XSN
TPoS Setup Guide

https://discord.gg/cyF5yCA

https://xsncoin.io

DISCLAIMER:
1 - **This guide only works when the XSN wallet is updated to V1.0.6 or later for both parties.** Please check with your merchant/owner to make sure both wallets are updated. You can download the latest wallet version at 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.
3 - This is just a guide and does not imply any guarantee or warranty. Please always back up your wallet and ask questions if you are unsure of anything. If you find an error or an appropriate addition to this guide, please let us know and we will update it. This does not imply any specific return on investment – invest in XSN at your own risk.

This guide is for setting up a TPoS contract in the XSN mainnet on a Windows OS. We have tried to explain this process as simple as possible. The procedure on another OS is very similar.

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 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 check with your merchant/owner to make sure both wallets are updated. You can download the latest wallet version at 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.

3 - This is just a guide and does not imply any guarantee or warranty. Please always back up your wallet and ask questions if you are unsure of anything. If you find an error or an appropriate addition to this guide, please let us know and we will update it. This does not imply any specific return on investment – invest in and use XSN at your own risk.

How to be an Owner

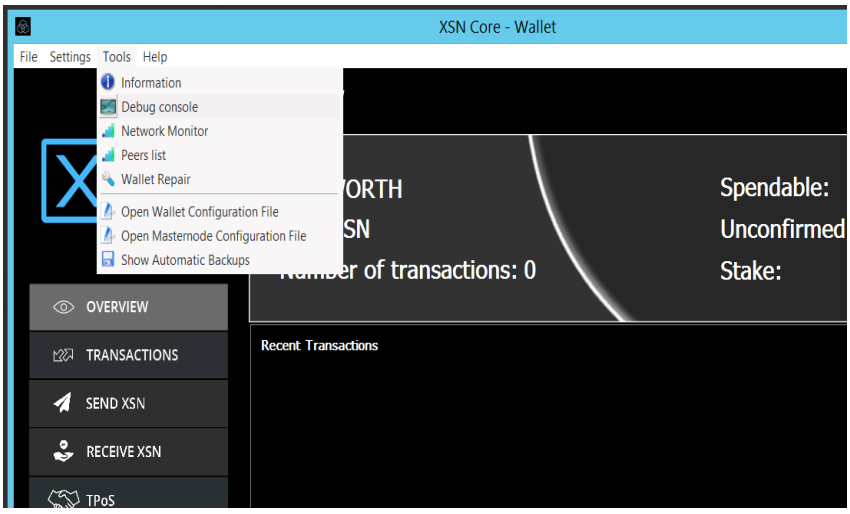
So how to be a coin owner? Input the merchant address (the address that merchant gives you), amount and commission into the inputs in the TPoS UI then click '**Stake**'. This is all you have to do.

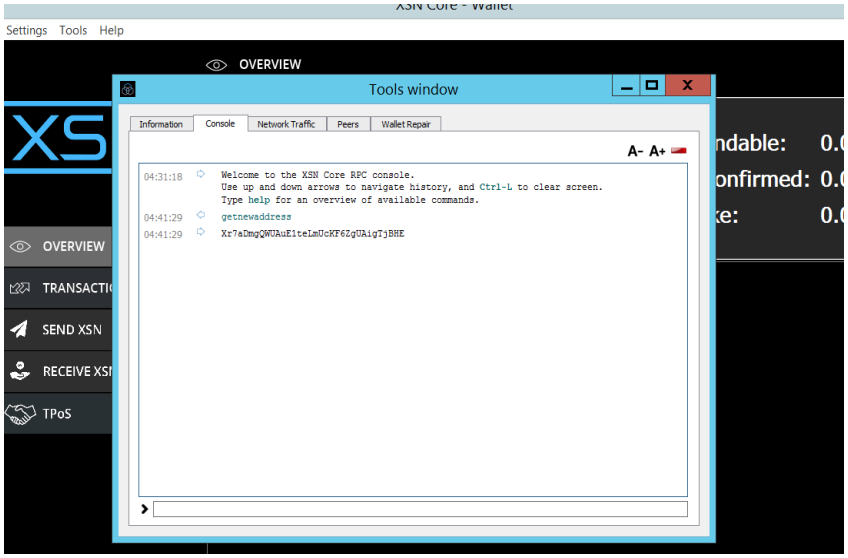
How to be a Merchant

The following guide will use the terms '*controller*' and '*remote*' to refer to wallets. The '*controller*' wallet is the main wallet held by the merchant while the '*remote*' wallet is a node merchant wallet. The '*controller*' wallet can be used to control multiple '*remote*' wallets. If you wish to simply TPoS your own coins and not provide services for others you can ignore the *controller - remote* titles and execute steps 1-9 all on 1 machine/VPS.

Step 1

On the *controller* wallet, create a new address (enter **getnewaddress** in the Debug Console) and copy this address in a notepad/word file.



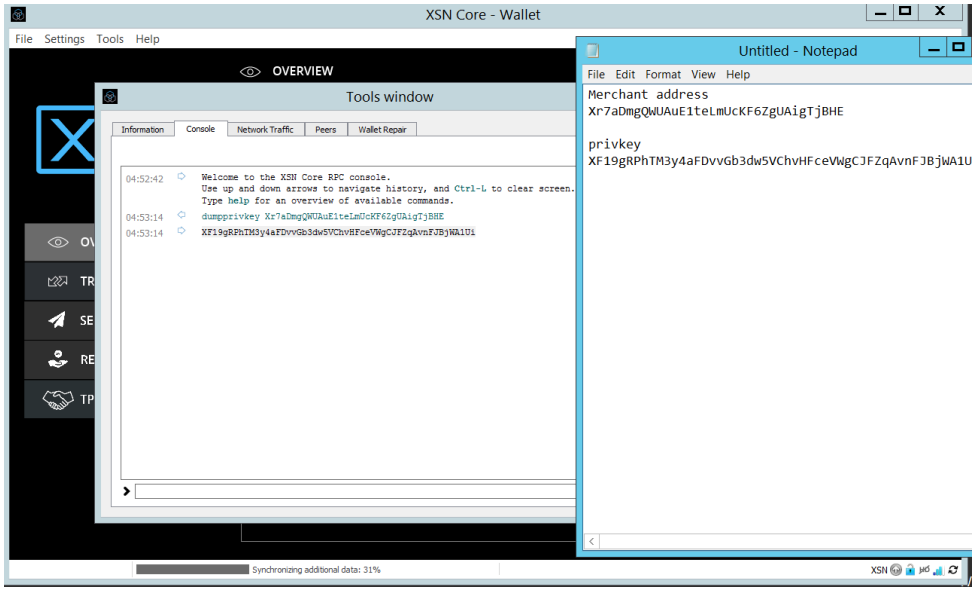


Step 2

Send the address from Step 1 to the coin owner you want to TPoS with, and have him create the contract in the *remote* wallet UI using the address generated in Step 1.

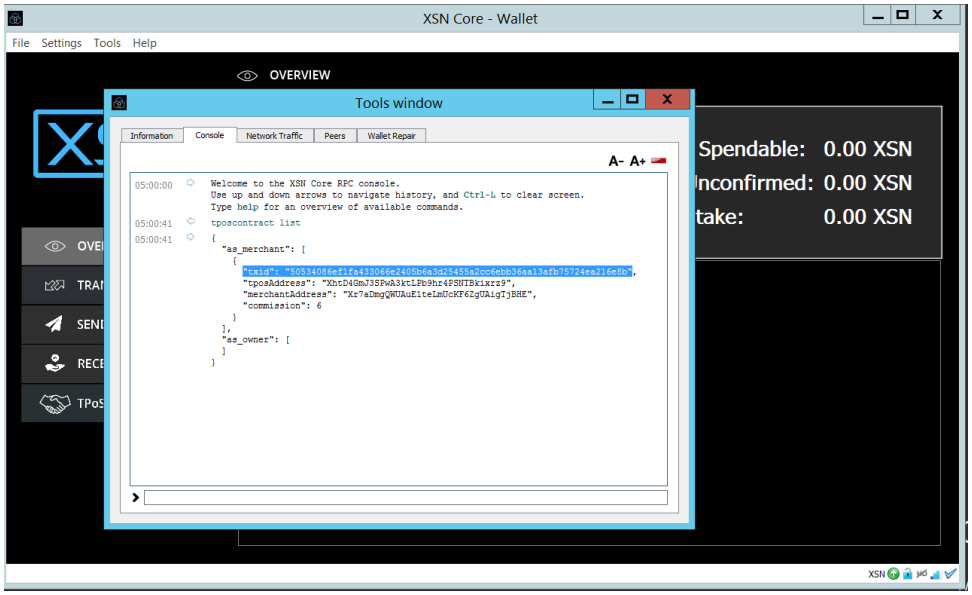
Step 3

Next in the *controller* wallet debug console execute **dumpprivkey 'result of step1'** and copy the output into a notepad/word file.



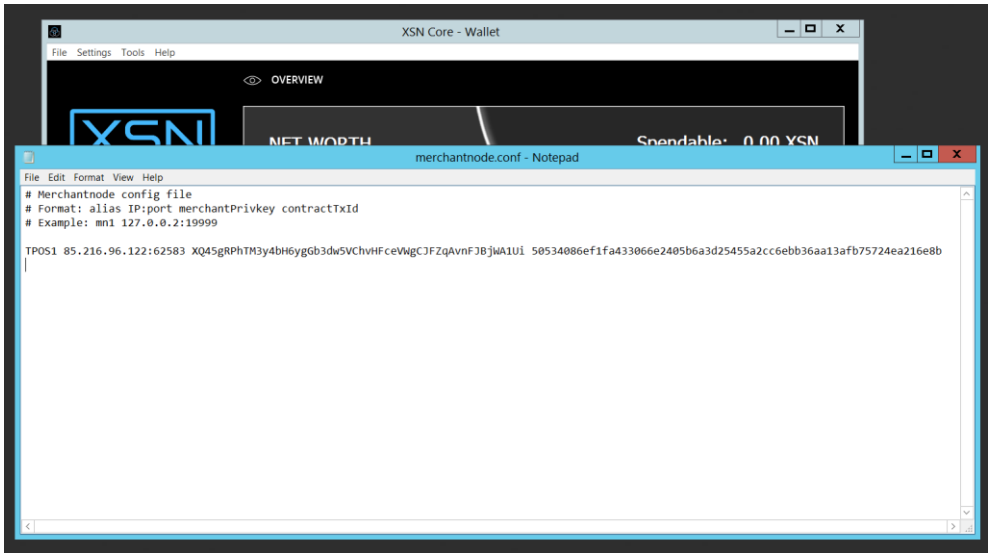
Step 4

On the *controller* wallet, execute **tposcontract list** in the debug console to get the transaction ID (txID) of the created contract. Copy this txID to the notepad/word file. You also can see the TPoS address (*remote* wallet address) and the *controller* wallet merchant address here.



Step 5

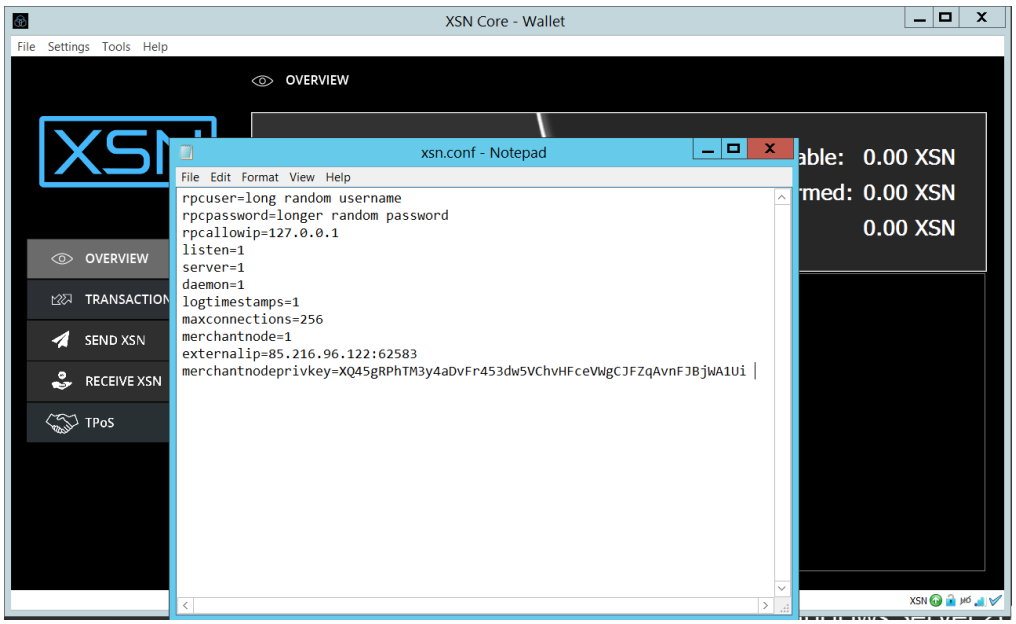
Next on the *controller* wallet, go to the XSNcore folder (default: C:\Users\(the pc name)\ AppData\Roaming\XSNCore), open merchantnode.conf (using notepad) and input the following line: **TPOS1 'merchant node IP':62583 'private key' 'txid'** where the private key is from Step 3 and the txID is from Step 4. Do not include the single quotes. Save the file and restart the wallet.



Step 6

On the *remote* wallet, go to the XSNcore folder, open xsn.conf (using notepad) and input the following lines then restart your wallet:

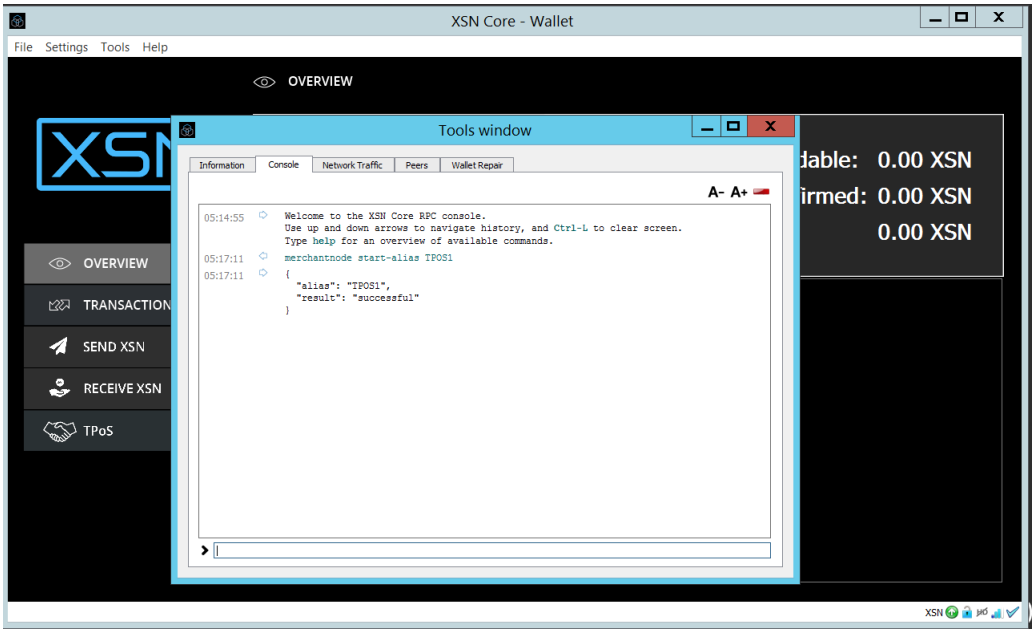
rpcuser=long random username
rpcpassword=longer random password
rpcallowip=127.0.0.1
listen=1
server=1
daemon=1
logtimestamps=1
maxconnections=256
merchantnode=1
externalip=’merchant IP’:62583
merchantnodeprivkey=’private key from step 3’



Step 7

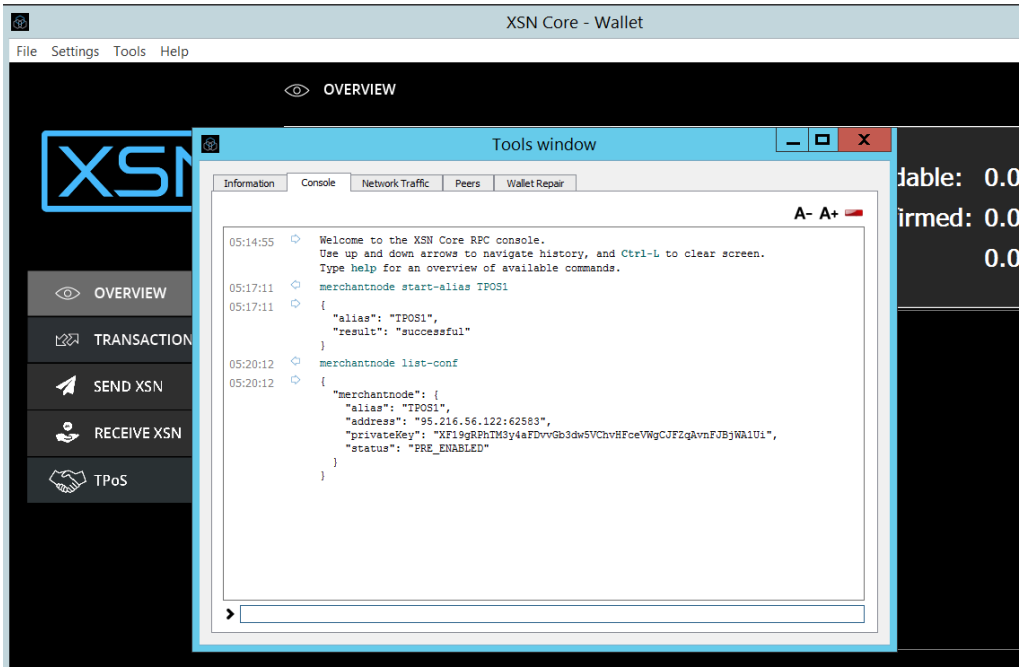
On the *controller* wallet, make sure you have restarted the wallet then open the debug console and input the following commad:

merchantnode start-alias TPOS1

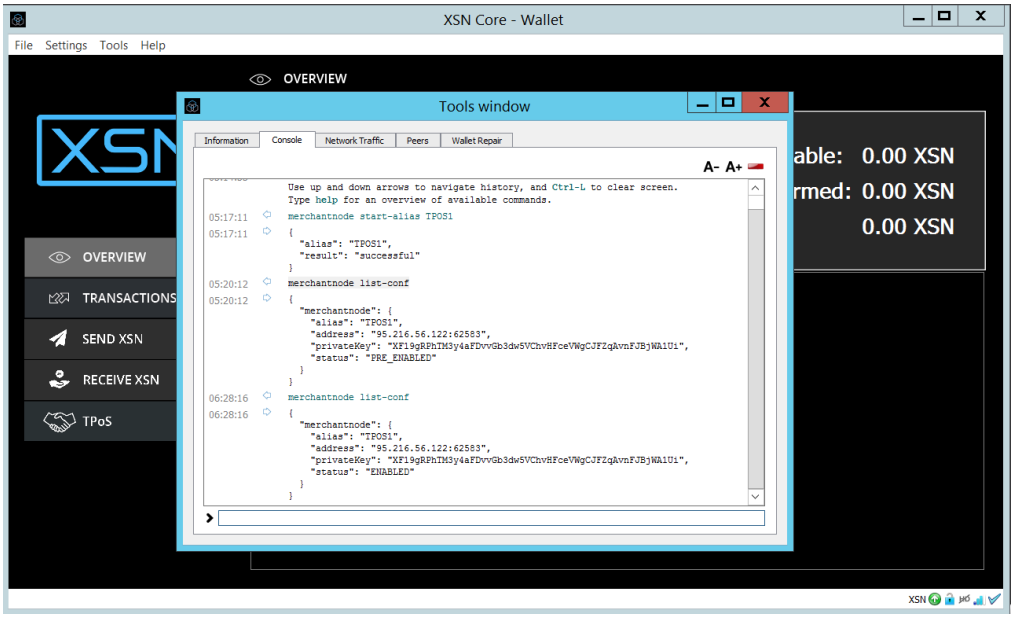


Step 8

On the *controller* wallet, in debug console input **tposcontract list-conf**. This will give you a list of your TPoS contracts. Right after step 7, your contract will be PRE-ENABLED.



You should wait for your contract to be ENABLED, which usually takes 15-30 minutes.

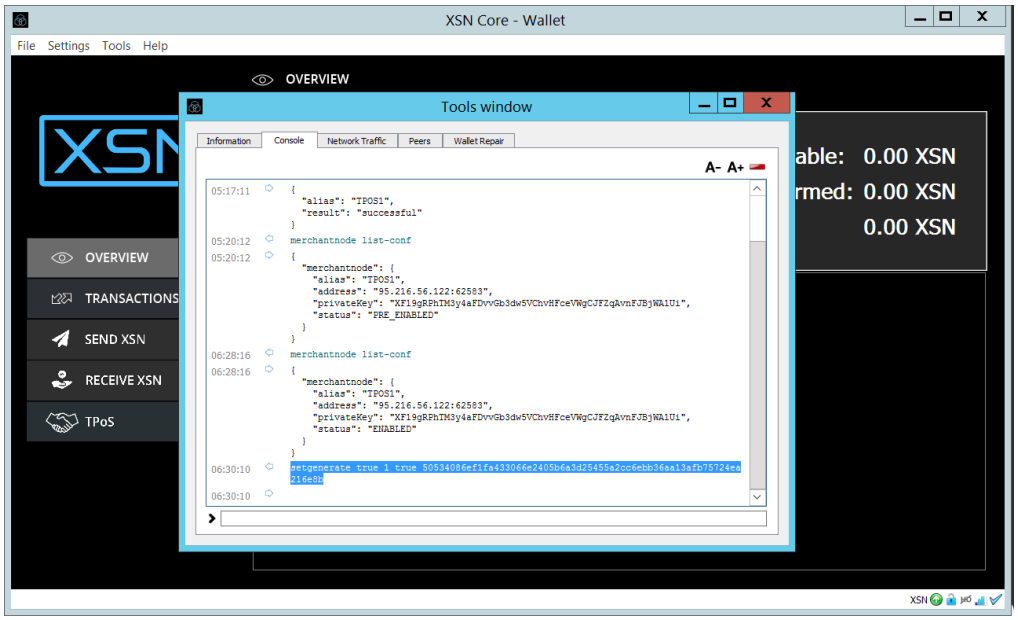


Step 9

As soon as your contract gets ENABLED, input the following command on the *remote* wallet:

setgenerate true 1 true 'txid from step 4'

With this command the merchant node starts staking.



How to be a merchant for several owners?

If you want to be merchant for several coin owners, you should have a *controller* wallet (like a person who has several masternodes), have one unique IP address per contract and manage your *remote* wallet nodes with your *controller* wallet.
For each contract you should add a separate line in merchantnode.conf of your *controller* wallet (Step 5).
You also should do step 7 on your *controller* wallet and step 6 and 9 on your VPS (*remote* wallet or TPoS node).

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