SANA

Storage area network anywhere

SANA Yellow Paper

Highly available and secure point-to-point regional node

network based on Swarm hard fork

SANA (Storage area network anywhere) is a p2p storage area node network that provides decentralized storage and communication services for blockchain applications. SANA uses hardware-supported Trusted Execution Environment (TEE) key storage for encryption services to realize data storage and transmission that cannot be tampered with or decrypted. The network relies on the ETH-xDAI network construction. The protocol codes are partly forked from Swarm's open source codes, and the storage protocol is fully encrypted for privacy. The SANA main network uses the Proof of Capacity (PoC) consensus algorithm. At the same time, the network has the characteristics of low GAS, high speed, high stability, and high security, which help to cope with the new challenges of personal data storage growth and data security in the future.

Contents

Abstract....2

1.Introduction....2

2. SANA Network....3

2.1 Swarm Network....3

2.2 ETH - xDai Stable Chain....3

2.3 TEE Storage Privacy Computing....4

2.3.1 Confidential Computing....5

2.3.2 Trusted Execution Environment....6

2.3.3 ARM TrustZone TEE....8

2.3.4 AMD SEV TEE....8

2.3.5 Intel SGX TEE....9

2.3.6 TEE Internal APIs....10

2.3.7 TEE Initiation Process....11

2.3.8 TEE in SANA....12

2.4 Dynamic Supply Balancing....14

2.5 Information Disclosure....15

3. Token Economy....15

4.Conclusion....16

5.References....16

Abstract

SANA (Storage area network anywhere) is a p2p storage area node network that provides decentralized storage and communication services for blockchain applications. SANA uses hardware-supported Trusted Execution Environment (TEE) key storage for encryption services to realize data storage and transmission that cannot be tampered with or decrypted. The network relies on the ETH-xDAI network construction. The protocol codes are partly forked from Swarm's open source codes, and the storage protocol is fully encrypted for privacy. The SANA main network uses the Proof of Capacity (PoC) consensus algorithm. At the same time, the network has the characteristics of low GAS, high speed, high stability, and high security, which help to cope with the new challenges of personal data storage growth and data security in the future.

1.Introduction

SANA aims to solve the opacity, poor security, high cost and discrete economic system of information in the current Swarm, promoting a highly scalable decentralized Internet infrastructure layer, and providing a completely independent and open decentralized infrastructure services for data assets. SANA's vision is to expand blockchain through p2p storage and communication by decentralized cloud computing and deployment of operative environment for computer systems and applications.

The distributed and smart features of the SANA network enable Ethereum and DAPP developers issue applications or updates without complicated network deployment. Developers can fully focus on the product inner logic without worrying about the underlying infrastructure, which will reduce development costs effectively. What’ s more, SANA will build a distributed network ecosystem with solid infrastructure, intermediate developers and DAPP developers, which is co-building, multi-sharing and effective. SANA is committed to provide creditable, reliable, and low-cost infrastructure for the application and prosperity of blockchain technology.

SANA provides computing, storage and bandwidth three-in-one resources for computing and storage. At the same time, it uses Proof of Capacity to reward infrastructure participants and contributors in accordance with network traffic. By measuring the usage of computing resources (computing, storage, and bandwidth) to incentivize and optimize the allocation of broadband and storage resources, SANA can provide network contributors and network users with settlement services and related financial payment services in an efficient, fair and transparent manner.

2. SANA Network

2.1 Swarm Network

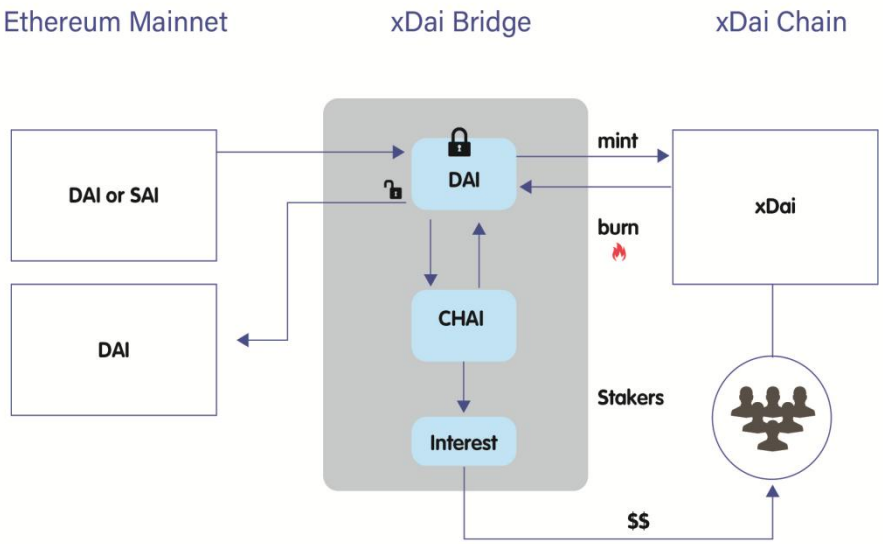
SANA is a brand new and open network forked upon Swarm. It has all the features and functions of the Swarm network. SANA has the same vision as Swarm and it is committed to building a decentralized storage and communication system for for a sovereign digital society. In the actual application of Swarm, we found that there are irreconcilable contradictions in some characteristics, so we forked a new network based on Swarm, which is used to achieve lower transaction costs, more suitable economic models of nodes, and more secure storage method.

Why fork upon Swarm?

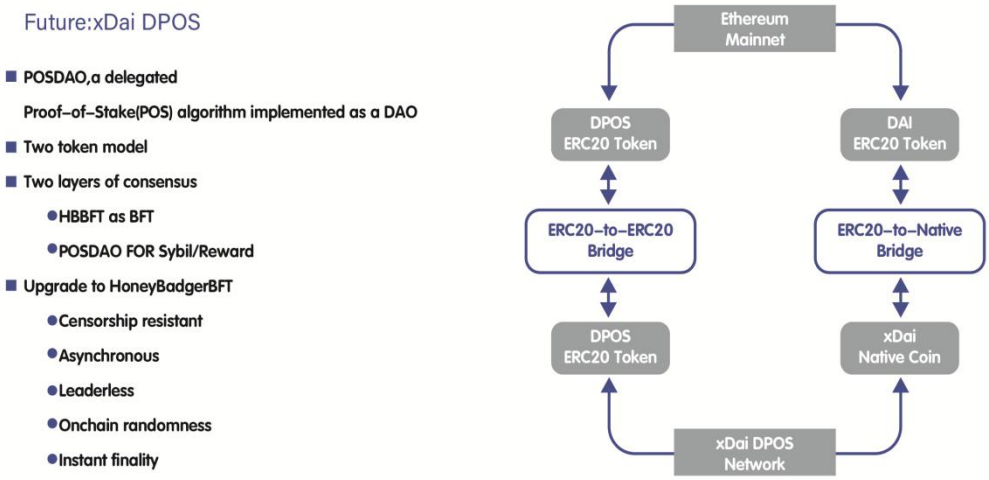
There is no doubt that Swarm's data network is better than most storage projects at present, but the shortcomings are also very obvious. For example, the seemingly ideal supply and demand relationship brings the incentive layer into an endless loop, and excessive sale of tokens has dampened the enthusiasm of miners and even the secondary market (which cannot be repaired). Ignorance of privacy calculations makes it impossible to identify low-stability nodes. We believe that the Swarm network is a very creative web3.0 network, but blockchain has never been a two-dimensional creature. It is three-dimensional and any mechanism may affect its future. We are very grateful to the contributions Swarm team made for the BZZ project. Because we firmly believe in the value of the Swarm network, we choose to help Swarm to make some very necessary changes at the most appropriate time. This value will belong to all people who firmly believe in the Swarm network.

2.2 ETH - xDai Stable Chain

xDai is Ethereum's Layer 2 sidechain based on EVM, bridging Dai stablecoin as the token, which is extensible and easy-to-use. The xDai Chain application provides users with fast transactions and extremely low gas costs. Because xDai Stable Chain is compatible with Ethereum, data and assets can be seamlessly transferred to the Ethereum mainnet. The SANA network is based on xDai Stable Chain to integrate the stability, scalability, security and high speed performance of xDai, which will open the door to exciting applications and use cases based on SANA network.



When the developers of SANA use the API interface of the main network to call the application, they only need to pay the corresponding $SANA as gas fee. There is no need to pay additional xDai or ETH. The SANA network will automatically convert and settle the corresponding tokens in smart contract.



2.3 TEE Storage Privacy Computing

What makes SANA unique in terms of data storage is the hardware Trusted Execution Environment (TEE) technology, where data storage and privacy computing is integrated for

efficient data slicing and distributed storage of privacy encryption. It ensures both the efficient use of distributed data and data privacy, realizing attack-resistant from software and hardware and prevention of network and node holders from evil conducts. Rights and interests of network users are well-secured, which is a huge improvement on the visitor request of Swarm network. SANA network uses TEE as the core technology for privacy encryption, which has been repeatedly mentioned by Polkadot Ecology member such as Crust, Phala, and Polkadot, who have officially introduced to their technology and application scenarios. TEE is often seen as a game-changer among current technologies and protocols, so what is it?

As a solution to data storage and privacy encryption for world's top institution, TEE provides a hardware isolation-based security world for proper security and program execution of sensitive data. TEE (Trusted Execution Environment), a trusted execution environment that can guarantee computing not disturbed by regular operating systems, and that is therefore it is called "trusted". This is achieved by creating a small operating system that can run independently in TrustZone's "safe world". In other words, it provides services in the form of direct system calling (handled directly by the TrustZone kernel).

TEE Hackathon

At 17: 30 London time on 9th October 2019, Trias hosted the TEE Hackathon themed on How to Use Trusted Computing and Layer-1 to Optimize Ethereum. Its first opening was at the University of Oxford. The hackathon focused on trusted computing, "-1" layer network, and Ethereum optimization applications, and it gathered online technology solutions for developers from around the world. This Hackathon was regarded as appreciation and recognition of TEE technology by Ethereum developers.

2.3.1 Confidential Computing

Confidential computing focuses on protecting the security of data in use. As a contrast, traditional encryption technology mainly protects the security of data at transmission and

storage. Different from homomorphic encryption, multi-party security computing, searchable encryption, and zero knowledge proof, the underlying technology of confidential computing is trusted execution environment (TEE) technology, and application scenarios include cloud (server), mobile terminal, edge devices, etc.

2.3.2 Trusted Execution Environment

The concept of Trusted Execution Environment (abbr. as TEE below) is not brand-new. TEE was first employed widely at fingerprint recognition on smart devices. Later, Intel found out that TEE has rich usage scenarios, so it began incorporating the technology into its own CPU in 2016. TEE was previously used in the game anti-piracy as well. Game manufacturers wrote the identification secret key of the legitimate game in advance to TEE. Once the device started the game, the relevant programs of the game would start to detect the secret key in TEE to verify the authenticity of the game, and this secret key and verification process are conducted in TEE, making it difficult for players to devour pirated games.

The execution environment is used to describe a set of external software and hardware interfaces of the environment, such as the instruction set, isolation requirements, etc. The objective of the trusted execution environment is to ensure that a task is executed as expected, including the confidentiality of the initial state, integrity, and the confidentiality and integrity of the run-time state.

Trusted terminals have three basic security functions:

1. Hardware isolation-based security execution environment: TEE provides a hardware isolation-based security world to protect the security and program execution of sensitive data. Implementing TEE requires division of the hardware and software resource of device into secure and non-secure worlds. The two worlds have independent systems resources, including registers, physical memory and peripherals, which can not be exchanged at will. Code and resources in the secure world are protected by strict control access policies, and processes in the non-secure world prohibit access to secure worlds to ensure that sensitive resources stored in the secure world are not illegally accessed or stolen by 'outsiders', effectively reducing the security vulnerabilities, chances of external attacks and invasion of viruses.

2. Platform based on trust chain integrity: TEE verifies the whole system from start gradually to later processes to ensure the integrity of the TEE platform. After the device is powered up, it loads the security boot program in the ROM and verifies its integrity with the root key. The boot program then enters the TEE initialization stage, starts the safe operating system, checks the key code at each stage during the starting process to ensure the integrity of safe OS while preventing unauthorized or malicious software operation; after the safe operating system is started, its runs the non-safe world boot program and starts the normal operating system. The secure start of the whole system of the mobile terminal is completed based on the trust chain, which can effectively

resist malicious behavior such as illegal tampering and code execution in the start process of TEE s.

3. Secure storage-based data confidentiality: Sensitive information such as user identity, private keys, and certificates demands high level of protection, and TEE relies on encryption and integrity protection technologies to protect the data and keys. TEE stores sensitive information such as user identity, keys, and certificates in security areas that can only be accessed or modified by trusted applications. Private key stored in the TEE can be used for encryption of user information to ensure the security of the sensitive information stored in the ordinary execution environment such as address book, SMS and other sensitive information in the ordinary execution environment.

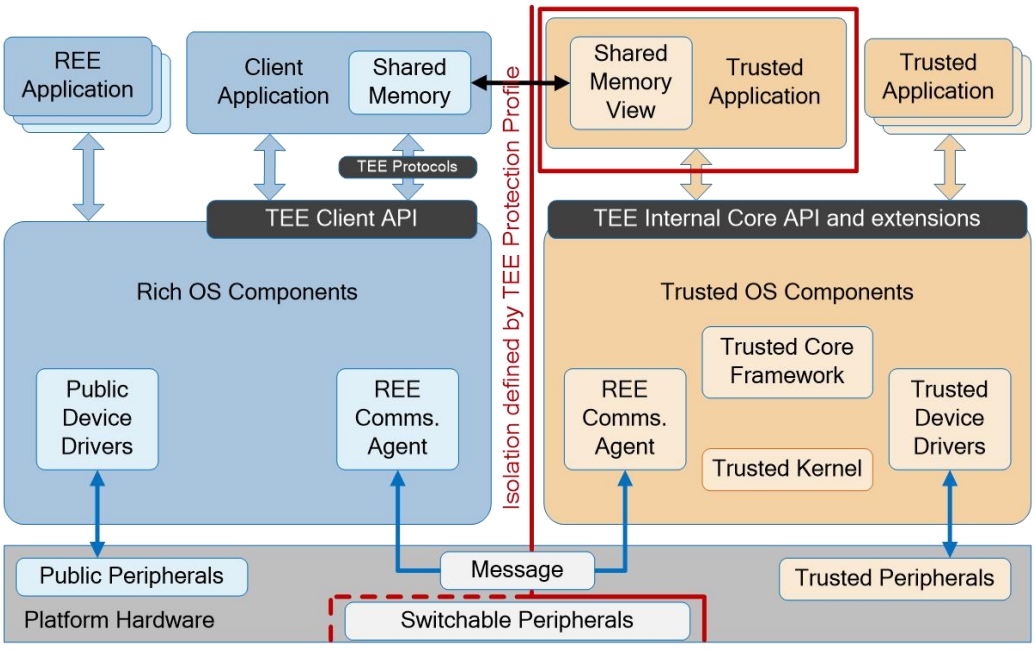
Trusted execution environments can be divided into:

1. Software Trusted execution environment:

Overshadow[CGL+,ASPLOS' 08], SP³[YS,VEE' 08], CloudVisor[ZCC+,SOSP' 11],InkTag[HKD+,ASPLOS' 13], Virtual Ghost[CDA,ASPLOS' 14], HypSec[LKN,Security' 19], etc;

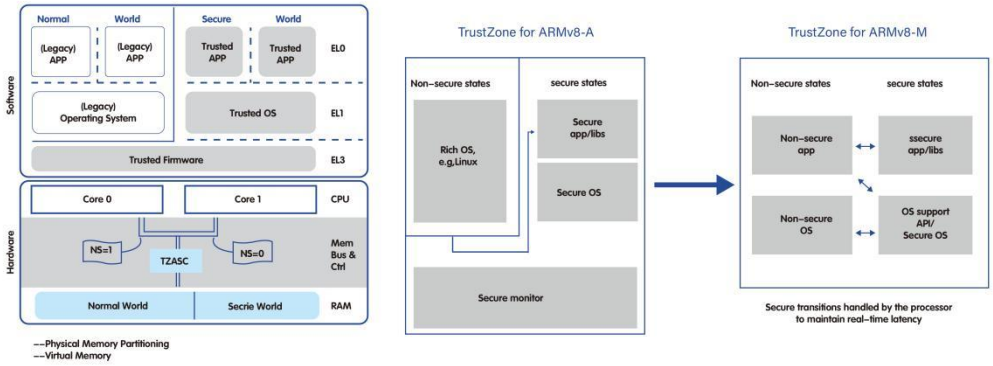
2. Hardware-trusted execution environment:

ARM TrustZone, AMD SEV, Intel SGX, etc.



TEE Software architecture

2.3.3 ARM TrustZone TEE

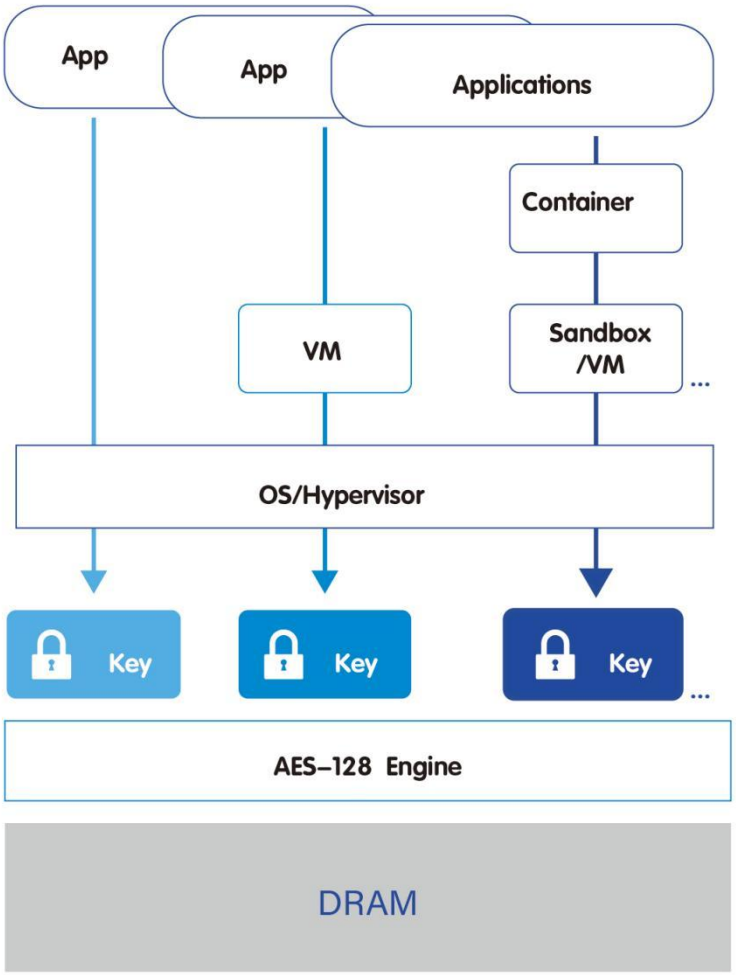


ARM TrustZone for Cortex-A & ARM TrustZone for Cortex-M

ARM TrustZone scheme is used for mobile TEE to build a secure world and non-secure world. We currently use Android or IOS with input elements such as fingerprint and facial information and other personal privacy data through TrustZone. TEE is isolated from the general APP and only saves the call interface so that the data in TEE is well protected even if the mobile device system is broken.

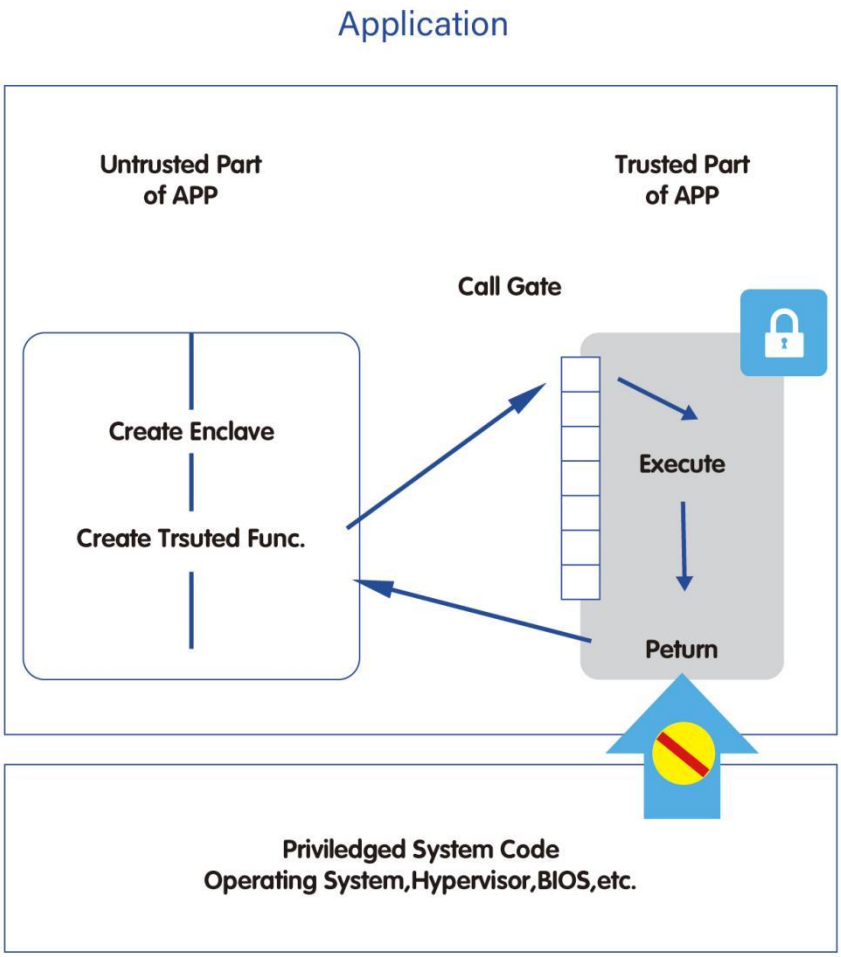
2.3.4 AMD SEV TEE

AMD's server chip contains Secure Encrypted Virtualization (SEV), which is an encrypted virtual machine memory on the server. The principle is that a small ARM chip built in the AMD's processor is specifically used to encrypt the memory of the virtual machine and to encrypt the register during state switching. SEV requires a certificate chain signed by the platform endorsement key to prove to the remote user, and that the physical memory of each VM is encrypted against physical and software attacks and that resource scheduling of VM is still managed by a hypervisor to have low privileges outside the caller.



2.3.5 Intel SGX TEE

The implementation of Intel Software Guard Extensions (SGX) TEE is by embedding TEE into the operation process so that TCB contains only CPU and TEE code itself. TEE code runs in user states (ring-3) with features like remote authentication, software attacks, physical attacks and low permissions. Thanks to the easy-to-use SDK and development environment of Intel, it has become the most widely used TEE platform in academia today, and one of the most popular TEE platforms used in blockchain projects.



2.3.6 TEE Internal APIs

1. TEE Internal Core API: provides TrustedOS functionality, communication with CA, communication of TA and TA, secure storage, cryptography, timer.
2. Other APIs: Built over Internal Core API and share error handling and API definition rules.
3. Private APIs: GP is not defined and cannot be used, and specific differentiation of products is allowed.

2.3.7 TEE Initiation Process

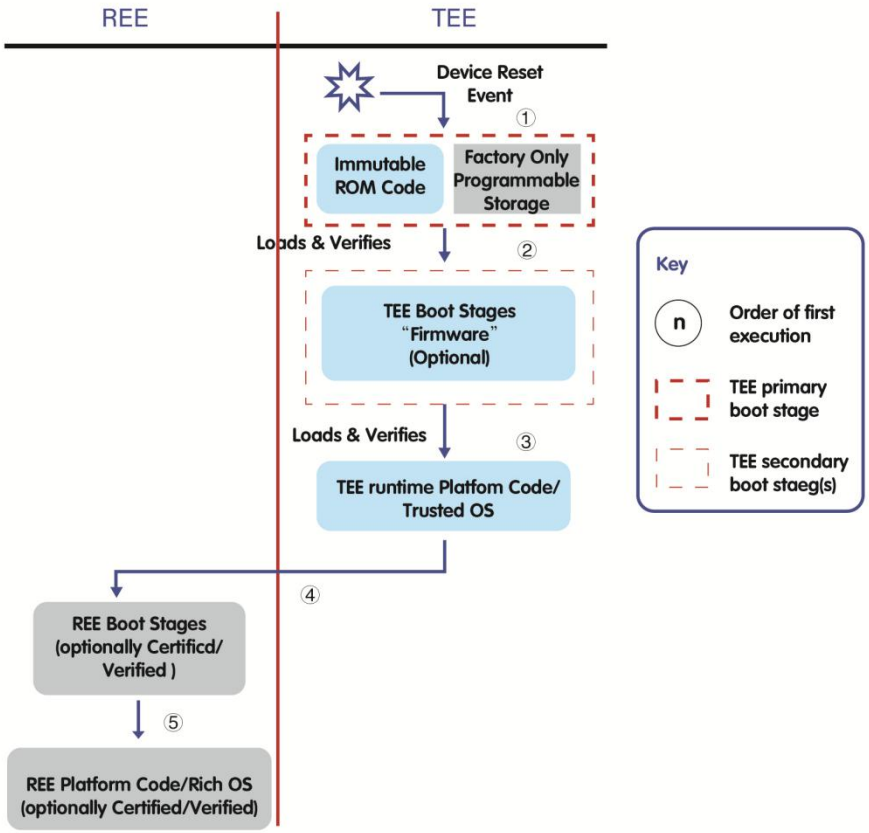
GP standard: The startup process performs only once when the system starts with request of the startup process to establish at least one trust root (RoT) as well as implementation of certain methods.

General starting of the ROM-based code: allowing other implementations to verify the loaded code in turn.

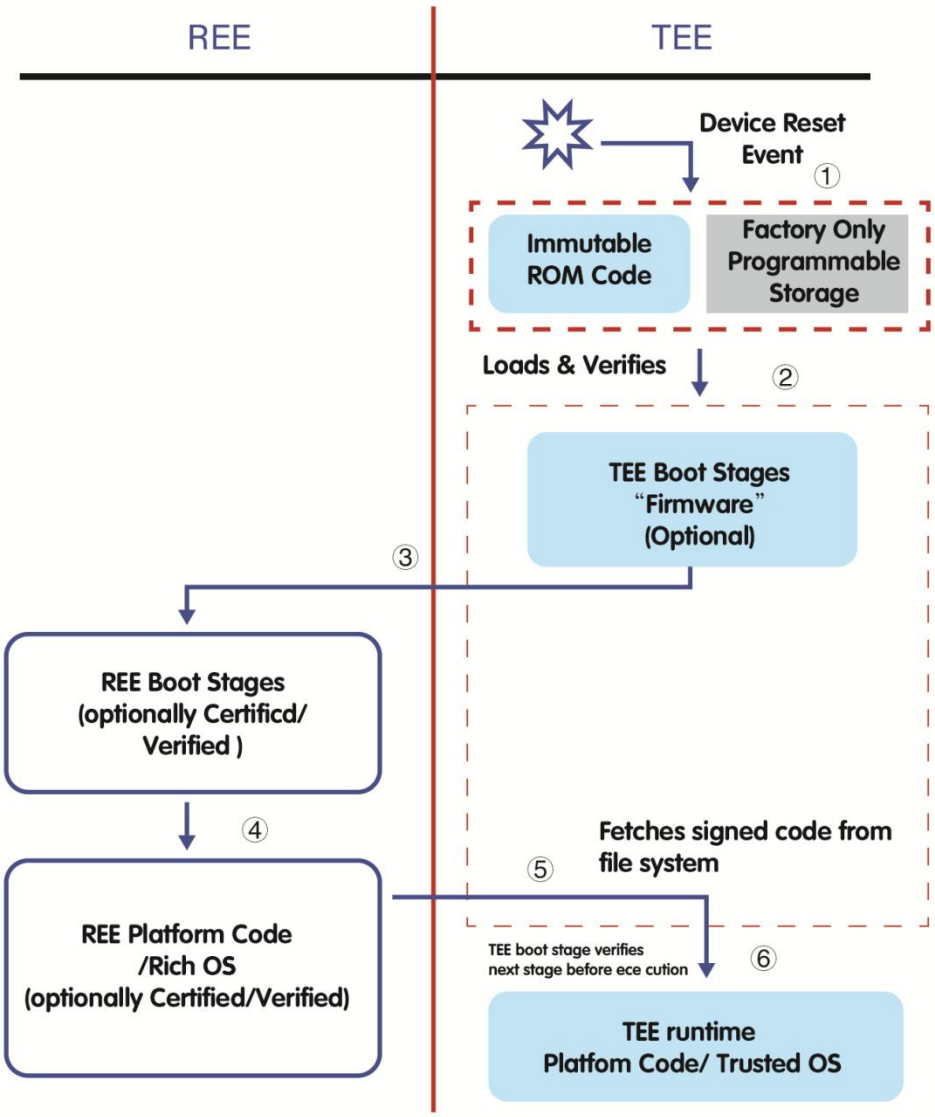
Generally, TEE starts first: prevents the REE interface from taking effect

The system can implement a TEE at startup (a subset of full TEE)

Start process 1: Trusted OS starts first, as shown below:



Start-up process 2: Trusted OS starts as required, as shown in the figure:



2.3.8 TEE in SANA

SANA storage solutions uses TEE encryption technology. TEE + blockchain hardware and software fusion framework is more practical compared with other cryptography schemes such as zero knowledge proof. In the case of meeting the most basic needs, smooth user experience is by no means a problem, because most of the verification links can be put into the TEE for execution. On-chain resource is not preoccupied.

Complete data acquisition and encryption can be uploaded locally via TEE, so that TEE can solve the problem of data authenticity preon-chained and facilitate the SANA network to improve security, performance and privacy.

- **Security.** Most public chain projects fail to guarantee safe operating environment of each node. On-chain data security can only be maintained by a large number of nodes reaching consensus. The number of nodes is obviously inversely proportional to the performance, bringing serious performance bottlenecks to the public chains. In comparison, SANA empower onchain data security of the entire network by ensuring that the code running in the machine is not tampered with and can be run in the manner specified by the blockchain protocol.

- **Performance.** We believe that the code in TEE is not tampered with and it can be executed as expected, so the blockchain can move part of the computation to the TEE environment, reducing the cost of global consensus and increasing the performance of the blockchain.

- **Privacy.** TEE can provide end-to-end privacy protection. Data from calculation to results can only be seen by the user himself.

Smart contracts

Smart contracts in blockchain are widely popular for realization of automated writing and execution of contracts, which benefits to improve system efficiency. However, due to its running on the blockchain with decentralized and distributed bookkeeping characteristics, data of the smart contract will be copied to all the nodes on the blockchain, accelerating the attack possibilities to a certain extent, resulting in the smart contract facing security risks such as rollback attack and reentry attack. Privacy and security of data is threatened.

Privacy protection is a hustle in the current blockchain operation. In some applications that highly value data security privacy, when smart contracts alone are difficult to meet application needs, SANA can provide solutions for distributed data storage + TEE to enhance the ability of smart contracts to combat security risks.

TEE Support

SANA will support both the Intel and AMD TEE chip technology platforms.

AMD SEV

1. The goal of SEV is to secure VM. Hash is included during verification of AMD signature. This firmware is the code embedded into the virtual machine and it allows the host to include coding in the TEE.
2. KVM enables users to transform Linux into a hypervisor, enabling the host computer to run multiple isolated virtual environments, namely a virtual client or virtual machine (VM).
3. Turn on KVM AMD SEV support to secure data memory for VM and further ensure the security of code running in VM.

Intel SGX

1. SGX is a new extension to the Intel architecture. It adds a new set of instruction and memory access mechanisms to the original architecture that allow applications to implement a container known as enclave.
2. Enclave is a protected content container for storing application-sensitive data and codes. SGX allows the application to specify the code and data sections to be protected. The code and data do not have to be checked or analyzed before the enclave is created, but the code and data loaded into the enclave must be measured. Enclave can prove itself to a remote authenticator and provide the required functional structure for safe key provision. User can also request a unique key that is combined with the identity of the platform and that can be used to protect data stored outside the enclave.
3. Data security-related code runs in the enclave container for security. The above-mentioned is the hard software used by different chips to realize security containers. Data encryption and decryption, node verification and other related processing code will run in the security containers to ensure the nodes feasibility, prevent cheating and malicious behavior of the nodes, and also ensure the long-term stable income of the nodes. Through the TEE transfer mode of the different chips mentioned above, the data encryption, decryption and black box operation can be executed after receiving the SANA network data.

SANA networks allow only the broadcast and verification of encrypted data by TEE technology. Each node will run inside and outside the independent space without violently crack the attack. All stored data will be encrypted or decrypted for the sake of user's privacy.

2.4 Dynamic Supply Balancing

SANA adopts a two-layer mining structure to effectively incentivize node holders and trusted miners. Node miners will receive private computing rewards when they provide stable online nodes and effective CPU computing capabilities. When data storage, data reading and other supply and demand functions are generated, miners will receive supply and demand rewards.

80% of the $SANA tokens will be produced by dynamic calculation, which will greatly increase the enthusiasm of miners.

SANA uses a way of wavebands to reduce mining production, which is a innovative creation. In the first year, the reward is 2000 tokens(N_b) for a single block. The 2000 tokens in a single block will be equally distributed to each node miner through the checkbook. Production will be reduced by 1%(H_d) every week, and effective nodes number will be counted every 2 months. If the growth target for nodes is reached, the block reward will be reset. If the target is not met, the production will continue to be reduced.

Algorithm of dynamic supply balancing:

$$N_b = 2000$$
$$N = N_b \times \left(1 - floor(H \div H_{\mathrm{D}}) \times 0.3\right) \times (1 - floor(H \% H_r \div H_d))$$

H Current block height

N_b Basic block reward

H_D Reduce production by 30% every 3,153,600 blocks, about 1 year

H_r Resetting the block reward every 518400 blocks to the initial reward of this year, about 2 months

H_d Reduce production by 1% every 120960 blocks, which is affected by H_r, about 14 days

2.5 Information Disclosure

SANA is an open source project independently initiated by a group of geek-spirited blockchain technology team. The project forked upon the Swarm open source codes. We have contributed the source code to the technical community. All project codes are available on GitHub (https://github.com/ethsana), and we will continue to update the latest progress of the project.

For more interaction, please visit: https://twitter.com/ethereumsana

3. Token Economy

SANA network issued $SANA, an ERC20 token based on the ETH-xDAI network as the governance token to stimulate transaction on the network and realize the function of recovery, redistribution and destruction of transaction fees, which will increase the demands of tokens.

Token Allocation

A total of 10 billion $SANA tokens will be minted, and the supply will be fixed by the smart contract.

- **80% of tokens will be produced by mining**
- **8% of tokens will be allocated to community technical contributors**
- **7% of tokens will be used for ecological development to support the construction and development of project ecological applications**
- **2% of the tokens will be used for the early liquidity providing**
- **3% of tokens will be used for airdrops**

4.Conclusion

SANA provides a better solution for the decentralized storage and communication service network. We hope that by building a more high-speed, convenient, low-cost, safe and reliable point-to-point storage area node network, we can serve the current storage and network service bottlenecks faced by blockchain applications. SANA will be a permissionless private network. It satisfies the demands for freedom of speech, data sovereignty and open market on the network, while maintaining security through integrity protection, anti-censorship and anti-attack capabilities.

The above contents cover the design and planning of the initial mainnet of SANA1.0. [1]

SANA is initiated and constructed by a group of technology enthusiasts with common ambitions. With this milestone, our journey has just begun. Join SANA[2] with us and accomplish the mission of data storage freedom.

[1]https://github.com/ethsana

[2]https://ethsana.com or https://ethsana.org

5.References

【1】Swarm Whitepaper and The Book of Swarm，https://docs.ethswarm.org/docs/

【2】xDai Stable Chain，https://www.xdaichain.com/

【3】xDai Bridge，https://dai-bridge.poa.network/

【4】Global Platform simple guide on TEE, http://www.globalplatform.org/mediaguidetee.asp

【5】Trusted Labs white paper on TEE security certification ，http://www.trusted-labs.com/spip.php?article238

【6】Global Platform http://www.globalplatform.org/

【7】TEE specifications http://globalplatform.org/specificationsdevice.asp

【8】TEE related press release: TI and Netflix， http://www.pcmag.com/article2/0,2817,2388090,00.asp

【9】Solacia and ST，http://www.electronics-eetimes.com/en/trustzone-ready-drm-technology-targets-set-top-boxes.html?cmp_id=7&news_id=222918014#

【10】Trustonic partners program，http://www.trustonic.com/news/release/trustonic-launches-t-dev-developer-program-establishes-trusted-services-ecosystem-with-tier-1-service-partners/en

【11】 Amazon. AWS Whitepapers & Guides, https://aws.amazon.com/whitepapers/

【12】 Microsoft. Windows azure，https://azure.microsoft.com/en-us/