WhitePaper

Gold-Backed Stablecoin

USD GOLD

By Legacy 1 Gold

& EIG Global Trust

Updated: 4 August 2025

ABSTRACT

Our gold backed stablecoin token, USD Gold (USDGOLD)[1], was created to provide financial entities a means to harness the enormous benefits of a digitalized currency backed by real assets, gold. We believe our real gold-backing is far superior vs other coins/tokens backed by nothing (most cryptocurrencies) or fiat instruments (most stablecoins). USDGOLD goal is to become the world's standard in digital assets in the spirit of the Bretton Woods Agreement.[2]

The USDGOLD Project is owned by Legacy 1 Gold LTD, a wholly owned subsidiary of EIG Global Trust and is incorporated in England & Wales. The USDGOLD stablecoin token is pegged permanently at 1000 to 1 ratio to the USD Dollar, thus a par value of One Thousand US Dollars ($1,000 USD). Each token will be priced to the hundred thousandths place (5 decimals). This peg value will not change regardless of the price of gold or supply or demand of the stablecoins (unlike Bitcoin or Meme coins the price is fixed).

The Proof of Reserves provided by co-project owner EIG Global Trust allocation of its reserved gold (Au) to Legacy 1 Gold. EIG Global Trust has allocated 50% of its initial total of $5 trillion of reserved gold (Au) bullion to back USDGOLD or $2.5 trillion value base on 29,530.82 metric tonnes of gold (Au) bullion. and additionally has $1 trillion conservatively valued of verifiable precious metals. USDGOLD are not directly tradable or exchanged for actual gold held by its project owner, Legacy 1 Gold LTD.

USDGOLD Total Supply is 2,500,000,000 (2.5 billion) tokens, 100% are authorized and minted with a potential market cap of $2.5 trillion USD if all tokens were deployed and placed into circulation. 80% of the funds from issuing USDGOLD will be used to back the token and the remaining 20% of USDGOLD will be split 14% for the Project Founders and 6% for Project Marketing and Operations. Tokens will be issued from the treasury based on partnerships and made public via the website www.usdgtoken.com and blockchain ledger The project owners hired leading cybersecurity cryptocurrency audit firm Hashlock Pty. Ltd to security audit USDGOLD, see Appendix A for full audit results. In summary, we strongly believe USDGOLD gold-backed stablecoin will lead the world's digital assets.

Table of Contents

INTRODUCTION

Stablecoins are a type of cryptocurrency that are primarily pegged to an asset primarily fiat currency like US Dollars (USD) at usually a ratio of 1 to 1. Stablecoins are assumed to be “stable” because they are backed by their Proof of Reserves (usually fiat currencies or financial instruments based on fiat currencies).

Fiat money is a government-issued currency that is not backed by a physical commodity, such as gold or silver, but rather by the government that issued it. The value of fiat money is derived from the relationship between supply and demand and the stability of the issuing government. The term "fiat" is a Latin word that is often translated as "it shall be" or "let it be done." Fiat currencies only have value because the government maintains that value; cannot be redeemed; and there is no utility to fiat money in itself.[6] Thus, fiat currencies can increase or decrease in relative value based on that country or block of countries monetary policy, economy, and amount held in financial reserves (usually gold).

Before fiat currency came about in the 1970s, governments would mint coins out of a valuable physical commodity, such as gold or silver, or print paper money that could be redeemed for a set amount of a physical commodity. Bretton Woods created a collective international currency exchange regime that lasted from the mid- 1940s to the early 1970s and today a lasting influence on international currency exchange and trade through its development of the IMF and World Bank. The Bretton Woods System required a currency peg to the U.S. dollar, which was in turn was pegged to the price of gold.[2]

The World Economic Forum reported that 2024 stablecoin transactions exceeded **$27 trillion USD,** or the total value of Visa and Mastercard combined. Why? Because stablecoins offer improved security, lower transaction fees, increased processing speed, blockchain enabled trackability, and reduced fiat currency forex volatility. This allows stablecoins to replace fiat for cross-border settlements, large sum bank transactions, digital currency exchanges for other fiat/crypto currencies, and even retail transactions.

Others Market Cap. Today's worldwide stablecoin market cap is ONLY $250 billion with leaders Tether ("USDT") having a market cap of $153 billion and Circle ("USDC") having a market cap of $62 billion. This low market cap cannot support Central or Commercial banks digital asset requirements or CBDCs. Only EIGBC and USDGOLD stablecoins have the collateral backing to support the worlds banking institutions digital currency needs. Additionally, other stablecoins must be obtained through public exchanges making accumulation and trading of large amounts difficult and cost prohibitive due to fees and amount restrictions. We can issue partner banks EIGBC and USDGOLD privately in large, denominated tranches.

Recently, gimmick gold backed stablecoins have been launched to provide an alternative method to purchase gold by for example, pegging 1 token to 1 gram of gold, silver, or other precious metals. The price of the token increases as the precious metal increases. The crypto project owners derive their profits through transaction fees and add-on costs like storage or shipping if the buyer wants to take possession of the actual precious metal.

USD GOLD (USDGOLD) TOKENOMICS

- Ticker Symbol = USDGOLD
- Total Potential Supply = 2.5 billion USDGOLD
- Par Value per USDGOLD = $1,000 ($1 thousand USD)
- Number of decimals = 5
- Pre-sold = 0
- Total in Circulation on Public Exchanges = 0
- Backing = USD Cash and its Equivalents + 29,530.82 metric tonnes of $2.5 trillion USD worth of Gold (Au) Bullion

We have resolved the above problems of Proof of Reserves by backing all the USDGOLD stablecoins by first using United States Dollars and its cash equivalents + double backing of 100% real assets, reserved gold (Au) assets and verified precious metals. In summary, our USD Gold (USDGOLD) stablecoin will disrupt the meaning of "backed" by truly having a stablecoin token backed by an actual asset gold and shielded by the world's inflationary driven economy. Additional benefits are vast and will be detailed in this Whitepaper.

EIG Global Trust went through extensive ten (10) months of regulatory reviews in multiple jurisdictions before the private launch of USDGOLD in May 2024. Our primary goal is to establish a stable gold backed digital currency that interacts with the worlds existing financial fiat-based assets (i.e. fiat currency, bonds, notes, and other banking instruments) from both governments and commercial banking. USDGOLD is vehicle to combine the real-world use of fiat assets with a digital currency that offers the cross-border transaction efficiencies and blockchain security, accountability, and audit capabilities.

USDGOLD is an excellent asset to meet capital requirements for collateralization to issue loans to consumers and hedge against inflationary factors mentioned above. Additionally, since our stablecoin can be exchanged for fiat currency like the US Dollar and Euro, we made it a priority to focus its adoption to countries who need to improve their intra-country payments (i.e. payroll for government employees and contractors) and inter-country payments (i.e. cross-border trade).

The USDGOLD also provides an excellent hedge and long-term investment against volatility in currency prices or crypto currencies. Since it is gold backed and not fiat-currency backed, investors receive the best of both worlds of the stability of gold as an asset and permanently pegged to $1,000 per USDGOLD Token. We believe our USDGOLD Token will be the world's leader in digital asset backed currency improving upon the Bretton Woods Agreement.

Finally, the term coin and token has been used interchangeably regarding stablecoins. Since USDGOLD will be running on another's blockchain, technically it is a token on that blockchain. We have chosen the Binance BNB Smart Chain (BSC)[9], a high-performance blockchain that allows developers to create smart contracts using the same programming language used by Ethereum. We chose the BSC blockchain for cost-effective, high scalability, interoperability, and large use base. See more about BSC in the technology stack section below.

THE USD GOLD (USDGOLD) PROJECT OWNERS

The USDGOLD project is owned by Legacy 1 Gold LTD, a private company wholly owned by

EIG Global Trust. Legacy 1 Gold LTD is incorporated in England & Wales, registration number 15631712, see filing UK Registration. The project owners charter demands a responsible corporate governance and operations including strong know your customer (KYC), anti-money laundering, and counter terrorist financing processes.

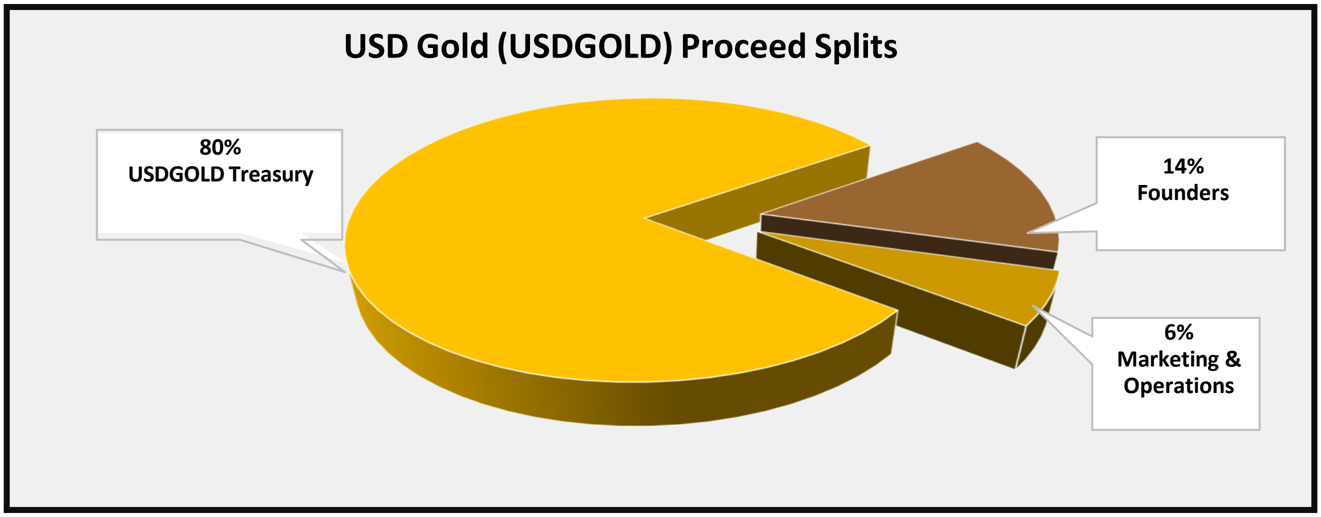
EIG Global Trust is a full service digital financial firm registered in Delaware, USA and the United Kingdom that provides asset management, project finance, investment banking, and advisory services driving digital transformation with emphasis on proactive fraud prevention and auditing.

We were conceived to manage partnerships with the world's financial community and develop digital economies in a responsible fashion. EIG Global Trust is leading the stable digital currency transition from the central banking establishment and their client countries commercial financial apparatus, into the digital venture and investment capital operations with a true cross border digital currency solution with heavy emphasis on project financing, mergers & acquisitions, gross domestic product enhancement, and liquidity into the marketplace.

The primary goal of the project owners is help convert from fiat to digital currency and bring socio-economic benefits to the world at the grass roots level by supplying a digital alternative to cash. This enables easier access to financial services and improving efficiency. Digital banking provides much needed access and ease of use particularly in developing nations where traditional banking and hard currency are limited in rural areas.

WHERE TO PURCHASE AND PROCEED SPLITS

The USDGOLD token will be available to purchase direct and via Project owners' websites www.usdgtoken.com and www.usdgsale.com. The proceeds generated from direct sales and exchanges will be split 3 ways, 80% USDGOLD Treasury, 14% Founders, 6% Company Marketing and Operations as illustrated in the chart below:



PROOF OF GOLD RESERVES

USD Gold's project owners, EIG Global Trust and Legacy 1 Gold are the custodians of the gold. Each USDGOLD token will be pegged to $1,000 US Dollars. When the USDGOLD token is first issued (circulated) from the Project owner (Legacy 1 Gold LTD) treasury, the price and amount of gold required to be held and custody will be established.

Transparency regarding the proof of amount of the gold used as USDGOLD backing is as follows: the initial $2.5 billion in gold (Au) bullion backing equals 29,530.82 metric tonnes and future updates will be provided to the public during quarterly audits and published on the EIG Global Trust website, www.eigglobaltrust.com.

USDGOLD will be paired with EIG Global Trust other stablecoin, EIG Bank Coin (EIGBC). This internal blockchain stablecoin has a high $1 million US Dollar (USD) peg value per coin to support collateral initiates by central bank including balance sheet / GDP enhancement, credit lines project financing, and Central Bank Digital Currency (CBDC). Commercial banks and private entities can benefit from partnering with USDGOLD project owners for digital financial transactions, wraps, trades, and cross-border payments. Unlike fiat, the blockchain ledger based digital currency is superior allowing for detailed tracking and accountability throughout the entire lifecycle.

REDUCED RISK MANAGEMENT

We acknowledge the growing hesitancy with investing in cryptocurrencies due to controllable (mismanagement or human error) and intentional maleficence from fraud and external hacks. We are fully transparent in both who we are, our regulatory backing, and our intentions. We have also launched on public recognized blockchain technology Binance Smart Chain (BSC) to alleviate the concern and risk of in-house build blockchains or outdated blockchains that require updates.

While we can secure the technology and gold reserves, each investor must remain diligent to avoid their own wallet and exchange account intrusions. But we feel extremely confident with our regulatory approvals and our central bank, government, and commercial banking partnerships that USDGOLD is the preferred method to invest in cryptocurrency for the purposes of long-term inflationary protection investments while avoiding the extreme volatility of non-backed cryptocurrencies like Bitcoin or memes. We strongly believe that the world will come to its senses and realize Bitcoin is limited in quantity, based on nothing except fear of missing out (FOMO) and backed by zero assets and to mention an enormous energy hog, inefficient, and delayed “real-time” transactions. In fact, the recent ETF launches used Bitcoin by default as it’s the only cryptocurrency the general public is aware of. We plan to change that narrative by focusing on the long-term future of the digital world based on a truly asset backed currency that is tangible, verifiable, and proven valuable over 1,000s of years.

TECHNOLOGY STACK

The BSC Blockchain.[11] USDGOLD uses Binance Smart Chain (BSC), a layer-1 blockchain built to support smart contracts, running alongside the Binance Chain, which was designed to support high transaction volumes. Binance Smart Chain implements the Ethereum Virtual Machine (EVM) to enable smart contracts, allowing developers to create or migrate Ethereum-based decentralized applications (dApps). BSC was designed based on Geth, an Ethereum execution client that handles transactions, deploys and executes smart contracts, and contains the EVM.

Evolution of BSC into BNB Chain. The Binance blockchain, built by the world's largest cryptocurrency exchange, has evolved since its launch in 2017. As decentralized finance (DeFi) applications enabled by smart contracts took off in 2020, Binance launched a parallel Binance Smart Chain to run alongside the Binance Chain and compete with the Ethereum blockchain.

BSC quickly gained popularity among developers and users in early 2021 as network congestion and high gas fees on the Ethereum blockchain increased the cost of transactions while slowing processing times. In 2022, BSC merged with the Binance Chain in a new dual-chain structure. The original Binance Chain has been renamed the BNB Beacon Chain and merged with BSC, meaning that Binance Smart Chain is now the BNB Smart Chain. Together, the two chains comprise the BNB Chain.

BNB Smart Chain Protocol. BNB Smart Chain brings programmability and interoperability to the BNB Beacon Chain using a combined delegated proof of stake (DPoS) and Proof-of-Authority (PoA) consensus mechanism known as Proof-of-Staked- Authority (PoSA).

PoSA uses a system of validators elected based on the number of tokens they stake. They take turns verifying transactions and adding them to the chain in new blocks.

Backup validators called "candidates" provide security, as in the event of a malicious attack that brings the validators offline, the candidates can report to the Beacon Chain, resume processing on BSC, and propose the re-election of active validators.

Advantages of BSC include:

- Short blocking time**:** BSC aims to achieve a short blocking time of three seconds on its live blockchain (mainnet). This means that transactions can be processed quickly, enabling faster confirmation and reducing potential delays.
- Fast confirmation of transaction finality**:** BSC emphasizes fast confirmation of transaction finality. This ensures that once a transaction is included in a block, it

is considered finalized and cannot be reversed or altered. This feature enhances the security and reliability of transactions on the BSC.

- EVM compatibility**:** BSC is fully compatible with EVM. This compatibility allows developers to seamlessly port their existing Ethereum-based applications and smart contracts to the Binance Smart Chain ecosystem. It also provides users with a familiar environment and access to a wide range of dApps.

TARGET MARKET:

Cryptocurrency Exchanges. USDGOLD tokens can readily accessible for purchase, exchange for other cryptocurrencies, and settled in fiat currencies. We plan to list USDGOLD on all BSC supported exchanges.

Governments. Legacy 1 Gold LTD project owners have developed deep ties to several country governments and their central banks. We believe USDGOLD can support their needs to convert their local economies from fiat to digital currency. One example could be paying government contractors in USDGOLD or government employees in USDGOLD.

Commercial Banks. A truly backed stablecoin to support and modernize traditional banking needs including cross-border payments, using USDGOLD as an inflationary hedge, asset management portfolio, and trading practices. Plus, since USDGOLD is back by gold (Au), this digital asset has greater collateral leverage ratios vs pure fiat currencies.

High New Worth Portfolios. USDGOLD provides a hedge against volatile fiat and cryptocurrencies.

Companies. Public and private companies could also use USDGOLD as an inflationary hedge, cross-border payments, and other traditional methods current fiat-currency provides.

EIG Global Trust Stablecoins are "Double Backed" by Gold (Au)

EIG Global Trust (Global Trust) stablecoins have double asset backing of both fiat and precious metals. This provides the liquidity benefit of fiat + the expandability and highly leverageable gold

(Au) and precious metals. Using secure and accountability of digital blockchains, combined with Global Trust founders' trusted banking and project management expertise, our digital asset solution offers modern financial products with better returns for governments, central and commercial banks, and financial entities.

- EIGBC and USDGOLD stablecoins are both pegged to the US Dollar (USD) and only redeemable/exchanged for USD. Neither stablecoins are redeemable for actual gold.
- Global Trust issuer terms state at least 80% of issued EIGBC & USDGOLD proceeds will remain in the Global Trust Treasury balance sheet for "double backing" asset backing purposes.
- The 1st Level of asset backing is USD and cash equivalents to cover the redeemable stablecoins and secure the hard assets. This balance will grow as proceeds grow.
- The 2nd Level of asset backing is hard assets of precious metals rights and ownership. Global Trust stablecoin backing have secured more than $2.5 trillion in reserved gold (Au) and $1 trillion in verifiable and registered precious metals and gold.
- Regulations require stablecoins to maintain at least 100% Proof of Reserve Ratio or the value of asset backing vs. value of issued stablecoins. Global Trust stablecoins exceed the standard 100%.
- None of the Proof of Reserves are tied to liens or debt. Global Trust is able to achieve the 100% ratio debt free partnering with reserved Gold (Au) holders and mineral rights owners.
- The gold (Au) and mineral rights owners' revenue share partnerships are paid in cash (USD), therefore; no "circular reference" exists i.e. backing the stablecoins & also paid in stablecoins.

What makes Global Trust double backing model unique and built for the global economy?

- Global Trust stablecoins are Gold (Au) backed providing superior leveraged ratios for credit lines & project financing that generates larger returns vs. other stablecoins cash and cash equivalent only.
- Current market leading stablecoins (USDC & USDT) are pegged, redeemable, and backed by cash and cash equivalents, loans, various bonds, and less than 5% in precious metals.

Their growth is limited by their availability of cash, limited stablecoins supply, and less returns compared to the Global Trust stablecoins since they are double backed cash (USD) and Gold (Au) assets.

Glossary of Terms[12]

Asset backed/ pegged cryptocurrency. Any stablecoin cryptocurrency whose price is pegged to a real-world asset i.e. It's not a "utility backed" cryptocurrency.

Bitcoin (BTC). The original, largest and best-known cryptocurrency.

Blockchain. The underlying technology is used by nearly all cryptocurrencies. A blockchain is essentially a complete ledger of transactions held simultaneously by multiple nodes on a network.

Collateralization. Use of a valuable asset to secure a loan against default and can be seized by the lender to offset any loss.

CeFi. Short for centralized finance. Finance is traditionally centralized because it relies on trusted intermediaries like banks (central, commercial, and online).

Circle (USDC**)**. A stablecoin that is pegged 1-to-1 with the U.S. dollar.

Coin. A colloquial term for a cryptocurrency with its own proprietary blockchain.

Cryptocurrency. A digital asset that can be used as a store of value or a medium of exchange for goods and services. Transactions are verified and recorded using cryptography by a distributed network of participants, rather than a centralized authority such as a bank or government agency.

dApp. Short for decentralized application, a dApp is an app that isn't controlled by a central authority. Twitter is an example of a centralized app, with users relying on it as an intermediary to send and receive messages. A dApp is distributed on a blockchain, allowing users to send and receive data directly without an intermediary.

DeFi. Short for decentralized finance. Finance is traditionally centralized because it relies on trusted intermediaries. For example, if you want to send money to a friend or relative, you rely on your bank to send it to the recipient’s bank. DeFi, on the other hand, requires no intermediaries. Participants can send and receive assets directly. In theory, this makes transactions faster and cheaper.

Exchange. A website or app that allows users to buy and sell crypto assets.

Ethereum. The second-biggest cryptocurrency by market capitalization after Bitcoin.

Fiat Currency. Traditional currencies are backed by the full faith and credit of a nation state. The U.S. dollar, the Euro or the British pound are fiat currencies.

Hodl – “Hold on for Dear Life”, to hold the cryptocurrency for long period of time often earning interest with withdrawal restrictions.

Initial Coin Offering (ICO). A fundraising mechanism in the cryptocurrency industry, akin to an Initial Public Offering (IPO) in the traditional financial sector that can gather resources directly from anyone with a crypto wallet.

Know Your Customer (KYC). Although not required, many crypto exchanges carry out certain identity checks on their customers under KYC rules.

Ledger. A record of transactions maintained by both centralized financial institutions and decentralized finance applications. Data for each transaction entered into a ledger may include times, dates, senders and recipients.

Market capitalization (cap). Also written as market cap, this is the total market value of a cryptocurrency. At the time of writing, all cryptocurrencies had a combined market cap of slightly less than $1 trillion.

Node. A computer or device connected to other computers or devices that all hold a copy of a blockchain. Each node supports the broader network by sharing information and validating transactions.

Proof of Reserves. The process by which the issuer of any asset backed decentralized digital token, cryptographically/mathematically proves that all tokens that have been issued are fully reserved and backed by the underlying asset.

Regulated. A market in which players must follow certain rules of risk fines and/or the loss of their operating license.

Smart contract. A program that executes itself on a blockchain when certain conditions are met, without the need for human intervention or an intermediary. Once completed, the contract cannot be changed or undone.

Stablecoin. A cryptocurrency that aims to maintain a fixed, unchanging market value that is pegged to another currency, commodity or financial instrument. As of this writing, the biggest stablecoins are Tether and USD Coin.

Tether (USDT). A stablecoin that is pegged 1-to-1 with the U.S. dollar.

Token. An individual cryptocurrency. Specifically, it’s a way to refer to a crypto that runs on a particular blockchain.

Volatility. A market condition in which prices frequently and unpredictably rise and fall as in prices or interest rates.

Total Circulation. Collective number of coins or tokens in circulation at any point in time.

Total Supply. Collective number of all coins or tokens in circulation, project owners’ treasury, or escrow any point in time.

Utility backed. A decentralized digital token whose value is derived from the usefulness of its application rather than just being a value transfer system.

Whitepaper. A technical document released alongside new crypto projects that explains how the system works.

Yield. A return on investment, expressed as a percentage.

References

[1] For more information on USD Gold (USDGOLD) and its project owner Legacy 1 Gold LTD, see www.usdgtoken.com

[2] Bretton Wood Agreement– Federal Reserve History https://www.federalreservehistory.org/essays/bretton-woods-created

[3] For more information on EIG Global Trust, see www.eigglobaltrust.com

[4] Reserved.

[5] For more information on EIG Bank Coin (EIGBC), see https://www.eigwallet.io/

[6] Fiat Currency – Investopedia https://www.investopedia.com/terms/f/fiatmoney.asp

[7] Reserved

[8] Reserved

[9] Binance BNB Smart Chain (BSC) - Harnessing Decentralization to Make the Impossible Possible https://www.bnbchain.org/en/bnb-smart-chain

[10] London Bullion Marketing Association (LBMA) - https://www.lbma.org.uk/prices-and-data/precious-metal-prices#/

[11] Binance Smart Chain (BSC) www.techopedia.com/difinition/binance-smart-chain-bsc by Technology Journalist Nicole Willing

Appendix A. Hashlock Pty Ltd Security Audit

Security Audit

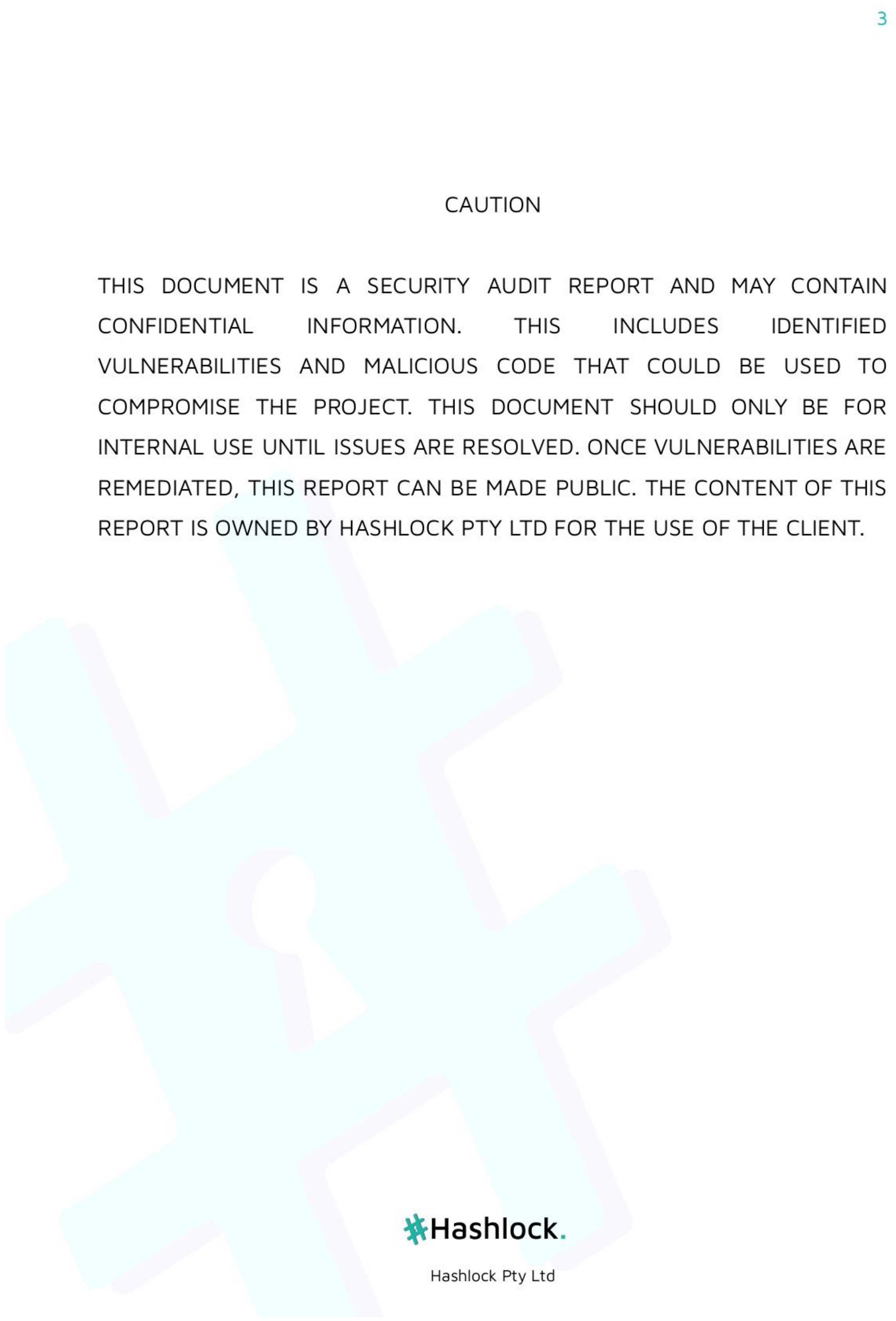
EIG Global Trust: USD Gold (USDG) Token

July 2024

info@hashlock.com.au

Hashlock Pty Ltd

Table of Contents



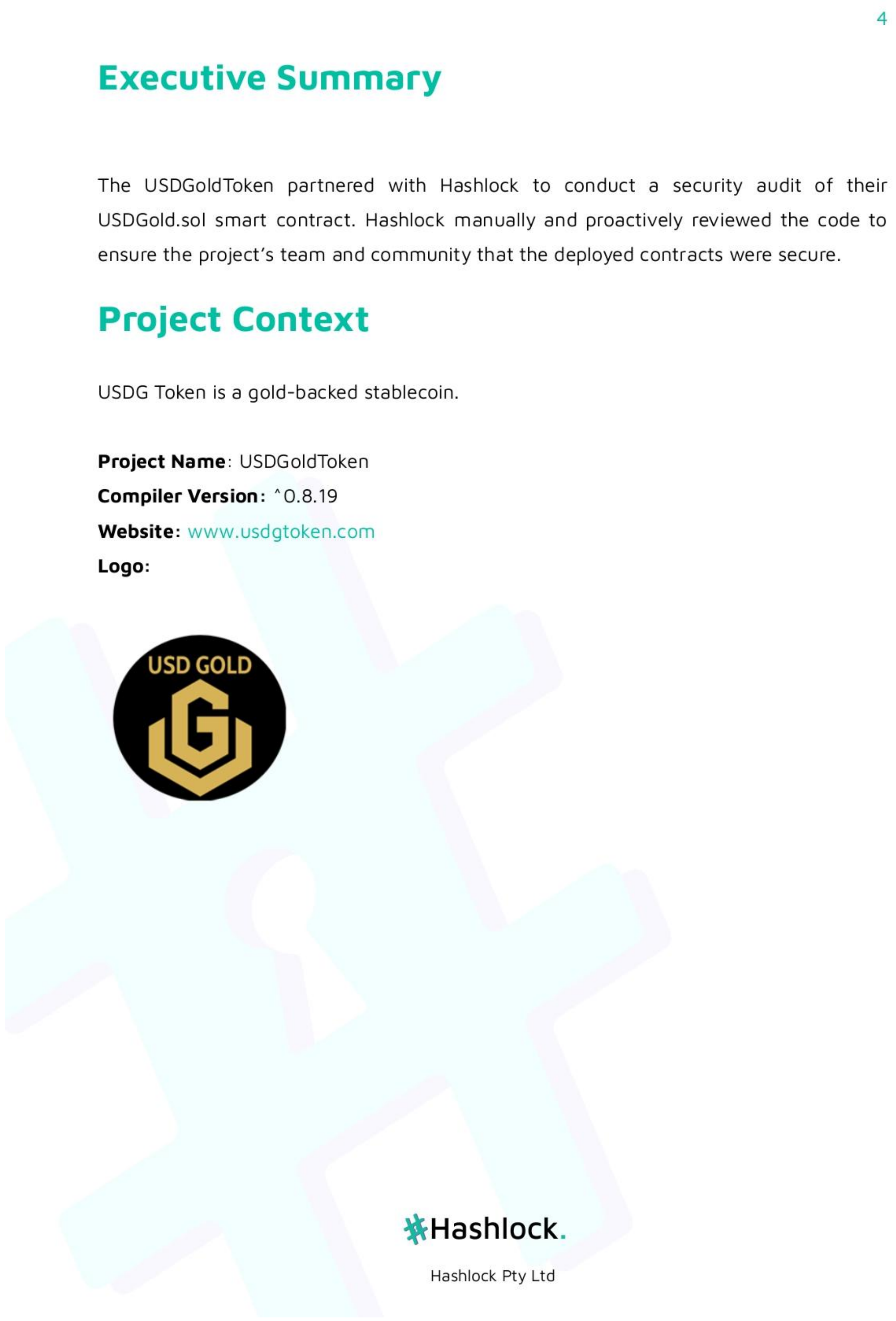
3

CAUTION

THIS DOCUMENT IS A SECURITY AUDIT REPORT AND MAY CONTAIN CONFIDENTIAL INFORMATION. THIS INCLUDES IDENTIFIED VULNERABILITIES AND MALICIOUS CODE THAT COULD BE USED TO COMPROMISE THE PROJECT. THIS DOCUMENT SHOULD ONLY BE FOR INTERNAL USE UNTIL ISSUES ARE RESOLVED. ONCE VULNERABILITIES ARE REMEDIATED, THIS REPORT CAN BE MADE PUBLIC. THE CONTENT OF THIS REPORT IS OWNED BY HASHLOCK PTY LTD FOR THE USE OF THE CLIENT.

Hashlock.

Hashlock Pty Ltd



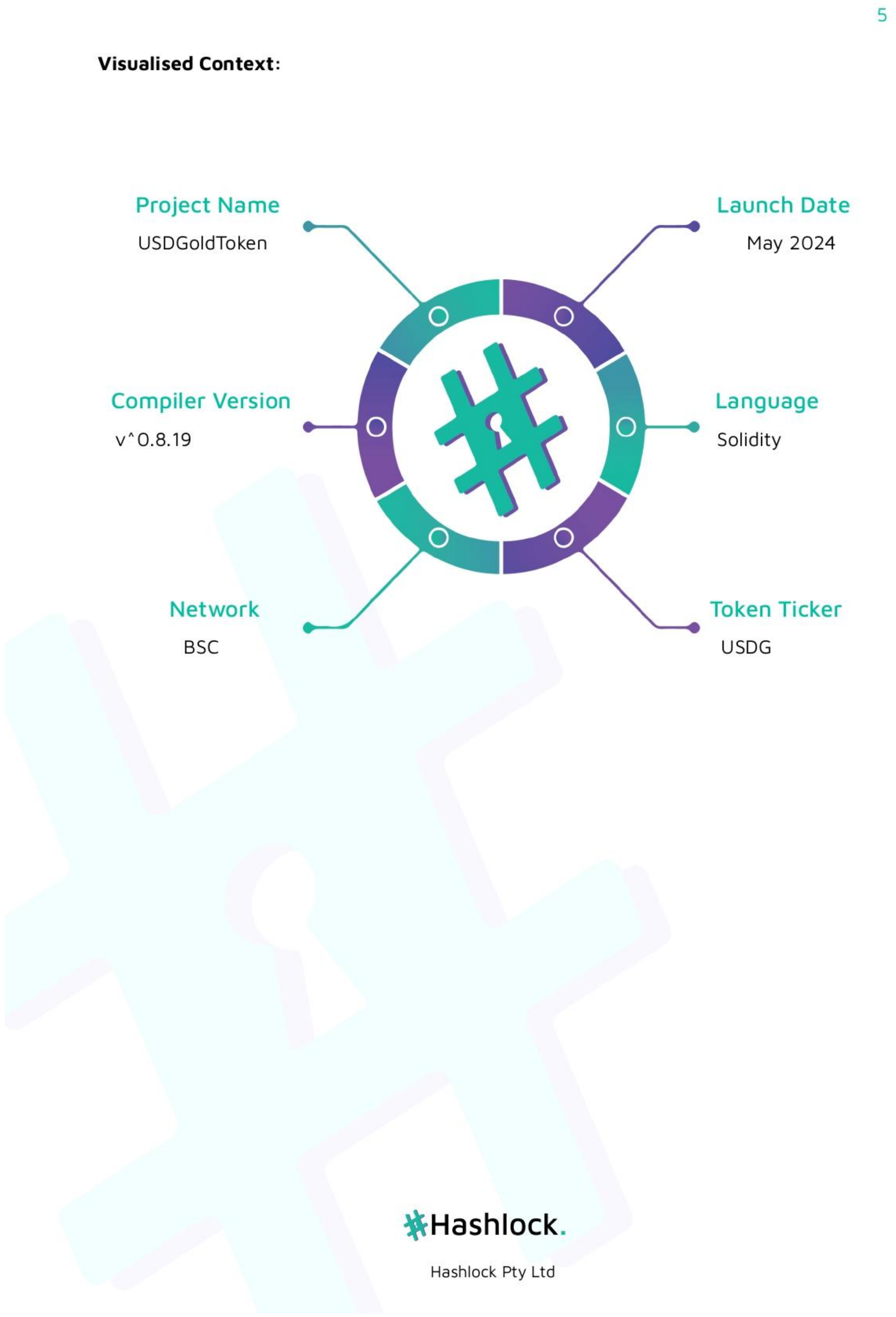
Executive Summary

The USDGoldToken partnered with Hashlock to conduct a security audit of their USDGold.sol smart contract. Hashlock manually and proactively reviewed the code to ensure the project's team and community that the deployed contracts were secure.

Project Context

USDG Token is a gold-backed stablecoin.

Project Name: USDGoldToken
Compiler Version: ^0.8.19
Website: www.usdgtoken.com
Logo:



5

Visualised Context:

Project Name
USDGoldToken

Launch Date
May 2024

Compiler Version
v^0.8.19

Language
Solidity

Network
BSC

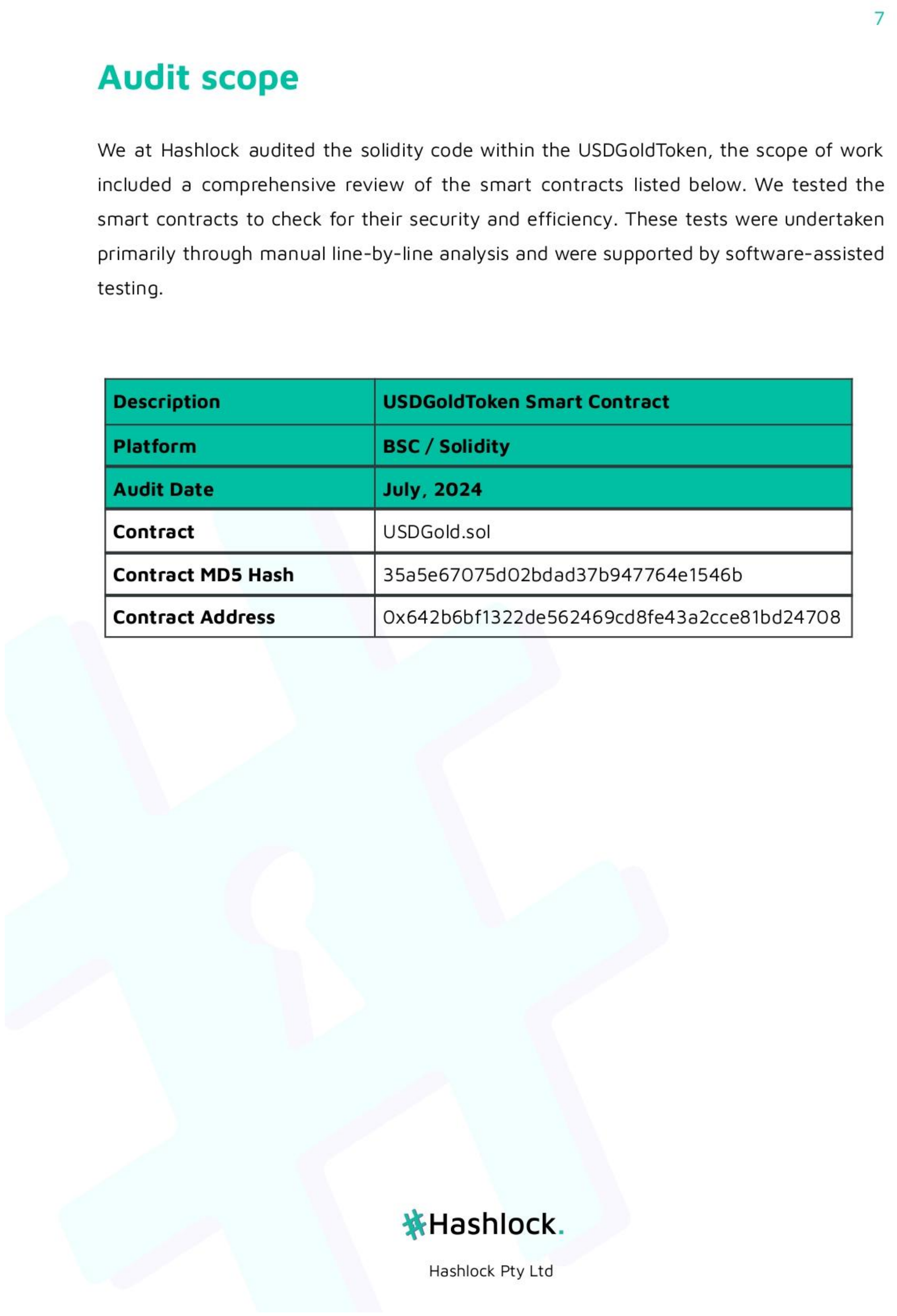
Token Ticker
USDG

Hashlock.

Hashlock Pty Ltd

Project Visuals:

USD GOLD
USDG TOKEN IS A TRULY GOLD BACKED STABLECOIN. THE NEW DIGITAL GOLD STANDARD



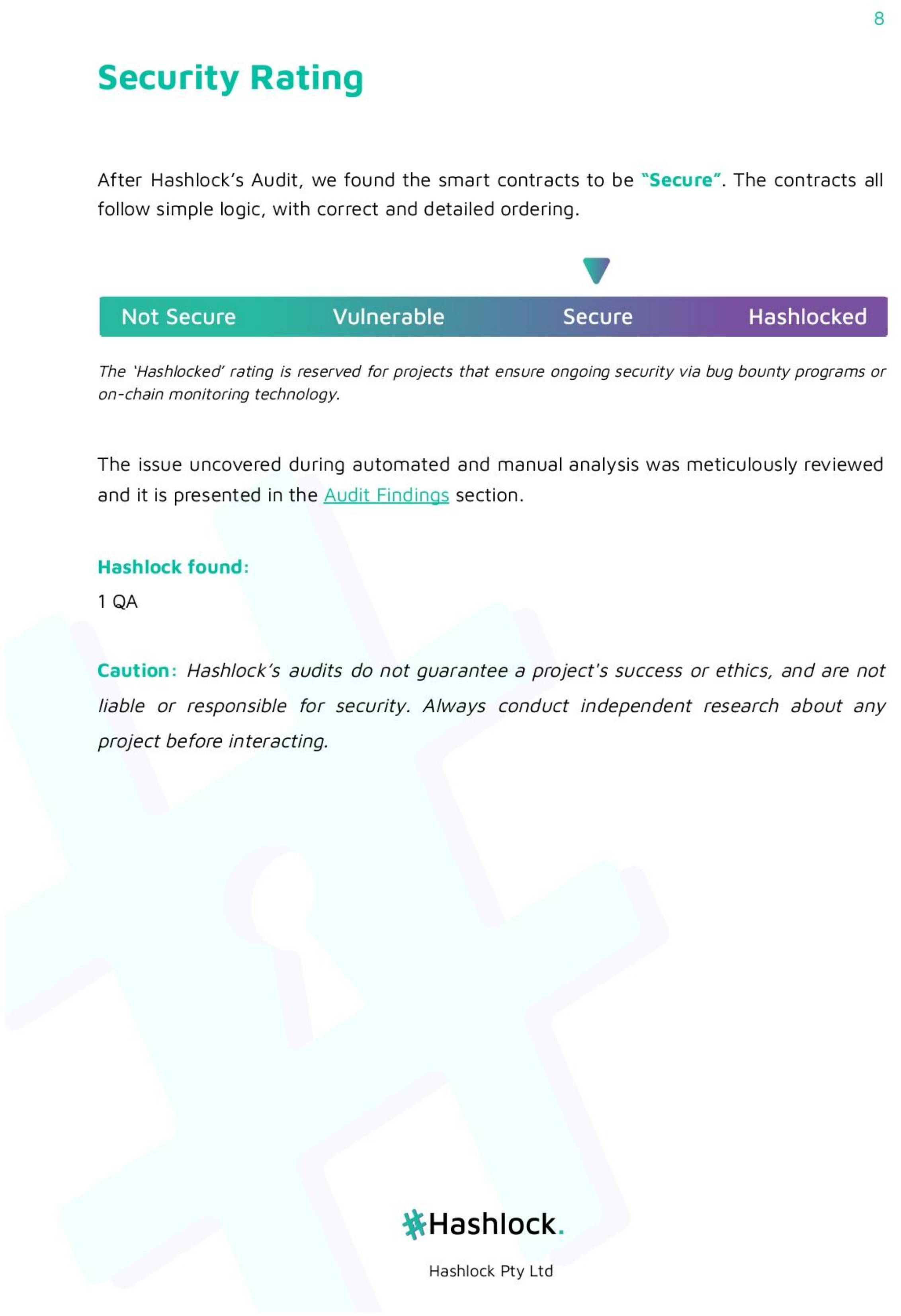
Audit scope

We at Hashlock audited the solidity code within the USDGoldToken, the scope of work included a comprehensive review of the smart contracts listed below. We tested the smart contracts to check for their security and efficiency. These tests were undertaken primarily through manual line-by-line analysis and were supported by software-assisted testing.

Description	**USDGoldToken Smart Contract**
Platform	**BSC / Solidity**
Audit Date	**July, 2024**
Contract	USDGold.sol
Contract MD5 Hash	35a5e67075d02bdad37b947764e1546b
Contract Address	0x642b6bf1322de562469cd8fe43a2cce81bd24708

Hashlock.

Hashlock Pty Ltd



Security Rating

After Hashlock's Audit, we found the smart contracts to be **"Secure"**. The contracts all follow simple logic, with correct and detailed ordering.

Not Secure
Vulnerable
Secure
Hashlocked

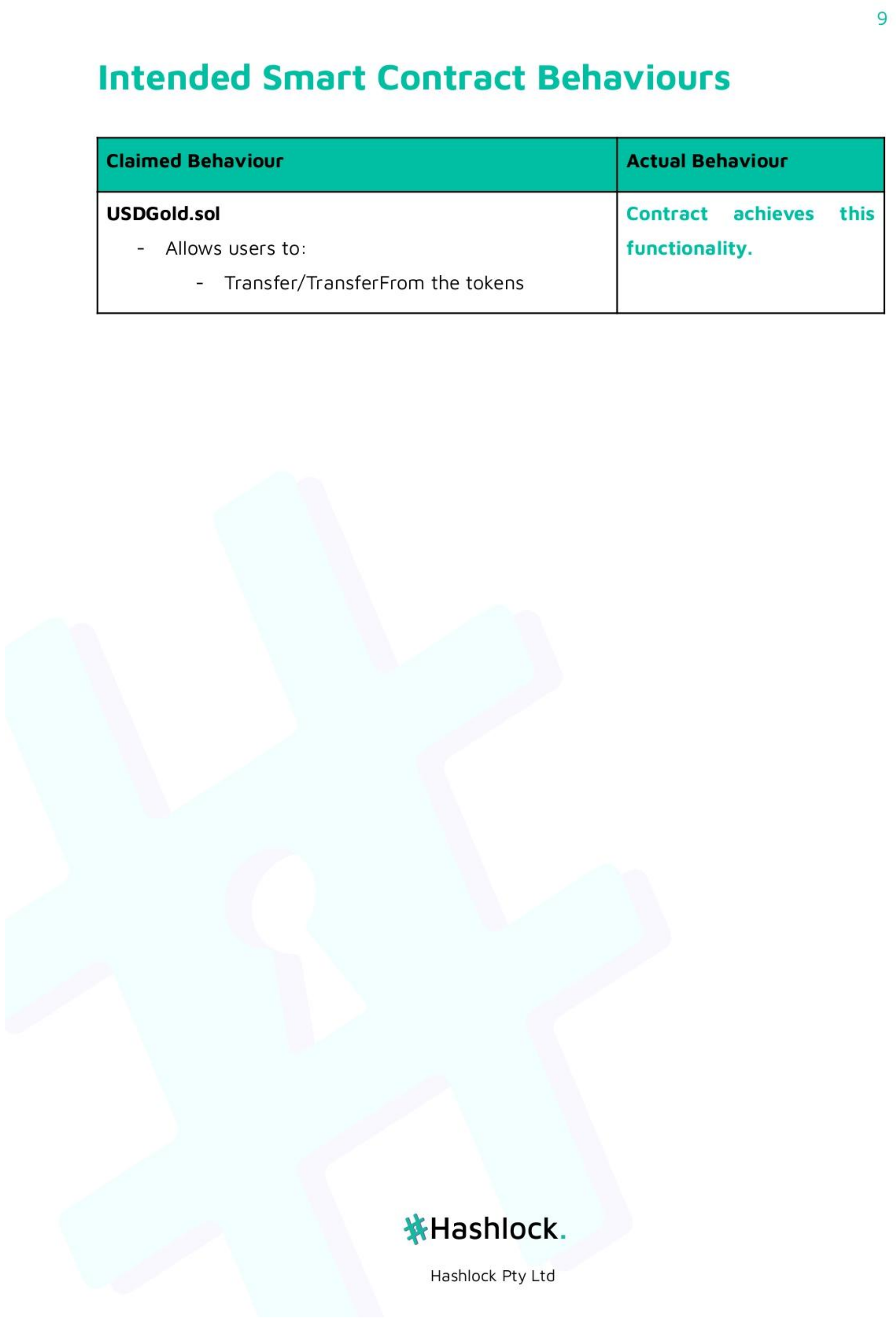
The 'Hashlocked' rating is reserved for projects that ensure ongoing security via bug bounty programs or on-chain monitoring technology.

The issue uncovered during automated and manual analysis was meticulously reviewed and it is presented in the Audit Findings section.

Hashlock found:

1 QA

Caution: *Hashlock's audits do not guarantee a project's success or ethics, and are not liable or responsible for security. Always conduct independent research about any project before interacting.*

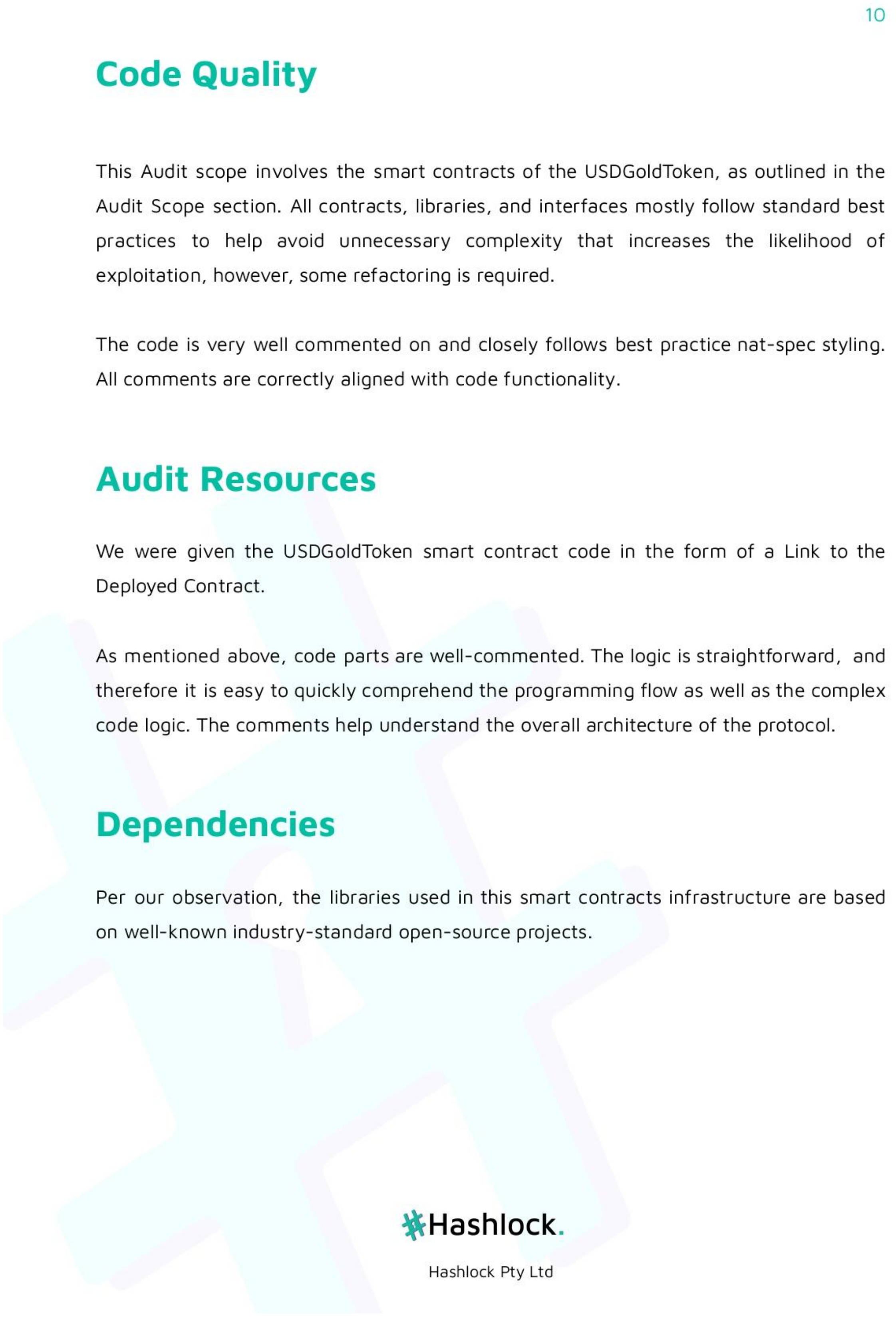


Intended Smart Contract Behaviours

Claimed Behaviour	Actual Behaviour
USDGold.sol - Allows users to: - Transfer/TransferFrom the tokens	Contract achieves this functionality.

Hashlock.

Hashlock Pty Ltd



Code Quality

This Audit scope involves the smart contracts of the USDGoldToken, as outlined in the Audit Scope section. All contracts, libraries, and interfaces mostly follow standard best practices to help avoid unnecessary complexity that increases the likelihood of exploitation, however, some refactoring is required.

The code is very well commented on and closely follows best practice nat-spec styling. All comments are correctly aligned with code functionality.

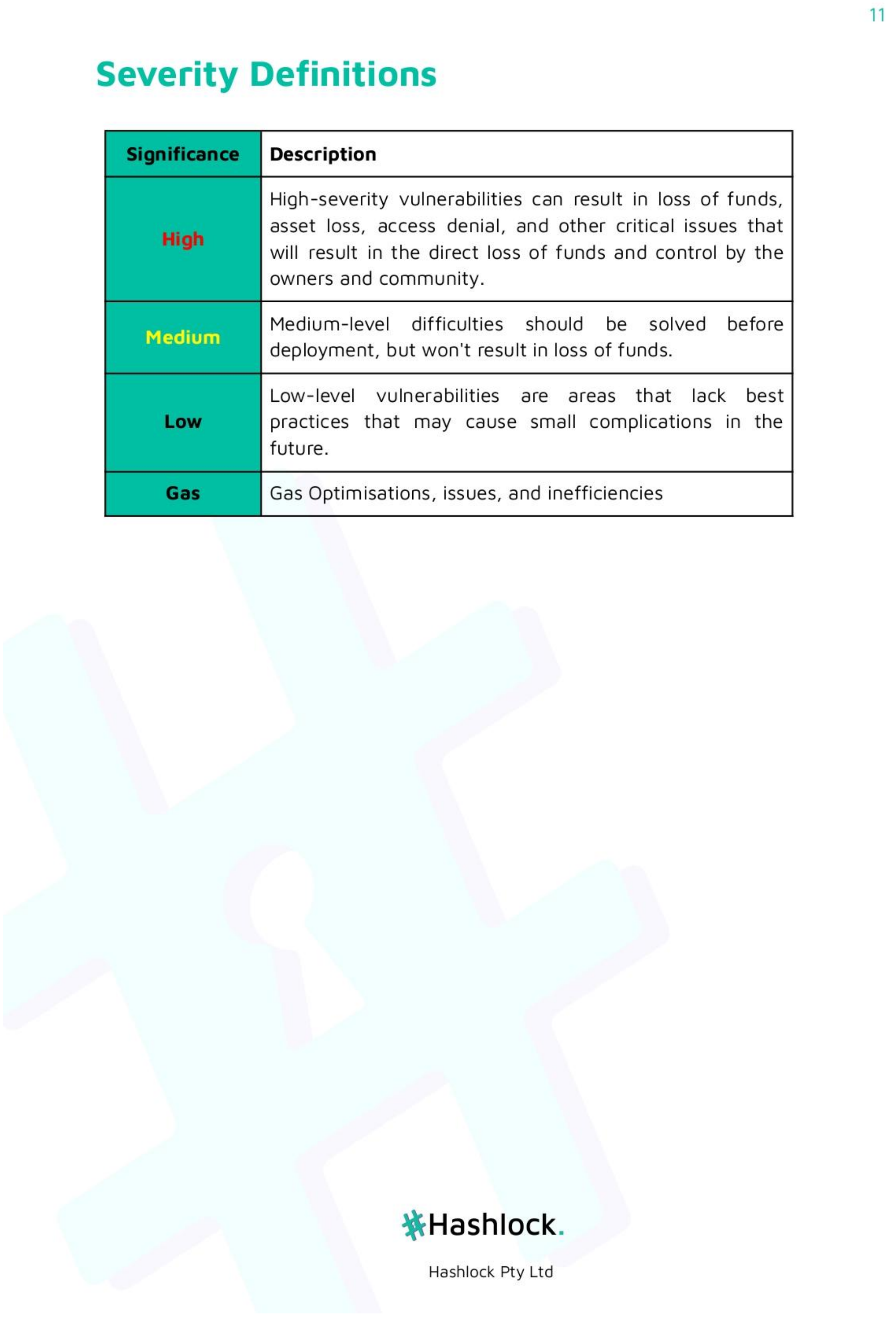
Audit Resources

We were given the USDGoldToken smart contract code in the form of a Link to the Deployed Contract.

As mentioned above, code parts are well-commented. The logic is straightforward, and therefore it is easy to quickly comprehend the programming flow as well as the complex code logic. The comments help understand the overall architecture of the protocol.

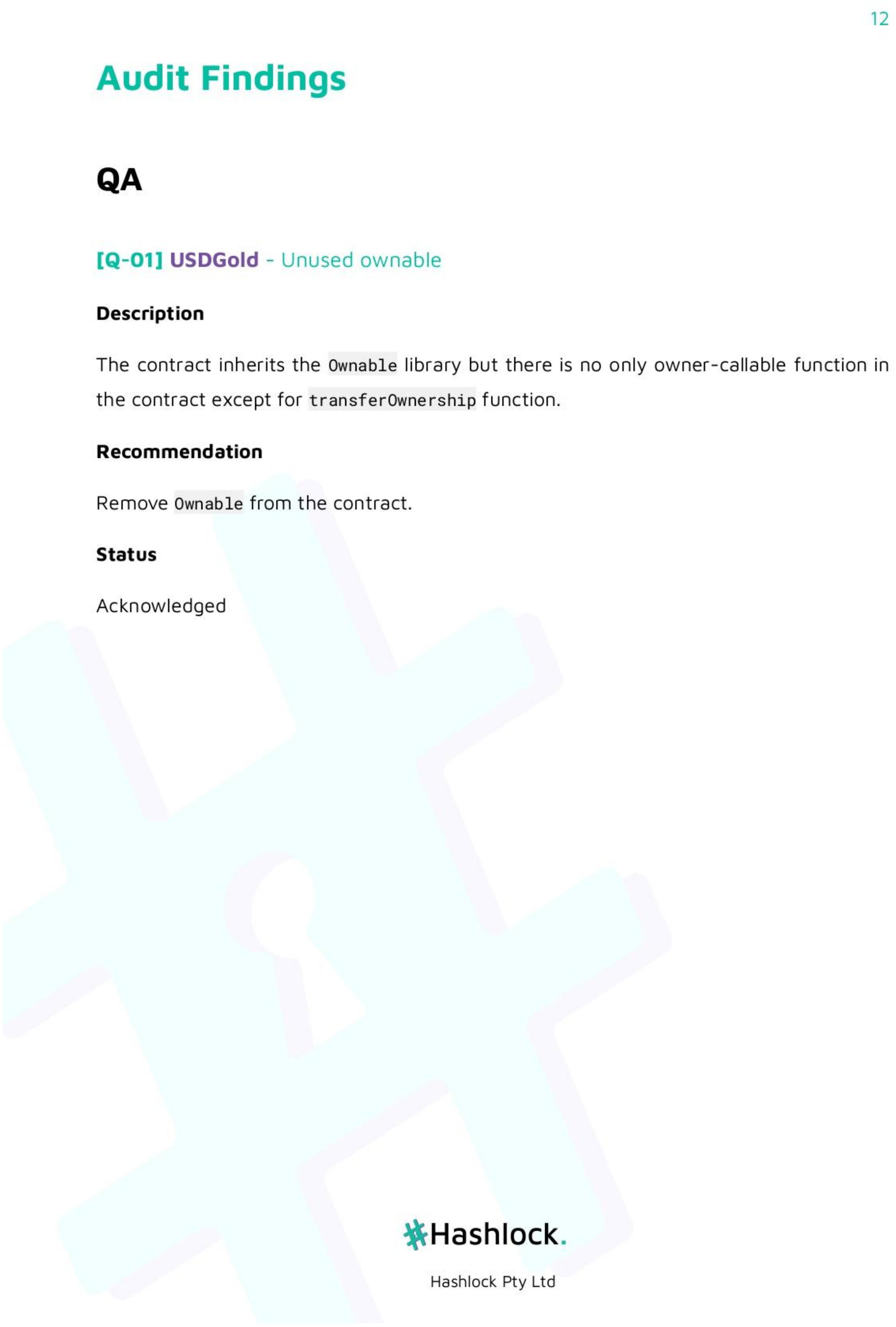
Dependencies

Per our observation, the libraries used in this smart contracts infrastructure are based on well-known industry-standard open-source projects.



Severity Definitions

Significance	Description
High	High-severity vulnerabilities can result in loss of funds, asset loss, access denial, and other critical issues that will result in the direct loss of funds and control by the owners and community.
Medium	Medium-level difficulties should be solved before deployment, but won't result in loss of funds.
Low	Low-level vulnerabilities are areas that lack best practices that may cause small complications in the future.
Gas	Gas Optimisations, issues, and inefficiencies



Audit Findings

QA

[Q-01] USDGold - Unused ownable

Description

The contract inherits the `Ownable` library but there is no only owner-callable function in the contract except for `transferOwnership` function.

Recommendation

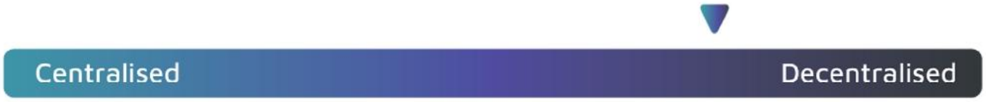
Remove `Ownable` from the contract.

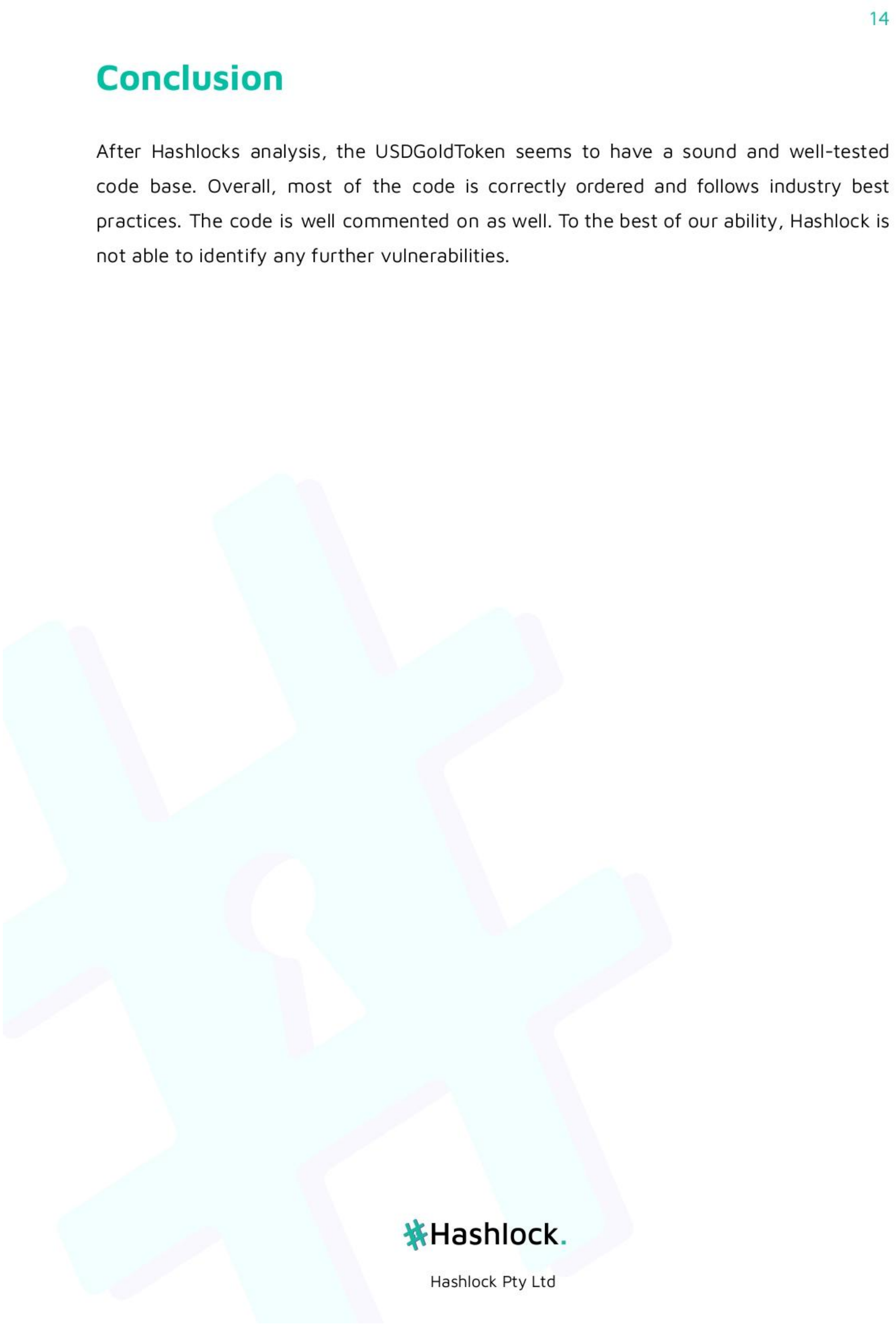
Status

Acknowledged

Centralisation

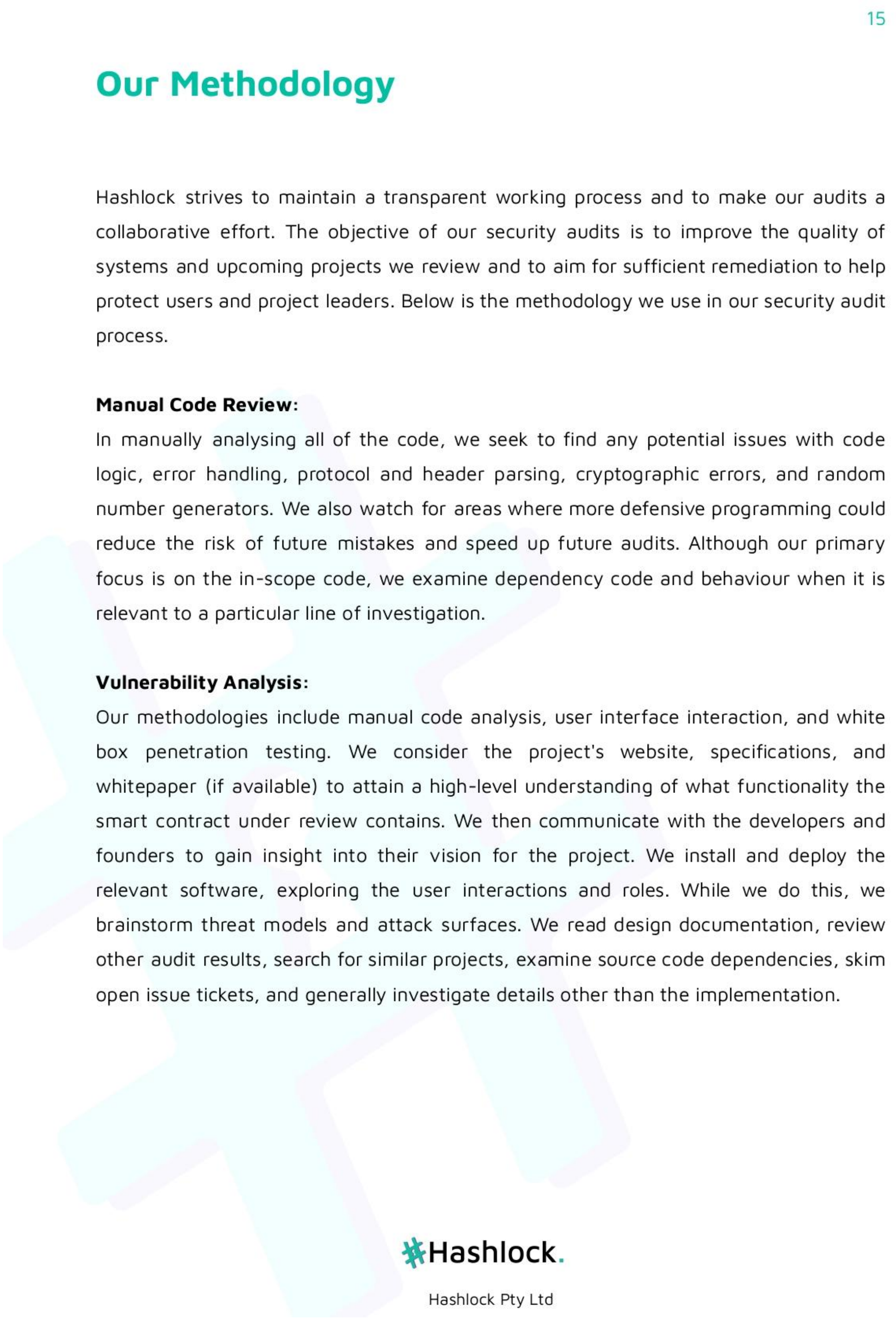
The USDGoldToken values decentralisation.





Conclusion

After Hashlocks analysis, the USDGoldToken seems to have a sound and well-tested code base. Overall, most of the code is correctly ordered and follows industry best practices. The code is well commented on as well. To the best of our ability, Hashlock is not able to identify any further vulnerabilities.

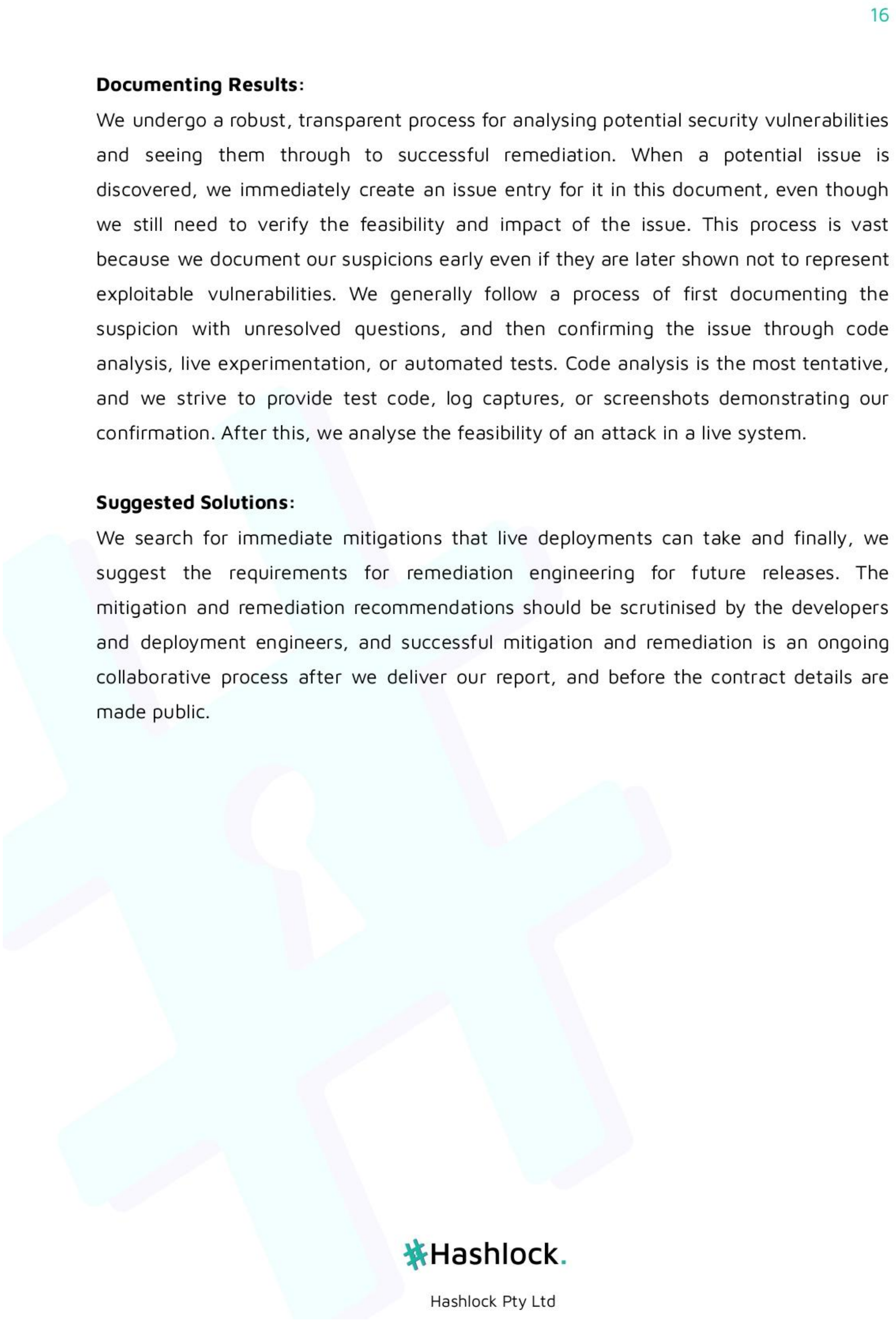


Our Methodology

Hashlock strives to maintain a transparent working process and to make our audits a collaborative effort. The objective of our security audits is to improve the quality of systems and upcoming projects we review and to aim for sufficient remediation to help protect users and project leaders. Below is the methodology we use in our security audit process.

Manual Code Review:
In manually analysing all of the code, we seek to find any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behaviour when it is relevant to a particular line of investigation.

Vulnerability Analysis:
Our methodologies include manual code analysis, user interface interaction, and white box penetration testing. We consider the project's website, specifications, and whitepaper (if available) to attain a high-level understanding of what functionality the smart contract under review contains. We then communicate with the developers and founders to gain insight into their vision for the project. We install and deploy the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.



Documenting Results:

We undergo a robust, transparent process for analysing potential security vulnerabilities and seeing them through to successful remediation. When a potential issue is discovered, we immediately create an issue entry for it in this document, even though we still need to verify the feasibility and impact of the issue. This process is vast because we document our suspicions early even if they are later shown not to represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, and then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this, we analyse the feasibility of an attack in a live system.

Suggested Solutions:

We search for immediate mitigations that live deployments can take and finally, we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinised by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the contract details are made public.

Disclaimers

Hashlock's Disclaimer

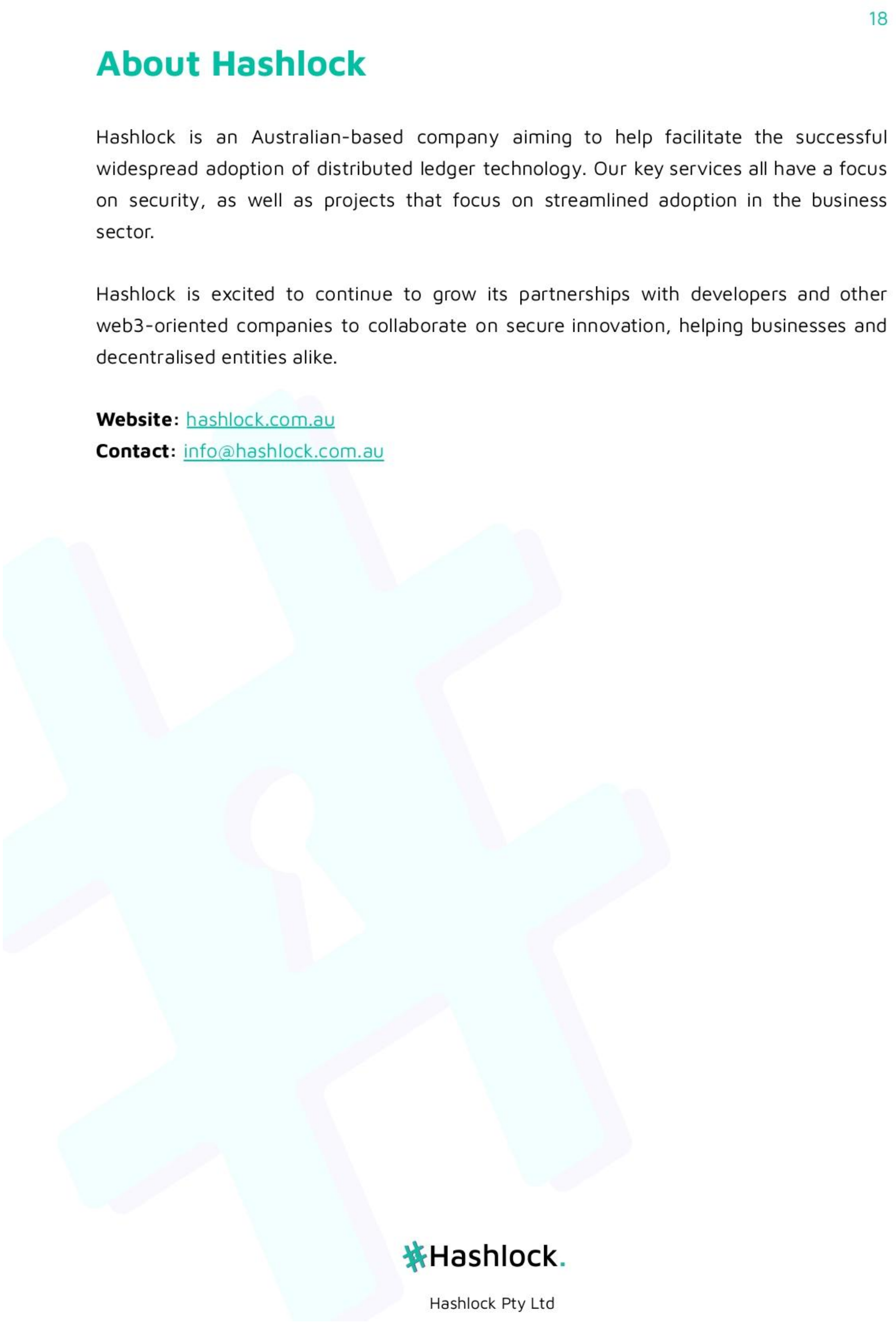
Hashlock's team has analysed these smart contracts in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in the smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

Due to the fact that the total number of test cases is unlimited, the audit makes no statements or warranties on the security of the code. It also cannot be considered a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only. We also suggest conducting a bug bounty program to confirm the high level of security of this smart contract.

Hashlock is not responsible for the safety of any funds and is not in any way liable for the security of the project.

Technical Disclaimer

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to attacks. Thus, the audit can't guarantee the explicit security of the audited smart contracts.



About Hashlock

Hashlock is an Australian-based company aiming to help facilitate the successful widespread adoption of distributed ledger technology. Our key services all have a focus on security, as well as projects that focus on streamlined adoption in the business sector.

Hashlock is excited to continue to grow its partnerships with developers and other web3-oriented companies to collaborate on secure innovation, helping businesses and decentralised entities alike.

Website: hashlock.com.au
Contact: info@hashlock.com.au