AMARSCITY

WHITE PAPER

1. Responsibility Disclaimer

Attention! The current white paper is for informative purposes only. Its content is not a sales promotion nor an offer of securities or financial securities. Read the document carefully to understand how the Amarscity Platform works.

Potential token buyers should carefully evaluate the risks and uncertainties associated with cryptocurrencies and familiarize themselves with all the information in this document before conducting any business.

2. Executive Summary

INTRODUCTORY SUMMARY

Worldwide, the number of inhabitants in urban areas is increasing, so 68% of the world's population is expected to live in urban areas by 2050. As cities continue to grow, sustainable development is increasingly dependent on the successful management of urban growth, especially in low- and middle- income countries, where urbanization is expected to be the fastest.

Most countries will face challenges in providing services to the population, including housing, transportation, energy system, infrastructure, employment, as well as basic services, such as healthcare and education. Integrated policies are needed to improve the lives of urban and rural residents, while strengthening the links between urban and rural areas, based on existing economic, social and environmental links.

Smart cities based on IoT technologies can contribute to improving the quality of life, but this "smart" urban landscape, with numerous connected devices and a large communication network, creates new security challenges – challenges that cannot be easily addressed by conventional solutions. Research has also shown that interoperability is an essential feature of smart devices that is more important to consumers than brand loyalty.

The Amarscity Platform is a solution to these challenges and more. Amarscity is creating standalone independent smart-city web solutions and a central station(powered by Amarscity-chain) that will offer security and interoperability to smart-city devices operations.

2.2 SMART CITY APPLICATIONS

Smart City is a collection of paradigms spread across different domains: economy, people, government, mobility, environment and life and addresses a variety of use cases: environmental monitoring, traffic analysis, utility monitoring, smart public transport, electronic voting system, ecommerce, jobs, local events, real-time incident reporting, medical services, e.t.c

Amarscity platform will create several standalone independent smart-city web applications, at least one every quarter (beginning from project launch.)

These applications will be powered by the Amarscity token - Amarscoin and will become well known brands in no time, with effective marketing..

2.2 CONNECTED DEVICES STATION

Security and interoperability challenges are two main situations that faces smart city operations. The collection and storage of personal data create a risk for the personal lives of every human being. This is exactly why blockchain technology opens up the possibility for all participants of such a process to collect and exchange their data with a high level of reliability and security without the involvement of a sole centralized administrator or intermediaries.

The Amarscity-Chain will not only be a platform on which mass of new data derived from smart cities can be safely stored and accessed by those who should have access to it, the chain will also serve as an interoperable platform that gives residents of smart cities greater say in the decisions affecting their hyper-local communities.

Through APIs, users will be able to connect IoT and AI devices to the Amarscity platform.

2.3 PAYMENT GATEWAY

E-commerce continues to grow exponentially each year. Currently, there are approximately 20 million digital stores in the world, and this number is expected to increase at a rate of 26% each year.

It is estimated that the total turnover(sales) of these e-commerce businesses in 2017 exceeded USD $2.1 trillion, 10.5% increase compared to 2016 (USD $1.9 trillion).

Through the Amarscity Payment Gateway, Performing payments will be possible in several ways in order to increase adoption and usage. We will be implementing some innovative ideas such as sending funds by e-mail, sms, and NFC

3. Introduction

Amarscity is a smart-city enhancement project that wants to elevate the lives of citizens through smart-city services that can be accessed from any location. Amarscity is creating the first smart-city multipurpose service delivery station powered by the INTERNET, IOT, BIGDATA, AI and BLOCKCHAIN TECHNOLOGY.

Our goal at Amarscity is to make life easy and interesting for citizens by creating a virtual city that impacts the life of its citizens physically wherever they are.

Smart city concept is not new; many of these systems existed well before the term “smart cities” was coined. The concept of Amarscity is a platform that unifies these systems for users.

Amarscity is creating a digital smart-city ecosystem that powers/enhances almost every human activity processes in the physical world, making life easy for her citizens. When you become a citizen of Amarscity, you enjoy awesome privileges exclusive to Amarscity ID holders. We envisioned Amarscity to be the final solution that resolves existing challenges faced by citizens from various nations of the world, governments, business and humanitarian organizations. Individuals, Businesses, retail shops, building facilities, consumers, would be able to interact with each other in a smarter and more effective manner through the Amarscity platform.

Amarscity will be powered by the native coin of the Amarscity blockchain - Amarscoin. Amarscoin is the virtual city’s transaction currency. Citizens of Amarscity will be able to carry out transactions on Amarscity Service Delivery Station and on her numerous apps only with Amarscoin. As part of our roadmap Amarscity will be upgraded to Amarverse when we are fully done with developing our own Metaverse some years away from now. Amarscoin is a cryptocurrency that will be accepted in the Amarscity Metaverse project as the currency for transaction. But before the Metaverse project, we aim to make Amarscoin become a global cryptocurrecy like bitcoin and used for everyday transactions both online and offline.

To achieve that, Amarscity plans to launch two smart–city apps every quarter of the year (every four months). Each one of these apps will work independently. Each has its own business management team with a goal to become a global brand within the shortest possible time.

So together with the launch of Amarscity web platform, we are also launching Amarvo(an independent Innovative Ecommerce platform like Amazon.com) and Amarwork(an independent innovative work platform like Upwork.com). The goal of everyone of our app is to become a global brand, powered by Amarscity-chain and Amarscoin.

When we're done building the Amarscity-chain and Amarscity multipurpose service delivery station, all our smart-city apps will be integrated into the station and all Amarscity verified citizens can start enjoying upgraded smart living; access smart-city services from a one-stop innovative centre.

4. Internet of Things

The Internet of Things (IoT) is rapidly emerging as the manifestation of the networked society vision - everything that benefits from a connection is connected. Yet, this far-reaching transformation is just the beginning. The number of connected IoT devices is expected to grow by 21% annually, rising to 18 billion+ in 2023 and the global market of IoT is expected to grow from 170 billion USD in 2017 to 560+ billion USD by 2023, at a compound annual growth rate of 26:9%. Though many industry experts and excited consumers have pegged IoT as the next industrial revolution or the next internet, there are three main problems that are holding back the massively development and adoption of IoT.

4.1 SCALABILITY PROBLEM

The majority of IoT devices are connected and controlled in a centralized way as of today. IoT devices are connected to back-end infrastructures on public cloud services or on premise server farms to transmit data and receive control commands. Currently, the scale of IoT is bottlenecked by the scalability and elasticity of these back-end infrastructures, servers and data centers. The substantially high operating cost of running the scale of IoT is unlikely to be covered by the profit from selling devices. Consequentially, many IoT vendors cannot provide cost-effective devices and applications that are scalable and reliable enough for real-world scenarios.

4.2 LACK OF PRIVACY

IoT is expected to enable mass participation of end users on mission critical services such as energy, mobility, legal and democratic stability. Privacy challenges originate from the fact that IoT interacts with the physical world in direct and automatic ways, and the amount of data collected will increase substantially when it scales up. Some of the common privacy threats, as enumerated are:

1. Identification: Associate a (persistent) identifier, e.g., a name and address or a pseudonym of any kind, with an individual;

2. Localization and tracking: Obtain an individual's location through different means;

3. Pro ling: Compile information dossiers about individuals to infer interests by association with other pro les and data sources;

4. Privacy-violating interaction and presentation: Conveying private information through a public medium and in the process disclosing it to an unwanted audience;

5. Life cycle transitions: Devices often store massive amounts of data about their own history throughout their entire life cycle that could be leaked during changes of control spheres in a device's life cycle;

6. Inventory attack: The unauthorized collection of information about the existence and characteristics of personal things, e.g., Burglars can use inventory data to check the property to find a safe time to break in;

7. Linkage: Linking different previously separated systems such that the combination of data sources reveals (truthful or erroneous) information that the subject did not disclose to the previously isolated sources and, most importantly, also did not want to reveal.

All these common privacy threats are due to data leak at device level; or, data leak during communication; or, more often, data leak by centralized parties.

4.3 LACK OF FUNCTIONAL VALUE

Most existing IoT solutions lack meaningful value creation. Being connected is the most used value proposition. However, simply enabling connectivity does not make a device smart or useful. A greater portion of the value that IoT produces comes from interaction, cooperation, and eventually autonomous coordination of heterogeneous entities. A few good analogies are that individual cells cooperate to build multi-cellular organisms, insects build societies, humans build cities and states. By cooperating, all these individuals unite to build something that has greater value than their own. Unfortunately, according to [29], 85% of legacy devices lack ability to interact or cooperate with each other due to compatibility issues. The data sharing for business and operational insights is nearly impossible.

5. Blockchain

Blockchain technology was introduced in 2008 and its first implementation, i.e. Bitcoin, was introduced a year later, in 2009, published in the paper Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto (alias). Essentially, blockchain is a distributed, transactional database that is shared across all the nodes participating in the network. This is the main technical innovation of Bitcoin and it acts as a public ledger for the transactions. Every node in the system has a full copy of the current chain state, which contains every transaction ever executed. Every block contains a hash of the previous block, linking these two together. The linked blocks become a blockchain.

5.1 INGREDIENT

A blockchain can be perceived as a four-dimensional continuum that has three horizontal layers including transaction and blocks, consensus, compute interface, and governance, one vertical layer.

Transaction and Blocks

As the lowest horizontal layer, signed transactions are gossiped among all nodes and blocks are generated by full nodes. This is the foundation of blockchain where transferring of digital assets (thus the inherent values) and account security are achieved via crypto primitives like elliptic curve signature, hash function and Merkle tree.

Consensus

The middle horizontal layer manifests the peer-to-peer nature of the blockchain, where all nodes within the network reach consensus on all internal states on chain via techniques like Proof of Work (PoW), Proof of Stake (PoS) and their variants, Byzantine-fault tolerance (BFT) and its variants etc. The consensus layer affects scalability the most. PoW is usually considered less scalable as compared to PoS.

In addition, this layer heavily impacts security in terms of double spending and other attacks focused on mutating the blockchain states in an unanticipated way.

Compute Interface

The first two horizontal layers form the shape of a blockchain while the Compute Interface layer is critical to make a blockchain useful, which encompasses extensibility and usability. For instances, smart contract has been implemented by Ethereum to enable programmability where one could count on the distributed "world computer" for executing the terms of a contract. Sidechain, together with merged mining, has also been developed intensively to support programmability. Second-layer protocols like Raiden network [25], state channel has been developed to extend the scalability of a blockchain at this layer. In addition, tools, SDKs, frameworks, and GUIs are also extremely important to usability. The Compute Interface layer gives developers the capability to develop decentralized apps (DApps), an essential part of making the blockchain useful and valuable.

Governance

As with organisms, the most successful blockchains will be those that can best adapt to their environments. Assuming these systems need to evolve to survive, initial design is important, but over a long enough timeline, the mechanisms for change are most important, which is known as the vertical layer governance. There are two critical components of governance:

- Incentive: Each group in the system has their own incentives. Those incentives are not always 100% aligned with all other groups in the system. Groups will propose changes over time which are advantageous for them. Organisms are biased towards their own survival. This commonly manifests in changes to the reward structure, monetary policy, or balances of power.

- Coordination: Since it is unlikely all groups have 100% incentive alignment at all times, the ability for each group to coordinate around their common incentives is critical for them to affect change. If one group can coordinate better than another, it creates power imbalances in their favour. In practice, a deciding factor is how much coordination can be done on-chain (e.g., votes to the rules of the system like Tezos, or even roll back the ledger if majority stakeholders don't like the change) vs. o -chain (such as Bitcoin Improvement Proposals (BIPs)).

5.2 OPERATIONAL MODELS

Blockchains can be categorized as permissionless and permissioned depending on how it is operated. For example, Bitcoin is permissionless meaning that anybody can create an address and begin interacting with the network, which is "build trust from trustless". In contrast, the permissioned blockchain is a closed and monitored ecosystem where the access of each participant is defined and differentiated based on role, which is "build trust from less trusted".

There are benefits and drawbacks to each approach. Regardless, all these considerations boil down to fundamental design trade-o s among trust, scalability, computation and complexity. For example, Bitcoin and Ethereum are blockchains built on top of trustless nodes because scalability is strongly desired. Hence, either lots of computation is needed (in the case of PoW) or more sophisticated consensus mechanism is needed. In contrast, Fabric is a permissioned blockchain where all nodes are considered as trusted and have cryptographic identities, e.g., issued by member services like Public Key Infrastructure (PKI), which makes them highly scalable with low computation and a relatively straightforward consensus mechanism.

Table 1: IoT Benefits From Blockchain Properties

Blockchain Property	IoT Benefits From
Decentralization	Scalability, Privacy
Byzantine fault tolerance	Availability, Security
Transparency & Immutability	Anchoring Trust
Programmability	Extensibility

6. Benefits & Challenges of Blockchain and IoT

Sensing and perception, transformation and transmission, and processing are the essence of most intelligent things on this planet. For IoT, while the sensing and perception layer is spontaneously distributed, the latter two are not for the time being, which is the root for most scalability, privacy and extensibility problems. We envision blockchain technology, if it serves as the spinal cord and nervous system of IoT, as the best candidate to address the aforementioned IoT-specific problems.

6.1 BENEFITS

By embracing blockchain technology, IoT immediately benefits from the following aspects thanks to blockchain's properties including decentralization, Byzantine fault tolerance, transparency and immutability. Table 1 summarizes how IoT benefits from blockchain properties.

Decentralization

Decentralization frees users and devices from centralized controlled and consistent monitoring, thus partially addressing the privacy concern imposed by centralized parties who monopolize the market and try to understand every aspect of user/device for their own benefits, e.g., advertising. Decentralization, under the context of cryptoeconomy, also indicates "elasticity" that is often defined as "the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible". A blockchain and the underlying cryptoeconomy can be designed in a way that is elastic enough and cost-effective enough for IoT scenarios and applications. For example, more blockchain nodes could be spun up if the network has enough computation tasks with enough incentives to perform.

Byzantine Fault Tolerance (BFT)

The objective of Byzantine fault tolerance is to defend against failures in which components of a system fail in arbitrary ways, i.e., not just by stopping or crashing but by processing requests incorrectly, corrupting their local state, and/or producing incorrect or inconsistent outputs. The Byzantine failure models real-world environments in which computers and networks may behave in unexpected ways due to hardware failures, network congestion and disconnection, as well as malicious attacks. BFT property can be leveraged to achieve many desired security properties in the context of IoT, e.g., eliminate man-in-the-middle (MITM) attacks as there is no single thread of communication that can be intercepted and tampered, make Denial of Service (Dos) attacks almost impossible.

Transparency and Immutability

Blockchain provides cryptographic assurances that the data anchored on the chain is always transparency and immutable, which can be useful in many scenarios, e.g., anchor states of the IoT world on the blockchain for the purpose of auditing, notarization and forensic analysis, identity management, authentication and authorization.

Programmability

Bitcoin came with basic programmability to allow a transaction to succeed only if the underlying small script execute successfully. Ethereum enhances this feature to achieve the Turing-complete smart contract which is written in high-level programming language and executed in a small virtual machine known as EVM. This programmability can be and should be extended to IoT devices, some of which currently only have simple and hard-coded logic that can't be further programmed once shipped.

6.2 CHALLENGES

Benefiting from common properties provided by blockchains does not mean every blockchain is suitable for IoT use. In fact, it doesn't seem like any existing public blockchain can be applied to IoT since there are quite a few challenging problems.

Native Privacy Guarantee Is Not Enough

Native privacy guarantees from blockchain can only help address the privacy pain point in IoT to the degree that it retains data on the chain rather than centralized servers, using pseudonymity. However, if a device's pseudonym is ever linked to its identity, everything it ever did under that pseudonym will now be linked to it.

No Silver Bullet Blockchain Exists

As mentioned above, IoT is a universe of heterogeneous systems and devices with different purposes and capabilities. It is impossible to and a silver bullet blockchain solution that suits most scenarios. For instance, a blockchain for coordinating millions of industrial IoT nodes should focus on high scalability and transaction throughput, while a blockchain for coordinating smart devices at home should focus on privacy and extensibility. At a macro level, the IoT devices as one specie is definitely evolving at a fast pace, i.e., new technologies are integrated, new standards are developed, new devices are manufactured with new capabilities. In contrast, at a micro level, the individual IoT device's capability, purpose and operational environment also keep changing over time.

Chain Operations Are Heavyweight

- In the IoT world, many devices are considered as weak nodes because they are:

- Incapable of performing PoW-based mining due to the power and computation constraints;

- Not able to store large amount of data (e.g., gigabyte level, not mentioning terabyte-level and petabyte-level) due to the power and storage constraints;

- Not able to verify all transactions by processing the whole blockchain;

- Not able to connect to peers all the time, depending on its uptime and connectivity quality.

Therefore, most existing blockchains are too heavyweight for IoT.

7. Built-in Privacy-Preserving Transaction

The privacy provided natively by Bitcoin and Ethereum is limited to pseudonymity. Transaction details are not confidential. The transaction amount and the assets being transferred, its metadata, and its relationships to other transactions, can be trivially learned by anyone. In fact, there are three aspects of privacy, sender privacy, receiver privacy and privacy of transaction details in this context. Various cryptographic schemes can be applied to address them.

Amarscity integrates stealth address for receiver privacy, ring signature for sender privacy and Pedersen Commitments for hiding transaction amount with the following innovations and improvements:

- A lightweight stealth address scheme is designed to exempt receivers from scanning the entire blockchain to be aware of incoming transactions;
- Ring signature is optimized to make it compact in size with a distributed trusted setup.

7.1 HIDE TRANSACTION RECIEVER WITH RELAYABLE PAYMENT CODE

Stealth Address

Stealth address technique originated from Cryptonote protocol [28], which solves the receiver problem using a "half round" Di e{Hellman key exchange protocol. Assuming Bob wants to hide the fact that he receives tokens from Alice, here is how it works:

1. Bob creates two pairs of private and public keys, denote as (a; A) and (b; B), where A = a G and B = b G, where G is the base point on an elliptic curve.
2. Bob publishes public keys (A; B) which are known as his stealth address;

3. Alice calculates and sends tokens to P = H(rA) G + B using a hash function H, a random big number r and Bob's stealth address B. This transaction is broadcast along with R = r G;

4. Bob watches all transactions, calculates P^0 = (H(aR) + b) G (since he knows a, b, R and G) with the hope that P^0 equals to P . If P^0 = P , Bob could spend tokens send to P^0 with private key H(aR) + b.

One obvious drawback of stealth address it that the receiver has either to scan all transactions (which is not ideal in an IoT world) in the network or rely on the assistance of a trusted full node (which compromises privacy to a certain degree).

Payment Code

Payment code has been designed to address the above drawback of stealth address with a certain sacrifice in privacy. The idea is that Alice notifies Bob of a payment code in a confidential way and Bob only watches transactions against addresses deriving from that code. Therefore, this proposal has two flows – notification, which is a one-time setup between two certain parties, and sending, which can happen multiple times between these two parties.

Assuming Alice has master public-private key pair ($mpub_{Alice}$; $mpri_{Alice}$) where $mpub_{Alice}$ = $mpri_{Alice}$ G and wallet public-private key pair ($wpub_{Alice}$; $wpri_{Alice}$) where $wpub_{Alice}$ = $wpri_{Alice}$ G; Bob has master public-private key pair ($mpub_{Bob}$; $mpri_{Bob}$) where $mpub_{Bob}$ = $mpri_{Bob}$ G, the one-time notification flow works as below:

1. Bob derives B_0 = b_0 G = ($mpri_{Bob}$ + Hash(0; seed; metadata)) G, converts it to an noti cation address addr(B_0), publishes it and listens on it

2. Alice picks a chain code cc at random; ($mpub_{Alice}$jjcc) is the payment code for Alice;

3. Alice calculates a shared secret S = $wpri_{Alice}$ B_0 and sends masked payment code P^0 = ($mpub_{Alice}$jjcc) HMAC512(xofS) to addr(B_0);
4. Upon receipt, Bob learns $wpub_{Alice}$, and recovers S = $wpub_{Alice}$ b_0, unmasks P^0 to obtain ($mpub_{Alice}$jjcc).

Once the notification flow is done, Alice and Bob establish one uni-directional private channel for sending tokens. The first sending flow works as below:

1. Alice derives a new address from the her payment code (that is already shared with Bob) by A_0 = a_0 G = $mpub_{Alice}$ + Hash(0; seed; metadata) G;

2. Alice selects the next unused public key derived from B_0. Note that B_0 is the unused public key for the first round.

3. Alice calculates the new shared secret S_0 = a_0 B_0, and calculates the ephemeral public key used to send the transaction to which is B_0^0 = B_0 + SHA256(S_0) G

4. Bob could derive A_0 non-interactively since he knows Alice's payment code, and only listens on address derived from B_0^0 = B_0+ SHA256(S) G and S = A $_0$ b_0.

5. Upon receipt, Bob could use the tokens with private key b_0 + SHA256(S_0).

The following sending flows works similarly.

Bob does not need to scan or rely on a full node to scan all transactions. The notification transaction does leak the intention of Alice wants to send something to Bob, but the actual \sending of something" is hidden from everyone else.

Relayable Payment Code

To further minimize the privacy leak, we designed the relayable payment code on top of the original payment code proposal. While the sending flow remains the same, we improved the notification flow to make it possible for Alice to secretly share her payment code with Charlie without using the notification transaction, assuming Alice and Bob have one uni-directional private channel, and Bob and Charlie have another uni-directional private channel. To achieve that, we leverage Hashed Timelock Contracts (HTLCs), which require that the receiver of a payment either acknowledge receiving the payment prior to a deadline by generating cryptographic proof of payment or forfeit the ability to claim the payment, returning it to the sender.

Assuming Charlie has master public-private key pair ($mpub_{Charlie}$; $mpri_{Charlie}$) where $mpub_{Charlie} = mpri_{Charlie}$ G. The improved notification flow works as follows.

1. Charlie derives $C_0 = c_0$ G = ($mpri_{Charlie}$ + Hash(0; seed; metadata)) G, converts it to an noti cation address addr(C_0), publishes it. Note that C_0 is published for Alice to calculate the shared secret, but not for receiving any transactions;

2. Alice generates her payment code ($mpub_{Alice}$jjcc) in the same way;

3. Alice calculates a shared secret S = $wpri_{Alice}$ C_0 and sends masked payment code P^0 = ($mpub_{Alice}$jjcc) HMAC512(xofS) with X tokens as incentive and HTLC($Hash^2$(cc)) to Bob using their uni-directional private channel, where HTLC, as part of the locking or redeem script, states that the tokens become spendable if the pre-image of $Hash^2$(v) is given, i.e., Hash(cc);

4. Bob, incentivized by the tokens sent over from Alice, sends P^0 , Y; Y < X tokens and HTLC($Hash^2$(v)) to Charlie using their uni-directional private channel;

5. Charlie, upon receiving Bob's transaction, calculates S = $wpub_{Alice}$ c_0 to un-mask Alice's payment code, and spent the transaction by disclosing Hash(cc), which makes Alice-to-Bob transaction spendable to reward Bob.

Once this flow is done, Alice and Charlie establish one uni-directional private channel for sending tokens. It is noteworthy that the routing of Alice's transaction could be multiple hops.

Our relayable payment codes over better privacy in terms of hiding the intention of "sending of something" on the chain by leveraging the existing private channels without adding any computation or storage overhead to the nodes, which, while designed for IoT scenarios, is usable for most blockchains like Bitcoin.

7.2 ENABLE CONFIDENTIAL TRANSACTION

Problem Statement

A typical transaction on the Bitcoin blockchain is shown in Figure 4. Essentially, a blockchain transactions is just a tuple ($fpk_{in;i}g$; $fpk_{out;j}g$; $fv_{i;j}g$), where $fpk_{in;i}g$ are input addresses, $fpk_{out;j}g$ are output addresses, and $fv_{i;j}g$ are transaction amounts among input and output addresses. Because Bitcoin transactions are stored in clear-text in the public ledger, it has raised a lot of security and privacy concerns.

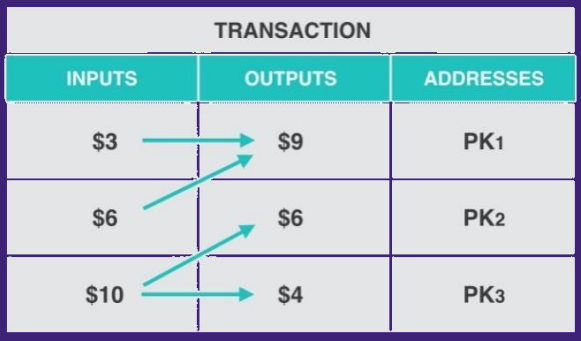

Figure 1: A Transaction on the Bitcoin Blockchain

The goal of confidential transactions (see Figure 5) is to enable only senders and receivers of transactions to reveal the $fv_{i;j}g$ values and conceal them from the rest of the world. Moreover, confidential transactions also allow other network entities to verify the validity of those transactions in question without seeing the actual amounts. The realization of confidential transactions on blockchain requires a number of advanced cryptographic techniques.

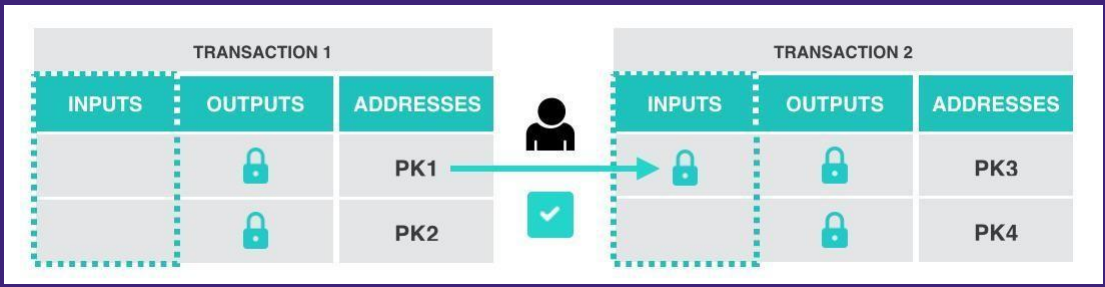

Figure 2: A Confidential Transaction with Public Verifiability

Cryptographic Building Blocks

Proof of Knowledge

A proof of knowledge, denoted by (P; V), is an interactive proof between a prover P and a verifier V , in which the prover wants to demonstrate that he knows some information. More specifically, P has (x; w) belonging to a relation R, where x is the problem and w is the solution (also called a witness). V knows x and he accepts only if P could convince V that he knows w.

Zero-Knowledge Proof

In a zero-knowledge proof protocol, the prover proves a statement to the verifier without revealing anything about the statement other than that it is true, which protects the prover against the malicious verifier, which attempts to gain more knowledge than what is intended. The protocol can be either interactive or non-interactive. The key difference with non-interactive proofs is that all interactions consist of a single message sent by the prover to the verifier. We use the notation NIZKPoK(;) : a = g ^ b = g to denote a non-interactive, zero-knowledge proof of knowledge of the values and such that a = g and b = g . All values not enclosed in parenthesis are assumed to be known to the verifier. When we use a non-interactive zero-knowledge proof to authenticate auxiliary data, the resulting scheme is referred to as signature of knowledge. Basically, a signature of knowledge scheme means that one in possession of a solution w to the problem x has singed the message m. For the above NIZKPoK, we use notation SoK[m](;) : a = g ^ b = g to denote a signature of knowledge on message m.

Ring Signature

The concept of ring signature was first introduced by Rivest et al. in 2001 as a special kind of group signature. In a ring signature, the message signer selects a set of ring members including themselves as the possible message signers. The verifier can be convinced that the signature was indeed generated by one of the ring members. However, the verifier is not able to tell which member actually generated the signature. Unlike a general group signature, a ring signature scheme does not involve designating a group manager for managing the set of ring members, thereby eliminating the possibility of revealing the identity of the actual message signer by the group manager. In order to provide anonymity in smart contract token transactions, a special kind of ring signature, so-called linkable ring signature, has been employed in the privacy-focused cryptocurrency Monero.

Linkable ring signature has additional property that any signatures generated by the same signer, whether signing the same message or disparate messages, has an identifier (called a tag) linking the signatures. This property enables third parties to efficiently verify that the signatures were generated by the same signer, without leaking the actual signer's identity. The linkable ring signature used in Monero is called a Multi-layered Linkable Spontaneous Anonymous Group Signature (MLSAG) [22], which is a ring signature on a set of key-vectors and has a communication complexity of O(m(n + 1)), where m is the number of public/private key pairs owned by the signer and n is the size of ring.

Accumulator

One-way accumulators, which were first proposed by Benaloh and de Mare, are defined as one-way hash functions with the property of being quasi-commutative. A quasi-commutative function f : X Y ! X satisfies that, for all x 2 X and for all y_1; y_2 2 Y , we have f(f(x; y_1); y_2) = f(f(x; y_2); y_1). A one-way accumulator allows us to combine a set of values into a secure digest and this digest does not depend on the order in which the values are accumulated. It can also be used to generate a witness that enables one to attest that a given value is actually part of the accumulator.

Commitment Scheme

A commitment scheme is a protocol enabling a user to commit to a value of his choice without revealing that value to the recipient of the commitment. In a later phase, when the user is asked to reveal the committed value, the recipient will have the means to verify that his revealed value is indeed unconditionally linked to his commitment. A commitment scheme should meet two requirements. While the hiding requirement prevents the recipient from learning the content of the commitment, the biding requirement prevents the user from cheating when opening this commitment.

In Pedersen commitment scheme [23], the domain parameters are a cyclic group G of prime order q, and generators (g_0; : : : ; g_m). For committing to the values (v_1; : : : ; v_m) 2 Z^m_q, one picks a random number r 2 Z_q and set the commitment

$$C = PedCom(v_1; : : : ; v_m; r) = g_0^{r} \prod_{i=1}^{m} g_i^{v_i} .$$

7.2.2 Our Improvements

RingCT 2.0, employs a cryptographic accumulator to further reduce the communication complexity to O(n) at the cost of additional computations. We note that although RingCT 2.0 reduced the communication complexity significantly when compared to MLSAG, the domain parameter generation of the accumulator requires a one-time \trusted setup" process liked Zcash. Hence one has to trust that whoever generated the secret parameters destroy them when they are done, which has raised security and privacy concerns for the system. To address this issue, our solution is to employ a secure multi-party computation (SMPC) protocol among a set of bootstrapping nodes of the blockchain to generate secret domain parameters in a secure and distributed manner. In addition, the following directions are currently being investigated to improve the RingCT-like protocols in terms of communication and computational overhead:

- A new linkable ring signature scheme with communication complexity less than O(n)
- A new approach for aggregating multiple linkable ring signatures
- A sigma protocol for trustless setup of secret domain parameters

We aim to propose a novel confidential transaction solution that is able to achieve a good trade-off between communication and computation cost.

7.3 PROVE TRANSACTION AMOUNT RANGE WITH BULLETPROOFS

As a drop-in replacement of Pedersen commitments, bulletproofs, a new non-interactive zero-knowledge proof protocol with very short proofs and without a

trusted setup, has been proposed recently, which reduces the size of a range proof from linear to sublinear and further reduces the transaction size without additional computation overhead. Since Bulletproofs fit Amarscity's design principle well, we are going to integrate bulletproofs into Amarscity.

8. Fast Consensus with Instant Finality

8.1 BACKGROUND

Proof of Work

Proof of Work (PoW) is the backbone to reach the global consensus of most blockchains, including Bitcoin and Ethereum. PoW makes it computationally di cult to construct a valid block and attach it to a blockchain. The longer the blockchain becomes, the harder it is to reverse any transaction recorded previously by the blockchain. To manipulate the blockchain, an attacker needs to own 51 percent of the whole computation power of a PoW-based blockchain network.

Although PoW provides an elegant solution for the global consensus of large distributed blockchains, it has several inherent drawbacks. The overall computation cost to maintain the global consensus is the same cost of the 51 percent attack. This means that even if the majority of the blockchain participants are honest, they still have to use a lot of electricity to maintain the blockchain, which is not suitable for the environment of IoT networks that usually favour energy efficiency.

In addition, on the level of individual devices, computing PoW usually costs a lot of CPU cycles and memory usage, which poses difficult requirements to the hardware manufacturing and costs of embedded IoT devices. Last but not least, PoW does not provide instant finality which is a critical property required to construct efficient cross-chain communication.

Proof of Stake

Proof of Stake (PoS) was proposed as an efficient alternative to PoW for blockchains reaching consensus, which aims to avoid the above mentioned issues of PoW. The basic idea of PoS is that a randomly chosen set of nodes vote on the next block, and their votes are weighted based on the size their of deposits (i.e. stake). If certain nodes misbehave, they may lose their deposits. In this way, without computationally intensive PoW, the blockchain can run much more efficiently, and can achieve an economic stability: The more stake a participant has, the more incentive the node has to maintain the global consensus, and the less likely the node misbehaves. There are a couple of public PoS designs and implementations, such as Tendermint that has been adopted by many applications.

Delegated Proof of Stake (DPoS)

Delegated Proof of Stake (DPoS) improves upon the idea of PoS in the way that DPoS allows participants to choose some delegates to represent their portions of stakes in the network. For example, Alice can send a message to the network to grant Bob the ability to represent her stake and vote on behalf of her. DPoS offers several benefits for our IoT applications:

- Small players can pool their stakes to have a higher chance together to participate in block proposing and voting, and share the rewards afterwards.
- Resource-constrained nodes can choose their delegates, so not all the nodes need to stay online to contribute to consensus.
- Delegates can be the nodes with strong power supply and network conditions, and also can be chosen dynamically and randomly, so we will have a higher overall availability for the network reaching consensus.

The typical cryptocurrencies using DPoS include EOS and Lisk:

Practical Byzantine Fault Tolerance

Practical Byzantine Fault Tolerance (PBFT) was proposed by Castro and Liskov in 1999 as an efficient and attack-resistant algorithm for reaching agreements in a distributed asynchronous network. We plan to use PBFT for the underlying voting algorithm of our DPoS consensus mechanism, because it is a concise and well-studied algorithm that provides quick finality that is critically important for building an efficient and salable blockchain. As demonstrated in Castro and Liskov's original paper, PBFT offers both availability and safety if at most a third of the network nodes are faulty or malicious, and the network cost of PBFT is very minimum, i.e. about 3 percent compared to unreplicated network system.

The typical cryptocurrencies based on PBFT include Stellar and Zilliaq.

8.2 Randomized Delegated Proof of Stake (Roll-DPOS)

To have a fast and efficient consensus mechanism with instant block finality in the context of IoT, we combine the concepts of DPoS, PBFT and Verifiable Random Functions (VRFs). VRF was first introduced by Micali et al. in [19] and is a family of functions that can produce publicly verifiable proofs for the correctness of their random outputs. At a high level, our proposed Roll-DPOS has four phases elect candidates, form committee, propose block and finalize block.

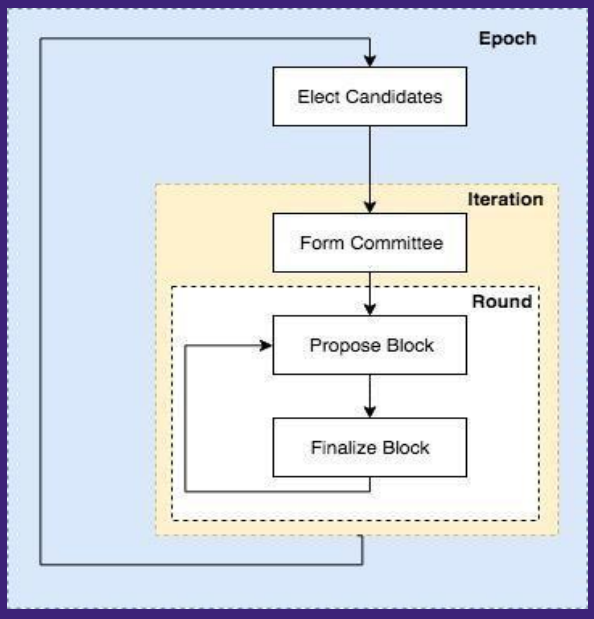

Figure 3: Randomized Delegated Proof of Stake (Roll-DPOS)

8.2.1 Elect Candidates

All notes in the Amarscity network could participate this phase in terms of voting for the committee candidates. To encourage nodes to vote, the system makes sure the blockchain and interact with it - the design is included in Satoshi's original Bitcoin whitepaper.

However, using PoS instead of PoW has a disadvantage for light clients. When verifying correctness of PoS based blockchains, clients need to download a list of public keys and signatures for block proposers and voters, and the sets of block proposers and voters may change for each block. Thus, when light clients come back online after staying online for a while, the clients may need to download a large number of public keys and signatures, and then verify all of them. To mitigate this performance issue, Vitalik, the inventor of Ethereum, has proposed creating periodic checkpoints on the blockchain, called epochs, for example every 50 blocks. Each checkpoint can be verified based on the previous checkpoint, such that light clients can catch up with the whole blockchain much faster.

9. Token on Amarscity Network

The native digital cryptographically-secured token of the Amarscity Network (AMSC) is a major component of the ecosystem on the Amarscity Network, and is designed to be used solely on the network. Prior to the launch of Amarscity mainnet, the token will exist as a BEP20 compatible token on the Ethereum blockchain, which will be migrated to a token on the Amarscity mainnet when the same is launched.

AMSC is required as virtual crypto fuel for using certain designed functions on the Amarscity Network (such as executing transactions and running the distributed applications on the Amarscity Network), providing the economic incentives which will be consumed to encourage participants to contribute and maintain the ecosystem on the Amarscity Network. Computational resources are required for running various

applications and executing transactions on the Amarscity Network, as well as the validation and verification of additional blocks / information on the blockchain, thus providers of these services / resources would require economic incentives for the provision of these resources to maintain network integrity, and AMSC will be used as the unit of exchange to quantify and pay the costs of the consumed computational resources.

AMSC is an integral and indispensable part of the Amarscity Network, because in the absence of AMSC, there would be no common unit of exchange to pay for these costs, thus rendering the ecosystem on the Amarscity Network unsustainable.

AMSC is a non-refundable functional utility token which will be used as the unit of exchange between participants on the Amarscity Network. The goal of introducing AMSC is to provide a convenient and secure mode of payment and settlement between participants who interact within the ecosystem on the Amarscity Network.

AMSC does not in any way represent any shareholding, participation, right, title, or interest in Amarscity, its brands, or any other company, enterprise or undertaking, nor will AMSC entitle token holders to any promise of fees, revenue, profits or investment returns, and are not intended to constitute securities in any Singapore jurisdiction. AMSC may only be utilized on the Amarscity Network, and ownership of AMSC carries no rights, express or implied, other than the right to use AMSC as a means to enable usage of and interaction with the Amarscity Network.

In particular, AMSC:

(a) is non-refundable and cannot be exchanged for cash (or its equivalent value in any other virtual currency) or any payment obligation by Amarscity or any of his brands;

(b) does not represent or confer on the token holder any right of any form with respect to Amarscity (or any of its brands) or its revenues or assets, including without limitation any right to receive future revenue, shares, ownership right or stake, share or security, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property), or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to the Amarscity Network, its brands, the Distributor and/or their service providers;

(c) is not intended to be a representation of money (including electronic money), security, commodity, bond, debt instrument or any other kind of financial instrument or investment;

(d) is not a loan to Amarscity or any of its affiliates, is not intended to represent a debt owed by Amarscity or any of its brands, and there is no expectation of profit; and

(e) does not provide the token holder with any ownership or other interest in Amarscity or any of its brands.

10. Amarscity Powered Ecosystems

The Amarscity blockchain supports a variety of IoT ecosystems, shared economies, smart home, autonomous vehicles, and supply chain, etc. Different types of developers leverage Amarscity in different ways. The developers supported by Amarscity include IoT hardware manufacturers, IoT device control system developers, smart home app developers, shared economies device manufacturers, supply chain data integrator, data crowdsourcing vendors, autonomous cars developers, etc. This section describes a few Amarscity powered ecosystems.

10.1 SHARED ECONOMIES

In recent years, many companies have focused on shared economies, from rides sharing such as Uber/Lyft/Didi, home sharing such as Airbnb, bikes sharing such as Mobike/ ofo, to small item level sharing like battery bank, umbrella, etc. They all provide people with a better living, although some of them are suffering from their business models. It is a different topic to discuss their business models; here we mainly focus on their technological architecture. Among all shared economies, ride sharing is the one that can't avoid human operation, viz., drivers. It is not an IoT powered economy. However, in the future, when autonomous car technology becomes mature and popular, ride sharing will be powered by IoT.

All IoT powered shared economies share some similarities: They all require a lock that can be opened by a deposit and rental fee. It is very possible and also efficient to power the whole sharing and returning process using an IoT device. In centralized world, the economies are powered by a centralized cloud. There are various drawbacks:

1. A large deposit is held by a company that may not be trustworthy. Recently, there have been many cases where the company that runs a shared bike service in China can't pay back deposits to its users;

2. The shared economies are not completely driven by community. Many shared things are owned by a company. This has caused a waste of society resource. Take shared bikes as example. When the shared bikes companies are out of business, the bikes are disposed.

3. Due to the centralized nature, the user data will be stored and controlled by one company. There are risk that either the cloud or the client can be hacked to obtain user data.

Amarscity, as an infrastructure, could be utilized to power these applications without the issues above and make shared economies decentralized and more efficient. Concretely, an Amarscity-powered shared economy provides the following benefits:

1. Deposit is completely settled by smart contract. With no one holding back the money, returning of the deposit is always guaranteed. Users don't have to trust the company to use the service.

2. Each shared thing realizes its value and mission in an autonomous way. In the ecosystem, it doesn't matter who owns the shared things in it. Everyone can own and contribute to the ecosystem. The economy can be run by community. As a result, companies can play a role of maintaining the IoT lock and manage the community. It is much lighter business model that companies can fast expand and serve more people.

3. Again, users don't have to trust the company to maintain their data. Their data is kept in the chain with privacy protection.

10.2 SMART HOME

In the existing smart home market, many IoT device manufacturers are still using out-of-date technologies to develop their products. They need a large amount of development work on their cloud. The cost of development and maintenance is high, and performance is low because of the round trip required to the cloud. Deploying their products onto Amarscity blockchain will largely reduce operating cost on engineering and cloud computing, and at the same time, largely increase the performance of their devices. In a simple smart light bulb example, with cloud technology, it takes two trips from user instruction to changing the state of a light bulb. Manufacturers are not cloud experts so often their service is not optimal. The round trip can take one to three seconds. This forces them to use cloud service by big IT companies. There are two downsides of using these cloud services:

1. Manufacturers can't fully control the availability of cloud services.

2. They need to continuously pay for the cloud service despite their one-time charge on selling their IoT devices.

3. There are risks of their cloud, client side, or intranet being hacked causing user data to be stolen or home security problems.

In contrast, Amarscity blockchain manages the devices locally and interact with public chain on the internet when necessary. The public chain is maintained by community. There is no maintenance cost for IoT manufacturers. Amarscity blockchain has privacy protection that can prevent leaking data or control being hacked even if the intranet is not safe.

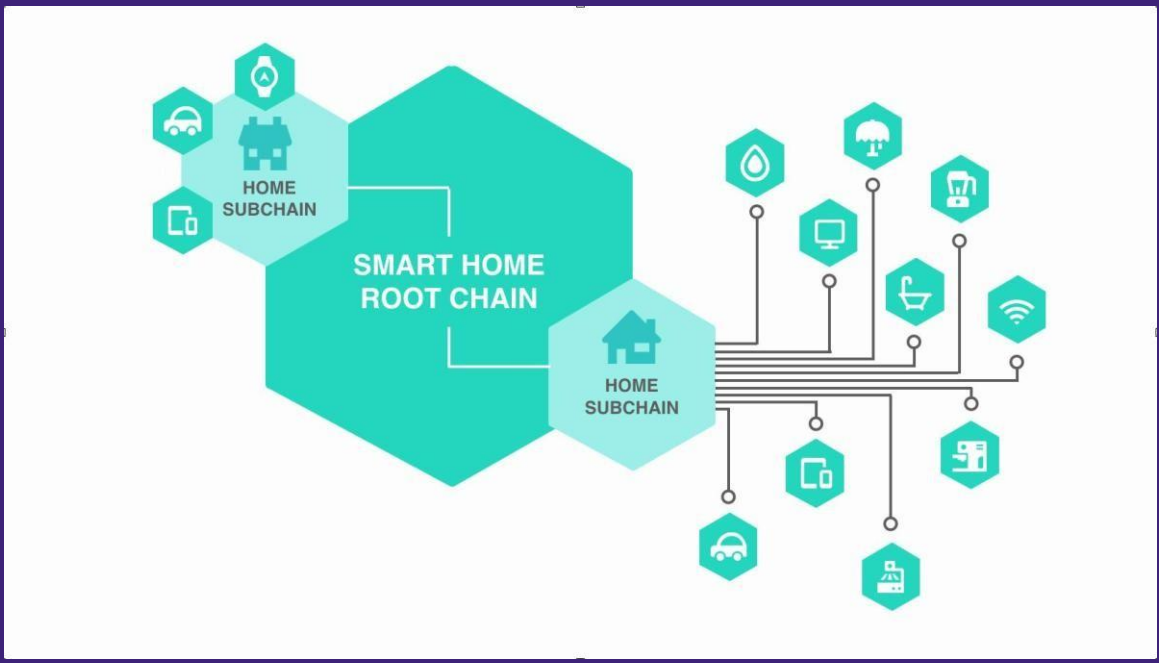

Figure 4: Amarscity Powered Shared Economy

In addition to allowing IoT manufacturers to deploy their IoT devices on Amarscity blockchain, Amarscity will partner with IoT chip makers to develop Amarscity blockchain-enabled chips to accelerate the design and manufacture cycles of IoT devices. IoT manufacturers will simply integrate the chip to get their devices supported by Amarscity blockchain.

10.3 IDENTITY MANAGEMENT

The growing world of IoT has impacted how Identity and Access Management (IAM) need to work. In terms of the identity of things, IAM must be able to manage user-to-device, device-to-device, and/or device-to-service/system. One straightforward way for identity management is to consider Amarscity blockchain as a decentralized PKI sys-tem (thanks to its immutability) where each entity is issued a cryptographic identity in the form of TLS certificate and the corresponding private. This certificate, which tends to be a short-lived one, is signed by the device's built-in and long-lived certificate and published on Amarscity blockchain (either rootchain or subchain).

Peers and other entities can access and trust the short-lived certificate anchored on the blockchain, and things can then authenticate when they come online, ensuring secure communication between other devices, services and users, and prove their integrity.

In addition, the built-in and long-lived certificates for devices could be arranged in hierarchy, like the conventional PKI, where parent devices could sign children certificate. With the hierarchy, revoking and rotating of certificates becomes possible. For example, if one device gets compromised, its parent device or even if grandparent device could sign a revocation command and send to the blockchain where the latter invalidate the device's certificate.

11. Amarscity Wallet

The Amarscity wallet is the safest way for users to store their Amarscoins. In addition, the portfolio offers multiple services such as Block explorer, leasing, voting system, Amarscity Market, payment of invoices, and management of debit cards. The wallet is going to be made available on the Web, Android, IOS and Desktop platforms. The Amarscity wallet is developed with a focus on security and being a flexible wallet. The users have total control over their coins and access to their assets at any time. To make a transaction on the blockchain, the user must perform a digital signature of their cryptocurrencies using a secret code, commonly known as a private key.

The sending and receiving of cryptocurrencies is simple and straightforward. The user can either enter the address manually or scan a QR Code. The Amarscity Wallet then quickly sends the transactions to the network. The block explorer is available for constant monitoring of the transaction’s confirmations on the blockchain. Transaction rates are calculated dynamically according to network congestion, preventing the transaction from being pending without confirmations or paying excessive fees.

The wallet also provides several features for the user. As mentioned previously, the wallet is flexible and can be customized according to the users needs.

11.1 WALLET FEATURES

CARD EXPENSES MANAGEMENT

The user will be able to manage and monitor all activities on their prepaid card. Expenses, balance, and recharges will be within the palm of the user's hand. Users will also be able to manage their private label tokens, which are given through the Amarscity loyalty program. In case of loss of the card, the user can cancel the card through the app itself. User will also be able to recharge their prepaid card with existing cryptocurrencies in the wallet, instead of having to make an additional purchase.

PAYMENT OF INVOICES AND MOBILE PHONE TOP-UP

Payment services for invoices and cell top-up are going to be available inspecific countries. The users of the Amarscity Wallet can quickly and safely pay for this service with their cryptocurrency. The wallet will also provide a thorough history of their payments.

The payment can be made by scanning the barcode or by typing their own phone number. There will be a small fee in order to execute the payment due to the Amarscity Platform liquidating the payment of the desired cryptocurrency.

12. Amarscity Prepaid Cards

With the Amarscity prepaid card, the user will be able to add credits by paying with Amarscoin or Bitcoin by simply using their mobile wallet or online Amarscity platform. Even people that are not familiar with cryptocurrency will be able use it due to its simplicity. This allows the user to be able to use their digital funds and assets for any physical business to purchase whatever they need.

12.1 CARD PAYMENT TERMINAL

The Amarscity card machine will be a modern device, with a low-cost appliance for formal and informal traders. It will allow them to have access to markets with the best rates.

The user can take the device anywhere, as it can be connected to the internet via Wi-Fi or GPS, allowing them to receive payments from any location at any time.

The device is very compact and lightweight. It will be able to receive a variety of payment methods such as traditional credit cards and debit cards, as well as cryptocurrencies such as Amarscoin and Bitcoin.

The user will also be able to choose if they want to receive those cryptocurrencies in fiat or keep it as a digital currency.

12.2 PAYMENT GATEWAY

The payment gateway is an interface that transmits data swiftly and securely between customers and retailers by using Amarscity. The Amarscity Gateway is an excellent facilitator for companies that do online business, whether it is an e-commerce, marketplace, app, digital game, and many more.

Through this gateway, payments will be processed with cryptocurrency or credit card. The fees charged by the service are very small, which makes our solution advantageous compared to others in the market.

Amarscity Gateway will also protect customer information through encryption, ensuring that the data can safely travel between the client terminal for the vendor and seller of Amarscity.

The payment will be deposited into the seller's wallet and the seller may choose to receive in it in fiat or digital currencies. This information is then stored, allowing the trader to have a listing of all transactions performed.

13. Amarscity Decentralized University

At Amarscity, we are building a fully Decentralized Online University that will be ready for launch few years from now. Amarscity Decentralized University will be a fully automated academic institution that will allow students to study online at various levels and earn various degrees without any human contact. Using the power of blockchain technology and IoT, we are building the first fully decentralized automated university in the world completely controlled by smart contracts. From admission, to matriculation, to fees payment, to lectures, to tests and examinations, to CGPA calculations, to graduation, e.t.c. Amarscity is automating the whole academic university/college process using Blockchain technology and the internet.

Among the benefits would be: Securing personal data that are enriched with significant details such as citizenship, migration, financial, and social information, e.t.c; Ensuring security of academic information systems; Creating a technological layer that can be used to secure the sharing and verification of learning achievements; Strengthening the security of educational records and increasing the correctness and reliability of data by limiting the possibilities of tampering; Avoiding any form of victimizations as a result of flaws in human relationships

A decentralized and secure university system is considered fundamental to optimizing the use of educational resources. As Amarscity-Chain prevents malicious attacks and data leakage, the higher levels of data security would benefit students as they would be able to make more informed educational decisions

14. Tokens Distribution

The total number of coins created for The Amarscity Platform is 500 billion. No more coins will be created.

25% of the coins will be utilized for the development team, company cashier for future investments, community awards on social networks, and partnership consolidation processes.

75% will be available for ICO.

Below is the detailed distribution:

Accounts	Amount (in Billions)	Percentage (%)
Reserve Fund	91	18.2
Strategic Partners	9	1.8
Development Team	15	3
Marketing & Bounty	5	1
Incentive for App Users	5	1
ICO	375	75

15. Initial Coin Offering (ICO) & Pre-ICO

ICO is a modern, innovative, and decentralized fundraising method for cryptocurrency projects and enterprises that can be characterized as an advanced crowdfunding system.

The process and concept are similar to that of an Initial Public Offering (IPO) that is used in the stock exchange world. Both the ICO and the IPO aim to raise capital, but in the ICO, the return of the investments will be in digital coins or tokens.

The Pre-ICO is the token sales warm-up that occurs before an ICO. During this stage, it is possible to obtain the assets at a price below what will be marked during an ICO. This is a great opportunity for investors to obtain an excellent valuation.

15.1 ICO PRICE

The process of trading the tokens will be divided into five stages, two during the pre-ICO and two during the ICO. If the ICO does not reach the desired maximum cap, the remaining balance of the tokens will be burned.

There will be four stages for the ICO:

Pre-ICO	68 billion $0.001 + 30% bonus	Limit of 300 million per investor
ICO	95 billion $0.008 + 20% bonus	Limit of 10 Billion per investor
ICO	138 billion $0.015 + 10% bonus	Limit of 20 Billion per investor
ICO	74 billion $0.035 + 5% bonus	Limit of 30 Billion per investor

15. Resources/Funds Distribution

The resources and funds that will be collected during the ICO process will be used to expand the development team, develop Amarscity blockchain, partner with IoT chip makers to develop Amarscity blockchain-enabled chips, purchase card machines from the manufacturer, legal adjustments of acquiring financial payments, structuring of departments of financial and accounting management, support and attendance, legal department, various server infrastructures, and marketing. We follow a solid structure while focusing on the quality of the team, adjusting to follow the roadmap as planned.

Here is how the funds and resources will be distributed:

Administrative	30%
Development	40%
Infrastructure	20%
Operational	5%
Legal	1%
Marketing	4%