Shadow DNA Litepaper v1.0.0

Anonymous Asset Layer on Polygon

Shadow DNA website:

https://shadowdna.github.io

Shadow DNA contract address:

0xc78e8e78829f8ec4207009001659030f2a3ea6e

Shadow DNA ticker(symbol): **SHADNA**

Shadow DNA chain(network) name: **Polygon PoS**

Shadow DNA chain(network) id: **137 (0x89)**

Table of Contents

Shadow DNA Litepaper v1.0.0 1

- **Project Introduction** 3
- **Token info** 5
- **Transparency** 5
- **Website - Shadow DNA WebUI** 6
- **Socials** 6
- **Shadow mechanism** 7
- **Faucet** 9
- **Tokenomics** 9
- **Roadmap** 10
  - **Journey1** 10
  - **Journey2+** 10

How to use Shadow DNA dapp 11

- **PartA1- Generate Shadow Account(ID)** 11
- **PartA2- Deposit to any Shadow Account(ID)** 12
- **PartB1- Withdraw from Shadow Account** 13
- **PartC1- Check Status of Shadow Account** 14
- **PartC2- Check Assets in Shadow Account** 14
- **PartD1- How to Generate Shared Shadow Account** 15
- **PartD2- How to Init Distribution for a Shared Account** 16
- **PartE1- Setup Proxy Shadow Account** 17

Project Introduction

- Have you ever wanted to run a web3 business within your partner anonymously and safe?
- Have you ever wanted to receive money/crypto while you don’t want to expose your real wallet address?
- Have you ever needed a place to sell any crypto directly and anonymously?
- Have you ever wanted a shared account on the blockchain with your partners to handle all received money/crypto according to your shares? For example Alice,Bob and Charlie own a business, Alice owns 50%, Bob owns 35% and Charlie owns 15%, so they need an independent tool to handle all received money always according to their share-cuts automatically and safe and onchain. So Alice,Bob and Charlie generate a Shared Shadow Account according to their cuts and then leave the rest to the application. Yes that’s what we want to offer you.
- Have you ever wanted to have an anonymous blockchain based bank which handles sells and receives for you while you are enjoying your day? Totally automate and always available for you and your customers at any time
- Do you want to keep your money/assets somewhere safe and totally under your control for anytime, without any limitation?

The answer to above questions is Shadow DNA.

And it is launched on the one of EVM networks, Polygon chain. Polygon PoS is our mainnet.

The project is already alive & deployed on Polygon mainnet. All source-codes are uploaded on shadna repo github.

Honestly, I'm the only team-member at this time(Feb2026), Yes I'm the founder and good in backend programming and finance. I did the hard-parts alone, coding a flawless smartcontract, The rest things such as WebUI and Graphics can be done by tools(AI,…).

Shadow DNA contract is upgradable. I made it upgradable because obviously I have big plans in longterm for our project. I might get some help in future from AI-model-coders to improve WebUI/Graphics because its totally safe to use AI for

UI/Graphic, no harmful bug happens. The important things are core and contract which as I told you earlier its done and already you may use it.

Doing most of the job by myself is actually better than hiring a group, because I do NOT want to see any bug/flaw on our smart contract. A perfect smartcontract can guarantee to work for good!

zk can wait. Shadow DNA is here to fill this gap in a simple way. In future when zk get fully deployed on all evm mainnets, then thanks to the upgradable structure, we can upgrade Shadow DNA (if needed) to have an extra layer of anonymity in Shadow DNA too.

You may wondering why I chosen Shadow DNA. Your wallet is your DNA and our app(Shadow DNA) just needs a shadow from your wallet to get mapped, no wallet-private-key shared/usage!

Your assets are only & only under your control, exactly self custody.

I suggest you to read Shadow mechanism section at below, to get familiar how Shadow DNA works.

Token info

- Shadow DNA contract address is: 0xC78E8E78829F8eC42070090016590300F2a3eA6e
- Symbol is SHADNA
- Mainnet is Polygon chain (chain id is 137 in decimal, 0x89 in hex)
- Max token supply is 300,000,000,000
- Token decimal is 18
- Launch date: 2026/Feb
- Shadow DNA smart contract is upgradable
- SHADNA token in Polygon explorer: 0xc78e8e78829f8ec42070090016590300f2a3ea6e
- Multiple Apps and Features will be added soon

Transparency

Contract codes are fully released for public and also source-codes verified on Polygonscan website officially.

Shadow DNA contract(SHADNA token): 0xc78e8e78829f8ec42070090016590300f2a3ea6e

Facets List:

- ERC20Facet: 0xf97376248aF19CcDa1DDEaFc0b937E838b4340b6
- AdminFacet: 0x1f549926d339EBb83B9605F58A4463e96a65931a
- ViewParamsFacet: 0x28dB59F6DaA71a9eACeaAaE6e2C127900DE1683d

Website - Shadow DNA WebUI

https://shadowdna.github.io/

Socials

- On Github: https://github.com/shadowdna/shadna
- On X(Twitter): @shadna_token
- On Telegram: @shadow_dna
- On Medium: https://medium.com/@shadowdna

Shadow mechanism

- Shadow account creation is a bit similar to Ethereum Address(account) generation. It works fully offline, just on your device.
- In simple, your wallet address + your new Auth as passphrase + fixed salt number are combined and generates a 256bit hash which is called Shadow ID. So each Shadow ID is related to the given wallet address at the generation process. your wallet addresses never saved on anywhere during Shadow generation. Nobody can guess the real wallet address behind of Shadow accounts. The only way to findout the real owner wallet address of a Shadow account is when a Shadow-account owner do withdraw, but it is still not easy, I'm going to talk about this at the end of Shadow mechanism, here.
- Shadow mechanism is responsible to handle all accounts totally on the blockchain. No third party is here. No off-chain process. Everything is fully handled by the Shadow DNA smart contract.
- Every Shadow account is anonymously and cryptographically mapped to one/multiple real wallet addresses, while nobody knows about it because of its hash mechanism(one-way encryption) to generate an ID.
- A Shadow account ID is a 32bytes (256bit) hash which is generated from a wallet address and an Auth phrase. So only the real owner of Shadow account can access/withdraw the assets. Wallet address and Auth phrase NEVER saved anywhere, so nobody knows anything about it!
- In Shadow mechanism if your Auth phrase get exposed/leaked/stealed, then still NOBODY can steal your assets! Because each Shadow account mapped and can be only withdraw to its owner wallet address only. YES, its true, thanks to the Shadow mechanism.

Generate ID generates a Shadow account depends on what you need:

- If you want to map one wallet address(receiver) then use Personal Shadow ID section
- If you want to map multiple wallet addresses(receivers) then use Shared Shadow ID section, for example: you and your partner should own 40% and 60%, so everything must be handled correctly to each wallet address, automatically and safe on the blockchain.

Technically a Shadow ID is a 256bit hash and can be generated totally offline by other tools too.

If you are a developer or willing to generate Shadow ID by yourself, then you need follow the algorithm according to js codes in WebUI (github.com/shadowdna/shadowdna.github.io)

To withdraw your assets you need to pay fee via $SHADNA token (Shadow DNA), currently the fee is configured to 0(ZERO), and i have plan to keep it zero for a long-time.

According to internal Shadow mechanism, any paid fee goes to the internal liqPoolToken pool. There is also an internal burn mechanism which is currently configured at zero(no burn). liqPoolToken pool has many uses in future.

SHADNA token going to have many other utilities too since I'm developing and adding more DApps on Shadow DNA.

The only possible way to expose the address behind a Shadow account:

You know each Shadow account is generated by hashing a compination of WalletAddress+Auth+FixedSalt and result is a 32bytes(256bit) ID, called Shadow ID.

During deposit into any Shadow ID, Its totally impossible for everyone to guess the real wallet.

During withdraw, you are sending Auth by your wallet address, so you are revealing Auth+WalletAddress. If anyone want to know which Shadow ID(account) is doing withdraw, then they need to compute hash of WalletAddress+Auth+FixedSalt everytime, and then they can realize who did the withdraw, The good news is I built a new feature to protect you for this. Shadow Proxy. You may checkout Setup Proxy Shadow Account guidance in below to find more.

Faucet

Faucet mechanism makes our community great.

Shadow DNA provides the onchain Faucet mechanism to give a small amount of $SHADNA token to whoever wants, automatically.

Just go to: https://shadowdna.github.io and then Connect Wallet(connect and choose your wallet to receive), and then Service Operations>Faucet and claim it.

The Faucet uses an internal pool called faucetPool. Faucet pool balance can be increased by anyone from Donate to Faucet section on WebUI.

Tokenomics

- 020B Airdrops & Rewards & Faucets in longterm, (rewardfund)
- 040B Team in longterm, (teamfund)
- 040B preSale_onchain, (presalefund)
- 050B DEX_listing, (dexfund)
- 050B Exchange(CEX)_listing, (cexfund)
- 100B Ecosystem-growth-longterm(developments, products, cooperates, campaigns, infrastructure, ambassadors, staffs), (treasuryfund)

Total 300B

Roadmap

*No specified time/period for each phase since we can not control timeframes due many parameters which are not entirely under our/your control, such as governments/companies/individuals conflicts and policy changes.

*Our objective in the roadmaps are to reach the goal while the exact time can not be measured.

*I am doing almost everything on my own and actually I'm enjoying. I don't need any fund/money for now, thanks I am good, so my plan is just develop more dapps for a while. no presale going to happen anytime soon, maybe 2026Q2+ or later. So if you are willing to own some $SHADNA token then I strongly suggest to do not lose the Airdrop events and Faucet.

*I'm NOT cooking a meme here, a REAL PROJECT takes time.

Journey1

- (DONE)Social Launch - basic
- Updating Documents on Github - daily/weekly/monthly
- (DONE)Releasing Shadow DNA smartcontract codes for public
- WebUI/Website/UX improvement[if needed]
- Random small Airdrops to active accounts, starts from 2026/Feb/11
- Faucet phase1 with 10,000,000 $SHADNA for everyone, no limit per wallet, starts from 2026/Feb/10
- Main big Airdrop phase1: 20,262 $SHADNA for first 10,000 users, date TBA
- Designing about upcoming features for Shadow DNA

Journey2+

- Updating docs[if needed]
- Updating WebUI[if needed]
- LetsP2P v1.0, Your Web3 Business, details TBA
- Play Win Earn v1.0, details TBA
- …[TBA]

How to use Shadow DNA dapp

Here is the user manual about how to use Shandow DNA dapps.

PartA1- Generate Shadow Account(ID)

- Step1- Visit Shadow DNA WebUI on https://shadowdna.github.io and go to DApp Center page, or you may also download and deploy(on your host) since WebUI is fully open-source.
- Step2- Click on Connect Wallet, although to just generate Shadow account you don't need to be online, so you may skip step2.
- Step3- To generate Shadow account, go to the Main Menu section, and click on Generate ID.
- Step4- You can generate two types of Shadow accounts(ID) here, Personal Shadow ID and Shared Shadow ID. for now I guide you based on Personal Shadow Account.
- Step5- At Personal Shadow ID section, you need to put your wallet address as Owner wallet address and choose a proper Auth phrase. If you didn't step2 then you need to write your wallet address in Owner wallet address manually and make sure you really have access to that wallet address for doing Withdraw later, because only owner can do the withdraw. DO NOT forget Auth phrase, there is no way to recover your assets/account since Auth is not saved anywhere!
- Step6- Click on Generate button and then get your ShadowID. You may give your shadowId to anyone, they can deposit[any erc20 token/native POL] into the given shadowId while the real address of owner remains hidden to depositors. Only owner(given address in step5) can do withdraw.

Notes

- Note1: Technically you have a private onchain-bank and your ShadowID can be accessed only by correct owner(wallet address) and correct Auth phrase.
- Note2: In step5, if you put another wallet-address or Auth, then you will get a different(new) Shadow account(id), so do not forget the given data.

- Note3: If your Auth gets exposed(stealed,leaked) then they(abusers) can NOT do withdraw because they need access to your wallet too. Withdrawal only can be done by the owner wallet address according to Shadow mechanism. So keep your wallet safe, always.
- Note4: Use different Auth for same wallet address if you need to have a new Shadow Account.
- Note5: If you forget Auth, or lose access to your mapped wallet, then you LOSE your assets forever, there is no other way to recover it.
- Note6: You may generate unlimited Shadow accounts by using different Auth phrases for same wallet address.
- Note7: Each shadow id starts with '0x' and follows by 64 hexCharacters(0-9,a-f), like this: 0xa1074e1b9465c7690c4aa657dc726ad335a255d430247bcd9b8a42b31449ece7.

PartA2- Deposit to any Shadow Account(ID)

- Step1- Before continue make sure receiver Shadow ID is correct because there is NO way to recover if you deposit into a wrong Shadow account!
- Step2- Visit Shadow DNA WebUI on https://shadowdna.github.io and go to DApp Center page.
- Step3- Click on Connect Wallet to connect and choose your wallet address.
- Step4- Go to the Main Menu section, and click on Deposit button.
- Step5- Input Shadow ID of receiver in Shadow ID.
- Step6- Now fill the Asset address with token address(if you want to send an ERC20 token). If you want to send native POL coin(not erc20 token) then just input 0x00 in Asset address.
- Step7- Input amount needed to be send by you, for example: 0.014
- Step8- Since users during Withdraw from shadow account must pay some $SHADNA as a withdrawal fee to contract(we call it Shadow Fee internally, and the fee amount is configurable), so Depositor may choose to sponsor those fee(then the user during withdrawal has no need to pay fee anymore). For default just choose No (No=receiver pays fee during withdraw, Yes=depositor sponsers withdrawal fee).
- Step9- Click on Deposit button.

Notes

- Note1: Depositor does NOT need to pay shadow fee($SHADNA) while can be a sponsor for it, totally optional.

PartB1- Withdraw from Shadow Account

- Step1- Visit Shadow DNA WebUI on https://shadowdna.github.io and go to DApp Center page.
- Step2- Click on Connect Wallet to connect and choose your wallet address.
- Step3- Go to the Main Menu section, and click on Withdraw button.
- Step4- After you connected your wallet then you need to fill the correct Auth phrase here. Smart contract(Shadow DNA) combines and match Auth and connected wallet address(msg.sender) automatically on chain to get your ID.
- Step5- Type the address of token in Asset address to withdraw from your Shadow account. If its native POL coin(not erc20 token) then just input 0x00.
- Step6- Type the amount of asset to withdraw in Amount, for example: 0.014
- Step7- Click on Withdraw button.

Notes

- Note1: Current Withdraw fee(Shadow fee) is set to 0(ZERO), and I will keep it on zero for a long-time.
- Note2: Withdrawal needs to pay Shadow fee if Shadow fee is required.
- Note3: If Shadow fee is required, then system automatically takes it from your Shadow Account(first try), or your wallet(second try).
- Note4: If Shadow fee is required, then according to Shadow algorithm the Shadow fee amount can NOT be so big, to make sure nobody stuck due lack of $SHADNA balance, a fair rule.
- Note5: Nobody can withdraw from your shadow accounts. Only someone who has access to correct wallet address(private key of your wallet) to do withdraw via correct Auth, so keep your wallet safe, always.

PartC1- Check Status of Shadow Account

- Step1- Visit Shadow DNA WebUI on https://shadowdna.github.io and go to DApp Center page.
- Step2- Click on Connect Wallet to connect and choose any wallet address.
- Step3- Go to the Main Menu section, and click on Check Account button.
- Step4- At Check Status section, input any Shadow ID to check its overall status including activity status, proxy, score.
- Step5- Click on Search button to view status of the shadow account.

Notes

- Note1: Everyone can use Check Account to view the stats for any Shadow account.

PartC2- Check Assets in Shadow Account

- Step1- Visit Shadow DNA WebUI on https://shadowdna.github.io and go to DApp Center page.
- Step2- Click on Connect Wallet to connect and choose any wallet address.
- Step3- Go to the Main Menu section, and click on Check Account button.
- Step4- At Check Assets section, input Shadow ID, and Asset address(token address for erc20, 0x00 for native POL coin).
- Step5- Click on Search button to view the balance of asset in shadow account.

Notes

- Note1: Everyone can use Check Account to view the stats for any Shadow account.

PartD1- How to Generate Shared Shadow Account

Let me tell you why you might need this, consider this scenario: Four partners decide to run a business, each one has shares(percent) on it, partner1:15%, partner2:20%, partner3:30%, partner4:35% , so every paid money from customers should be always divided correctly between the partners according to their shares. Dividing manually always leaves some doubts and risks suchs as errors or argues, who divides the money? someone is cheating to others?…

So this is one of best features if you and your partners needed a private shared account which handles the shares/cuts automatic & safe while each receiver real wallet-address remains anonymous.

So the partners doesn't know about the real wallet address of eachother! They just know about percent rate of eachother.

- Step1- Each partner needed to generate a Personal Shadow ID, so each one must follow PartA1- Generate Shadow Account(ID) to generate a personal Shadow account before continue.
- Step2- At Shared Shadow ID section, choose an Auth phrase(shared) for shared account, this is better to be different than the Auth phrase(personal) generated in Step1.
- Step3- Now input each Shadow ID of partners within its Share percent, and click Add to list button, each time, do it for all partners(Shadow accounts).
- (Optional), For Step3, you may also input partners info by paste data in List - Owners & Shares if you already did it before.
- Step4- Click on Generate button.

Notes

- Note1: All partners can share the final list(List - Owners & Shares) to eachother, since whoever has shared Auth and the list, then can do the Distribution to those Shadow accounts.
- Note2: Do NOT forget the list of partners and theirs shares, since its not saved anywhere, and you need it during withdraw.

- Note3: Any change in IDs/Percents/Auth causes to generate a new shared Shadow ID.
- Note4: Distribution can be only done if Shadow accounts and percents and shared Auth are all correct.

PartD2- How to Init Distribution for a Shared Account

Now its time to distribute money from the shared account to the partners according to their shares percent.

- Step1- Visit Shadow DNA WebUI on https://shadowdna.github.io and go to DApp Center page.
- Step2- Click on Connect Wallet to connect and choose any wallet address.
- Step3- Go to the Main Menu section, and click on Share(Distribution) button.
- Step4- Input token address in Asset address if its ERC20. input just 0x00 if its native POL coin.
- Step5- Input correct Shadow ID and Share percent of each parner and click on Add to list, repeat it for all partners(Shadow accounts).
- Step6- Click on Distribute button.

Notes

- Note1: Wrong/Forget about partners info(id/percent), stops distribution, nothing happens, there is NO other way.
- Note2: Distribution can be only done if Shadow accounts and percents and shared Auth are all correct.

PartE1- Setup Proxy Shadow Account

They are a lot of reasons to set a proxy Shadow account on your current account, such as:

- After each withdraw, your real wallet-address might get exposed, so you set a proxy to receive upcoming deposits automatically on a new shadow account anymore.
- You already have many Shadow accounts, and now you just want to forward upcoming deposits to same/new shadow account anymore.
- …

You can setup a proxy shadow account to forward all new incoming deposits from your current shadow account to a new shadow account, automatically forever.

This is a great feature when you have multiple shadow accounts and then decide to gather all upcoming deposits to a single fresh shadow account.

- Step1- Visit Shadow DNA WebUI on https://shadowdna.github.io and go to DApp Center page.
- Step2- Click on Connect Wallet to connect and choose correct wallet address which is related to your current Shadow account.
- Step3- Go to the Main Menu section, and click on Proxy button.
- Step4- Input your current Shadow id in Current Shadow ID which is related to your current connected wallet-address.
- Step5- Input your current Auth phrase of current shadow id.
- Step6- Input your NEW Shadow id in New Shadow ID. You may checkout PartA1-Generate Shadow Account(ID) if you need help.

Notes

- Note1: You can disable proxy by input 0x00 in New Shadow ID, anytime.
- Note2: Old balances/assets wont move to new Shadow account. Proxy only works for upcoming deposits.
- Note3: Multi-step forwarding is NOT supported, checkout below examples(correct&wrong exps) to understand it before continue.

Correct Examples

- You set a proxy on account#A to forward upcoming deposits to account#B.
- You change proxy on account#A to forward upcoming deposits to account#C.
- You have already multiple accounts(#A,#B,#C,#D), so you set proxy for each one(A,B,C) to forward upcoming deposits all into account#D, gathering them all into one account.

Wrong Examples

- You set a proxy on account#A to forward it to account#B, and then set a proxy on account#B to forwarded to account#C again, SORRY, any deposits will be only forwarded from A to B in this scenario, NOT to C anymore, just one-step forwarding, NOT multi-step!

#Remember_Privacy