

ZPAYae Whitepaper

V.1.0

31 May 2020



Decentralising the Gulf

Disclaimer

This document is a white-paper representing current and future developments of ZPAYae platform and our ecosystem. This white-paper is for information purpose only and should not be considered as an exact guiding document depicting all future intent of ZPAYae platform, unless specified explicitly.

The subject, matter and products enclosed in this white-paper are currently under development and are not yet deployed. ZPAYae makes no representations or warranties for successful implementation or development of such technologies, innovation and platform or achievement of any other implementation or activities illustrated in the paper.

It further disclaims all the warranties implied by any law or legal authorities till the extent permitted by law. No person or company is entitled to rely on the content and promises illustrated in this paper or any other inferences drawn from it, which includes relation to any interactions with ZPAYae or the technologies elaborated in this white-paper. The information present in this publication is derived from data obtained through the sources which are believed by ZPAYae to be reliable and is presented in good faith and forecasted as ZPAYae strongly believes in it, but with no warranties or guarantees. Contents of this paper regarding accuracy, completeness or suitability of the information specified, are as per the sources available at the time of its drafting and should be not relied on and shall not confer remedies or rights upon, by holders of security, creditors or other equity holders or any other person.

ZPAYae (ZPAE) disclaims all the liability for any damage or loss of capital, interest or property of any kind (whether foreseeable or not) which may arise from any company or person acting on any information and opinions relating to ZPAYae, the ZPAE platform, or our ecosystem contained in this paper or any other information presented regarding any further enquiries.

Some images used in this document may be subjected to copyright but are pursuant to the fair use regulation. Any opinion or illustration expressed in this paper reflects the current judgement of the author of this white-paper publication and may not exactly represent the opinion of ZPAYae. The information reflected herein may change without any prior notice. ZPAYae does not have any constraint to update, modify or ameliorate any projection, forecast, opinion or estimate set forth, or subsequent changes which makes the data inaccurate.

ZPAYae, its directors, contractors, employees or representatives do not have any liability or responsibility to any recipient or person (whether by negligence of misstatement, or by reason).

Neither ZPAYae nor its advisors independently take any guarantee of the information including projection, prospects and forecasts presented in this white-paper. Each recipient or person is to rely solely on its own investigation, knowledge, assessment and judgment of the matter which is subject of this publication and any other information which is made available via further enquiries or to satisfy accuracy of projections.

Whilst ZPAYae have made every effort to ensure the authenticity of the facts and forecasts made in this white-paper. Any forecast, projections or plans mentioned in this white-paper publication may not be achieved due to several risk factors like market volatility, legal or regulatory exposure, corporate actions, defects in technology development, unavailability of information and all other risks. Zela may provide website's hyperlinks of entities present in this white-paper, though the inclusion of any link does not imply that ZPAYae recommends, endorses or approves any material on the linked website.

Such linked websites should be solely accessed by your own risk and ZPAYae does not accept any responsibility for any such material or consequences of it. This white-paper is only available on <https://www.zelaapay.ae> and may not be reproduced, redistributed or passed on to any other entity.

The distribution of this white-paper may be restricted by regulations or law in certain countries. By accessing this white-paper publication, recipient agrees to be bound with foregoing limitations.

CONTENT

- **Abstract**

- **Introduction**

- **Architecture**

- Blockchain
- Sharding & Plasmatic Enhancements
- The ERC elements
- Demand based Incline

- **Distribution**

- Private Distribution of ZPAE
- Shaping UAE thru Crypto
- Digital Mode of Exchanging Value

- **Products Driven Ecosystem**

- Approach
- POS
- ZPAYae Debit Card

- **External Exchanges**

- STEEX
- EMIREX
- Further Integrations

ABSTRACT

As the digital finance world is poised towards the evolving emergence of cryptocurrencies, the entire ecosystem is seeing a soar in usability as well as easier accessibility of capital for businesses being unlocked. In these shifting paradigms - rise of transactional utilities thru tokens have become one of the most talked about phenomena of the cryptographic realm. These technological & financial advances have not only simplified the process of dealing with investors but also have secured the fundamentals of investing for an individual by enabling asset driven investments which can be liquidated at later stages – the utility or security tokens. ZelaaPayAE has created an idealistic product where the coin is impeccably backed up against - its POS that work as a mode of spending our ZPAE token at physical merchants around United Arab Emirates. ZelaaPayAE has also debuted a crypto prepaid debit card which can be used at merchants around UAE and people will be able to spend ZPAE thru it at later this year. This is probably the only platform in all of Emirates that enables trading of cryptocurrency physically at mainstream stores through plastic cards and fiat.

INTRODUCTION

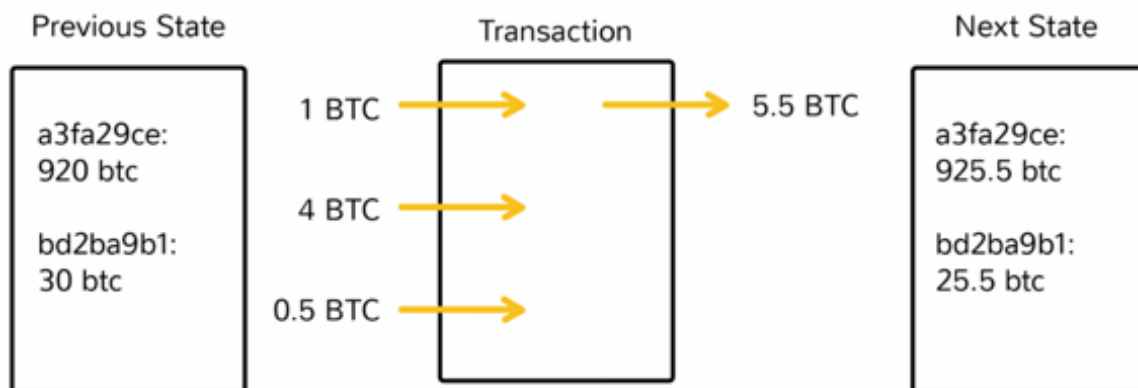
The ZelaaPayAE Whitepaper v.1.1 is a revised edition of a further global vision from the company itself. This Whitepaper contains brief details, landscapes, technical specifications and business models to help identify the project and explain our platform to the reader and stakeholder.

ARCHITECTURE

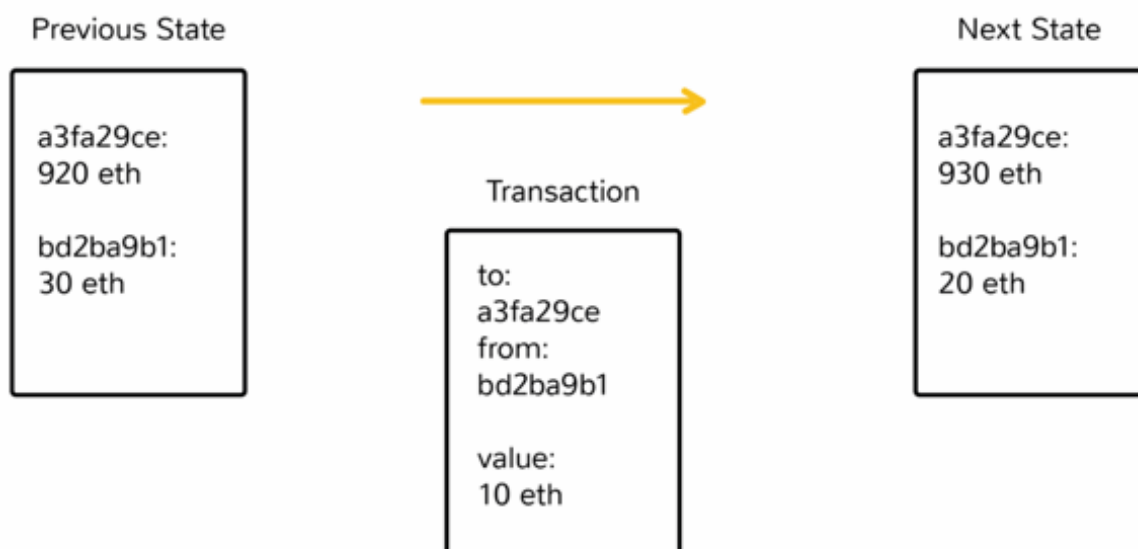
Blockchain

ZPAYae is laid on the Ethereum network and is an ERC20 token. The structure of the ethereum blockchain is very similar to bitcoin's, in that it is a shared record of the entire transaction history. Every node on the network stores a copy of this history. The big difference with ethereum is that its nodes store the most recent state of each smart contract, in addition to all of the ether transactions. For each ethereum application, the network needs to keep track of the 'state', or the current information of all of these applications, including each user's balance, all the smart contract code and where it's all stored. Bitcoin uses unspent transaction outputs to track who has how much bitcoin. While it sounds more complex, the idea is fairly simple. Every time a bitcoin transaction is made, the network 'breaks' the total amount as if it was paper money, issuing back bitcoins in a way that makes the data behave similarly to physical coins or change. To make future transactions, the bitcoin network must add up all your pieces of change, which are classed as either 'spent' or 'unspent'. Ethereum, on the other hand, uses accounts. Like bank account funds, ether tokens appear in a wallet, and can be ported (so to speak) to another account. Funds are always somewhere, yet don't have what you might call a continued relationship.

Bitcoin

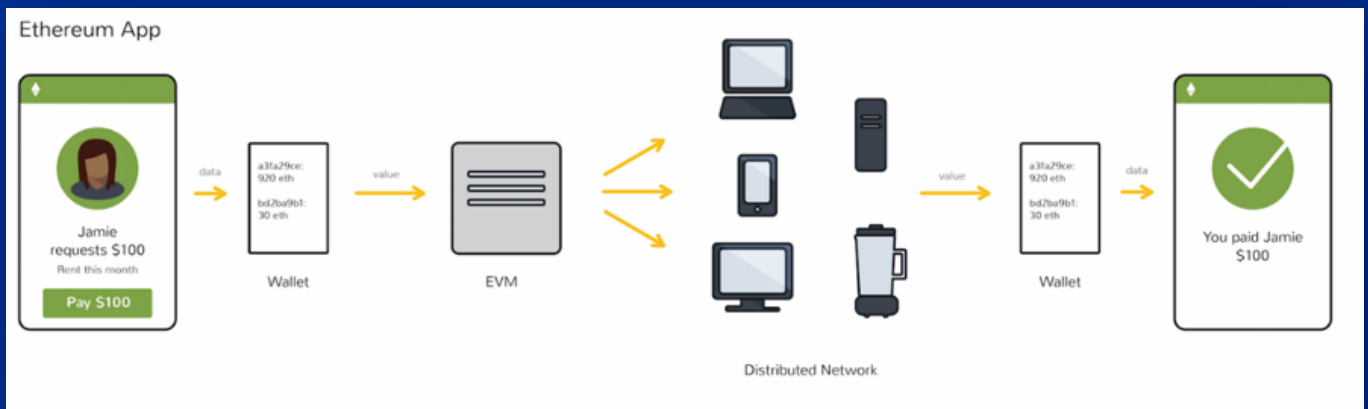


Ethereum



With ethereum, every time a program is used, a network of thousands of computers processes it. Contracts written in a smart contract-specific programming languages

are compiled into 'byte-code', which a feature called the 'ethereum virtual machine'



(EVM) can read and execute. All the nodes execute this contract using their EVMs.

Remember that every node in the network holds a copy of the transaction and smart contract history of the network, in addition to keeping track of the current 'state'. Every time a user performs some action, all of the nodes on the network need to come to agreement that this change took place. The goal here is for the network of miners and nodes to take responsibility for transferring the shift from state to state, rather than some authority such as PayPal or a bank. Bitcoin miners validate the shift of ownership of bitcoins from one person to another. The EVM executes a contract with whatever rules the developer initially programmed. Actual computation on the EVM is achieved through a stack-based byte-code language (the ones and zeroes that a machine can read), but developers can write smart contracts in high-level languages such as Solidity and Serpent that are easier for humans to read and write.

Sharding Enhancements

Currently, every single node running the Ethereum network has to process every single transaction that goes through the network. This gives the blockchain a high amount of security because of how much validation goes into each block, but at the same time it means that an entire blockchain is only as fast as its individual nodes and not the sum of their parts. Currently, transactions on the EVM are not parallelizable, and every transaction is executed in sequence globally.

The scalability problem then has to do with the idea that a blockchain can have at most 2 of these 3 properties:

- *Decentralisation*
- *Scalability*
- *Security*

If we have scalability and security, it would mean that our blockchain is centralised and that would allow it to have a faster throughput. Right not, Ethereum is decentralised and secure.

How can we break this trilemma to include scalability in the current model? Well can't we just increase the block size, or in Ethereum's case, the GAS_LIMIT, to increase throughput? While in theory this can be a right approach, the more we keep increasing it, the more mining will be centralised around nodes running on supercomputers that would bring a higher barrier to entry into the system.

A smarter approach is the idea of blockchain sharding, where we split the entire state of the network into a bunch of partitions called shards that contain their own independent piece of state and transaction history. In this system, certain nodes would process transactions only for certain shards, allowing the throughput of transactions processed in total across all shards to be much higher than having a single shard do all the work as the main-chain does now.

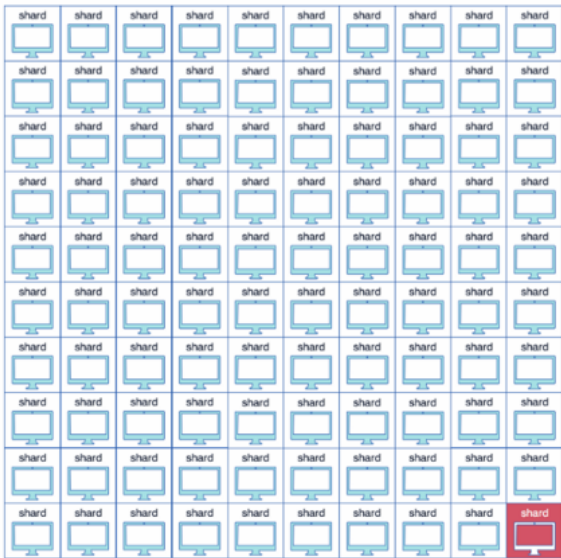
Before we dive into how a sharded blockchain actually works, let's go over some important vocabulary:

- **State** : the entire set of information that describes a system at any point in time. In Ethereum, this is the current account set containing current balances, smart contract code, and nonces at a given moment. Each transaction alters this state into an entirely new state.
- **Transaction** : an operation issued by a user that changes the state of a system
- **Merkle Tree**: a data structure that can store a large amount of data via cryptographic hashes. Merkle trees make it easy to check whether a piece of data is part of the structure in a very short amount of time and computational effort.
- **Receipt**: a side-effect of a transaction that is not stored in the state of the system, but is kept in a Merkle tree so that its existence can be easily verified to a node. Smart contracts logs in Ethereum are kept as receipts in Merkle Trees, for example.



With this in mind, let's take a look at how Ethereum 2.0 would work. We will create a side-chain known as a random beacon chain that stores hashes to main chain blocks in its own blocks. This side-chain will be a full Proof of Stake system implementing Casper FFG and will provide a source of distributed randomness that will allow us to build a sharding system on top of it.

The problems with sharded blockchains become more apparent once we consider that possible attacks on the network. A major problem is the idea of a Single-Shard Takeover Attack, where an attacker takes over the majority of collators in a single shard to create a malicious shard that can submit invalid collations. How do we solve this problem?



1% Attack

“ In 100 shards system, it takes only 1% of network hash rate to dominate the shard. ”

The Ethereum Wiki's Sharding FAQ suggests random sampling of validators on each shard. The goal is so these validators will not know which shard they will get in advance. Every shard will get assigned a bunch of validators and the ones that will actually be validating will be randomly sampled from that set.

To begin, we will deploy a contract on the main chain called the Validator Registration Contract, where people will burn 32ETH in exchange for becoming a validator in this side-chain. The beacon chain will periodically check for registered validators and consequently queue up those that have burned ETH into the contract. This beacon chain will serve as a coordination device for a sharding system, as it will allow for distributed pseudo-randomness that will be critical for selecting committees of validators on shards. The source of randomness needs to be common to ensure that this sampling is entirely compulsory and can't be gamed by the validators in question.

On each shard, we would have nodes called proposers that would be tasked with creating a cross-link on the beacon chain, which is a specific structure that encompasses important information about the shard in question.

These cross-links are like mini-descriptions of the state and the transactions on a certain shard.

A typical cross-link would tell us the following information:

- Information about what shard the collation corresponds to (let's say shard 10).
- Information about the current state of the shard before all transactions are applied.
- Information about what the state of the shard will be after all transactions are applied.
- Signatures from at least $2/3$ of all collators on the shard affirming shard blocks were legitimate.

What about if a transaction happens across shards? For example, what if I send money from an address that is in shard 1 to an address in shard 10? One of the most important parts of this system is the ability to communicate across shards, otherwise we have accomplished nothing new.

An initial idea is use the concept of receipts for this system to work. Raul (Address on Shard 1) Wants to Send 100 ETH to Jim (Address on Shard 10)

- A transaction is sent to Shard 1 that reduces Raul's balance by 100 ETH and the system waits for the transaction to finalise.
- A receipt is then created for the transaction that is not stored in the state but in a Merkle root that can be easily verified.
- A transaction is sent to Shard 10 including the Merkle receipt as data. Shard 10 checks if this receipt has not been spent yet.
- Shard 10 processes the transaction and increases the balance of Jim by 100 ETH. It then also saves the fact that the receipt from Shard 1 has been spent.
- Shard 10 creates a new receipt that can then be used in subsequent transactions.

This Sounds So Complex for Solidity Devs and Ethereum Users to Understand! How Will We Educate Them on Sharding?

They don't need to. Sharding will exist exclusively at the protocol layer and will not be exposed to developers. The Ethereum state system will continue to look as it currently does, but the protocol will have a built-in system that creates shards, balances state across shards, gets rid of shards that are too small, and more. This will all be done behind the scenes, allowing devs to continue their current workflow on Ethereum.

Beyond Scaling: Super-Quadratic Sharding and Incredible Speed Gains

To go above and beyond, it is possible that Ethereum will adopt a super-quadratic sharding scheme (which in simple English means a system built from shards of shards). Such complexity is hard to imagine at this point but the potential for scalability would be massive. Additionally, a super-quadratically-sharded blockchain will offer tremendous benefits to users, decreasing transaction fees to negligible quantities and serving as a more general purpose infrastructure for a variety of new applications.

The ultimate ideology of educating Zelaa's stakeholders and readers is to make them understand the level of architecture and our technical strength in terms of the blockchain that we currently have within our system. Ethereum to Ethereum 2.0 will only enhance the blockchain and make it a robust and fast processing blockchain in the universe.

ERC Elements

In 2015, Ethereum issued technical specifications for tokens on the Ethereum blockchain. Tokens that conform to these specifications are known as ERC20 tokens. (ERC stands for Ethereum Request for Comments.) In essence, ERC20 tokens are smart contracts that run on the Ethereum blockchain. While ERC20 tokens function within the framework set by the Ethereum team, the framework is broad enough to simultaneously allow developers considerable flexibility in the design and function of the tokens. Most tokens created through ICOs on Ethereum are ERC20 compliant.

The ERC20 standard has 6 functions and 2 events. The standard was created to enable interoperability across applications, exchanges, and interfaces. The functions describe how tokens can be transferred and how token-related data can be accessed. The events lay out formatting guidelines for transfers and approvals. Smart contracts on Ethereum, including all ERC20 contracts, are written in Solidity.

```

contract ERC20 {

    // 1. Gets the total token supply
    function totalSupply() constant returns (uint totalSupply);

    // 2. Gets the account balance of the account identified by 'address_owner'
    function balanceOf(address _owner) constant returns (uint balance);

    // 3. Sends '_value' amount of tokens to the '_to' address
    function transfer(address _to, uint _value) returns (bool success);

    // 4. Sends '_value' amount of tokens from the '_from' address to the '_to'
    // address
    function transferFrom(address _from, address _to, uint _value) returns (bool
    success);

    // 5. Approves '_spender' to withdraw the '_value' amount from your account; this
    // function can be called multiple times until the value of your account is 0. each
    // time this function is called it overwrites the current allowance with '_value'
    function approve(address _spender, uint _value) returns (bool success);

    // 6. Returns the amount that '_spender' is allowed to withdraw from '_owner'
    function allowance(address _owner, address _spender) constant returns (uint
    remaining);

    // 7. This event is triggered whenever tokens are transferred
    event Transfer(address indexed _from, address indexed _to, uint _value);

    // 8. This event is triggered whenever 'approve (address _spender, uint _value)'
    // is called
    event Approval(address indexed _owner, address indexed _spender, uint _value);

}

```

Description of the 8 various components that make up the ERC-20 token smart contract. Each contract includes 6 functions and 2 events.

Customisation :

ERC20 tokens can be customised to enable to following features:

1. Automatic buying and selling: you can peg the token's value to that of another token or currency by creating a fund that automatically buys or sells tokens to maintain the balance.
2. Auto refill: transactions on the Ethereum blockchain require payments to miners in 'gas'. You can program your token to auto-refill gas for future transactions once if it falls below a certain level.
3. Adding a central mint that can change the number of tokens in circulation: this could be useful if your token mirrors or simulates government currencies.
4. Freezing tokens: if instructed to do so by a regulatory body, you can freeze the tokens owned by that user and unfreeze them when required.
5. Proof of work: you can tie your token supply to the supply of Ether by programming a contract to run "merged mining" with Ethereum. A miner who finds a block in Ethereum then also gets a predetermined number of your tokens as a Block Reward.

DISTRIBUTION

Private Distribution of ZPAE

The distribution of ZPAE was done after our successful launch on top of the Burj Khalifa at an exclusive invite-only event which was attended by the royal family offices of Sharjah, Abu Dhabi and Dubai, the event was also attended by the top influential business personnels of Dubai and key government representatives.

We privately distributed ZPAE towards strategic alliances and partnerships with key people and royals that we now have onboard.



Shaping UAE thru Crypto

United Arab Emirates comprises of a 54 million people population and makes for one of the most rapidly growing economy and country on the planet which has changed drastically in recent decade, having a strong vision for giving the best to the people who live in the Emirates.

With a \$3.46 Trillion GDP and more than \$100 billion invested into transforming financial technologies just the last year, Dubai continues to prove that it is one of the finest and active financial hubs around the globe which welcomes and boosts innovation.

ZPAYae understands that perspective and works to spread the power of blockchain based transactions around the Gulf by making it more accessible for people and to simplify the process for them and bridge the gap between traditional spending of fiat and crypto.

Digital Mode of Exchanging Value

In an era of virtually active communities, leveraging the major phenomena of the 21st century is a crucial segment and aspect of the ZPAYae ecosystem. Especially taking the drive from fiat to virtual currencies - our products, ecosystem, distribution of assets and the decentralised automation of processes is an ultimate mandate. We often try to hinder and restrict physical intervention in our product approaches.

The convergence between the physicality and the virtuality of the product defines our ideal strategy to leverage digitalisation all over the Arab Emirates.

Therefore ZPAE is an ideal cryptocurrency for Dubai, Abu Dhabi, Sharjah and other parts of the Arab Emirates.

PRODUCTS DRIVEN ECOSYSTEM

Approach

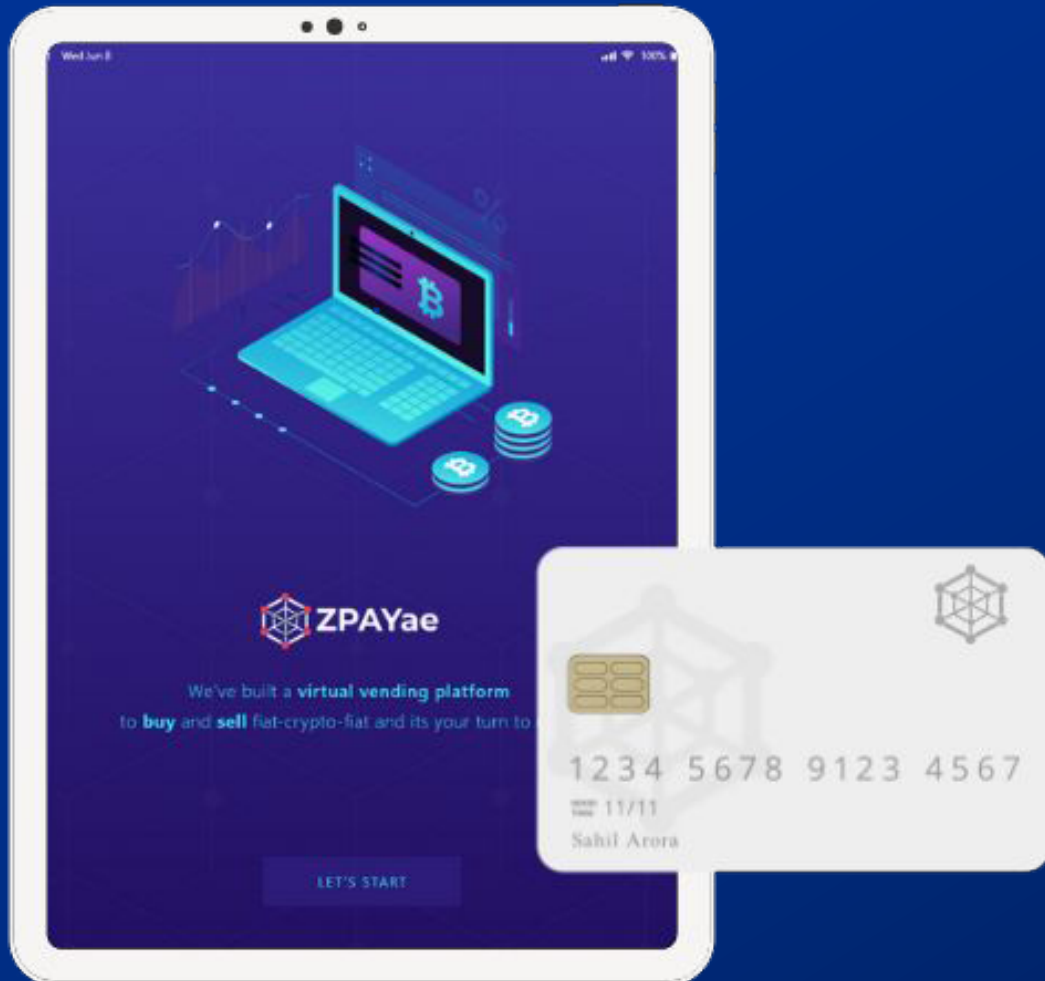
At ZPAYae, we are building products and platforms that transform your crypto-assets into a digital token, ZPAE. We call it “crypto-assets” because major use of virtual currencies today is not mainstreamed to a global extent and therefore is often traded on exchanges to earn ROI. Transforming it into a cryptocurrency is basically when we make your virtual currencies usable and spendable across the world so that it has increased utilities and you not only keep it as an asset but as a mode of payment in daily use. In UAE, we are penetrating the entire merchant market by targeting acceptance of ZPAE at high transactional volume segments such as retail, automobile and real-estate to start off with.

ZPAYae Point-Of-Sales

A Simple POS device to accept ZPAE

Anybody can pay for things they wish to buy using ZPAE on our physical POS terminals at retail stores/cafes/hotels etc using their ZPAYae Crypto Debit Card

- Select from a wide range of curated merchants to buy products from using ZPAE.*
- As we build a large network of our POS terminals, we make it more accessible to the customers by being available at top public places around UAE.*
- Fast processing and almost instant credit of value to merchants and smooth transfer of ZPAE from your wallet at the time of purchase.*
- Users need very basic identity proof such as a driving license or a passport to perform a quick Know-Your-Customer formality to start using the ZPAYae Debit Card.*



The platform works by a decentralised admin panel that is offered to every operator on which the operator connects a hot wallet and sets a transaction fee which is synced real-time on the POS terminal for that specific device.

ZPAYae Debit Card

ZPAYae crypto-centric debit card works like any traditional Visa or MasterCard but it allows you to spend your ZPAE at our ZPAYae POS terminals by a tap, swipe or chip in.

Our physical card syncs with our mobile wallet for users to let them manage their spending of ZPAE and to top-up the card, convert fiat to ZPAE and more such activities.

The ZPAYae debit cards will be acceptable overall in Dubai by end of 2020.



EXTERNAL EXCHANGES



EMIREX
إِمْرِكْس

STEX

SIMPLIFIED WAY OF STORING AND USING WEALTH

ZPAYae at the forefront makes it decentralized and easier to store, share or use your wealth in the format of a cryptocurrency that not only allows you to transfer AED in a click but also grows your wealth substantially as the cryptocurrency moves up in value.

We are growing rapidly daily across United Arab Emirates as we are partnering with royal offices and roping in key business people to enable a smooth drive for us to deploy and build our utility presence around the Gulf.

This is one of those times when we see a convergence between physical and digital money and the transformation of it will be seamless and iconic.



The Digital Currency of Royalty

zelaapay.ae