uncloak Related Parties: Any affiliate of Uncloak Platform, and its and their founders, directors, officers, employees, advisers, agents, and representatives

Launch: Uncloak Platform makes UNC available for use with Uncloak

Token Sale Terms: The terms and conditions applicable to the process for participating in the Token Sale will be described in a document which Uncloak Platform will make available separately from this White Paper.

Crypto Wallet: The digital wallet to which payment for UNC will be made. The technical requirements will be described in the Token Sale Terms.

References

Chaudhary, K. (2017). DLP Solutions: Evaluation Tips And More. Computer Weekly, [online] Volume(Issue), pages. Available at: http://www.computerweekly.com/tip/DLP-solutions-Evaluation-tips-and-more [Accessed 8th April 2017]

Dignan, L. (2016). Your Biggest Cybersecurity Weakness Is Your Phone. Harvard Business Review, [online] Volume(Issue), pages.Available at: https://hbr.org/2016/09/your-biggest-cybersecurity-weakness-is-your-phone [Accessed 8th April 2017]

Dredge, S. (2016). Facebook Scammers: Expert Advice on How to Stay Safe. Journal, [online] Volume(Issue), pages. Available at: https://www.theguardian.com/technology/2016/mar/21/facebook-scammers-safety-cybersecurity [Accessed 8th April 2017]

Gammons, B. (2017). 6 Must-Know Cybersecurity Statistics for 2017 | Barkly Blog. Barkly, [online] Volume(Issue), pages. Available at: https://blog.barkly.com/cyber-security-statistics-2017 [Accessed 8th April 2017]

Harris, J. (~2014). Antivirus Software. Essential Guide: Secure Web Gateways, From Evaluation to Sealed Deal, [online] Volume(Issue), pages. Available at: http://searchsecurity.techtarget.com/definition/antivirus-software [Accessed 8th April 2017]

Haynes, J. (2017). Backdoor Access to Whatsapp? Rudd's Call Suggests a Hazy Grasp of Encryption. The Guardian, [online] Volume(Issue), pages. Available at: https://www.theguardian.com/technology/2017/mar/27/amber-rudd-call-backdoor-access-hazy-grasp-encryption [Accessed 8th April 2017]

Hughes, B. (2017). The Internet of Things: An Overview. Computer Weekly, [online] Volume(Issue), pages. Available at: http://www.computerweekly.com/opinion/The-internet-of-things-an-overview [Accessed 8th April 2017]

Last name, First initial. (Year published). Governance and Regulatory Compliance. IT Governance, [online] Volume(Issue), pages.Available at: https://www.itgovernance.co.uk/compliance [Accessed 8th April 2017]

Moulds, J. (2017). Cyber Security Takes Centre Stage in The Age of Trump. The Guardian, [online] Volume(Issue), pages. Available at: https://www.theguardian.com/small-business-network/2017/jan/16/cyber-security-centre-stage-age-trump-investment-hackers [Accessed 8th April 2017]

Rouse, M. (~2012). Data Loss Prevention (DLP). Essential Guide: Unified Threat Management Devices: Understanding UTM And Its Vendors [online] Volume(Issue), pages. Available at: http://whatis.techtarget.com/definition/data-loss-prevention-DLP [Accessed 8th April 2017]

Scholfield, J. (2016). How Can I Remove a Ransomware Infection? The Guardian, [online] Volume(Issue), pages. Available at: https://www.theguardian.com/technology/askjack/2016/jul/28/how-can-i-remove-ransomware-infection [Accessed 8th April 2017]

Smith, M. (2016). Huge Rise in Hack Attacks as Cyber-Criminals Target Small Businesses. The Guardian, [online] Volume(Issue), pages.Available at: https://www.theguardian.com/small-business-network/2016/feb/08/huge-rise-hack-attacks-cyber-criminals-target-small-businesses [Accessed 8th April 2017]

Thielman, S. (2016). Can We Secure the Internet of Things in Time to Prevent Another Cyber-Attack? The Guardian, [online] Volume(Issue), pages. Available at: https://www.theguardian.com/technology/2016/oct/25/ddos-cyber-attack-dyn-internet-of-things [Accessed 8th April 2017]

Woolf, N. (2016). DDos Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say. The Guardian, [online] Volume(Issue), pages. Available at: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet [Accessed 8th April 2017]

EOS.IO Technical White Paper [online] Available at: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md