CertiK (CTK)

Written by Lucia Uwalaka **Created on December 22, 2021.**

TABLE OF CONTENTS.

INTRODUCTION.

CertiK Chain, rebranding as Shentu Chain, is a pioneer in blockchain security that uses best-in-class AI technology to protect, secure and monitor blockchain protocols and smart contracts. CertiK's mission is to secure the cyber world. More than 300 billion worth of cryptocurrency is powered by blockchain technology. Huge stakes which are not reliable or secure are placed on these blockchain systems. With shared public ledger systems, blockchain-based applications are exposed to hackers' attacks as any bug is easily exposed and can lead to substantial financial losses. Starting with blockchain, CertiK applies cutting-edge innovations from academia into an enterprise, enabling mission-critical applications to be built with security and correctness, from deployment to post-deployment.

CertiK is a decentralized proof engine that mathematically ensures that blockchain ecosystems are bug-free and hacker-resistant. It is a security-first, delegated proof-of-stake (PoS) blockchain built with the Cosmos SDK for the trustworthy execution of mission-critical applications, including DeFi, NFTs, and autonomous vehicles. It aims to act as the basis for securely building blockchain infrastructure and decentralized applications.

Depending on the level of the security score, audited blockchain projects of any protocol may be eligible for a ShentuShield membership, which is a flexible, decentralized reimbursement system for any crypto asset that is irretrievably lost or stolen due to security issues. ShentuShield memberships are open to all community members of these eligible blockchain projects, providing a safety net to holders of crypto assets in case anything unexpected happens.

CertiK is one of the fastest-growing and most trusted companies in blockchain security. To date, they have collectively worked with over 1800 enterprise clients, helped secure over $310 billion worth of digital assets, and detected over 31,000 vulnerabilities in blockchain code. Some of their clients include leading projects such as Aave, Polygon, Binance Smart Chain, Terra, Yearn, and Chiliz. CertiK raised over $140 million and was backed by Coatue, Tiger Global, Sequoia, and Hillhouse Capital.

Background

CertiK was founded in 2018 by professors of Columbia University and Yale University, Ronghui Gu and Zhong Shao, respectively.

Ronghui Gu is the inaugural Tang Family Assistant Professor of Computer Science at Columbia University. His thesis work on building certified OS kernels received the Yale Doctoral Dissertation Award and was nominated for the ACM Doctoral Dissertation Award. He is the primary designer and developer of CertiKOS, the first verified concurrent OS kernel, and SeKVM, the first verified commodity cloud hypervisor — major milestones toward building safe and secure systems software. Gu received an Amazon Research Award, an SOSP Best Paper Award, and a CACM Research Highlight for his work in systems verification. He obtained his Ph.D. degree from Yale University in 2016 and a bachelor's degree from Tsinghua University in 2011.

Zhong Shao is a Professor of Computer Science at Yale University. He earned his Ph.D. in Computer Science from Princeton University in 1994. During his early career, he was a key developer and author of many key compilation phases used in the Standard ML of New Jersey compiler and also one of the first to build a type-based intermediate representation in a functional-language compiler. He designed and developed the first production-quality type-preserving compiler for the entire Standard ML 1997 language extended with higher-order modules and was the main architect of the FLINT certifying infrastructure.

How It Works

First, a client submits any smart contract or any other system source code to CertiK, which then transforms its correctness to some equivalent mathematical problem, breaks it down into smaller ones and broadcasts them to the entire CertiK network. CertiK network nodes collaborate to solve these maths problems and receive rewards. While Bitcoin achieves ledger synchronization with a contrived hash function problem which wastes a lot of electricity, CertiK converts this power into actual academic and industrial values. The solutions found by the individual nodes are summarised at the CertiK blockchain and can be used at any time to validate the proof itself. CertiK assembles these solutions into a certificate to the original problem, either proof that the system is bug-free and hacker-resistant or some examples that triggered a loophole. The certificate is released back to the client. While CertiK uses blockchain technology, it is not restricted to it. The excess computation of proof power can also serve as a shield to protect off-chain systems such as self-driving cars.

While a CertiK audit can reveal exploits and other security weaknesses to blockchain outfits, they do not fix any of the issues. The audit simply finds them and offers advice for patching security holes to companies. Over 500 blockchain companies have partnered with or received auditing from CertiK. Among those are companies like PancakeSwap, 1Inch and Tether.

Key components of the CertiK Chain include:

- **Security Oracle:** The Security Oracle is powered by a decentralized network of operators that use industry-leading security technologies to evaluate the reliability of mission-critical smart contracts, such as those used in DeFi. It guards on-chain transactions and protects crypto projects from malicious attacks by conducting real-time security checks powered by a decentralized network of operators. In exchange for these real-time, updatable scores, these operators receive CTK rewards. The Security Oracle is interoperable with any protocol, allowing its users to make educated decisions before interacting with smart contracts. Smart contracts integrated with the Security Oracle may flag and prevent malicious transactions from occurring, preventing situations of crypto-asset loss.

- **CertiKShield (or ShentuShield) Reimbursement Pool:** This decentralized membership system enables flexible, decentralized reimbursements of lost, stolen or inaccessible cryptocurrency from any protocol due to network issues. Reimbursement decisions are fully made at the discretion of the members of ShentuShield, who may be blockchain projects or individual community supporters.

By leveraging the real-time Security Oracle scores and CertiK Chain's governance system, a decentralized network of members may provide collateral, receive rewards, and vote on claim requests to protect the blockchain communities. Members may participate by contributing their collateral as Collateral Providers, purchasing protection for their crypto as Shield Purchasers, or both. Collateral Providers earn staking rewards on their staked CTK while also earning a share of the fees contributed by Shield Purchasers. Shield Purchasers reserve funds from the Pool to be used as reimbursements for their crypto assets, paying a fee in CTK that goes directly to the Collateral Providers. CertiK has committed 1,000,000 CTK to be used to fund the Binance Smart Chain CertiKShield Reimbursement Pool.

- **DeepSEA:** DeepSEA is a secure programming language and compiler toolbox compatible with CertiK Chain's virtual machine (CVM), along with the Ethereum Virtual Machine (EVM), the Ethereum WebAssembly (eWASM) and Ant Financial's AntChain. DeepSEA has been awarded research grants from Ethereum, IBM-Columbia, and Qtum to push forward its hyper-secure programming language. While coding in DeepSEA, mathematical proofs are automatically generated to prove alignment between the intended specification and the actual code, allowing for greater depth of formal verification and correctness.

- **CertiK (or Shentu) Virtual Machine (CVM, now SVM):** While fully compatible with EVM, the SVM enables on-chain security parameters to allow smart contracts to interact differently with each other in accordance with their risk tolerance and based on the security certificates of other smart contracts. For instance, a lending contract may only provide a loan to a DAO contract if it demonstrates provable security. The SVM also allows users to access, check, and incorporate smart contracts and blockchain security information. Additionally, it is designed to support a smart contract sandbox, isolating the operation of smart contracts (especially those that have yet to be secured) from the rest of the system.

The CTK Token

CTK is the native digital utility fuel of Shentu Chain, serving as the core utility for on-chain functionalities such as operating the Security Oracle and ShentuShield systems and voting for governance decisions within the network. It has the following use cases:

- Gas consumption for smart contract operations;
- Staking for network consensus;
- Rewards for participating in the Security Oracle network;
- Collateral and reimbursements for CertiKShield;
- Community voting for decentralized network governance.

CertiK has raised 39.43 million USD from two rounds of private token sales, where 38.00% of the CTK total token supply has been sold at $0.77 per CTK during the first private sale where 29 million CTK were sold, and the second sale where 9 million CTK were sold at $1.90 per CTK.

CTK has a circulating supply of about 62 million CTK coins and a total supply of about 100 million tokens. The Binance Launchpool Allocation is 1.5 million CTK, and the initial circulating supply was about 22 million CTK. From the token supply, the token allocation is as follows: 1.5% to the Binance Launchpool, 29% to the first Private Sale, 9% to the second Private Sale, 10% to the team, 25% to the Foundation, 17.5% to the Community Pool and 8% to the CertiKShield Pool.

Positives

- CertiK has a partnership with Nebulas to provide smart contract security verification for DApps built on the platform. They also have a partnership with IoT security infrastructure project IOTex.
- Both the current and future market size is significant. For example, in a blog post, the team showed how the CertiK platform could have been used to easily highlight the simple code vulnerability that led to a $1 billion loss in Beauty Chain's valuation. Another example is the massive DAO hack that led to Ethereum's hard forking into ETC and ETH. More recently, a bug was discovered in the ICON smart contract that prevented token transfers from ERC-20 to ICON coins - the same bug found previously in the Yggdrash project. Furthermore, researchers estimate over 34,000 Ethereum smart contracts currently contain exploitable bugs, plus the amount of smart contracts has grown from 100,000 to 1 million from 2016-2017. Given these facts and the rate of cryptocurrency proliferation, it's hard to see how platforms like Certik will not become an essential part of future ecosystem development.
- They have a strong social media presence, with a 20,000+ strong Telegram, a few hundred YouTube subscribers, 800+ Twitter followers and a fairly active Medium.
- The core team leaders have very strong academic credentials, holding 3 PHDs from Yale between them. They also developed CertiKOS, the first fully verified concurrent OS kernel.
- On average, formal verification of smart contracts and blockchain code costs $100,000. So, unlike many projects, CertiK has a revenue model for funding future development.
- The CTK token is at the center of the ecosystem with various functions. Thus, its value should appreciate with network adoption.

Negatives

- Multiple projects have been hacked after going through audits done by Certik.
- There is competition from established projects like Quantstamp and Zeppelin. However, the solutions from both projects and others in the space are very human-intensive and do not involve much automation, so they are far less scalable than CertiK. So, despite this minor con, CertiK has a good chance to become a dominant player.
- CertiK's SubReddit currently has only two subscribers. Since Reddit has a massive cryptocurrency community, this is an important but often overlooked community that needs development especially given how much the platform relies on community contribution.
- None of the current team have any listed experience developing blockchain projects. Given their technical credentials, this is not a major con.
- The roadmap which is currently available does not go any further than June 2018, so it is overdue for an update. Also, their targets for partners and the available list of partners do not match. So, either the team failed to meet their targets or have not published updates yet.
- No public GitHub repositories to judge development progress so far. While there are some demo videos and code snippets available online, and it does look as though development is going well, there is no demo available for testing, so we cannot fully verify this.
- From DeFi Safety, when discussing audits on 88mph on April 15, 2021, "Only the Quantstamp audit really seemed to check the details; it makes the CertiK and PeckShield audits seem a little hollow. It is interesting to read all three as they review the same code."
- CertiK also once again got called out for a 'weak audit' by DeFi Safety on June 17, 2021.

Exchanges Where You Can Buy CTK Tokens

- Binance
- Gate.io
- Bitfinex
- ZT
- Bitrue

Works Cited

https://coinmarketcap.com/currencies/certik/.

https://www.certik.com/company/about/.

https://research.binance.com/en/projects/certik.

https://www.youtube.com/watch?v=aEn2UaqeHho&ab_channel=CertiK.

https://seas.yale.edu/faculty-research/faculty-directory/zhong-shao.

https://medium.com/foothill-ventures/founders-lessons-ronghui-gu-of-certik-53c39c76e3b8.

https://dyor-crypto.fandom.com/wiki/CertiK_(CTK).

https://www.securities.io/how-to-buy-certik-ctk/.

https://www.coinlore.com/coin/cryptyk/exchanges.