XSN coin

TPoS Setup Guide

https://discord.gg/cyF5yCA

https://xsncoin.io

Contents

Introduction

What is TPoS?

At its very core, the modern banking system is based on a simple paradigm - 'Trust'. We give our money to banks and they provide us with services in return (deposits, loans, and investments). While we could perform these services ourselves, it has proven much more convenient to use this centralized, trust-based system.

To mitigate the potential for abuse presented by such a global centralized system, decentralized blockchain-based assets (such as Bitcoin) have been introduced. To secure a decentralized network and ensure users cannot double-spend their funds, Bitcoin utilizes a Proof-Of-Work (PoW) algorithm, which requires miners to prove that they've spent a certain amount of computational resources in order to make an attack on the network uneconomical. PoW networks aren't financially ideal as only miners can receive block rewards and transaction fees in return for precious resources, whereas regular users do not see any ROI from holding their coins.

This is where Proof-Of-Stake (PoS) networks come in; the transaction confirmation mechanism shifts from a burden of proof of the expenditure of resources over to total stake held - transactions are confirmed by simple nodes who hold large balances, and the greater the balance the user holds, the more likely they are to receive fees and block rewards. While this significantly reduces the amount of resources required to confirm transactions and effectively allows the average user to see positive ROI on balances held, this system still requires a user to maintain connectivity at all times, to do so via a high-bandwidth connection, and for their wallets to be unlocked 24/7. During any timeframe in which all aforementioned conditions aren't met, the user is skipped by the network and does not receive their fair share of stake rewards.

XSN has devised a solution to the problems being faced by users of decentralized networks today: Trustless Proof-Of-Stake (TPoS). TPoS essentially allows users to own a stake in XSN, a Proof-Of-Stake currency, and have any other node (merchant nodes) do the staking for them using their high-bandwidth continuous connectivity (to ensure maximal rewards distribution) while not having to share any spendable balance or private keys with the node owner. Your funds are yours and yours alone, and will safely and securely grow over time even while you sleep.

To accomplish this, we have created a multi-layered cryptographic architecture that expands the private-public key paradigm, called Triplet-Based Encryption. This three-layered model will

feature a public key, which serves as a public address and stores unspent balances, a private key, which can authorize the spending of a balance stored on the public address it was used to create, and a "shared" key. The shared key is created whenever a user chooses to allow a merchant node operator to stake their funds and its sole purpose is to authorize the staking of a user's balance. It cannot spend or move the balance around; for those the private key is required. Now that a user has a new key that can be used for remote staking only and the private key no longer needs to be disclosed, the concept of trust is once again eliminated, allowing the economics of the XSN network to prosper.
We believe TPoS will be the next stage of evolution in terms of guaranteeing ROI on balances, and our adoption strategy will ensure it becomes the standard across financial services worldwide.

DISCLAIMER:

1- **This guide only works when the XSN wallet is updated to V1.0.6 or later for both parties.**
Please checks with your merchant/owner to make sure both wallets are updated.
Here you can download the latest version:
https://github.com/X9Developers/XSN/releases

2- You should never send your coins to anyone; with TPoS contracts you only hand over the staking permission to a merchant using the TPoS UI in your wallet.

How to be an Owner

To be an owner, it is actually pretty simple.

- Open your XSN wallet, go the TPoS tab on the left hand side of your wallet.
- Input the given Merchant Address (This will be given to you by the merchant)
- Input the amount of coins you wish to stake – remember you need to have 1 extra XSN in your wallet. For instance, you hold 10,001 XSN, you input 10,000 XSN as the stake amount.
- Input the agreed commission amount
- Click on Stake
- Job done, you have just entered into your first TPoS contract.

How to be a merchant

Please note the following assumptions used for this guide:

- You are using a Windows based Operating System (OS) on your VPS and have installed the latest XSN v1.0. 6 or later wallet.
    - Please note - your client must be using the same wallet version as you.

- You can download the latest version from here:

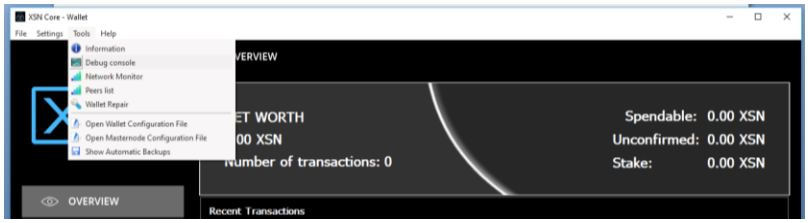
  https://github.com/X9Developers/XSN/releases

Note – If you only want to create a TPoS for your own coins, you can ignore all Controller & remote titles and execute steps 1-9 all on 1 machine/VPS.

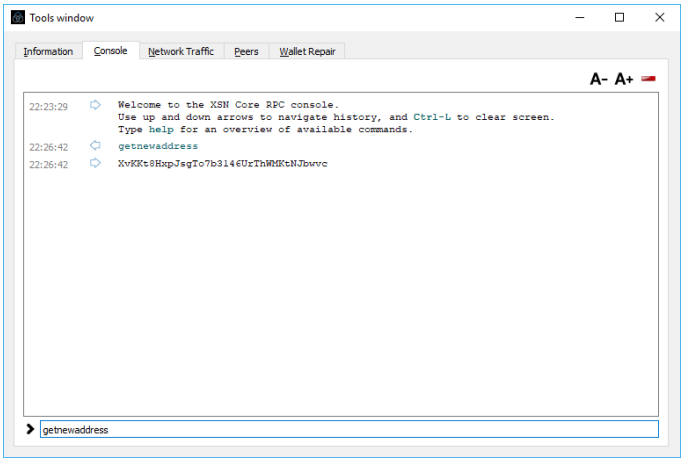
Step 1. – Controller Wallet – Generating your Merchant Address

Open your controller wallet, this is the wallet where you want the commission earned from staking to go to and is usually on your computer, not the VPS.

Once open, you will need to open the Debug Console by using the “tools” option.



Once the Debug Console has opened, type in: **getnewaddress** which will provide you with your Merchant Address that is used for creating a TPoS contract.



Please take note of this address, and copy it into a document such as Notepad.

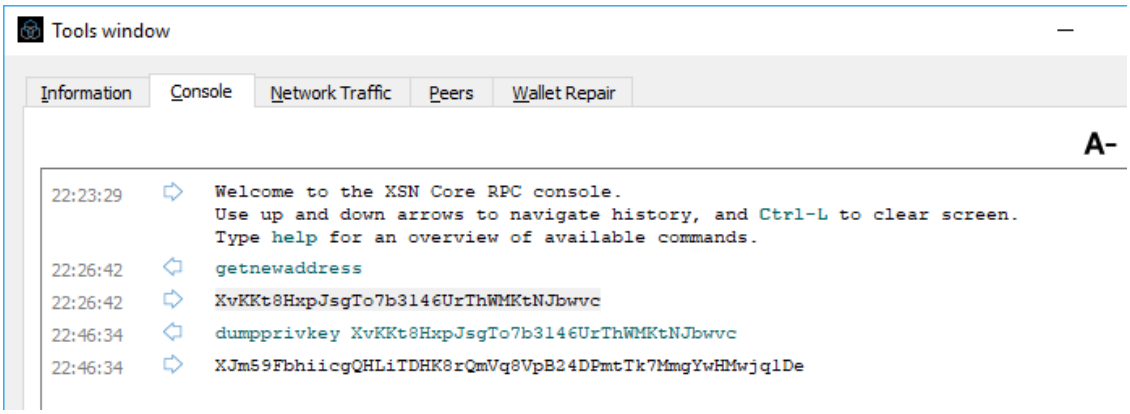
Step 2 – Send your Merchant Address to Client

Send your Merchant Address that you got from Step 1 and send this to the client you are creating the TPoS with.

They will need to create a TPoS contract within their own wallet using the TPoS tab – if they need help, refer to the "How to be an owner section".

Step 3 – Controller Wallet – Generating your Private Key

In your Controller Wallet debug console execute **dumpprivkey followed by the Merchant Address** and copy the output in a notepad/word file.



Step 4 – Wait for Client to Create TPoS contract

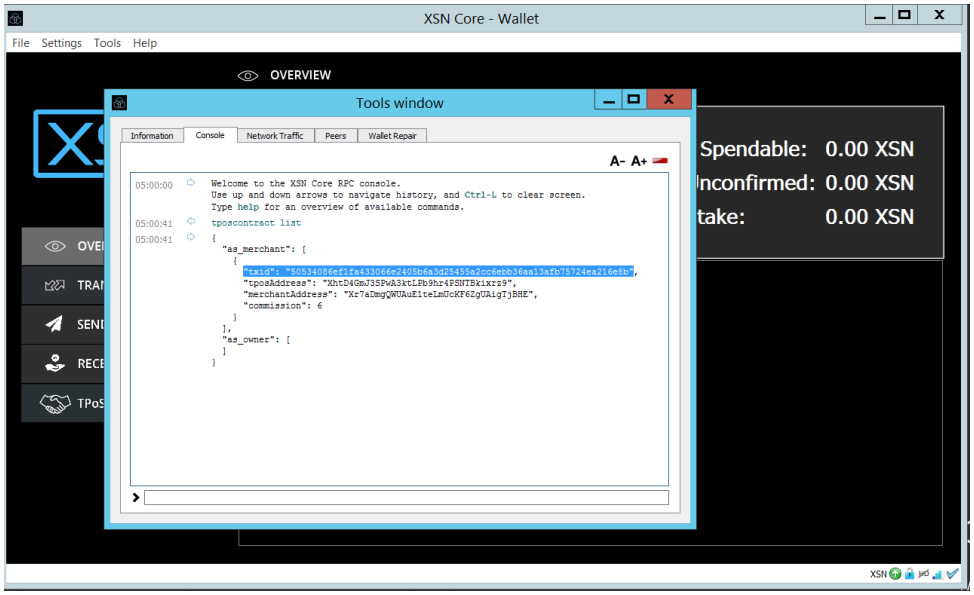
Wait for the client to create the TPoS contract – ask them to confirm once done, or wait for your wallet to send you a notification that you have an incoming transaction.

Step 5 – Controller Wallet – Obtaining the Transaction ID

On controller wallet, in debug console and type in **tposcontract list**

This will provide you with the Transaction ID (txid) of the contract your client has created. Copy this txid to the notepad/word file and keep a record of it!

You can also see your clients address within this if you wish to keep a record of it.

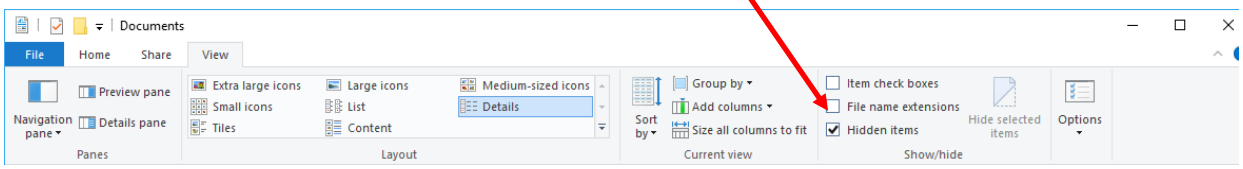


Step 6 – Controller Wallet

You will need to go to the XSNcore Folder, which is usually located as follows:

C:\Users\(the pc name)\AppData\Roaming\XSNCore)

If you cannot find the AppData Roaming folder, you will need to click “View” in your folders, and tick the box saying “Hidden Items” on the right side.



Once you are in the XSNCore folder, you will need to open the merchantnode.conf (right click, and open with notepad). Input the following line:

TPOS1 'merchant node IP':62583 'private key' 'txid'

The ‘merchant node IP’, is the IP address your VPS you will be using.

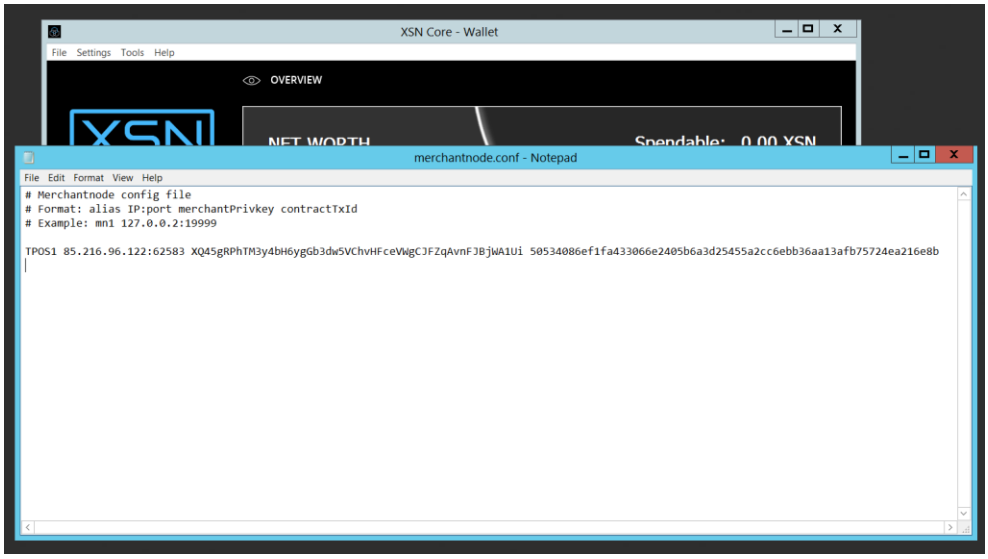
The Private Key was generated in Step 3, the txid was Step 5

If you are creating more than one TPoS contract, you will add an extra line for each one:

TPOS1 'merchant node IP':62583 'private key' 'txid'

TPOS2 'merchant node IP':62583 'private key' 'txid'

TPOS3 'merchant node IP':62583 'private key' 'txid'



Step 7 – Remote Wallet (VPS) – Setting it up for a TPoS

Open your remote wallet then go to the tools open, and click “Open Wallet Configuration File” and input the following text – once inputted, restart your wallet.

rpcuser=long random username
rpcpassword=longer random password
rpcallowip=127.0.0.1
listen=1
server=1

daemon=1

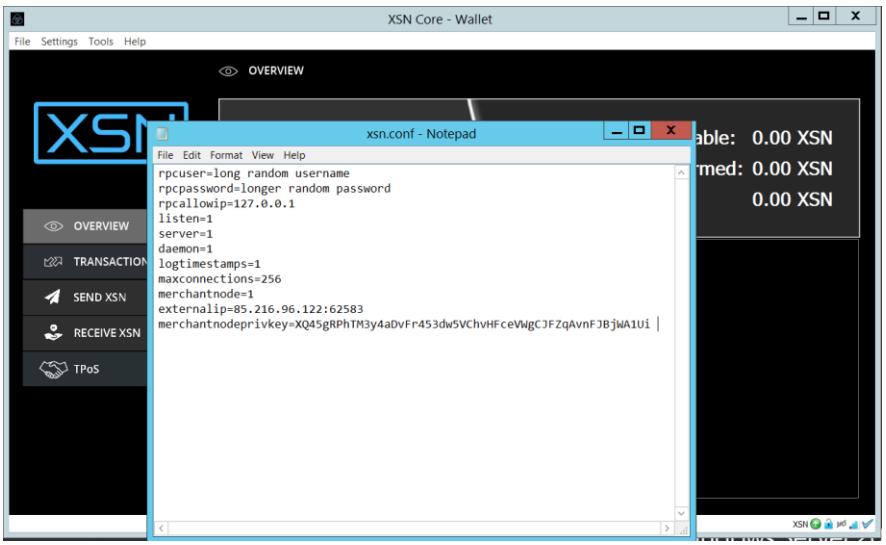
logtimestamps=1

maxconnections=256

merchantnode=1

externalip=’merchant IP’:62583

merchantnodeprivkey=’private key from step 3’



The above will work for **one** TPoS contract, if you want to create multiple TPoS Contracts, you will need to follow the below extra Steps.

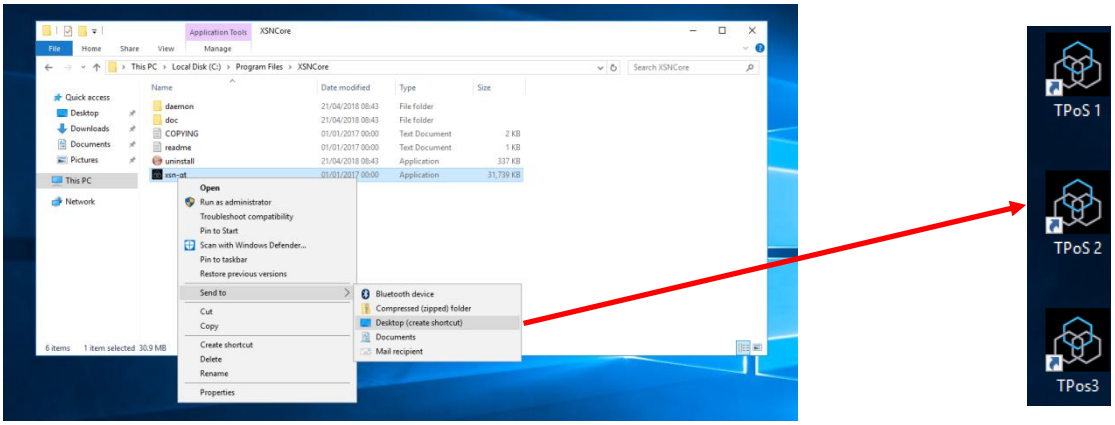
Note: You must have a unique IPv4 for every TPoS contract.

Step 7.1 – Remote Wallet (VPS) – Setting it up for a TPoS – Multiple TPoS

Only do the following steps if you are creating multiple TPoS on the same VPS

Navigate your way to your programe file where you saved the original XSN wallet.

Once there, right click on the xsn-qt file, and then choose "Send to" followed by Desktop. This will create a short cut for you.



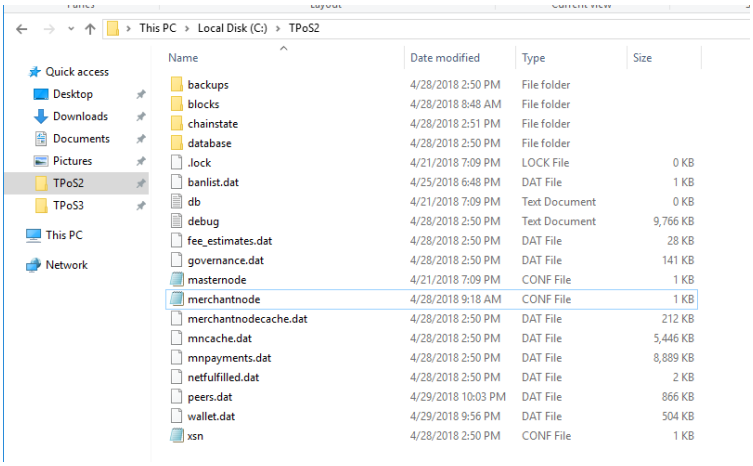
Do this step for every extra TPoS you are going to create – Rename them to keep track of them.

Step 7.2 – Remote Wallet (VPS) – Creating a New Directory for TPoS 2 and above

Create a new Folder on your C:\ Drive, for example C:\TPoS2 (create a new folder location for each TPoS you will run).

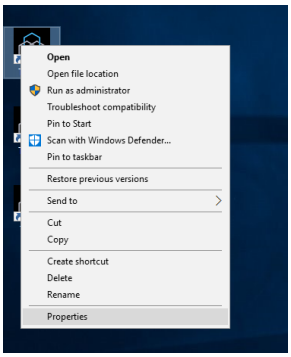
Copy all the files and folders located in, and paste it into your new folder locations above:

C:\Users\(the pc name)\AppData\Roaming\XSNCore)



Step 7.3 – Remote Wallet (VPS) – Changing Director for TPoS2+ Short Cuts

With the shortcuts you created earlier to your desktop for TPoS2 etc. You must right-click on TPoS2, and click on “Properties” from the list of options:

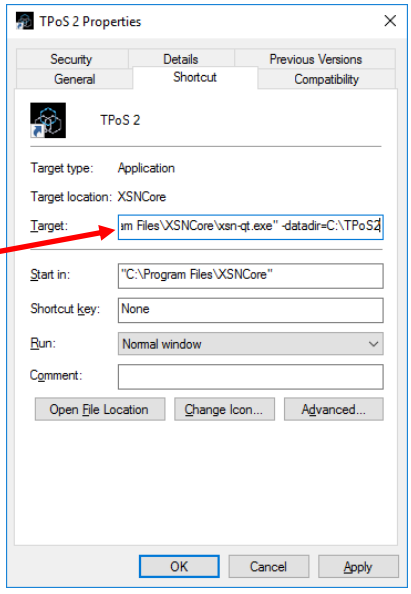


The properties window will now open. You will need to add an extra line on “Target” location, which will link to the folders you created earlier:

…\xsn-qt.exe" **-datadir=C:\TPoS2** (TPoS2 is the name of the folder you would have created)

The target location will now look like this:

"C:\Program Files\XSNCore\xsn-qt.exe" -datadir=C:\TPoS2



Repeat this step for your other TPoS shortcut, just remember to amend the -datadir=C:\.. to the next location.

Step 7.4 – Remote Wallet (VPS) – Multiple TPoS – Config Setting

Open your remote wallet on the shortcut you created for TPoS2, then go to the tools, and click "Open Wallet Configuration File" and input the following – once inputted, restart your wallet.

rpcuser=long random username
rpcpassword=longer random password
rpcallowip=127.0.0.1

rpcport=67854

listen=1
server=1

daemon=1

logtimestamps=1

maxconnections=256

merchantnode=1

externalip='merchant IP':62583

merchantnodeprivkey='private key from step 3'

For TPoS 3, you change the rpcport= to 67855 and so forth.

Remember you need a unique IP for each TPoS!

Step 8 – Controller Wallet

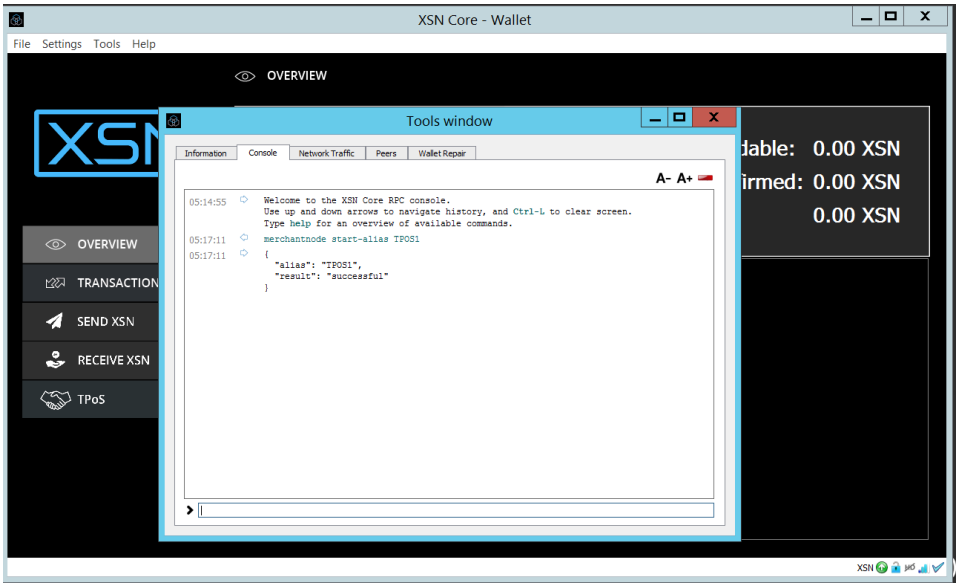
Go back to your controller wallet, but make sure you have restarted this wallet.

Wait for it to finish syncing with the blockchain.

Now, go to tools then open the open debug console and input the following commad:

merchantnode start-alias TPOS1

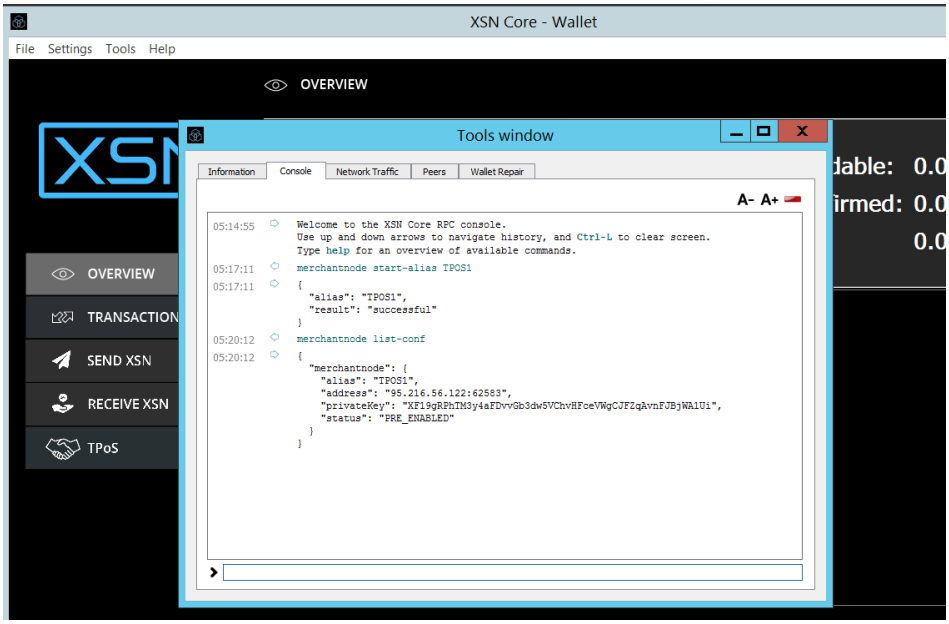
Change the TPOS1 to whatever TPOS you are starting – I.e. TPOS2 or TPOS3



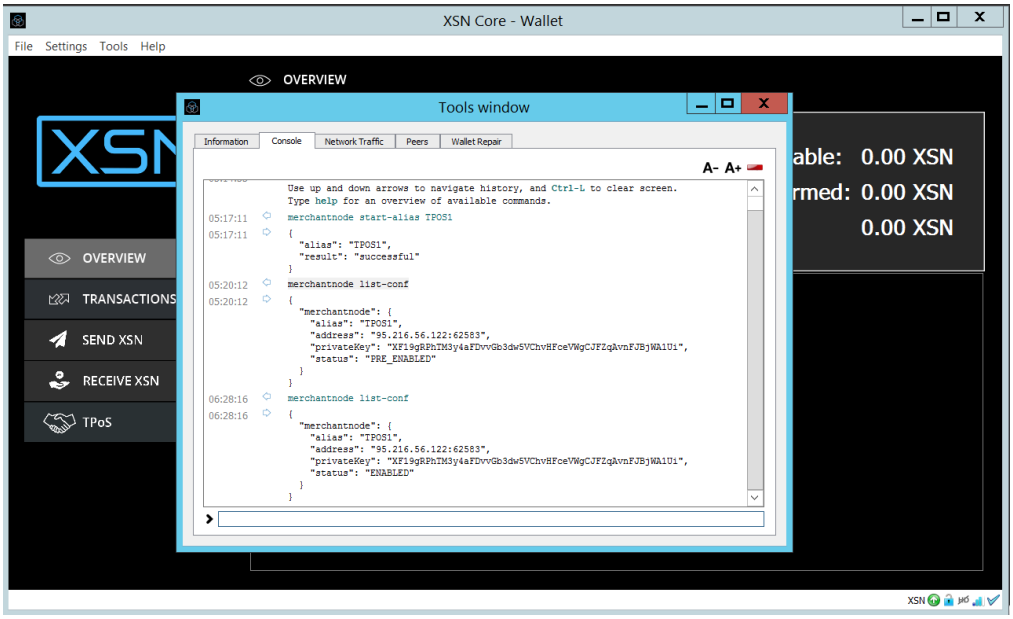
Step 9 – Controller Wallet

Again, in the debug console input **merchantnode list-conf**

The Status will be Pre-Enabled.



You should wait for your contract to get **ENABLED**; it **usually takes 15-30 minutes**.



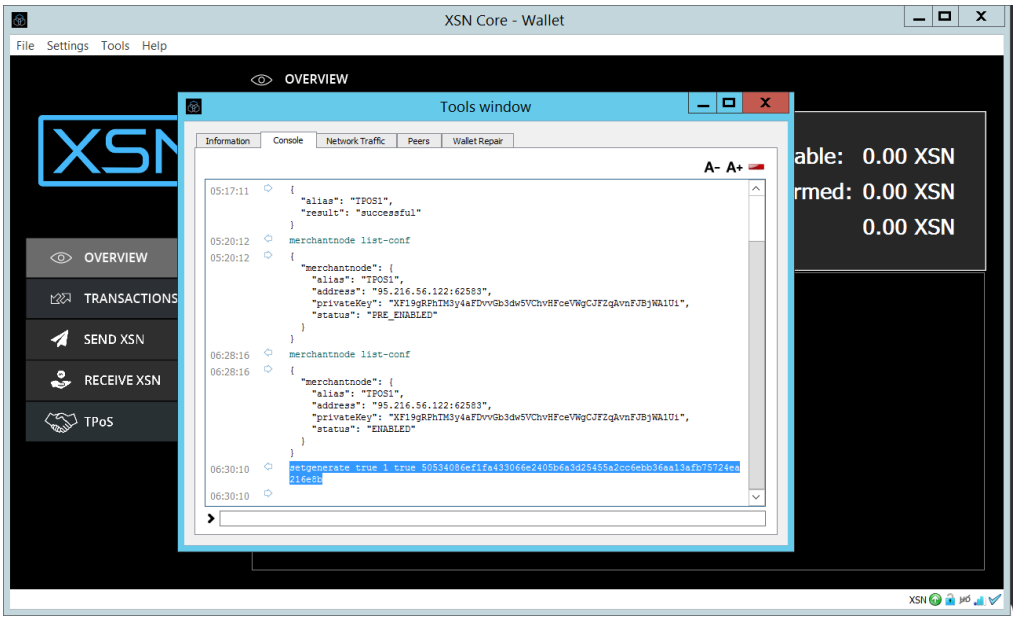
Step 10 – Remote Wallet (VPS)

As soon as your contract gets ENABLED in the Controller wallet, go to your Remote Wallet and input the following command on your remote wallet:

setgenerate true 1 true [‘txid from step 5’]

With this command the merchant node starts staking.

Remember – if you are running more than one TPoS, you will need to enter the right txid for each TPoS Shortcut you created.



Need further help?

Join our discord - https://discord.gg/cyF5yCA if you have any question.