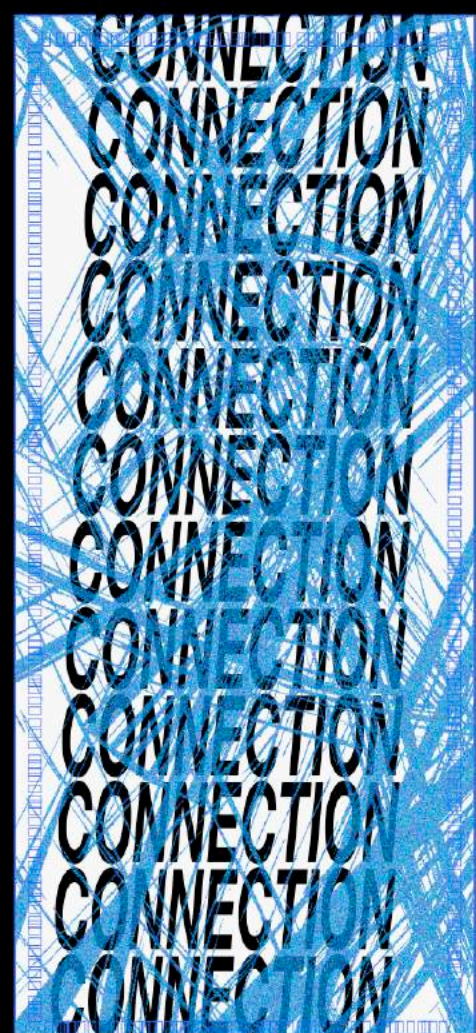
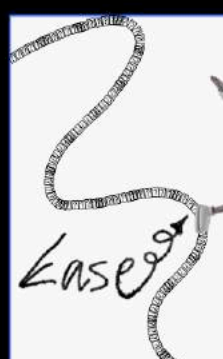




Scalable, secure, commercial-grade blockchain that runs on end-user devices.



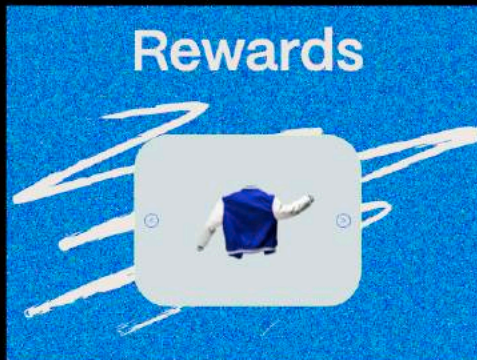
Stylish



control



[access]



COMPREHENSIVE 综合的

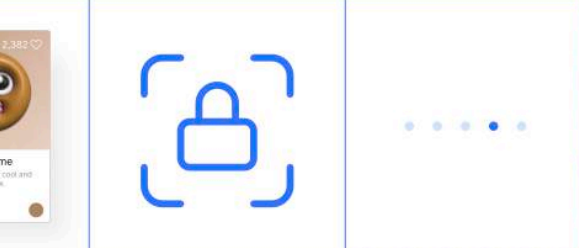
zeWallet

2023

Good afternoon!

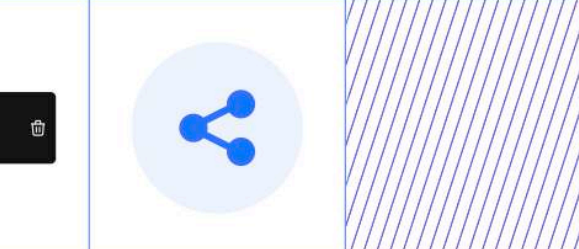
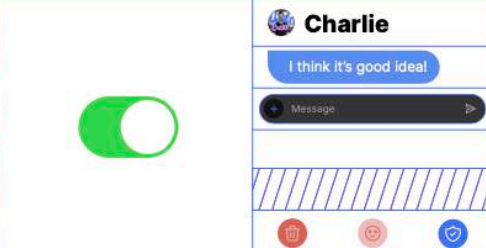
\$2592.01 Portfolio value

45 AMT Mining rewards



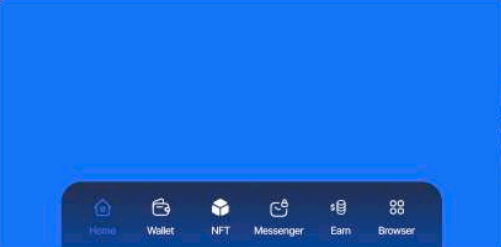
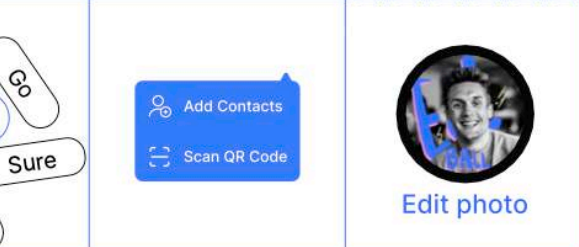
\$7687.25 MyWallet

Send Receive Swap Buy



Next

Import Wallet Create Wallet



1. Summary

AmazeChain aims to be the vanguard of a new era in blockchain technology, leveraging end-user devices such as smartphones and PCs as decentralised mining nodes. This approach allows for unparalleled scalability, efficiency, and security, aiming for mass adoption across various data transmission applications—including transactions, messages, and file-sharing.

AmazeWallet, the proprietary application for both iOS and Android, serves as the operational node for mobile users.

- Github: <https://github.com/WeAreAmaze/amc>
- Website: <https://amazewallet.com/blockchain/>
- Testnet: <https://testnet.amazechain.com>
- Mainnet: <https://mainnet.amazechain.com>
- Twitter: <https://twitter.com/AmazeChain>
- Contact: hello@amazewallet.com

2. Context

Limitations of centralised systems

Blockchain technology has the potential to dramatically change society, well beyond just financial transactions. It paves the way for transparent governance, decentralisation of power, and direct, peer-to-peer connectivity.

Risks with centralisation include:

- Centralised financial oversight
- Corporate monopoly over user data

Rather than leveraging technology for solutions, many policymakers resort to protectionism, a backward-looking approach that undermines the tenets of a modern, open society. The concentration of resources also stifles competition and raises serious concerns about data privacy and security.

Potential and direction of decentralisation

The inherent "trustless" nature of blockchain—enabled by its transparent, immutable ledgers—eliminates the need for middlemen, authoritative figures, or cumbersome bureaucracy. This feature allows individuals to transact directly with one another with a level of trust and security that was previously unattainable in centralised systems.

The meteoric rise from the Bitcoin whitepaper to a \$3 trillion industry in just a decade underscores its transformative impact.

The way forward: Scalable mobile adoption

While blockchain has come a long way, it needs to continue evolving to stay ahead of existing systems, particularly in rule-making and governance. Self-updating, transparent protocols are essential—but they are only a part of what the technology can and should aim to achieve.

For blockchain technology to become genuinely transformative, the industry needs to focus on driving scalable mobile adoption in the coming years. With billions of smartphone users worldwide, a significant number of which are becoming 5G-enabled, the mobile platform offers an unparalleled opportunity for mass adoption. By making blockchain technology more accessible and user-friendly on mobile devices, we can overcome one of the most significant barriers to its widespread use.

This mobile-first approach doesn't just offer convenience; it also serves as a gateway to financial inclusion and decentralised governance, particularly in regions where traditional infrastructures are lacking or inefficient. In essence, scalable mobile

adoption can make blockchain not just an alternative but the preferred choice for secure, transparent transactions and governance on a global scale.

Put simply, for blockchain to be a viable, long-term solution, it must outperform existing systems by continually updating its rule-making capabilities and focusing on scalable mobile solutions. By doing so, blockchain has the potential to reshape our societal systems profoundly, decentralise economic power, and offer a more transparent form of governance that relies on rules rather than authority.

3. Solution

With 7 billion smartphones globally, half of which are expected to be 5G-ready this year, mobile-first access to blockchain technology is more relevant than ever. AmazeChain aims to bridge this gap.

Technical Features

- High Scalability: Over 300,000 TPS (transactions/second) in real-world conditions.
- Data Efficiency: Reducing the typical data load with only 0.0067% data consumption of that of the traditional Merkle Trees, thanks to a proprietary algorithm.

Components

- Smart Contracts: Support for Rust, C++ and Java languages.
- Compatibility: Works with UTXO, EVM, MOVE and WASM protocols.
- Optimisation: Uses sharding, layering, Zk-EVM, and Zk-SNARK for best performance.
- Security: Quantum-resistant algorithms ensure transaction safety.

4. Vision

Our vision is a new kind of internet ('Web3') that can help decentralise power and build a more equitable world, especially online. It should be suitable for running all kinds of smart contracts and decentralised applications at a large-scale. Our network also supports continuous upgrades without forking.

Goals

We have several goals in building AmazeChain:

Scalable performance

While ensuring security and trust AmazeChain can support billions of people using, transferring, and querying the network at the same time, with throughput and performance capable of meeting the growing needs of global businesses moving online. We reduce the time and cost of a single transaction to less than a cent, by the system design and lack of manual coordination between nodes.

Point-to-point communication

Under the constraints of current communication hardware (such as fibre optic cabling and 5G) and individual consumer bandwidth, we allow anyone to connect directly and in a trustless way to share files, payments, messages, media content, stream video and other daily needs.

Storage capacity

We support commercial data storage needs, by storing newly generated and historical information across the network in a reliable, redundant, and fault-tolerant manner. That includes transaction ledgers, real-time backups of phones/PCs, media, files, and collaborative work.

Privacy protection

AmazeChain uses modern encryption technology to protect user privacy, ensuring that personal data is not compromised by companies or hackers, while also complying with local regulatory requirements. From the perspective of information security and asset value, our protocol allows data generators to achieve autonomous data management.

Universality

Anyone, at any time, at any place, can access and use our open, public blockchain, while any application or transaction can be published on Amaze without permission.

Security

Security is paramount in any system. We ensure commercial-grade security of data and transactions for large-scale financial applications, using quantum-resistant cryptography.

Delivering value

Compared with traditional decentralised platforms, our innovation enables the network to share storage, computing power, and bandwidth resources—improving overall efficiency. It enables anyone to create value on the chain through new applications, products and economies, and obtain income through multiple channels (including real world).

Benefit

Amaze not only acts as a financial network for the creation and exchange of digital token value, like the first and second generation blockchains, but it also supports a large number of users to truly participate in our network services based on their real economic and other needs, which gives the key quality to creating a sustainable ecosystem with momentum. Similar to centralised economies, the 'economic ecology' of our chain ecosystem comprises the production, consumption, and trading of value by users. In addition to token exchange and investment, AmazeChain also supports a large number of online and offline transactions for the production and consumption of network services.

AmazeChain offers higher incentives than the standard inflation rate through services that are rooted in real economic needs—such as social media, e-commerce, data storage, peer-to-peer payments, mobile games and more. It is a value-creating ecosystem for all participants, where everyday mobile users mine our native currency for running the node infrastructure upon which businesses may pay to store and exchange data.

5. Principles

In 2017 we outlined our technical goals. These principles have guided the development of our chain ever since.

Simplicity: The protocol should be kept as simple, readable, and maintainable as possible, even if it may lead to some limits in data storage or timeliness. Ideally, developers should be able to follow the specifications and requirements, and implement any application that uses blockchain technology, and further promote the vision of an open protocol for everyone. In general, this is our most important principle. Complexity is only added when it can bring significant benefits.

Universality: The blockchain should provide a Turing-complete scripting language that any programmer can use to build mathematically defined smart contracts or transaction types. You can use our platform to deploy on-chain e-commerce transactions, issue digital tokens, establish Daemons or Skynet—and more—without any restrictions or obstacles.

Decoupling: Our platform is based on several independently developed protocols. The parts of the protocol should be designed as modular and separable as possible. In the development process, our goal is to create a series of protocols that require as few and as small changes as possible when optimising or upgrading, and the protocol will continue to run without any further modifications. For this reason, we implement some innovative features (such as hashes, improved Kate proofs, and RSA accumulators) as standalone, fully functional libraries. In this way, even if AmazeChain does not need to use certain features, they can still be used in other protocols. Development based on Amaze should be maximally decoupled to benefit the entire blockchain ecosystem—not just itself.

Agility: The details of the AmazeChain protocol are constantly changing. We will carefully design software architecture and high-level structures such as using sharding roadmaps, abstract execution, and only including data availability in consensus. In the later stages of development, computational testing may reveal some opportunities for iterative development, such as protocol architecture or AMC virtual machines, to greatly improve scalability or security. If we or others discover such breakthroughs, we will make sure to quickly adopt them for the benefit of the ecosystem.

Non-discrimination and censorship resistant: The protocol aims to provide a broad range of flexibility and does not actively limit or prevent specific types of usage. All regulatory mechanisms in the protocol aim to directly control functions, rather than to oppose specific bad applications. Developers can run infinite loop scripts on top of Amaze as long as they are willing to pay transaction fees for each computation step.

Collaborative Inclusiveness: We emphasise a cooperative and inclusive design, supporting shard communication, value exchange, and function sharing. Not only that, AMC can also connect different blockchains, even linking Bitcoin and Ethereum as two interconnected shards, achieving transfers, script execution, and contract calls—opening the door to a new round of innovation. In addition, AmazeChain can directly interact with mainstream DeFi protocols and cryptocurrencies (like Bitcoin and Ethereum).

6. Structure

Overview

We reuse existing internet infrastructure and hardware—especially mobile phone devices—to verify transactions and secure the network. Our network uses a VDF-VRF POS consensus mechanism. The system design has distinct advantages over existing blockchain networks, including optimising storage, sharding, layered architecture, scalability, zero-knowledge proofs, upgradeability, and transparent governance, among others. It also avoids the significant energy consumption or the demanding hardware of POW chains.

AmazeChain uses independently developed protocols to support various applications. Its Blockchain Distribution Network (BDN) ensures rapid broadcasting while maintaining data consistency. The miner-plus-verifier structure keeps energy consumption low, and achieves effective final consensus for single block production through step-by-step decision-making. Moreover, the sharding network allows parallel processing of multiple transactions, while layered processing supports batch processing of transactions, generating proofs, off-chain contract execution, and outsourced computing capabilities.

The network consists of six layers: data layer, network layer, consensus layer, incentive layer, contract layer, and application layer.

How miners produce blocks

In the AmazeChain network, the Proof-of-Stake (PoS) consensus is overseen by a unique set of participants known as "mobile validators" or "virtual miners." These miners activate their roles by locking-up a specified amount of AMT tokens—either 50, 100, or 500—and are included in a specialised registry that keeps track of their addresses, statuses, and submitted attestations. To secure the network, the staked AMT tokens are stored in a smart contract.

Once successfully staked, these miners become eligible for random selection to generate a new block every 8 seconds. The rewards for these newly minted blocks are recorded in a Coinbase address, commonly labeled as the "Miner Address" in the blockchain explorer. Each active miner has an associated pool of pending rewards, details of which can be viewed in the blockchain explorer's list of miner validators.

When a miner's pending rewards reach or exceed 0.5 AMT, these rewards are automatically batch-distributed to their account at specific intervals. This approach avoids generating a massive number of transfer records by distributing rewards for

each block to hundreds of thousands of miners. This mechanism not only ensures the network's secure and efficient operation but also effectively manages and logs the activities and statuses of a large number of validators.

There are three steps for miners produce a block on AmazeChain:

- Proposal
 - Verification
 - Confirmation
1. Proposal involves a global sorting of transactions, checking the pre-sorted layers, marking the dependencies of input and output states, and non-parallel transactions, generating input states and proofs, and generating zkEVM proofs of the processing, output states, and commitments—thus minimising data and generating sorting structures.
 2. Verification tasks are parallel processed by thousands of computer nodes, with very little calculation for polynomial commitment and zkEVM proof verification, which can be done with regular devices including smartphones and PCs. The time is mainly spent on receiving data and returning multi-signature results.
 3. Confirmation includes merging the received verification results, and using redundancy and game theory algorithms to prevent hacker collusion. Two thirds of the votes received by the system are valid. In case of mass node downtime or a regional internet outage, the system will delay final confirmation and record the correct transaction information.

Transaction processing

Many networks process transactions and contracts one by one. But to be able to process multiple transactions in parallel, the double-spending problem—which is the direct and indirect spending problem of the same address—must be solved. We use state sharding to solve the double-spending problem and coordinate communication, value exchange, and feature sharing between shards. The system can even connect Bitcoin and Ethereum as two shards for transfers, script execution, and contract calls.

The layered structure comes from the Lightning Network, which is iterated through technologies such as side chains, state channels, Plasma, and Rollup; using smart contract layers, transaction layers, and proof-outsourcing technology so that transactions and contracts can be quickly chained, and consensus reached after batching, merging, and pre-processing.

Broadcasted transactions, transaction pools, consensus communication, proofs, block data, and blockchain state are quickly distributed across the network through BDN to achieve consistency and scalability.

Distributed applications are divided into a smart contract layer and an application interaction layer, utilising the computational power, bandwidth, and storage resources provided by the blockchain to implement upgradability and transparent governance through nodes for remote procedure call (RPC) service and Web3 calls.

Node components

1. The smartwallet app runs on the mobile phone, uses WiFi/5G to connect to the internet, and can initiate transactions, sign them and broadcast to a transaction pool, verify ZK proofs and execute transactions, as well as generate blocks and add to the blockchain, based on the hash provided by block proposers.
2. Block proposers are located on servers, running on an IDC gigabit shared network, and can receive transactions, initiate proposals (propose bundles of transactions into blocks), verify the signature of smartphone nodes, and upload data.
3. Storage nodes need high-performance servers and run on IDCs directly connected to one another, and can package, execute block bodies, generate blocks and ZK-SNARK proofs.
4. The Blockchain Distribution Network (BDN) is located on servers, running on IDC gigabit shared network, and can cache blocks as well as provide verification, RPC function, address indexing, address visualisation, hash signature verification services, IPFS services, BT, Web, historical ledger, historical status and other services, and provides downlink data.
5. The blockchain browser also runs on the server, located on IDC's gigabit shared network, can query information, transaction conditions, query balance or detailed transaction information through wallet address, and provide data statistics, such as the total number of blocks, new wallet addresses, and transaction records.
6. The performance monitor also runs on the server, located on IDC's gigabit shared network, can query the number of nodes, busyness, network, CPU, storage, performance, etc.

7. Developer Requirements

Knowledge base

To understand the Amaze public chain technology, one needs to possess some foundational knowledge including blockchain basics, programming language fundamentals, smart contracts, principles of cryptography, data structures and algorithms, decentralisation and distributed systems, front-end frameworks, etc.

In addition, non-technical skills such as curiosity, determination, and resilience are necessary. Our public chain open-source project is composed of a group of software programming engineers who develop according to the white paper and the AmazeChain Improvement Proposal (AIP). Developing the chain involves a wide range of areas including communication protocols, peer-to-peer networks, databases, cryptography, language interpretation, RPC and websocket, etc. It also represents a fundamental shift in the current financial system and offers the opportunity to help reshape the world financial system. However, in the world of cryptocurrency, errors and security vulnerabilities could have more dire consequences than traditional projects. Therefore, a formal and rigorous development process is necessary.

Before writing code, it is suggested to have some minimum recommended skills, including a reasonable understanding of blockchain, experience in some C-like language, understanding of data structures and their impact on performance, familiarity with unit testing and debugging experience, etc. Additionally, it's crucial to understand the area undergoing changes and the code it depends on, as well as the code that depends on the changes.

The recommended skill set largely depends on the specific area of contribution. For example, if you wish to contribute to cryptographic code, you need to have a good understanding of security and performance impacts. The standards of programming languages like C++, Go, and Rust need to be adhered to. Finally, it is recommended to master basic blockchain knowledge and language fundamentals before starting to write code in order to better understand and construct the code.

Development practice

Developers should work within their skill set and submit pull requests when they believe their feature or bug fix is ready to be integrated into the main branch.

In development practice, we strongly advocate the method of "share early, share often". The basic premise of this approach is to announce your plans before starting work and to present your changes as a series of small, reviewable commits, so you can share your progress with the community at any time.

This approach has several benefits: firstly, announcing your feature work plan can avoid duplicating work; secondly, it allows for discussion, which can help you achieve your goals in a way that's consistent with the existing architecture; thirdly, it minimises the chance of you spending time and energy on changes that may not align with community consensus or existing architecture and may therefore be rejected; finally, incremental development helps ensure you stay on the right track with the rest of the community.

Sharing your progress early and often ensures that your changes get merged into the main branch faster and you stay up to date with the main codebase.

Testing

In the design of all core packages, achieving complete test coverage is one of the main design objectives. Since errors in digital currency software could potentially result in people losing real money, every effort must be made to ensure the code is as accurate and error-free as possible. To achieve this goal, thorough testing is critically important.

Unless the new feature you are submitting is trivial, it may be rejected unless it also comes with sufficient test coverage, including tests for both positive and negative conditions. That is to say, tests must ensure your code functions correctly when given both correct data and incorrect data error paths.

Programming languages like Go and Rust provide excellent testing frameworks that allow for the direct writing of test code and checking of coverage statistics. Therefore, all new code should be tested to ensure that the code behaves correctly when given expected values and can gracefully handle errors.

When you fix a bug, it should be accompanied by tests to demonstrate that the bug has been resolved and to prevent it from reoccurring in the future.

Documentation and Comments

Each function should be commented to indicate its intended purpose and any assumptions. Function comments should always start with the function's name, and

comments should be complete sentences because they allow for various automated presentations. A good rule of thumb is to imagine yourself as a person completely unfamiliar with the code, then ask yourself whether the comment provides enough information for you to understand the function's purpose and how to use it.

For exported functions, comments should include detailed information that a function caller might need to know and/or understand.

Comments should appear within the body of the code, but they should explain the intent of the code, not merely point out the obvious. Due to the development of multi-monitor programming and laptop display resolutions, it is no longer required for each line of comments to be no more than 72 characters and to increase indentation levels.

Code Review

All submitted code must undergo a code review before being merged into the main branch. This process is performed by the project maintainers and typically includes other submitters interested in the area.

The timing of a code review depends on factors such as the number of requests to be reviewed, the size and complexity of the contribution, adherence to guidelines, and the reviewer's understanding of your submission. For example, if you submit a holistic change involving the content of multiple subsystems, a longer review time is obviously required. It may be necessary to break the submission into several smaller, manageable submissions.

Noting the points above, most small changes will be reviewed within a day, while large or impactful changes may take several days. This is also the benefit of adhering to early sharing, as sharing is often the practice of development.

The main purpose of a code review is to ensure the code follows the development code standards. Additionally, other checks are carried out:

- Code has good stability and no security issues;
- Code correctly uses existing APIs and integrates well with the overall architecture;
- The changes are considered appropriate by community consensus.

After the code review, if there are no issues, changes will be accepted immediately. If there are any doubts or issues, you will receive feedback as well as the next steps to be executed. In some cases, the code reviewer or interested submitter may help you rewrite the code, but usually, they will only provide feedback so you can make

necessary changes. This process will continue until the code is finally accepted. Once your code is accepted, it will be integrated with the main branch. Normally, it will be rebased and merged quickly, as we prefer to keep a clean commit history over complex merge commits. However, regardless of the specific merge method used, the code will be integrated with the main branch.

The code checklist includes:

- Submitted code is commented according to code documentation and comments;
- For new code: it comes with tests, which run both positive and negative (error path) conditions (if applicable);
- For bug fixes: the code is accompanied by new tests that trigger the error being fixed to prevent rework;
- Any new log statements use the appropriate subsystem and logging level;
- Code has been formatted;
- Running tests do not cause any test failures;
- Running static analysis tools do not report any issues;
- Running source code inspection tools to check code norms do not report any new issues not previously present.

8. Code Fundamentals

Account

In the system, an account is represented by a 20-byte address, which originates from the last 20 bytes of the account's public key hash. When displayed in plain text, there are two formats:

- Base58 encoding format, for example: 14xfJr1DArtYR156XBs28FoYk6sQqirT2s
- Hexadecimal (HEX16) format, for example:
0x9156a7cdab767ffe161ed21a0cb0b688b545b01f

UTXO Type, Balance Type, Zk Type

The account supports both UTXO and Balance types. In the UTXO type, the account funds represent the sum of available funds owned by the account (i.e., the amount of all unspent UTXOs).

In the balance system, the internal storage of the account includes three parts:

- The latest transaction sequence number (check number), a counter to ensure each transaction is processed only once (to prevent double-spending).
- The current account balance.
- Account information, including a nickname (domain name), contract code (Code), or storage (Data), by default this is empty.

Zero-knowledge (Zk) system addresses are one-time addresses, the sender and receiver create a random obfuscated address for each transaction. The account includes a private view key, a private payment key, and a public address.

Sharding

The system sharding is based on the account address, and each "full node" within a shard is responsible for storing all transactions, contracts, and states of its respective shard.

1. First level: The system is divided into 256 shards according to the first byte, where the 0th shard is the beacon chain.
2. Second level: The system is divided into 65,536 shards based on the first two bytes.
3. Third level: The system is divided into 16,777,216 shards according to the first three bytes.

Thanks to validators using stateless proofs and ZKVMS for verification, they can complete verification tasks across all shards. Thus, when Amaze carries out sharding, it does not reduce the overall security of the system.

Transactions

Format

Transaction type || Byte array

The above fields are defined as follows:

- Transaction type: A value from 0 to 0x7f (to be compatible with RLP encoding, the first byte of a transaction is always greater than or equal to 0xc0), which can represent up to 128 transaction types (including UTXO transactions, balance transactions, token transactions, time-limited transactions, batch transactions and proxy transactions, contracts, data on-chain, etc.).
- Byte array: An arbitrary byte array defined by the transaction type.

In the UTXO transaction type, initiating a transaction requires signing a transaction in P2PKH, P2PK, MS (up to 15 keys), P2SH formats, etc., with a private key. The OP_Return format is used for data on-chain and does not involve a payee.

UTXO transactions contain one or more inputs and one or more outputs. Each input includes a reference to an existing UTXO and a cryptographic signature created by the private key corresponding to the owner's address. Each output contains a new UTXO joining the state.

In the balance transaction type, initiating a transaction requires signing a transaction data packet with a private key, which can contain multiple transactions. Each transaction includes the payee's address, transfer amount, optional transaction fee, transaction sequence number (check number), etc.

In Ethereum, the sender's address is derived through signature calculation, which requires verification signature calculation of the ECDSA elliptical encryption algorithm, and this process takes a long time when the transaction volume is large. Moreover, since the sender's address is unknown, it's impossible to accurately judge and process double-spending, nor determine whether the payee of one transaction is the sender of another transaction, resulting in all transactions having to be executed in sequence. The Amaze transaction structure includes the sender's address, which is convenient for broadcasting in related shards, supports "out-of-order" concurrent execution,

avoids related transaction conflicts, achieves lock-free concurrent execution, thereby improving transaction efficiency.

Script/Contract Execution

UTXOs can be owned not only by a single public key but also by complex scripts written in stack-based programming languages. In this mode, to spend such a UTXO, the data satisfying the script requirements must be provided. In fact, the basic mechanism of public key ownership is also implemented through scripts: the script takes elliptic curve signatures as input, verifies the transaction, and the address owning the UTXO. If the verification is successful, it returns 1; otherwise, it returns 0.

Complex scripts can be applied to different scenarios. For example, a script can be created that requires at least two out of three private keys to confirm a transaction (multisig), which is useful for company accounts, savings accounts, and certain business agents. Scripts can also be used to reward users who solve computational problems. It is even possible to create a script that says, "If you can prove that you have sent a certain amount of dogecoins to me, this UTXO is yours." Essentially, the UTXO system allows decentralised exchange of different cryptocurrencies.

In transaction types, the contract virtual machine types can be specified as EVM, WASM and MOVE. Additionally, to be compatible with Ethereum, the following methods can be adopted: if the recipient's address is empty, it is for creating a contract; if the recipient's address is a contract address, it is for invoking a contract, and the Data field represents the parameters.

WASM is a lightweight, efficient, and hardware-agnostic virtual machine specification developed by a community team within the World Wide Web Consortium (W3C) composed of mainstream browser vendors. Amaze utilises the compact and fast-loading binary format of the WASM virtual machine for debugging, testing, experimentation, optimization, learning, teaching, or writing smart contract programs, leveraging hardware performance to achieve native execution efficiency.

Since contracts are Turing complete, they can be applied to almost any scenario.

Transaction Pool

After signing the transaction, it is broadcasted to the nodes of the relevant shard. When a node receives a broadcasted transaction, it verifies the signature and, upon successful verification, adds the transaction to the transaction pool and continues broadcasting within the shard (sending it to nodes that haven't received this

transaction yet). For transactions of the multisig type, they are added to the transaction pool after the signature merging.

Consensus Block Production

Nodes within the shard elect a block producer through fast convergence FVRF consensus, who processes and executes transactions in the transaction pool to generate a verifiable proof. Validators vote and add VDF signatures after verifying the correctness of the proof. Within the scheduled time frame for validating the shard, at least 2/3 of the signatures from 128 validators are required to add the block to the cross-linked beacon chain.

Ethereum assigns block producers and validators to different shards using the beacon chain, where the subset of nodes is dynamic and processes shards in order of blocks. On the other hand, Amaze uses cryptographic proofs for processing, different from other chains' shard designs, where block producers and validators are set on a global scale, solving the security issues of shards. Although generating proofs requires additional computational work, the verification speed is fast, and the computational power requirement is low (achievable on smartphones). The Amaze beacon chain is mainly used to generate check blocks containing verifiable cross-link information provided by the shard's internal state and transaction contents.

Transaction Execution

Transaction Execution

In the UTXO system, the steps for executing a transaction include:

1. For each input of the transaction:
 - If the referenced UTXO is not in the current state (S), return an error message.
 - If the signature does not match the owner's signature of the UTXO, return an error message.
2. If the total value of all input UTXOs is less than the total value of all output UTXOs, return an error message.
3. Return the new state S', where all input UTXOs are removed from the new state S and all output UTXOs are added.

In the balance system, the steps for executing a regular transaction are as follows:

1. Check if the balance is sufficient for payment.

2. Deduct the payment amount from the sender's balance and increase the receiver's balance.
3. Return the new state, which includes the updated balances of both parties.

Code Execution

Contract code is written in a low-level bytecode language based on stack-based programming, known as "virtual machine code." The code consists of three types: EVM, WASM, and MOVE. These codes are composed of a series of bytes, where each byte represents an operation.

Generally, code execution is an infinite loop process where the program counter (initialised to zero) continuously performs operations, incrementing the program counter with each operation until the code execution is complete, fuel is exhausted, an error is detected, or a STOP or RETURN instruction is encountered. The zero-knowledge proof system generates proofs for code execution.

Node Synchronisation

Each participant is a full node: Traditional chains have become so large that users have to rely on mining farms to run nodes, which goes against the original decentralised idea of blockchain and makes the network more vulnerable to 51% attacks. However, AmzaeChain's mobile node blockchain allows anyone to easily connect and verify transactions in a peer-to-peer manner like a full node, ensuring a high level of censorship resistance and security of the blockchain.

Zero-knowledge-driven elegant solution: AmzaeChain does not adopt the brute force computational method of Proof of Work (PoW), but achieves true large-scale decentralisation through advanced cryptographic techniques and recursive zero-knowledge proofs.

Initial Synchronisation

The theoretical design goal of blockchain is to empower users. When the majority of people can execute rules through the verification of an immutable public ledger, power is held by the majority rather than a minority. This decentralised structure allows transactions to take place in a trustless environment.

However, in practice, this is not always the case. For traditional blockchains like Bitcoin and Ethereum, new participants must verify the correctness of every transaction since

the inception of the network, which amounts to hundreds of terabytes of data. Most individuals cannot afford the computational power required to independently validate such massive chains, resulting in the reliance on increasingly powerful mining entities.

This means that most people cannot join the peer-to-peer network anymore, leading to a compromised decentralisation where the distribution of power is affected, and the network becomes more susceptible to censorship.

We offer an elegant solution: To significantly reduce the amount of data that each user needs to download through easily verifiable and consistently sized cryptographic proofs. Participants do not need to start from scratch and independently validate the entire chain block by block like other chains. Instead, they utilise recursive zero-knowledge proofs to fully verify all blocks, networks, and transactions from the beginning of the sub-chain. Then, mobile nodes can store compact proofs instead of the entire chain, processing transactions and contracts from the current moment onwards. Due to the constant proof size, it remains accurate and available even as many users accumulate years of transaction data.

Stateless Blockchain

Supporting a single transaction (or a group of transactions, a series of consecutive transactions, a single block, a group of blocks, a series of consecutive blocks) inputs (such as block headers, transaction sets within blocks, account information, contract storage information, etc.) with polynomial proofs or zero-knowledge proofs. After ZkEVM execution, outputs are generated, verified (without the need for a full ledger and full state), and signed (multi-signature).

Distributed Concurrent Execution and Verification

This execution and verification can be performed through single-machine multithreading concurrency, GPU concurrency, cross-machine concurrency, and distributed computing—without requiring permission or access thresholds, and can even be performed at any time across different time and space for verification.

State Sharding

Blockchain participants only need to possess the genesis block (or re-genesis block or anchor) along with block headers containing timestamps and difficulty verification. The hardware networking requirements are low, and continuous outputs can be merged into subsets of states, achieving the effect of state sharding.

Proposers/Validators

Proposers choose the most competitive valid block header. Only block builders need to process the entire block (which can also be achieved through the use of decentralised oracle protocols for distributed block building), while all other validators and users can efficiently verify the block through data availability sampling.

9. Algorithms

1. Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (Zk-SNARK)

For transactions and smart contracts, zero-knowledge proof technology allows verifying the correctness of a computation's outcome without executing or knowing the specific content of the computation. This is achieved by performing specified verification calculations on the data and comparing the expected results to determine if the "computation" has been correctly executed. zk-SNARKs can provide proofs for computations that generate specific outputs, and the verification of these proofs is much faster than directly executing the corresponding computations.

It enhances scalability by allowing one person to verify and generate a proof for a block, which can then be efficiently verified by others in the network without each person having to spend a significant amount of time on direct execution. In terms of privacy, users can prove ownership of certain unspent assets in a transaction without revealing the complete source and destination of the assets.

This addresses the issue of information leakage caused by transaction transparency in blockchain platforms like Bitcoin, such as revealing the identities of transacting parties and transaction amounts.

2. RSA Accumulator

Unlike Bitcoin's Merkle Tree, Ethereum's Trie, and Merkle Patricia Tree, AmazeChain uses RSA accumulators to store, update, query, prove, and verify the ever-changing blockchain state.

3. KZG Polynomial Commitment

KZG Polynomial Commitment allows proving any number of elements in a vector using only one group element. This approach can be used for verifying nodes, light clients, and stateless blockchains, reducing network transmission and enabling fast verification.

4. Inner Product Argument (IPA)

IPA utilises bilinear groups to prove the correctness of the "inner product" of Pedersen commitments without the need for a trusted setup. By computing the sum of products of each component in two vectors, where one vector is set to a certain power, its inner product becomes the evaluation of a polynomial at a specific point. The basic strategy is to use a "divide-and-conquer" approach, decomposing a problem into multiple similar subproblems rather than attempting to solve it all at once.

When the subproblems are sufficiently decomposed, they can be easily solved. The prover submits some information, and then the verifier initiates a challenge that leads to the next commitment. Although referred to as a game, it does not imply that the proof must be interactive. The Fiat-Shamir algorithm allows us to transform an interactive proof into a non-interactive one by replacing the challenge with a collision-resistant hash value of the commitment. Inner product proofs are used to verify polynomial evaluations.

Soundness means that when the prover follows the corresponding operations, they can convince the verifier that the conclusion is correct. Completeness means that a cheating prover cannot pass the verifier's validation with an incorrect proof, or the success rate is very low.

(Note: Some terms in the IPA explanation may require further context to fully understand their meaning and implications.)

Blockchain Distribution Network (BDN)

To ensure data synchronisation, rapid network-wide consensus, and continuous operation of the system in the event of large-scale network disconnections (splitting into multiple parts) without compromising the decentralised nature of the network, we achieve this goal through a neutral Blockchain Distribution Network (BDN).

RoaringBitmap (Efficient Compressed Bitmap)

Bitmap indexing is widely used in databases and search engines to significantly improve query speed through bit-level parallelism. However, bitmap indexes consume a large amount of memory, leading to the adoption of compressed bitmap indexes.

RoaringBitmap is an excellent compressed bitmap index that outperforms common schemes such as Run-Length Encoding (RLE) with Word-Aligned Hybrid (WAH) and

Concise (compressed, combinable integer sets) in terms of compression efficiency and query performance.

RoaringBitmap serves a similar purpose to a Bitmap (e.g., indexing) but offers superior performance and space utilisation. It has been applied in many mature open-source big data platforms. The main ideas behind RoaringBitmap include:

1. Divide the 32-bit range ($[0, n)$) into 2^{16} buckets, with each bucket having a Container to store the low 16 bits of values.
2. When storing and querying values, split the value k into the high 16 bits ($k \div 2^{16}$) and low 16 bits ($k \bmod 2^{16}$), locate the corresponding bucket based on the high 16 bits, and then store the low 16 bits in the respective Container.
3. Two types of containers: Array Container and Bitmap Container. Array Container stores sparse data, while Bitmap Container stores dense data. If the number of integers in a Container is less than 4096, a sorted array of Short type is used to store the values. If it exceeds 4096, a Bitmap is used for storage.

Big Data ETL (Extract, Transform, Load)

ETL is the process of extracting, transforming, and loading data from source systems to target systems. ETL is commonly used in areas such as data warehousing, decision support, real-time analysis, data mining, and data intelligence. Its main purpose is to integrate diverse, partially structured, and non-uniform standard data into a unified data warehouse, providing a quality-assured data source for analysis and decision-making. Amaze utilises ETL for efficient analysis and processing of blockchain's historical ledger data, arbitrary spatiotemporal states, account transaction records, and contract storage.

Verifiable Delay Functions (VDF)

A Verifiable Delay Function (VDF) takes an input value and, after a certain amount of time, produces a result that can be easily verified. VDFs employ sequential computation algorithms, and their execution time can be predicted, making it impossible to accelerate them through parallel computation. The proof process can be quickly verified. VDFs not only reduce the immense energy consumption associated with Proof-of-Work (PoW) but also address the issue of hackers conducting 51% attacks, where they gain majority control over signatures and long-term computational difficulty.

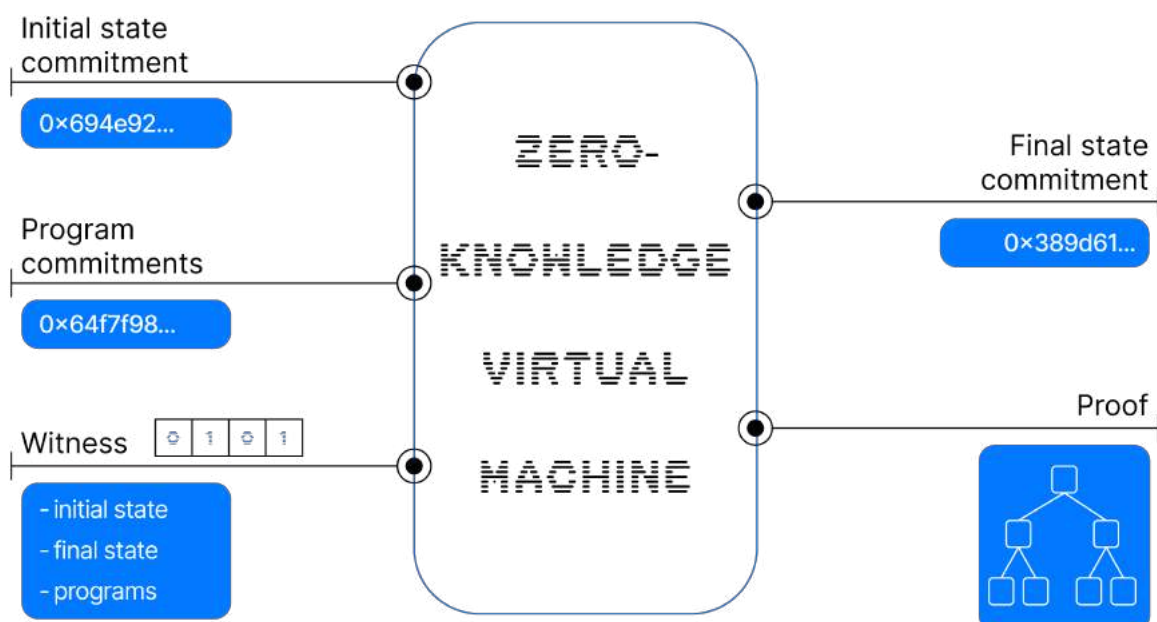
Zero-Knowledge Virtual Machine (zkEVM):

zkEVM is a virtual machine designed to support zero-knowledge technology for verifying program correctness by generating zero-knowledge proofs. Unlike traditional virtual machines, zkEVM proves the correctness of program execution, including the validity of inputs and outputs used during the operation.

As a result, thousands of transactions and contract executions do not need to be redundantly executed by each node. Instead, a small amount of verification computation ensures the correctness of transaction and contract execution.

zkEVM can be divided into three parts: the execution environment, proof circuits, and verification program.

1. Execution environment: This is where programs (smart contracts) run in zkEVM, functioning similarly to the Ethereum Virtual Machine (EVM). The execution environment takes the initial state and current transaction to generate a new (final) state.
2. Proof circuits: These generate zero-knowledge proofs to verify the validity of computational transactions in the execution environment. Proof circuits take input from the previous state, transaction inputs, and resulting state information to complete the proof generation process. The prover then obtains a concise proof of the validity of that specific state transition.
3. Verification program: This program verifies the validity proof, including the input and output states. The verification program performs computations on the provided proof to confirm that the submitted output state is correctly calculated based on the input state.



10. Implementation

We have successfully implemented solutions to address each of the goals outlined in the previous section.

Transaction Performance

Improving transaction performance relies on architecture design, consensus algorithms, and optimising 'computation, communication, and storage.'

In the overall architecture design, two key strategies ensure improved transaction performance: "sharding" and "layering." Sharding enables parallel processing of transactions, while layering combines a group of transactions into a single transaction for processing. Each key strategy improves performance by orders of magnitude, resulting in a million-fold overall performance improvement (effectively multiplication).

During the transaction process, the consensus adopts the FVRF algorithm. Regardless of the number of nodes, the required participation, communication, and computation for consensus remain relatively constant rather than linearly increasing. Therefore, scaling the system does not significantly decrease consensus speed.

Another method to reduce computational overhead is to allow only one node, the "block producer," to perform calculations, execute transactions, and generate proofs, while other nodes handle verification. The computational requirements for the verification process can be completed within milliseconds using a simple smartphone, reducing resource consumption compared to the high-energy-consuming Proof-of-Work (PoW) miners required by Bitcoin and Ethereum.

Additionally, significant overall performance improvements can be achieved by using RSA accumulators for state processing, employing Kate polynomial commitments for global miners, and validating lightweight nodes for stateless blockchain.

Communication Capability

Communication encompasses three main aspects: node discovery, data transmission, and RPC services. Amaze's P2P network is implemented based on a three-layer architecture: network layer, routing layer, and switching layer. It incorporates NAT traversal, relay proxy protocols, multiplexing streams, and BDN technology, all built on top of Libp2p.

In addition to transaction broadcasting and block synchronisation, Amaze's powerful P2P communication network can support billions of users simultaneously sending messages, images, videos, files, and engaging in multi-party conferences.

Storage Capability

Unlike IPFS, we have built a completely new distributed storage system. Each node can provide storage space, bandwidth, and online time services to other nodes. This system can be used to store the distributed ledger for the blockchain and securely backup photos, files, and short videos generated by smartphones, laptops, and computers. By establishing a mutual assistance service among nodes, a healthy and sustainable storage market is created.

Privacy Protection and Data Sovereignty

AmazeChain utilises a privacy protection system based on zero-knowledge proofs, which can completely conceal the information of transaction parties and transaction amounts during transfers. If users choose to prioritise privacy over real-time transfers, the Amaze system can also hide transaction times and quantities (i.e., the number of transactions within a specific time period), making it difficult to trace and analyse specific transfers on the network.

The privacy protection level can be chosen to "support regulation" to enable regulatory oversight and auditing by national regulatory authorities. The underlying protocol of our ecosystem supports a data sovereignty, transaction, and circulation system where data producers own their data. They can securely transact with different levels of permissions based on this data to maximise the value of data assets.

This includes providing past transaction information to counterparties as proof of transaction credit and capability, granting specific access and usage permissions to specific merchants based on consumer preferences, granting certain data access permissions to advertisers to share ad revenue, and granting corresponding research permissions to governments and non-governmental organisations.

Universally Applicable, Open, and User-Friendly

The Amaze platform overcomes the limitations of the first and second-generation blockchain technologies that require substantial power and hardware resources,

allowing users to participate in various transaction activities with just an ordinary smartphone.

The Amaze platform adopts low-energy and fully decentralised Proof-of-Stake (POS) consensus technology, which eliminates the need for complex and expensive data centre environments or significant investment in mining equipment. This ensures platform scalability, rapid deployment, and convenient operations.

The unique recoverable key feature of the Amaze platform supports the recovery of lost or partial private keys, and safeguards the security of account recovery from private keys by preventing denial-of-service (DOS) attacks, enhancing the platform's security capabilities.

Our platform also supports offline payment transactions, allowing verification of transactions even when both parties are offline. Smart contracts on AmazeChain support multiple commonly used programming languages, including Java, C++, and Rust, making smart contract design, programming, testing, and deployment more accessible.

As an open platform, Amaze supports compatibility with various traditional blockchain protocols, including Bitcoin's UTXO, EOS's WASM, Ethereum's EVM, and Diem's MOVE.

Industry-Leading Security

Blockchain, as a decentralised or multi-centric trust mechanism, has had a significant impact on people's trust systems compared to traditional centralised trust mechanisms.

This has led to increased attention and research on security technologies in blockchain. Our team have conducted in-depth research on the key technologies and security architecture of blockchain, utilising P2P network technology, distributed ledger technology, asymmetric encryption and decryption technology, consensus mechanism technology, and smart contract technology to achieve comprehensive protection of data integrity, non-repudiation, privacy, and consistency.

Additionally, we have analysed new security threats and countermeasures, including techniques to prevent denial-of-service attacks caused by transaction storms, ciphertext access control technology to protect the privacy of blockchain information, and key management technology to prevent loss or leakage of keys resulting in digital asset loss.

Furthermore, we have explored potential new security issues and solutions that may arise from the integration of blockchain technology with artificial intelligence, big data, the Internet of Things, cloud computing, and mobile internet technologies.

One important issue affecting the development of blockchain is its security. From the perspective of network cryptography analysis, blockchain developers need to address security issues in algorithms, protocols, implementations, usage, and systems.

As blockchain technology is increasingly applied in core areas such as finance and cybersecurity, which have high security requirements, solving its security issues is a prerequisite for widespread adoption. We take a defensive approach and have designed the VRF dynamic consensus mechanism and BLS heterogeneous redundant signature mechanism to construct a comprehensive blockchain security architecture.

Our team has defined and analysed the security of blockchain in detail, proposed appropriate parameter selection schemes, and tested the efficiency of signature mechanisms. In the future, we will consider effective solutions and deployment strategies for the challenges faced by the BLS heterogeneous redundant signature mechanism, such as the large size of post-quantum cryptographic algorithm public keys and slow algorithm speeds.

Economic Efficiency

Compared to traditional decentralised networks, Amaze has significant cost advantages. Users only need a smartphone to become a node in the Amaze network, eliminating the need for reliance on server clusters in data centres, which significantly reduces the participation cost of blockchain transactions. Our consensus mechanism is based on Proof of Stake (POS) rather than Proof of Work (POW), avoiding substantial energy consumption, and a large number of nodes ensure network security and decentralisation.

The low staking token voting method significantly reduces the opportunity cost of voting, increases token liquidity, and reduces asset occupation. Through sophisticated software design, we enable the sharing of network storage, computing, and bandwidth, greatly reducing network infrastructure investment and hardware operating costs.

Compared to centralised networks, our network also demonstrates significant cost advantages. The extensive use of program-based automation for transactions, clearing, and accounting operations greatly reduces the operational cost of transactions.

Compared to traditional centralised networks, the marginal cost of commercial operations is almost zero, resulting in stronger economies of scale and network effects. Large-scale public chains require validation by all participating nodes, and our transaction consensus mechanism based on zero-knowledge proofs enables low verification costs while increasing the difficulty of fraudulent transactions. After multiple transactions, previous transaction behaviour constructs a naturally transparent credit database, which can reduce the due diligence cost of transactions and enhance transaction quality.

11. Ecosystem Growth

Profit Growth: Value Enhancement of Our Ecosystem

In the AmazeChain network, individual users contribute their idle storage, computing power, and bandwidth of their nodes (such as smartphones, personal computers, or servers) to the network while using various applications. Based on this contribution, users receive corresponding rewards—including 'mining'. This mutual assistance approach combines consumption with production, thereby improving overall efficiency.

The platform possesses the capability of fast verification and synchronisation of the entire ledger, allowing transactions and program-based automated clearing and accounting to be conducted in real-time. The platform even supports automatic batch and periodic transactions, such as automatic monthly tuition payments for children studying at university. Program-based automated transactions, clearing, and accounting reduce labour costs, eliminate the need for token staking during voting, and improve asset turnover by shortening the entire transaction process.

The accumulation of a large amount of transparent and tamper-proof historical data increases user loyalty and stickiness, contributing to long-term value accumulation with customers.

Sustainable Development: Our Persistent Growth Strategy

Unlike economic systems designed to rely on continuous external funding or investments (such as Ponzi schemes) or limited fee revenues generated solely from on-chain payments, investments, or gaming transactions, we achieve sustainable development by creating value, generating content, processing information, and providing various services (such as attestation, traceability, electronic licences, financial services, real estate registration, corporate credit, contracts, and medical data, etc.). As a network service provider with strong revenue potential, we aim to complement or even partially replace certain centralised network services.

Our network is capable of providing most of the services offered by centralised networks, which were not commercially viable on a large scale due to technological limitations in the first and second-generation blockchain technologies. We provide these user-friendly and convenient network services at a lower cost, with stronger privacy protection and higher reliability. These services meet real-world needs and have significant market share, such as the demand for higher-level privacy protection

in social media and the interconnection and transaction needs of a large number of nodes in the Internet of Things.

The design principle of AMC is that in order to sustain the long-term development of its economic system, the economic system must continuously improve technology and optimise resources to provide economic returns higher than the inflation rate.

Scalability: Our Self-evolutionary Capability

In the current technological environment, we have become accustomed to regular or even automatic updates of applications, games, and browsers. Developers fix bugs before problems arise and add new features as better solutions emerge. Like any other software, blockchain also needs periodic upgrades to adapt to technological advancements. However, compared to upgrading centralised applications, games, or browsers, the upgrading process of blockchain is more complex. Traditional blockchain upgrades require network forks, which usually take months to complete, and contentious hard forks may lead to community divisions.

We break this inherent pattern, allowing the blockchain to self-upgrade without the need for chain forks. This forkless upgrade is achieved through our transparent on-chain governance and system contracts. With this feature, Amaze ensures that the project can remain agile, adaptive, and continuously evolve with demand and technological advancements. Furthermore, it greatly reduces the associated risks brought by contentious hard forks, which are significant events for many organisations and systems.

12. Applications

Amaze achieves public transparency, immutability, non-repudiation, and traceability of all data and information without the need for third-party endorsement. As a foundational protocol or technical solution, we effectively address the problem of efficient transactions between parties lacking mutual trust and enable the free transfer of value. The platform features Turing-complete smart contracts, operates 24/7, is decentralised, supports enterprise-level security, and ensures continuous and accurate operation even in the event of individual or partial node failures.

Compared to other blockchain technologies such as Bitcoin and Ethereum, Amaze brings significant improvements, including:

- Near-instant transaction confirmation
- Low energy consumption, low cost, and high usability
- Processing capacity of hundreds of thousands of transactions per second
- Support for billions of account nodes (meeting the connectivity needs of everyone worldwide and future IoT device connectivity needs)
- Support for enterprise-grade security for financial applications

The main application advantages of our platform lie in its high compatibility, scalability, and support for large-scale decentralised applications. While some traditional blockchain platforms have Turing completeness, complex applications often need to be split into multiple smart contracts due to code size and memory limitations, resulting in slow execution speeds and high costs. Amaze successfully addresses these issues.

Payment System

Traditional Bitcoin payments take about an hour to confirm, which is not suitable for scenarios requiring instant transactions, such as buying coffee in a Starbucks queue. The transaction fees for Ethereum and Bitcoin are often over \$10, making them unsuitable for small-value payments. If 10,000 payment transactions occur simultaneously on the Bitcoin network, it becomes congested, and miners have to pause all other activities, resulting in a processing speed of only 3 transactions per second and a network congestion time of nearly an hour.

We have made significant improvements in this regard, with transaction performance reaching hundreds of thousands of transactions per second, surpassing the combined total of all online payment giants in the current market. Moreover, the fees are extremely low, and the transaction confirmation time is within seconds, making it

highly suitable for supporting high-volume transaction flows during peak shopping periods such as Black Friday, Labor Day, Thanksgiving, and Lucky Bag festivals.

Banking Solutions

The financial applications offered by Amaze not only support account opening, staking, loans, and remittances for blockchain banks but also meet the transaction, payment, and transfer needs of billions of accounts. Amaze ensures near-instant transaction confirmation, operates 24/7 with uninterrupted online service, has no single point of failure, and supports transaction security at a financial-grade level.

Insurance Services

The Amaze platform can provide a range of trusted and secure blockchain insurance applications, including smart contract signing, underwriting, third-party claims, and loss assessment services. Users from around the world can participate and collectively provide protection for customers who have experienced accidents and misfortunes. Amaze's oracle makes actuarial calculations more reasonable, and this innovative insurance model can continuously enhance its payout capacity through methods such as appreciation of digital assets.

Innovation in Search Engines

Amaze utilises blockchain technologies and solutions such as digital signatures and data on-chain to significantly improve the credibility and authenticity of search content. By providing more accurate, authentic, and trustworthy search results, Amaze sets new standards for the search industry, innovates search engines, and opens up new paths for blockchain business models.

E-commerce

E-commerce is disrupting traditional consumer and retail industries, and Amaze's blockchain technology takes the "producers selling goods to consumers through e-commerce platforms" model a step further by enabling "direct sales of goods from producers to consumers." Our blockchain platform achieves traceability and tracking of product origin and logistics by putting transaction data on the chain, greatly reducing the circulation of counterfeit goods.

We enable near-instant point-to-point payments, supporting e-commerce transactions and payments in the virtual world anytime and anywhere. The Amaze e-commerce platform also functions as a dynamic "credit" database, where the inherent "trust" of blockchain technology ensures the quality of on-chain data. Every type of product, merchant behaviour, consumer behaviour, funds, logistics, and even reviews are permanently recorded and publicly transparent.

The trading scope of the AmazeChain e-commerce platform has greatly expanded. It can trade not only traditional goods but also a wide range of original knowledge products, virtual products, and services, such as teaching courses, cultural and intellectual dissemination, foreign languages, guitar lessons, yoga, art including digital art, legal consultations, gaming coaching, and more. Amaze effectively establishes rights for these products and services, enabling their circulation and transactions.

Applications in the Gaming Field

Our platform combines blockchain, gaming, and network computing power to provide game participants with a reliable economic system, virtual identities and assets, powerful social connections, and an open content creation platform. The self-organising form of blockchain community governance better supports the user-generated content (UGC) model in gaming.

We support rich and flexible DeFi applications, ensuring a sustainable, transparent, and fair economic system. In traditional centralised games, there is often a lack of transparent and fair economic systems, and players' investments are not always proportional to their returns. However, on AmazeChain, all virtual identities and assets in games can be traded fairly on the platform. Equipment, decorations, and land ownership in games can all become virtual assets that can be traded fairly.

Metaverse

The Metaverse is a virtual world constructed and innovated through technologies such as public chain distributed databases, trust mechanisms, and identity recognition. This world is mapped and interacts with the real world, forming a digital living space with a new social system.

The Metaverse essentially represents the virtualization and digitization process of the real world, deeply transforming content production, economic systems, user experiences, and physical world content. With the support of shared infrastructure, standards, and protocols, and through the integration and evolution of various tools and platforms, a complete Metaverse gradually takes shape.

It utilises augmented reality technology to provide immersive experiences, generates mirrors of the real world through digital twin technology, constructs an economic system with blockchain technology, and tightly integrates the virtual world and the real world in terms of economic systems, social systems, and identity systems, allowing every user to participate in content production and world editing.

Amazechain, with its powerful processing capacity and storage, enables billions of users to smoothly access virtual identities, assets, and engage in creation, communication, and experiences in the Metaverse, thereby propelling human civilization to a new stage.

Short Video Field

Amaze provides a massive shared storage space across the entire network for short videos, supporting content display, comments, rankings, and community trading gatherings. Users can watch videos based on their preferences and also utilise AI technology for personalised video recommendations. Additionally, anyone can issue NFTs to showcase their artistic talents.

Storage Services

Amaze provides on-chain storage space with arbitrary durations, multiple redundant backups, and massive sharing. This includes backing up contacts, messages, photos, software, and videos on mobile phones; backing up files, work, and data on computers or laptops; backing up personal social relationships, growth experiences, travel experiences, medical health data, and even genetic data.

12. Governance

Amaze is not controlled by any individual or organisation, and its business model and community are full of innovation. The decision-making process of the whole Amaze ecosystem is based on the design of future decision-making processes and procedures.

Advanced business models and community members lead the transformation of production relations and business models. Amaze community members often play multiple roles: protocol core development team, collaborative development team, application/tool developers, miners, operational nodes, application and data users, and data producers.

- Token holders: Individuals or organisations holding any amount of native currency.
- Protocol core development team (core dev team): The team responsible for developing and maintaining the platform and protocols, such as the Blockchain Development Network (BDN).
- Collaborative development team: Participates in and is responsible for the development of improvement proposals through technical proposals to support new features, upgrades, or processes.
- Application/tool development team: Developers responsible for designing, deploying, and operating applications (such as wallets, games, DeFi, NFT, etc.) based on our chain or tools that interact with it (such as wallets, testing tools, standardised deployment toolkits, etc.).
- Miners: Nodes in the network responsible for broadcasting, validating, or mining blocks.
- Operational nodes: Operational nodes that increase the operation of block transactions and storage by sharing network bandwidth, computing power, and resources.
- Application and data users: People who access and use blockchain applications and data.
- Data producers: Individuals who generate data and information on the blockchain.

Our global, diverse community is a bottom-up-driven self-organised network where no single person or node controls community operations. The stronger the self-organising capability, the stronger the system's ability to maintain and generate new features. For example, leading companies in the retail industry such as Amazon, Apple iTunes, and Netflix are similar in some ways to self-organising trading platforms. They provide continuous development suggestions based on the purchasing behaviour of customer communities. Creating self-organising trading systems helps attract buyers away from competitors whose customers are often isolated and lack information. The advantage of bottom-up organisations is that they motivate everyone by giving them a voice.

As an open platform, AMC is designed to achieve unrestricted access for people at all times and in all locations. There is no need for any specific permission to publish applications, participate in transactions, join the Amaze community, or network.

The network presents a flat hierarchical structure consisting of numerous nodes that can directly communicate and transact with each other. This peer-to-peer communication and transaction model greatly enhances transaction efficiency while reducing transaction costs.

Community-driven governance: Amaze does not belong to any individual or organisation. Unlike the traditional pattern of critical matters and changes being decided by a board of directors or shareholders in large corporations, Amaze's governance is community-driven.

The community collectively takes responsibility for discussing, proposing, and deciding on future strategies, directions, and changes to support the continuous development, upgrades, and evolution of the Amaze community and network.

Decentralised, bottom-up governance based on protocol rules: Amaze's governance process determines a series of changes regarding Amaze protocols, operations, business, and community. The governance process here does not involve who can use the Amaze platform because it is open and permissionless. Amaze's long-term planning goal is to build a platform with unrestricted access. At the same time, Amaze's governance does not involve who can or cannot publish applications or engage in transactions.

The Operation Council

The representative institutions within the Amaze community include two main committees: the Amaze Operation Council and the Amaze Technology Council.

The Amaze Operation Council is responsible for handling changes unrelated to blockchain technology. These changes are discussed and voted upon by the community, and it is up to the community to decide whether to veto or implement them. The main responsibilities of this council include, but are not limited to, governance mechanisms for non-technical issues, operational strategies, network data, and security compliance.

The Amaze Operation Council is managed fairly and transparently by individuals who hold Amaze tokens. Any suggestions related to non-technical developments in Amaze can be submitted to the Operation Council by community members through proposal

submissions (only requiring the wallet address holding Amaze tokens). Council members must hold a certain balance of Amaze tokens and are responsible for the initial review of any non-technical proposals.

Submitted proposals undergo initial review, rejection, requests for additional materials, or board review. They are then ranked based on proposal balances. Some major proposals will be submitted for community-wide voting and discussion.

During the first Operation Council meeting, it is determined which types of proposals require community-wide voting and discussion. This is typically based on an evaluation of the proposals' impact on nodes, user satisfaction, and funding.

On the other hand, the Amaze Technology Council is responsible for determining the technological evolution path of Amaze. Changes decided by the Technology Council, once consensus is reached, are often encoded into the code and automatically executed.

The Technology Council

The Amaze Technology Council leads and is responsible for the technical decision-making of the entire community. The decision-making process involves several stages:

Proposal publication: Firstly, proposals (Amaze Improvement Proposals, AIPs) should be detailed enough to be deployed immediately upon acceptance by the Technology Council. Before proposal publication, the proposer should gather feedback on the proposal and manage related deployment, operational, and security risks.

Proposal submission and presentation: The proposal is then submitted to the Technology Core Council, which consists of the core development team, collaborative development team, and application/tool development team. The proposal will be publicly discussed on the community's technical forum. Possible outcomes include: the proposer being asked for more information or modifications to the technical solution, the proposal being rejected due to insufficient importance or inability to bring sufficient improvement compared to development efforts, or the proposal being evaluated as a network upgrade to be deployed in the future.

Generating the final proposal: In the final proposal stage, which involves several rounds of modification and discussion based on the discussion to achieve the formation of the final proposal that is more secure and better meets the requirements.

Inclusion of AIP in network upgrades: Once the final proposal is approved by the Technology Council, tested, and executed, it will be included in the network upgrade plan.

Network upgrade: Lastly, the proposal will be deployed and officially run on the Amaze mainnet.

Through these steps, the Amaze Technology Council continuously guides and promotes the technological progress and improvements of Amaze.

13. Foundation

The establishment of the Amaze Foundation is aimed at realising our grand vision: to enable anyone, anywhere, at any time to access a low-cost, peer-to-peer decentralised and trustable network.

The main responsibilities of the foundation are to incubate and manage technology and applications in the field of decentralised network software protocols, especially those that leverage modern cryptographic methods to protect decentralisation and are committed to maintaining the stability of the Amaze ecosystem.













To achieve this goal, the foundation will dedicate itself to funding or assisting in the development and deployment of projects aligned with its mission, including but not limited to:

1. Innovative blockchain technologies and encrypted messaging protocols to enhance the security and efficiency of the network.
2. Development and optimization of peer-to-peer network infrastructure, such as libp2p and devp2p, to improve network stability and scalability.
3. Design and implementation of cryptographic economic mechanisms and value transfer networks, such as Distributed Autonomous Organization (DAO) software and non-fungible tokens (NFTs) for personal data, to promote the development and diversity of economic activities.
4. Innovation and application of data storage and publishing systems, such as IPFS, to ensure data security and availability.

Through these efforts, the Amaze Foundation aims to drive the development of decentralised technology and provide support to a broader community and ecosystem.

14. About Us

We're mainly tech people, like marketers and developers, who get Web3. With over 75+ people worldwide and 400+ coding contributors from places like Dell, Amazon and Binance, we know how to build apps and software that people love using—like WeChat. The chief architect of our chain, Jay, is a world-renowned cybersecurity expert and early Bitcoin and Ethereum contributor who wishes to remain anonymous to the public.

 JW App Development Lead	 Matt Marketing Director	 Jay CSO
 Ed COO	 Jeffrey CEO	 Faye Quality Assurance Lead
 Belen Lead Visual Designer	 Jan Front-end Developer	 Jack Chain Development Lead
 Jim Back-end Developer	 Andrew Community Manager	 Tom CPO

References and Advanced Reading:

1. [Intrinsic value](#)
2. [Smart property](#)
3. [Smart contracts](#)
4. [B-money](#)
5. [Reusable proofs of work](#)
6. [Secure property titles with owner authority](#)
7. [Bitcoin whitepaper](#)
8. [Namecoin](#)
9. [Zooko's triangle](#)
10. [Coloured coins whitepaper](#)
11. [Mastercoin whitepaper](#)
12. [Decentralised autonomous corporations, Bitcoin Magazine](#)
13. [Simplified payment verification](#)
14. [Merkle trees](#)
15. [Patricia trees](#)
16. [GHOST](#)
17. [StorJ and Autonomous Agents, Jeff Garzik](#)
18. [Mike Hearn on Smart Property at Turing Festival](#)
19. [Peter Todd on Merkle sum trees](#)

15. Risk and Disclaimers

This white paper is provided for assistance only and is not intended to be and must not be taken alone as the basis for any purchase decision. Buying Crypto/NFTs involves significant risks and may prompt a deficiency of an essential or whole measure of the cash and a prospective buyer should have the financial ability and willingness to accept such risks (including risk of complete loss of a buyer's investments into any Crypto/NFT, for which no recourse would be afforded to the buyer). Prior to making a purchase of a Crypto/NFT, the buyer should carefully consider and evaluate all the information in this white paper as well as other factors that may be recorded in other documentations or through the buyer's own due diligence.

Each buyer should perform and is deemed to have made their own independent investigation and analysis of the Crypto/NFT and all other relevant matters as they deem necessary to arrive at an independent evaluation of a purchase. Among others, the performance of a Crypto/NFT is subject to risk factors that are outside of AmazeWallet's reasonable control. For example, cryptographic tokens may be subject to confiscation or potentially burglary: programmers or other malevolent gatherings or associations might endeavour to impede AmazeWallet's framework/network in different ways, including malware assaults, disavowal of administration assaults, agreement-based assaults, Sybil assaults, smurfing, and parodying which may bring about the deficiency of your cryptographic tokens or the lack of your capacity to access or control your cryptographic tokens. There might be no cure on such occasions, and holders of cryptographic tokens are not guaranteed any remedy, discount, or remuneration. As a result, there can be no assurance or guarantee that a purchase of Crypto/NFT will be realised and that capital loss will not occur. Loss of the entire principal amount invested is also a possibility, which buyers must be willing to accept and undertake before each purchase.

Prospective buyers should therefore have regard to their own investment objective and financial circumstances and should consider and evaluate their own investment objective and financial circumstances fully before deciding whether to purchase a Crypto/NFT. In deciding to purchase or participating in the AmazeWallet ecosystem, you expressly acknowledge, accept and assume the following:

Regulatory status:

Changes in laws or regulations, or the interpretation of such, may have legal, tax, or accounting consequences that may bring about adverse effects to the performance and/or development of a particular Crypto/NFT or the general ecosystem of such cryptographic tokens. As it stands, the administrative status and regulatory attitude towards cryptographic tokens and computerised resources presently differ from jurisdiction to jurisdiction. Governments worldwide are currently (and continue to) exploring the benefits, risks, regulations, security, and applications of crypto assets and as such, it is conceivable that regulatory oversight of the cryptographic tokens and cryptocurrency industry will continue to evolve, and governments may take on more restrictive positions in respect of cryptocurrencies, decentralised finance and/or the cryptographic tokens and cryptocurrency industry, whether in certain aspects or

generally. Such positions include issuing more targeted and specific regulations, guidelines, arrangements, or rules relating to cryptographic tokens, computerized resources, blockchain innovation, or blockchain applications, which may directly or indirectly confine the ability of cryptographic symbolic holders to own, hold, sell, convert, exchange, or utilize cryptographic tokens. The potential increase in regulatory oversight may consequentially result in an increase in the buyer's exposure to legal, compliance, and other related costs. Potential buyers ought to consider the entirety of the abovementioned and survey the nature of significant hazards autonomously and seek their own independent professional and legal advice (where necessary) before proceeding to make any purchases.

Regarding Forward-Looking Statements:

The business and operations of AmazeWallet may be affected by various market and environmental factors relating to the macro economy, technology, regulatory changes, changes in market conditions, and competitive pressure. To this end, this whitepaper contains certain forward-looking statements relating to the business and operations of AmazeWallet which would be dependent on such aforementioned factors. Such forward-looking statements may include assessments and suppositions that are based on AmazeWallet's subjective determination of our relative market positioning, liquidity, financial and competitive strengths and physical conditions (amongst others). In like manner, these factors could cause genuine change to the outcomes or results that may vary tangibly from those communicated in this whitepaper. There can be no assurance that such statements are made on accurate measures of the market and the further prospect of the market. As such, they should not be taken as an indication of, and do not guarantee, the outcome or prospects of any purchase of the cryptographic token or assets that a buyer intends to commit and should be taken as made on the date of this whitepaper

Licenses and approvals are not assured in all jurisdictions.

As highlighted above, the regulatory landscape surrounding cryptographic tokens and assets is currently still evolving and developing across various jurisdictions. To this end, AmazeWallet shall perform due diligence and shall regularly monitor the legal and regulatory developments of each jurisdiction. We endeavour to comply with all applicable laws and regulations of each jurisdiction in which we operate and will make every effort to secure all the required licenses and approvals in such jurisdiction with respect to our business activities.

However, notwithstanding the above, any changes to the regulatory environment of a particular jurisdiction may not be foreseeable by us. In addition, the application process and approval timeline of the requisite licenses vary from jurisdiction to jurisdiction and the position adopted by certain jurisdictions currently with respect to cryptographic tokens and assets may be that such activities are not specifically regulated. As a result, there can be no assurance that the features outlined in this whitepaper and AmazeWallet's risk management process will prevent conduct standards from being compromised.

Given the uncertainties outlined above, the features mentioned in this whitepaper may need to be restructured or rescheduled from time to time, depending on the regulatory developments in the various jurisdictions as well as the approval process by the relevant regulatory authorities. The technological progress and build-up of the community are also other factors that may affect the development of certain features. As a result, the expected launch date and/or roll-out date of such features may differ from that as estimated in this white paper. Further, during the development phase, AmazeWallet may also rely upon our partnerships with different licensed third-party entities. In the event that such entities no longer hold the licenses required (for reasons unforeseen and uncontrolled by AmazeWallet), the ability of AmazeWallet to offer the associated services will similarly be impacted. Such cascading effects may also divert the time and resources of AmazeWallet's operations and activities.

Not financial advice:

This whitepaper does not constitute any investment advice, financial advice, trading advice, or a recommendation on the merits of purchasing, trading, selling, creating and/or buying of cryptographic tokens or assets or NFTs (whether featured in this whitepaper or otherwise) and should not be relied on in connection with any other contract or purchasing decision. The statements in this whitepaper also do not represent the position undertaken by any other affiliates and their respective officers, directors, managers, employees, agents, advisors or consultants.

Buyers are strongly urged to consult their own professional and tax advisers with respect to their contemplated purchases and with specific reference to their own personal financial situation and to only commit to such investment upon having fully studied and understood the underlying risks, process and background entirely.

This is not a sale of security:

This whitepaper is not a prospectus or a financial service offering document as defined under any relevant statutory provisions nor does it constitute an offer to sell or solicit any offer to buy any security, investment products, regulated products, or financial instruments. In AmazeWallet, the cryptographic tokens featured are not structured as securities or to be traded as securities. AmazeToken holders also do not have legal or equitable rights in AmazeWallet or any of its affiliates, including any equity, shares, units, royalties, profit, returns, or income in AmazeWallet or any other company or intellectual property linked with AmazeWallet.

No representation:

The statements (including any data, proclamations or conclusions whether express or inferred) generally included in this whitepaper is not an indication, guarantee or portrayal to any buyer, potential buyer or related persons thereof. AmazeWallet is also not responsible for any conclusions extracted or data composed out of the contents of this whitepaper. This whitepaper, together with any other documents or information referred to herein should not be regarded as an independent evaluation and analysis of any investment in or performance of the cryptographic assets contained.

As presented in this whitepaper, AmazeWallet is a work in progress and thus, the contents in this white paper will be continuously updated from time to time, including details relating to the key features and parameters offered. As such, the features depicted in this whitepaper should not be taken to be an indication of the exact features upon fruition. Any plans, future projections, or possibilities depicted in this whitepaper should also not be taken as a portrayal or guarantee as to its accomplishment or sensibility. Nothing in this record is or should be depended upon as a commitment or portrayal concerning the contents in this whitepaper. To the widest extent permissible under any applicable law, AmazeWallet is not liable for any misfortune or harm of all sorts suffered by any individual, whether predictable or otherwise, due to any reliance on the descriptions, data and contents contained in this whitepaper or any data access or received from AmazeWallet with respect to the same.

Views of AmazeWallet:

The perspectives and assessments communicated in this whitepaper represent those of AmazeWallet only and nothing in this whitepaper should be taken as the opinion or position with regards to any strategy or position made by any administration, semi-government, authority, or public body of any jurisdiction. AmazeWallet also does not assume any obligation to notify any individual as to any changes in law or regulatory position of any applicable jurisdiction from the date that this white paper is issued or updated.

Third-Party data and references:

This whitepaper may contain information and references obtained from other third-party sources. While it is the discretion of the administration of this whitepaper to accept that such information is dependable and to use it as it deems appropriate, the information relied upon is based on free review and has not been subject to any further investigation by any professional bookkeeping or other authoritative guides and sources. As such, AmazeWallet does not warrant or represent the exactness and quality of such third-party information and references reflected in this whitepaper.

References made in this whitepaper (whether to other organisations or cases in any manner howsoever) are for illustrative purposes only and any such reference should not be taken as an affiliation, partnership, or association of AmazeWallet to the same. All references to 'dollars', USD, or '\$' are references to the United States Dollars unless otherwise noted.

Other risks:

In addition, the potential risks briefly mentioned above are not exhaustive. Other factors not referred to herein may affect the future performance of any of the contents. Accordingly, none of AmazeWallet or its affiliates should be deemed nor do we purport to provide any assurance about the performance or development of the features or the return of invested capital or profits of any investor.

Translations:

This whitepaper and any related materials are provided in English. Any translation or interpretation provided in this whitepaper is for reference only and its accuracy has not been confirmed by any professional body. In the event of any inconsistency between the interpretation or translation of any content in this whitepaper, the English version shall prevail.

Restricted transmission:

This whitepaper should not be taken or communicated to any individual or body where the conveyance or spread of this whitepaper is precluded or limited by any applicable law.

Graphics/ Designs/ UX/UI interfaces/Illustrations:

All designs used in this whitepaper are for illustrative purposes only and specifically, illustrations with cost references do not convert to actual evaluating data.

AmazeChain, AmazeWallet, and AmazeToken are registered trademarks.

 **Amaze**Chain