

3. Operational Verification

3.1 Certificate Verification Tool

This section presents the log output obtained when running the certificate verification tool in a real execution environment.

3.1.1 Server Side (cardano_verifier.mjs)

```
Server Startup Log
% node cardano_verifier.mjs
[INFO] system - START VALIDATION.
[INFO] system -   ┐ calc hash: 50c26925660413b7b9068bd0da80446b9f98f9662e87a347bb89eb4513bc19aa
[INFO] system -   │ new block: height:2998357, time:1734493576
[INFO] system -   └ prev hash: d58303c8f264309b61b575e2d8362bc0a86f325fc4bc761a7913b8f16800de37
[INFO] system -   ┐ calc hash: d58303c8f264309b61b575e2d8362bc0a86f325fc4bc761a7913b8f16800de37
[INFO] system -   │ new block: height:2998356, time:1734493563
[INFO] system -   └ prev hash: 74b8322dfd4b77c58f5135d2788f0f108d0dc88bd0d2c6cb786f76c12efb42ad
[INFO] system -   ┐ calc hash: 74b8322dfd4b77c58f5135d2788f0f108d0dc88bd0d2c6cb786f76c12efb42ad
[INFO] system -   │ new block: height:2998355, time:1734493514
[INFO] system -   └ prev hash: bad3781064c1dfbe1960fa647ae4cf097dbaac9639d9087944d0f59e5aee5357
[INFO] system -   ┐ calc hash: bad3781064c1dfbe1960fa647ae4cf097dbaac9639d9087944d0f59e5aee5357
[INFO] system -   │ new block: height:2998354, time:1734493494
[INFO] system -   └ prev hash: 4335293f7fd86532944281577f9208528c140ccc539f616e886a80ba813d975f
[INFO] system -   ┐ calc hash: 4335293f7fd86532944281577f9208528c140ccc539f616e886a80ba813d975f
[INFO] system -   │ new block: height:2998353, time:1734493478
[INFO] system -   └ prev hash: 52d6a2bd1c177926135d78b809dabf0c76b2a1434f79031d9d437fd33c5bb38e
[INFO] system -   ┐ calc hash: 52d6a2bd1c177926135d78b809dabf0c76b2a1434f79031d9d437fd33c5bb38e
[INFO] system -   │ new block: height:2998352, time:1734493471
[INFO] system -   └ prev hash: 9243437e19f0d24cc57aa26cfc45afc5b5eae1d251c621eebdb1bd9467a369c3
[INFO] system -   ┐ calc hash: 9243437e19f0d24cc57aa26cfc45afc5b5eae1d251c621eebdb1bd9467a369c3
[INFO] system -   │ new block: height:2998351, time:1734493451
[INFO] system -   └ prev hash: 19a950deb3633fcf4f8bfb5736b24c2e40fa6dd75260f43f996d6bbb25b7d01c
```

```
[INFO] system -  ┐ calc hash: 19a950deb3633fcf4f8bfb5736b24c2e40fa6dd75260f43f996d6bbb25b7d01c
[INFO] system -  | new block: height:2998350, time:1734493416
[INFO] system -  └ prev hash: c45a1cde7cdf3cbce6fffc31e35ae48be949cf228ca53a6a3ec4dc636014f56a9
[INFO] system -  ┐ calc hash: c45a1cde7cdf3cbce6fffc31e35ae48be949cf228ca53a6a3ec4dc636014f56a9
[INFO] system -  | new block: height:2998349, time:1734493332
[INFO] system -  └ prev hash: b284e460c9cd9656c090d8e77517c96f6175855363dde6de20426dbb1c89702f
[INFO] system -  ┐ calc hash: b284e460c9cd9656c090d8e77517c96f6175855363dde6de20426dbb1c89702f
[INFO] system -  | new block: height:2998348, time:1734493317
[INFO] system -  └ prev hash: 9797ca07e538627cc16561fc84f82c5c16a26f2e171f6f5d324513c51bd360d2
[INFO] system -  ┐ calc hash: 9797ca07e538627cc16561fc84f82c5c16a26f2e171f6f5d324513c51bd360d2
[INFO] system -  | new block: height:2998347, time:1734493307
[INFO] system -  └ prev hash: ead1e7427962ef2d1db0fa0a759232bb2ad165ea6b146533327df5708c7236d2
[INFO] system -  ┐ calc hash: ead1e7427962ef2d1db0fa0a759232bb2ad165ea6b146533327df5708c7236d2
[INFO] system -  | new block: height:2998346, time:1734493259
[INFO] system -  └ prev hash: cb050b9f253b24e8e21c36113d1f50f9875b763c820edd96f313e4065773663a
[INFO] system -  ┐ calc hash: cb050b9f253b24e8e21c36113d1f50f9875b763c820edd96f313e4065773663a
[INFO] system -  | new block: height:2998345, time:1734493244
[INFO] system -  └ prev hash: de621f35d9c33c37b68dbbe7eff96f6c1189982a2eedba0ba360bb1aa40d312e
[INFO] system -  ┐ calc hash: de621f35d9c33c37b68dbbe7eff96f6c1189982a2eedba0ba360bb1aa40d312e
[INFO] system -  | new block: height:2998344, time:1734493242
[INFO] system -  └ prev hash: afdcb57d7d17c5bb86800345bac682f92da3dd8d437ca1ac28a93c5b31a76d18
[INFO] system -  ┐ calc hash: afdcb57d7d17c5bb86800345bac682f92da3dd8d437ca1ac28a93c5b31a76d18
[INFO] system -  | new block: height:2998343, time:1734493241
[INFO] system -  └ prev hash: 71ea4c84c5394ceb9fb96874c0703230f4efc5cd3332f634614df5a59f65e60c
[INFO] system -  ┐ calc hash: 71ea4c84c5394ceb9fb96874c0703230f4efc5cd3332f634614df5a59f65e60c
[INFO] system -  | new block: height:2998342, time:1734493221
[INFO] system -  └ prev hash: 667930f7520673df13f27be4f7138315159af269a8e80e89af918dbba3a16382
[INFO] system -  ┐ calc hash: 667930f7520673df13f27be4f7138315159af269a8e80e89af918dbba3a16382
[INFO] system -  | new block: height:2998341, time:1734493215
[INFO] system -  └ prev hash: eb62400a4877d1dfe9e3b9e49ea15d8f5e719e1ceec4c41120c41009d7f7fd55
[INFO] system -  ┐ calc hash: eb62400a4877d1dfe9e3b9e49ea15d8f5e719e1ceec4c41120c41009d7f7fd55
[INFO] system -  | new block: height:2998340, time:1734493186
[INFO] system -  └ prev hash: ddf1a4d2d534d9e9657c88d5e136d2230927d282eb80b74f3ac400cb0c431351
[INFO] system -  ┐ calc hash: ddf1a4d2d534d9e9657c88d5e136d2230927d282eb80b74f3ac400cb0c431351
```

```

[INFO] system - | new block: height:2998339, time:1734493180
[INFO] system - └ prev hash: d85f59d9ca2572bb08d55f490a20779d665f07a48e95b0b88593d809456b54e3
[INFO] system - ┐ calc hash: d85f59d9ca2572bb08d55f490a20779d665f07a48e95b0b88593d809456b54e3
[INFO] system - | new block: height:2998338, time:1734493164
[INFO] system - └ prev hash: 4d6e9048fa8b14ad92f9e5d8c291178742ccbd8e74a1ec3a59aec491dfc8e12e
[INFO] system - ┐ calc hash: 4d6e9048fa8b14ad92f9e5d8c291178742ccbd8e74a1ec3a59aec491dfc8e12e
[INFO] system - | new block: height:2998337, time:1734493140
[INFO] system - └ prev hash: f352ce45c839e92b4dab9aad64dc8c471005a52d747abf1b3da04fab974470c3
[INFO] system - ┐ calc hash: f352ce45c839e92b4dab9aad64dc8c471005a52d747abf1b3da04fab974470c3
[INFO] system - | new block: height:2998336, time:1734493139
[INFO] system - └ prev hash: 8948e0d0d90f3026468b4db6cfc4011e6e8119b0f667273053bc74d8eaa8f1a7
[INFO] system - ┐ calc hash: 8948e0d0d90f3026468b4db6cfc4011e6e8119b0f667273053bc74d8eaa8f1a7
[INFO] system - | new block: height:2998335, time:1734493101
[INFO] system - └ prev hash: 040e31155b519a4e5f2fc603151324ec8fa0938809d3e55b407af3ee183e8cad
[INFO] system - ┐ calc hash: 040e31155b519a4e5f2fc603151324ec8fa0938809d3e55b407af3ee183e8cad
[INFO] system - | new block: height:2998334, time:1734493024
[INFO] system - └ prev hash: 03dc57a94d33f5d098a4ec12e7366374a61d8839f66136e7fc13a1964ed5e5ac
[INFO] system - ┐ calc hash: 03dc57a94d33f5d098a4ec12e7366374a61d8839f66136e7fc13a1964ed5e5ac
[INFO] system - | new block: height:2998333, time:1734492927
[INFO] system - └ prev hash: b11e359b921a712d3e292a5000210dccf9876c0cae8df071a9fa52b1e10ad183
[INFO] system - ┐ calc hash: b11e359b921a712d3e292a5000210dccf9876c0cae8df071a9fa52b1e10ad183
[INFO] system - | new block: height:2998332, time:1734492921
[INFO] system - └ prev hash: 28ab34a9efb5ec9aefc1ba4149db6730490fc49756180593194aa43aa8f6ced4
[INFO] system - ┐ calc hash: 28ab34a9efb5ec9aefc1ba4149db6730490fc49756180593194aa43aa8f6ced4
[INFO] system - | new block: height:2998331, time:1734492896
[INFO] system - └ prev hash: 2a50b75a0a705a6bd917f9333f72c9b45be8c7dfb5c0da9f4782fecbc1e08c92
[INFO] system - ┐ calc hash: 2a50b75a0a705a6bd917f9333f72c9b45be8c7dfb5c0da9f4782fecbc1e08c92
[INFO] system - | new block: height:2998330, time:1734492866
[INFO] system - └ prev hash: 2390ea0281d9e4980cf22845dc38f9bf61dffa2ac4e9da96cb83875b48d83f43
[INFO] system - ┐ calc hash: 2390ea0281d9e4980cf22845dc38f9bf61dffa2ac4e9da96cb83875b48d83f43
[INFO] system - | new block: height:2998329, time:1734492856
[INFO] system - └ prev hash: 9c2086d94d3374dc624494189578d4f3f94b75ca6acd7e69a42ae60601e23a50
[INFO] system - ┐ calc hash: 9c2086d94d3374dc624494189578d4f3f94b75ca6acd7e69a42ae60601e23a50
[INFO] system - | new block: height:2998328, time:1734492847

```

```
[INFO] system -  ⌞ prev hash: d2ae69d88398aad046d5a9e1be646fc091a049130e298af6e67c32e3c5626ae6
[INFO] system -  ⌞ calc hash: d2ae69d88398aad046d5a9e1be646fc091a049130e298af6e67c32e3c5626ae6
[INFO] system -  | new block: height:2998327, time:1734492807
[INFO] system -  ⌞ prev hash: 6e6be60898bc43537bc4d1915dc25f3077c1b55c71f28a5687005f8773286602
[INFO] system -  ⌞ calc hash: 6e6be60898bc43537bc4d1915dc25f3077c1b55c71f28a5687005f8773286602
[INFO] system -  | new block: height:2998326, time:1734492803
[INFO] system -  ⌞ prev hash: 16a2b60c400bc79e438574ce237f521cf943575f761420b95859909910515e1b
[INFO] system -  ⌞ calc hash: 16a2b60c400bc79e438574ce237f521cf943575f761420b95859909910515e1b
[INFO] system -  | new block: height:2998325, time:1734492706
[INFO] system -  ⌞ prev hash: 36673f537b04027808d1cf7bb94290281b01342cddb08c03f10760a61102f113
[INFO] system -  ⌞ calc hash: 36673f537b04027808d1cf7bb94290281b01342cddb08c03f10760a61102f113
[INFO] system -  | new block: height:2998324, time:1734492703
[INFO] system -  ⌞ prev hash: 0659b710e257267ab8b1495c38d23254d78f8702b406d62b9a5362e4b64f0938
[INFO] system -  ⌞ calc hash: 0659b710e257267ab8b1495c38d23254d78f8702b406d62b9a5362e4b64f0938
[INFO] system -  | new block: height:2998323, time:1734492685
[INFO] system -  ⌞ prev hash: 4f90ccc3ba3ac8fdf20a571a562070265b72e7bff14642516129cbd922f06fcd
[INFO] system -  ⌞ calc hash: 4f90ccc3ba3ac8fdf20a571a562070265b72e7bff14642516129cbd922f06fcd
[INFO] system -  | new block: height:2998322, time:1734492642
[INFO] system -  ⌞ prev hash: e0e98a21330418a9a534bfe60db9d7af50b4afd30791763ef6ab7e537115a94f
[INFO] system -  ⌞ calc hash: e0e98a21330418a9a534bfe60db9d7af50b4afd30791763ef6ab7e537115a94f
[INFO] system -  | new block: height:2998321, time:1734492628
[INFO] system -  ⌞ prev hash: f80e55b5ae21b781c9fa4fd904b32d8efd28b8156aabfdbc53e1e21e56338e72
[INFO] system -  ⌞ calc hash: f80e55b5ae21b781c9fa4fd904b32d8efd28b8156aabfdbc53e1e21e56338e72
[INFO] system -  | new block: height:2998320, time:1734492587
[INFO] system -  ⌞ prev hash: c1d676fc8ca5d5befcaa3e4374e862fee79182e4751c6197091b921d3bae1841
[INFO] system -  ⌞ calc hash: c1d676fc8ca5d5befcaa3e4374e862fee79182e4751c6197091b921d3bae1841
[INFO] system -  | new block: height:2998319, time:1734492582
[INFO] system -  ⌞ prev hash: e8d744ffb01e97b9c140d4943558b899f5161a154ba4f8332a4447db18d26a24
[INFO] system -  ⌞ calc hash: e8d744ffb01e97b9c140d4943558b899f5161a154ba4f8332a4447db18d26a24
[INFO] system -  | new block: height:2998318, time:1734492558
[INFO] system -  ⌞ prev hash: 22942f081a6ff40dc39c26d2a360046589046e94b810ddec1ce9167ee5622b0a
[INFO] system -  ⌞ calc hash: 22942f081a6ff40dc39c26d2a360046589046e94b810ddec1ce9167ee5622b0a
[INFO] system -  | new block: height:2998317, time:1734492535
[INFO] system -  ⌞ prev hash: 556c09ccab8d41e4fcfa78918ff732aefe7b050e0407b15b00fb60eda0ba1665
```

Catalyst Report for Cardano Block chain #1200231 M-3

```
[INFO] system -  ┐ calc hash: 556c09ccab8d41e4fcfa78918ff732aefe7b050e0407b15b00fb60eda0ba1665
[INFO] system -  | new block: height:2998316, time:1734492474
[INFO] system -  └ prev hash: 927b865a82eae863c132eeaf63a6660c810937c7739d0c5252fbff44c315a51
[INFO] system -  ┐ calc hash: 927b865a82eae863c132eeaf63a6660c810937c7739d0c5252fbff44c315a51
[INFO] system -  | new block: height:2998315, time:1734492460
[INFO] system -  └ prev hash: 78e1e95a73df48b9d629e688e263ad19d5f717e336167b2c9890d41c8d5737e1
[INFO] system -  ┐ calc hash: 78e1e95a73df48b9d629e688e263ad19d5f717e336167b2c9890d41c8d5737e1
[INFO] system -  | new block: height:2998314, time:1734492427
[INFO] system -  └ prev hash: f9dbcaaa35a9f8294199bcfe711bce8db0f9dbcd9b2c2a5dbd16b5f94b1fa0d
[INFO] system -  ┐ calc hash: f9dbcaaa35a9f8294199bcfe711bce8db0f9dbcd9b2c2a5dbd16b5f94b1fa0d
[INFO] system -  | new block: height:2998313, time:1734492420
[INFO] system -  └ prev hash: a76260869387d7e28dc7aece6f03c273863b992e62874010a50fad564c1ff998
[INFO] system -  ┐ calc hash: a76260869387d7e28dc7aece6f03c273863b992e62874010a50fad564c1ff998
[INFO] system -  | new block: height:2998312, time:1734492406
[INFO] system -  └ prev hash: 84aefe6e8a073501765666bc841b8a9f289c7c263ec40b9dec1f21c1da46bcec
[INFO] system -  ┐ calc hash: 84aefe6e8a073501765666bc841b8a9f289c7c263ec40b9dec1f21c1da46bcec
[INFO] system -  | new block: height:2998311, time:1734492404
[INFO] system -  └ prev hash: e1740e4e4fde9c930aff380aa8c6c5df83c7ba75fc5ad1478bb13b84ac75f868
[INFO] system -  ┐ calc hash: e1740e4e4fde9c930aff380aa8c6c5df83c7ba75fc5ad1478bb13b84ac75f868
[INFO] system -  | new block: height:2998310, time:1734492356
[INFO] system -  └ prev hash: 2a4ce3f47b4dd0783fcb8e69e142cc4e0013fbde8dea03bc51f55d50a92bdb
[INFO] system -  ┐ calc hash: 2a4ce3f47b4dd0783fcb8e69e142cc4e0013fbde8dea03bc51f55d50a92bdb
[INFO] system -  | new block: height:2998309, time:1734492350
[INFO] system -  └ prev hash: 46d78bae4857a4bfe4d0a89d681966924029f20a9114d6af179e12c111078339
[INFO] system -  ┐ calc hash: 46d78bae4857a4bfe4d0a89d681966924029f20a9114d6af179e12c111078339
[INFO] system -  | new block: height:2998308, time:1734492231
[INFO] system -  └ prev hash: f835bbfee9eeca2e0a36729bb71bd8c894a894a01407df40b5c84648ded432d2
[INFO] system -  ┐ calc hash: f835bbfee9eeca2e0a36729bb71bd8c894a894a01407df40b5c84648ded432d2
[INFO] system -  | new block: height:2998307, time:1734492184
[INFO] system -  └ prev hash: 035807cfb561381b98f8ab0ab94783ae7583c294e760c43b440d970a15f25c71
[INFO] system -  ┐ calc hash: 035807cfb561381b98f8ab0ab94783ae7583c294e760c43b440d970a15f25c71
[INFO] system -  | new block: height:2998306, time:1734492148
[INFO] system -  └ prev hash: 70c84ea8b0fff6909dee464eed37e920c3960b4a7d737e53980352a62254768d
[INFO] system -  SUCCESS:ALL BLOCKS VERIFIED.
```

3.1.2 validation.html

3.1.2.1 Operation in the Browser(chrome only)

The following outlines the procedure for operation in this environment:

(1) Prepare the three types of verification files:

- 【1】Issuer Data : keys.json
- 【2】Credential Data : vc.json
- 【3】IPDC Reception Data : cardano_head_2998335.json

※This file is in the GitHub 'sample' folder.

(2) Launch your browser (Chrome) with the following options

```
"C:¥Program Files¥Google¥Chrome¥Application¥chrome.exe"  
--disable-web-security --user-data-dir=C:/chrome_dev
```

※This is for Windows OS.

(3) Load validation.html.

※Drag and drop validation.html into your browser..

(4) Register the verification files: 【1】, 【2】, 【3】

(5) Click the "Start Validation" button.

3.1.2.1 Issuer Verification

Operational log of issuer verification.

```
====Issuer Verification====
```

```
Known Issuer Information:
```

```
[
  {
    "account": {
      "address":
"addr_test1qq54kguth0dtagn4j5skz3qwcm7tz2qrj8klrllfpfefe2pftv3chw76h638t9fpv9zqa3huky5q8y0d
7817jznjnj5qscstrm",
      "publicKey": "3745f60982871f6d49d0eb0cf1b02b4eafd128479933311292387df6ed86fcad"
    }
  }
]
```

```
Known Issuer Public Key:
```

```
3745f60982871f6d49d0eb0cf1b02b4eafd128479933311292387df6ed86fcad
```

```
Issuer Verification Result:true
```

3.1.2.2 Tamper-Resistance Verification and Issuer Legitimacy Check

Operational log of tamper-resistance verification and issuer legitimacy verification.

====Tamper-Proof Verification====

TX Payload:

84a400818258203f01c67ba4f0fd985eb22e3fb86fee59e8407adf1c345c2c871f52f97a25a3850001818258390
 0295b238bbbdabea275952161440ec6fcb1280391edf1ffe90a729ca8295b238bbbdabea275952161440ec6fcb1
 280391edf1ffe90a729ca81b0000000253828fc0021a00030d400758209d18dbac3ebdde6a45a2e4f342b6950ea
 fef5b5fef00022cba5828e1c4f46b73a100818258203745f60982871f6d49d0eb0cf1b02b4eafd1284799333112
 92387df6ed86fcad58404d8a93673d0739af083141f1949e34c7bcb07cfb04112a54b21676908c6e3ab0591985a
 d9e2f79c8d6c00a1d5ef9643eae5d179b1f7ac83723b85c325eba008f5a11902d1a66840636f6e746578748178
 2668747470733a2f2f777772e77332e6f72672f323031382f63726564656e7469616c732f76317163726564656
 e7469616c5375626a656374a671617574686f72697a6564526567696f6e7381a266726567696f6e745072656665
 637475726520412c204369747920426a76616c6964556e74696c6a323032342d31322d33316e636572746966696
 36174696f6e7381a3696973737565446174656a323032332d30352d303168697373756564427978184c6f63616c
 20547261696e696e6720496e737469747574656474797065781b48656176794d616368696e65727943657274696
 669636174696f6e62696478196469643a6578616d706c653a766f6c756e746565722d303031646e616d65684a6f
 686e20446f6564726f6c6578184865617679204d616368696e657279204f70657261746f7266736b696c6c73837
 3457863617661746f72204f7065726174696f6e7342756c6c646f7a6572204f7065726174696f6e744372697369
 7320436f6d6d756e69636174696f6e6269647475726e3a757569643a31323334352d36373839306c69737375616
 e63654461746574323032342d31312d30335430303a30303a30305a66697373756572a262696478326874747073
 3a2f2f64697361737465722d726573706f6e73652d6865616471756172746572732e6578616d706c652e6f72676
 46e616d65781e446973617374657220526573706f6e736520486561647175617274657273647479706582745665
 7269666961626c6543726564656e7469616c7821446973617374657252656c696566566f6c756e7465657243726
 564656e7469616c

TX Object:

[object Object]

TX Creator (Signer):

3745f60982871f6d49d0eb0cf1b02b4eafd128479933311292387df6ed86fcad

Signature:

4d8a93673d0739af083141f1949e34c7bcb07cfb04112a54b21676908c6e3ab0591985ad9e2f79c8d6c00a1d5ef
9643eae5d179b1f7ac83723b85c325eba008

Signature Target Payload:

a400818258203f01c67ba4f0fd985eb22e3fb86fee59e8407adf1c345c2c871f52f97a25a385000181825839002
95b238bbbdabea275952161440ec6fcb1280391edf1ffe90a729ca8295b238bbbdabea275952161440ec6fcb128
0391edf1ffe90a729ca81b0000000253828fc0021a00030d400758209d18dbac3ebdde6a45a2e4f342b6950eafe
f5b5fef00022cba5828e1c4f46b73

Signature Target Hash:

78c086ed166780e3aba2ef9f440958a106d242574321fc3f9fdb01607a3bf778

Signature Verification: true

3.1.2.3 On-Chain Integrity Verification

Operational log of on-chain integrity verification.

```
====On-Chain Verification====
```

IPDC Reception Block Header:

```
{
  "time": 1734493101,
  "height": 2998335,
  "hash": "192e5e5b208631f6c8aabf8818afeae54e06989303dd8e8a7d3a047cbad1516d",
  "slot": 78809901,
  "epoch": 186,
  "epoch_slot": 99501,
  "slot_leader": "pool1u4x4ly6qyx9fs9k2lt7f9hpa2gftd52fee67jcmuhnt7qqae3x0",
  "size": 1801,
  "tx_count": 3,
  "output": "19631381188",
  "fees": "851039",
  "block_vrf": "vrf_vk138vkpd9e89ya905atmp4lmp3hlgzpttkxwjx584f6m6k29y328stzx5yt",
  "op_cert": "9c96335e0f6c9f999e1374b053968c69a74ba1b9b8aa35e897666f0ab0df2e98",
  "op_cert_counter": "6",
  "previous_block": "6cb4be8de4163f5bd2dafa7e310a37bf7e076752280048cb4b54af10b31a1fd6",
  "next_block": null,
  "confirmations": 0,
  "ipdc_previous_block":
    "040e31155b519a4e5f2fc603151324ec8fa0938809d3e55b407af3ee183e8cad",
  "block_body_hash": "cb6f834005f12e069d1300f596c0e59dbcf8a896e9cef191e64827bc77866f8f1",
  "ipdc_hash": "8948e0d0d90f3026468b4db6cfc4011e6e8119b0f667273053bc74d8eaa8f1a7"
}
```

Transaction Hash:

78c086ed166780e3aba2ef9f440958a106d242574321fc3f9fdb01607a3bf778

Leaf:

25cb7a839811f4398e8887df936e4e68b623b32bf54f5480d88882edbef0b821

Merkle Path:

```
[  
  {  
    "position": "left",  
    "hash": "25cb7a839811f4398e8887df936e4e68b623b32bf54f5480d88882edbef0b821"  
  },  
  {  
    "position": "right",  
    "hash": "5c3286df6ac15de24fb7b0183a245f58530029f8fb1bc41f8e8af3881a7a8ec4"  
  }  
]
```

Merkle Root:

cb6f834005f12e069d1300f596c0e59dbcfa896e9cef191e64827bc77866f8f1

On-Chain Verification Result:true

end