Creating a BiblePay Foundation Satellite Pool (C#):

1. Windows 2012 Server is recommended, but any windows server should work that allows hosting of asp.net with .NET framework 4.7.2.
2. A dual core server with 4gb of ram or higher is recommended. It is highly discouraged to attempt to run on a single core or with less ram, as MSSQL server will constantly page.
3. Since it costs $20 more per month on vultr to rent a cloud compute 80gb 4gb dual core server (windows 2012 x64 r2), you may burn your own ISO of Windows 2012 R2 by buying a license (for example, windows 2012 r2 standard r2 can be purchased here for $80: https://softwarelicense4u.com/us/windows-server-2012-r2-standard-license-download), then you burn the ISO and upload it to vultr and boot the OS. This allows you to rent a standard dual core vultr linux node for half price ($20 per month) in contrast to $40 per month.
4. Boot the node and set the administrator password, and create a backpack of credentials on your local machine so you can refer to these credentials.
5. Download MSSQL-DEVELOPER-2019 from here: https://www.microsoft.com/en-us/sql-server/sql-server-downloads (see halfway down the page, for development use, or buy a license for MSSQL 2019 SQL server, or install MSSQL-2019-EXPRESS). Any one of these options allow the pool to run, but technically you will need to buy a license if you do not choose a free option.
6. Install MSSQL SERVER 2019 on the new server. Install MSSQL Configuration Management Studio on the server. Set the SA password to be strong.
7. Modify MSSQL with "MSSQL Configuration Manager" to bind the default tcp adapter to port 1433. Expose port 1433 to be listening for SQL traffic (this is so you can connect from your home machine for administration). Test the configuration remotely to ensure MSSQL is listening on 1433.
8. Set up the firewall: Run Microsoft firewall. Add firewall rules to open port 3001, 4444 for inbound traffic (this allows the world to attach to the pool). Do not block these ports by ip range.
9. Restrict the firewall to only allow 1433 to be accessed by your home IP range.
10. Modify the firewall to allow SMB inbound traffic to only be accessed by your home IP range.
11. Optional: Set up RDP access, add a firewall rule and test RDP. Otherwise you will need to log in via the vultr console.
12. Follow instructions on creating a mapped SMB share from the Pool server to your home computer. In my case I mounted the pools c$ drive as R:\$. Make it so the connection is persistent for redeploys.
13. After 10 days or so of operation, or earlier, check the event log | security events to make sure no one is trying to hack in the box. (You will see this as an event log entry each time a hacker tries to log in as administrator, as a FAILED security audit login attempt). If they are, you need to modify your firewall rules to block all login related traffic (these are usually netbios, smb, or default firewall rules by Microsoft that allow the entire IP scope). In my case, I modified the SMB file

print sharing inbound rules, and SMB login inbound rules, to be restricted down to my single IP. Then the security events stopped.

14. Install MS visual studio 2019 on your home machine. https://visualstudio.microsoft.com/downloads/
15. Load the "Foundation.sln" solution.
16. Compile it.
17. Right click on Saved | Publish. Click Configure to configure the deployment publish options. Configure the target location to point to the mapped drive of 2012 server: r:\inetpub\wwwroot\Saved
18. Deploy the code.
19. From the 2012 server, go to w3svc (IIS7).
20. Add a new site. Point to the root directory (c:\inetpub\wwwroot\Saved).
21. From file explorer, navigate to c:\inetpub\wwwroot\Saved\Uploads.
22. Grant write access to the application pool user : Right click on the folder properties | Security | Edit | Add | Locations | Add : "IIS AppPool\applicationpoolname". OK.
23. Log file should be written by default to c:\inetpub\wwwroot\Saved\Uploads\foundation.log (check this)
24. Set up the configuration key values in c:\inetpub\wwwroot\bms.conf
25. Download the bms.conf sample file from github. Todo: explain how to change the key values for each key.
26. Download the backup of the sql server seed tables. The file can be downloaded from: _____saved.bak _here_.
27. Restore the database backup of "saved.bak" into the MSSQL server and ensure the database "saved" exists.
28. Test a query from your home machine using MSSQL Server Management Studio. If you do not have MSSQL-SMS, please download it from https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver15.
29. Log in to yourdnsname.domain.com, Log in as SA, Select database Saved, Select * from Orphans. Verify our 78 orphans show up.
30. Installing a free LetsEncrypt HTTPS certificate: after confirming your site can be accessed from port 80 (for example, navigate to yoursite.dns.com via HTTP), then download 'wacs.exe' (this is letsencrypt for windows) from here https://github.com/win-acme/win-acme. Run wacs, and just create a simple letsencrypt certificate for the site name.
31. Then restart IIS, and verify the binding is present in W3SVC-IIS7 manager (Sites | Foundation | Manage Bindings). Verify the site responds to https traffic.