

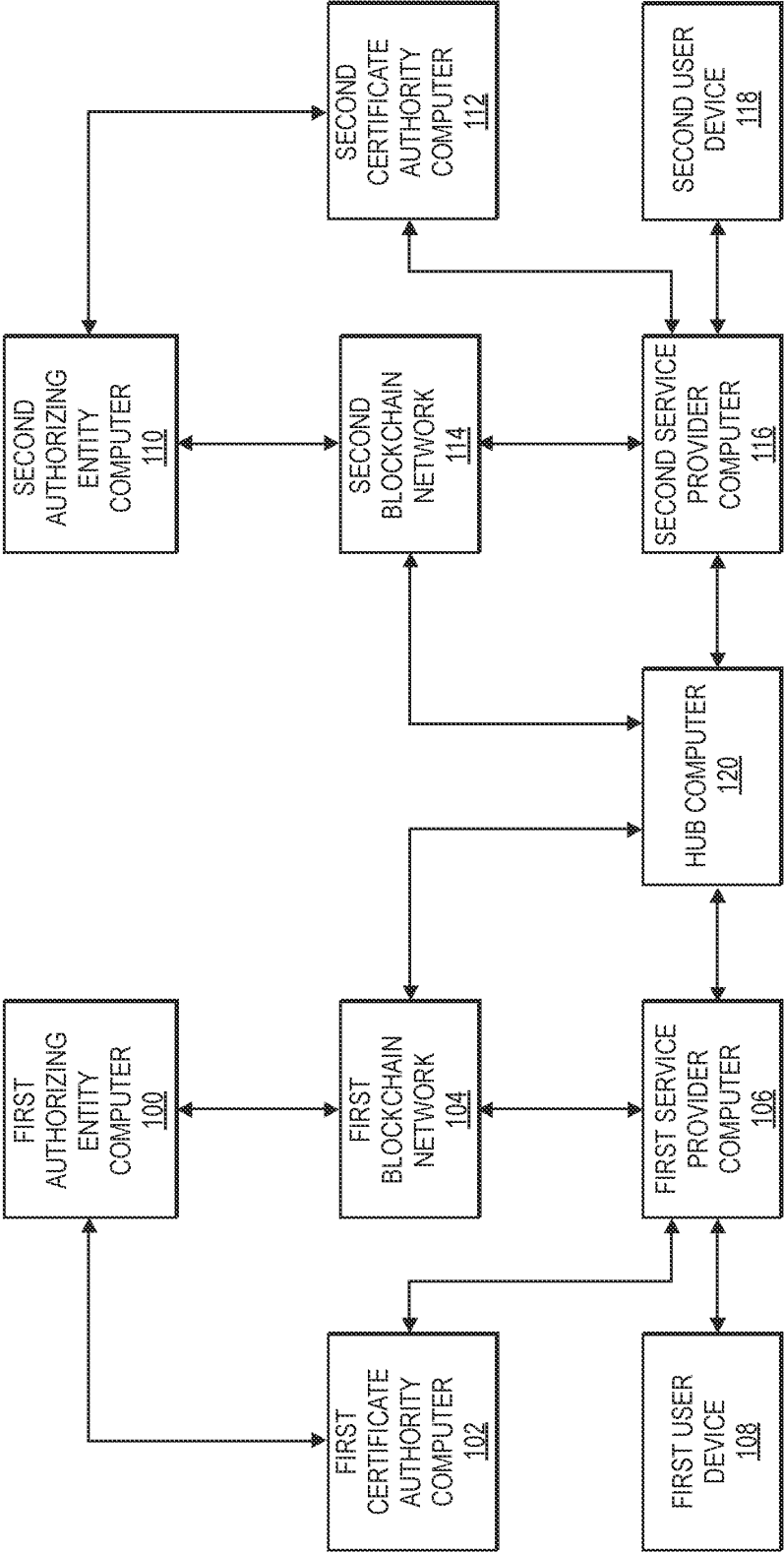


FIG. 1

2/15

| SMART CONTRACT<br>200                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b><u>Init(cid, vk1, vk2, T):</u></b></p> <ol style="list-style-type: none"> <li>1. Set channelID <math>\leftarrow</math> cid, <math>vk_S \leftarrow vk_1</math>, <math>vk_C \leftarrow vk_2</math>, disputeTime <math>\leftarrow</math> T</li> <li>2. Set status <math>\leftarrow</math> "Active", finalidx <math>\leftarrow</math> 0, finalCredit <math>\leftarrow</math> 0, serverDeposit <math>\leftarrow</math> 0, clientDeposit <math>\leftarrow</math> 0, channelExpiry <math>\leftarrow</math> 0, closeRequestor <math>\leftarrow</math> <math>\perp</math></li> </ol> <p><b><u>GetParams():</u></b></p> <p>Output[channelID, <math>vk_S</math>, <math>vk_C</math>, disputeTime]</p> <p><b><u>GetState():</u></b></p> <p>Output[status, finalidx, finalCredit, serverDeposit, clientDeposit, channelExpiry, closeRequestor]</p> <p><b><u>Deposit(amount):</u></b></p> <ol style="list-style-type: none"> <li>1. Abort if status = "Active"</li> <li>2. Abort if caller.vk <math>\neq vk_S</math> and caller.vk <math>\neq vk_C</math></li> <li>3. If caller.vk = <math>vk_S</math>, then set serverDeposit <math>\leftarrow</math> serverDeposit + amount</li> <li>4. If caller.vk = <math>vk_C</math>, then set clientDeposit <math>\leftarrow</math> clientDeposit + amount</li> </ol> <p><b><u>InitClose():</u></b></p> <ol style="list-style-type: none"> <li>1. Abort if status <math>\in</math> {CooperativeClosing, Closed}</li> <li>2. If status = "Active", then channelExpiry <math>\leftarrow</math> currentTime + disputeTime, status <math>\leftarrow</math> "UnilateralClosing" and closeRequestor <math>\leftarrow</math> caller.vk</li> <li>3. If status = "UnilateralClosing" and caller.vk <math>\leftarrow</math> closeRequestor, then set status <math>\leftarrow</math> "CooperativeClosing"</li> </ol> <p><b><u>Withdraw():</u></b></p> <ol style="list-style-type: none"> <li>1. Abort if status <math>\in</math> {Active, Closed}</li> <li>2. Abort if status = "Active" and currentTime &gt; channelExpiry</li> <li>3. Invoke <math>vk_C.transfer(clientDeposit + finalCredit)</math> and <math>vk_S.transfer(serverDeposit - finalCredit)</math></li> <li>4. Set status <math>\leftarrow</math> "Closed"</li> </ol> <p><b><u>Claim(cid, idx, clientCredit, txAmount, hash, expiry, secretReceived, <math>\sigma</math>, secret):</u></b></p> <ol style="list-style-type: none"> <li>1. Abort if idx <math>\leq</math> finalidx</li> <li>2. If secretReceived = 0, abort if currentTime &gt; Expiry or if Hash(secret) <math>\neq</math> hash</li> <li>3. If caller.vk = <math>vk_S</math>:       <ol style="list-style-type: none"> <li>(a) Abort if SigVerify([channelID, idx, clientCredit, txAmount, hash, expiry, secretReceived, <math>\sigma</math>, <math>vk_C</math>] <math>\neq</math> 1], <math>vk_C</math>) <math>\neq</math> 1</li> <li>(b) Abort if txAmount &gt; clientDeposit + clientCredit</li> <li>(c) Update finalCredit <math>\leftarrow</math> clientCredit - txAmount</li> </ol> </li> <li>4. Update finalidx <math>\leftarrow</math> idx</li> <li>5. Invoke InitClose()</li> </ol> |

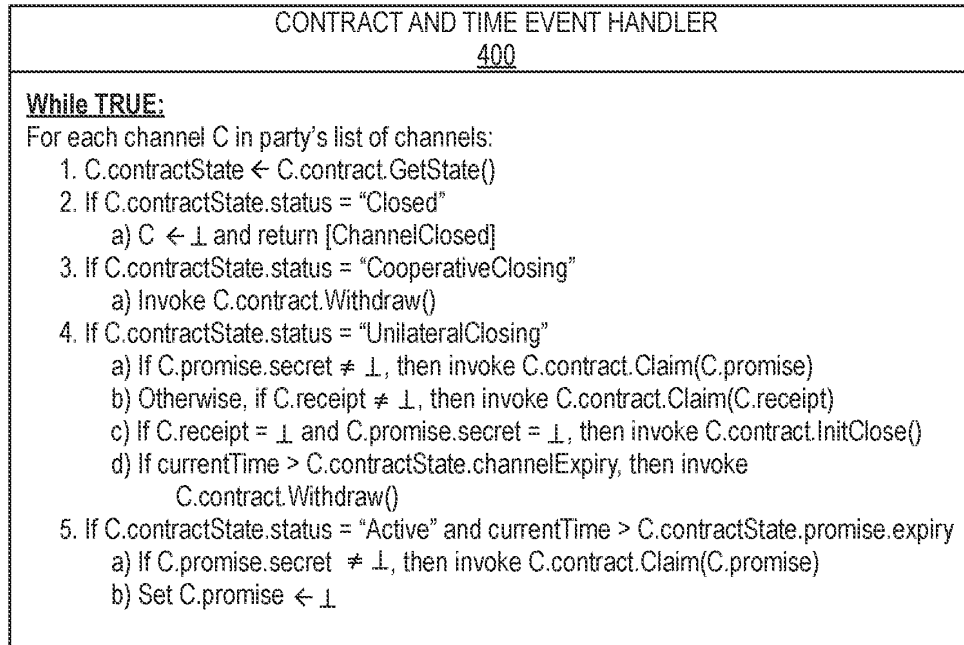
FIG. 2

3/15

| HELPER FUNCTIONS<br>300                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b><u>CreatePromise(cid, state, txAmount, hash, expiry, sk):</u></b></p> <ol style="list-style-type: none"> <li>1. Set secretReceived <math>\leftarrow 0</math></li> <li>2. Output [cid, idx, clientCredit, txAmount, hash, expiry, secretReceived, <math>\sigma</math>],<br/>where <math>\sigma = \text{Sign}[\text{cid}, \text{idx}, \text{clientCredit}, \text{txAmount}, \text{hash}, \text{expiry}, \text{secretReceived}]</math></li> </ol>                                                                                           |
| <p><b><u>VerifyPromise(promise, cid, state, txAmount, hash, expiry, vk):</u></b></p> <ol style="list-style-type: none"> <li>1. Set secretReceived <math>\leftarrow 0</math></li> <li>2. Output SigVerify(promise.<math>\sigma</math>, [cid, idx, clientCredit, txAmount, hash, expiry, secretReceived], vk)</li> </ol>                                                                                                                                                                                                                         |
| <p><b><u>CreateReceipt(cid, state, sk):</u></b></p> <ol style="list-style-type: none"> <li>1. Set txAmount <math>\leftarrow \perp</math>, hash <math>\leftarrow \perp</math>, expiry <math>\leftarrow \perp</math>, secretReceived <math>\leftarrow 1</math></li> <li>2. Output [cid, idx, clientCredit, txAmount, hash, expiry, secretReceived, <math>\sigma</math>],<br/>where <math>\sigma = \text{Sign}[\text{cid}, \text{idx}, \text{clientCredit}, \text{txAmount}, \text{hash}, \text{expiry}, \text{secretReceived}]</math></li> </ol> |
| <p><b><u>VerifyReceipt(receipt, cid, state, vk):</u></b></p> <ol style="list-style-type: none"> <li>1. Set txAmount <math>\leftarrow \perp</math>, hash <math>\leftarrow \perp</math>, expiry <math>\leftarrow \perp</math>, secretReceived <math>\leftarrow 1</math></li> <li>2. Output SigVerify(receipt.<math>\sigma</math>, [cid, idx, clientCredit, txAmount, hash, expiry, secretReceived], vk)</li> </ol>                                                                                                                               |
| <p><b><u>UpdateLocalState(localState, promise, increaseCredit):</u></b></p> <ol style="list-style-type: none"> <li>1. localState.idx <math>\leftarrow</math> localState.idx + 1</li> <li>2. If increaseCredit = 1, then localState.clientCredit <math>\leftarrow</math> localState.clientCredit +<br/>promise.txAmount</li> <li>3. Otherwise, localState.clientCredit <math>\leftarrow</math> localState.clientCredit –<br/>promise.txAmount</li> <li>4. Output localState</li> </ol>                                                          |

FIG. 3

4/15

**FIG. 4**

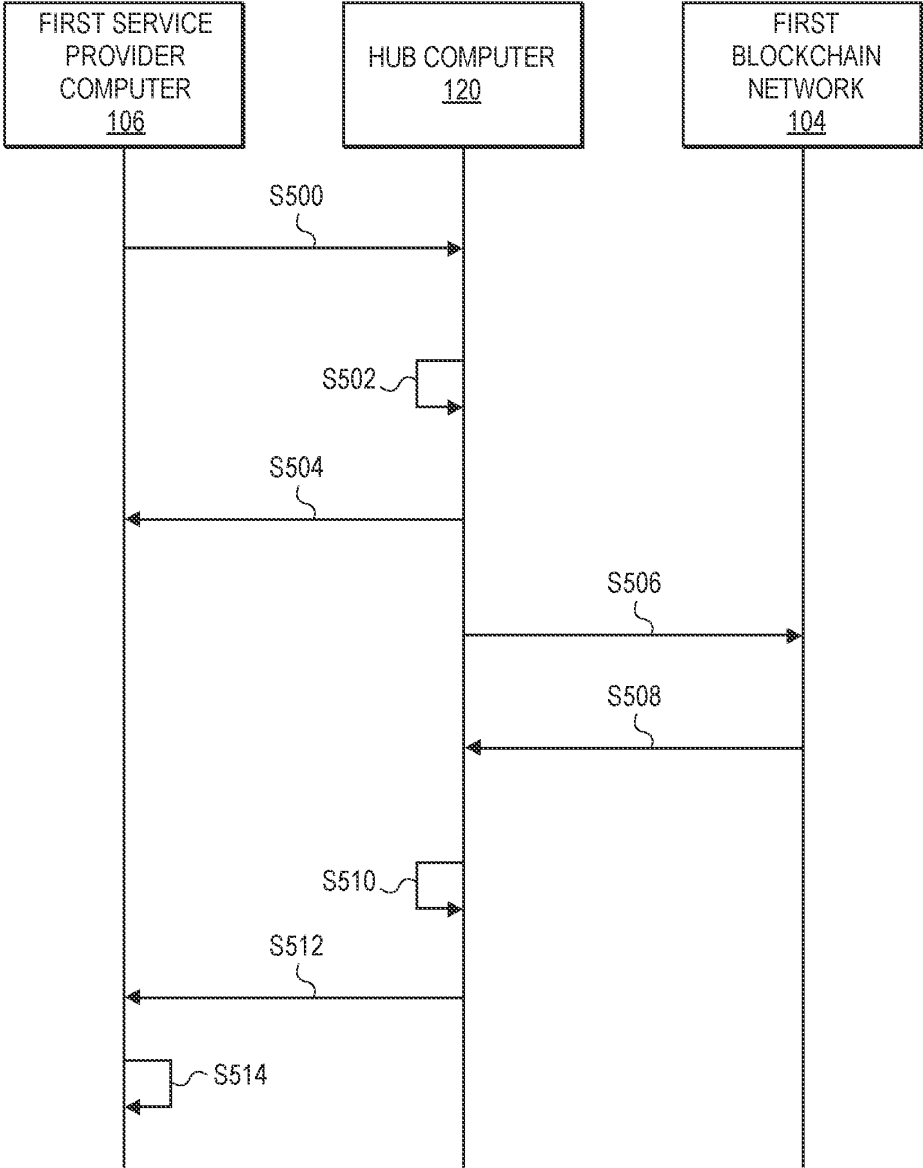


FIG. 5

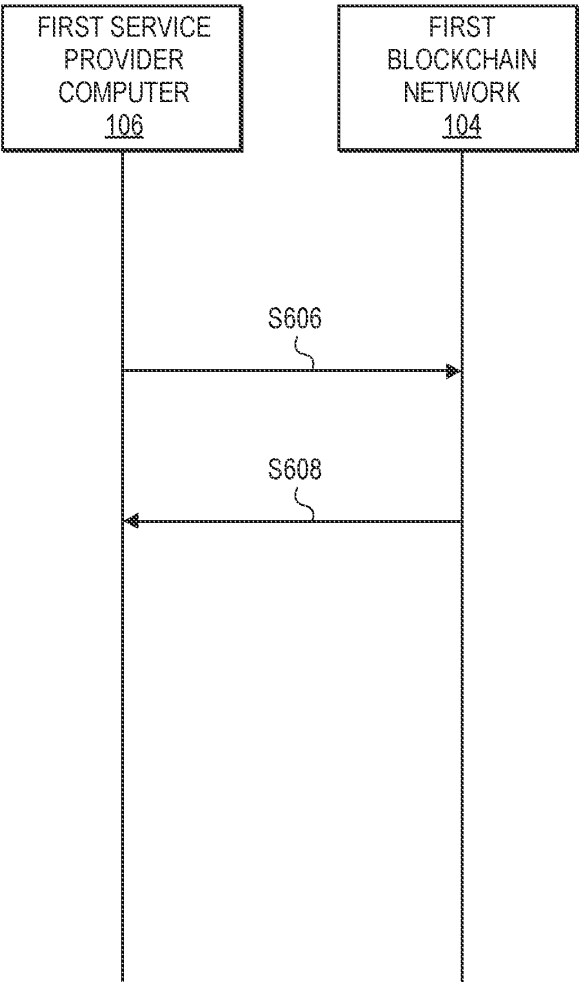


FIG. 6

7/15

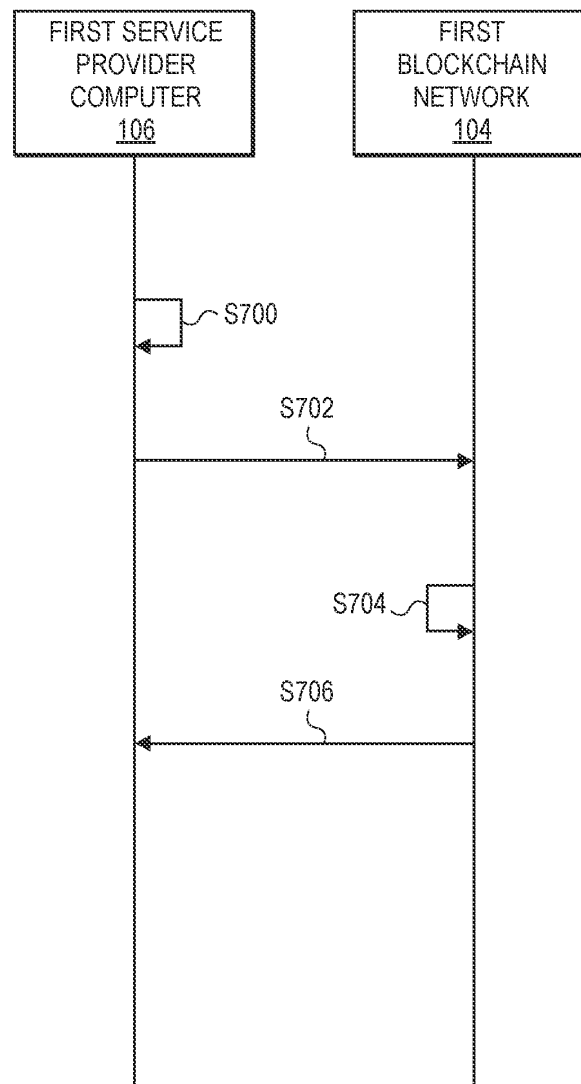


FIG. 7

8/15

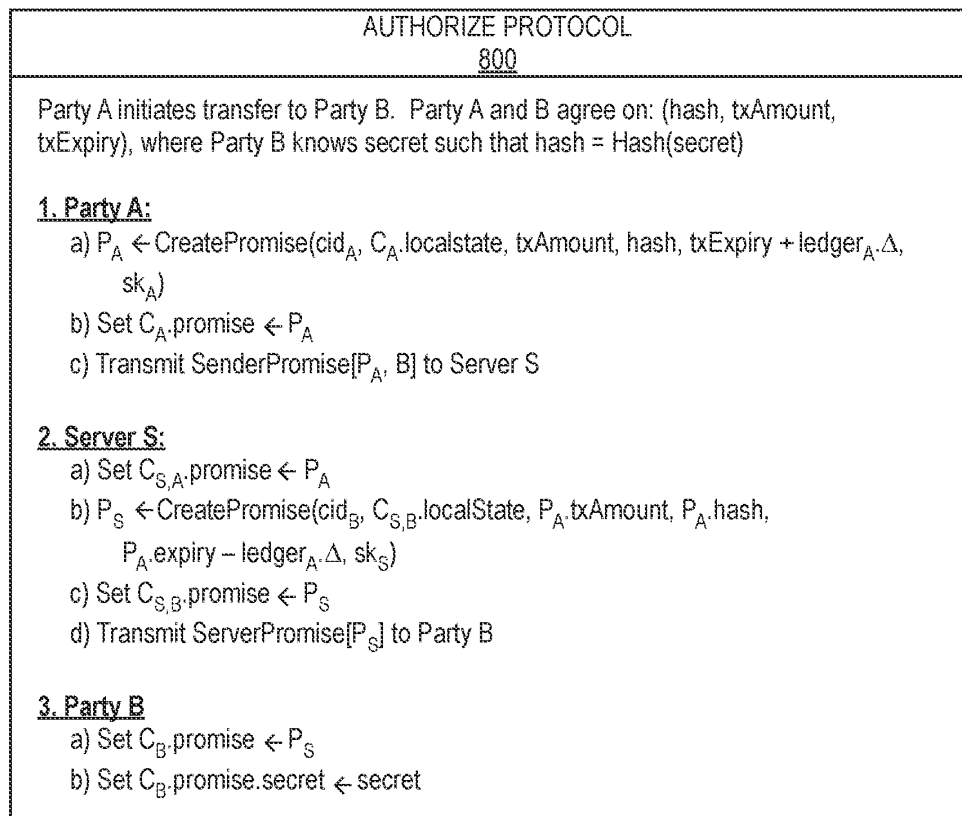


FIG. 8

9/15

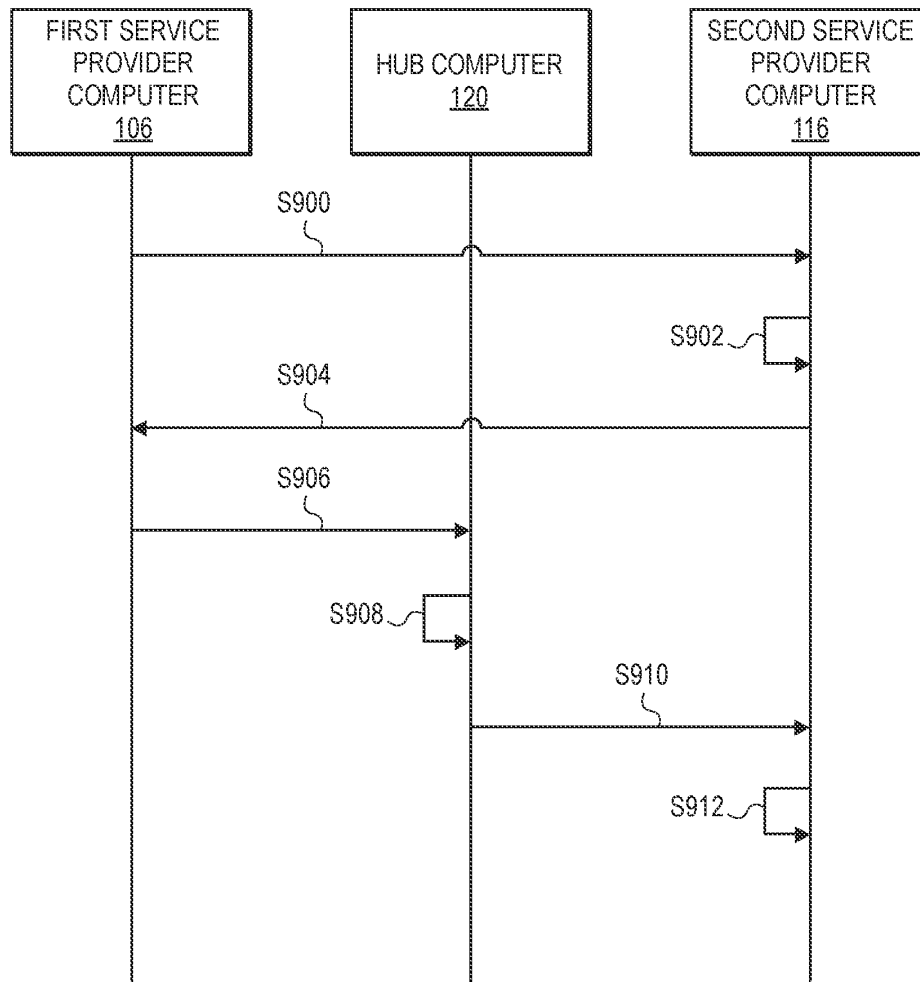
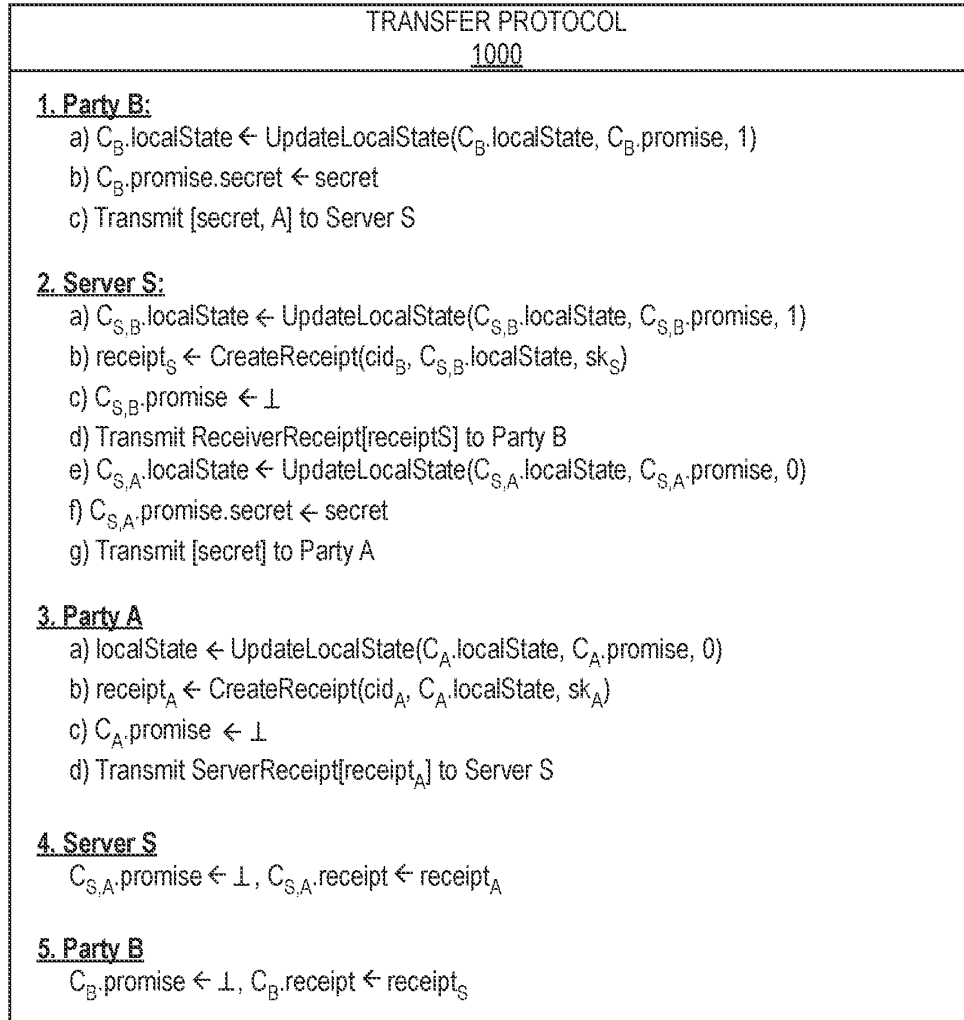
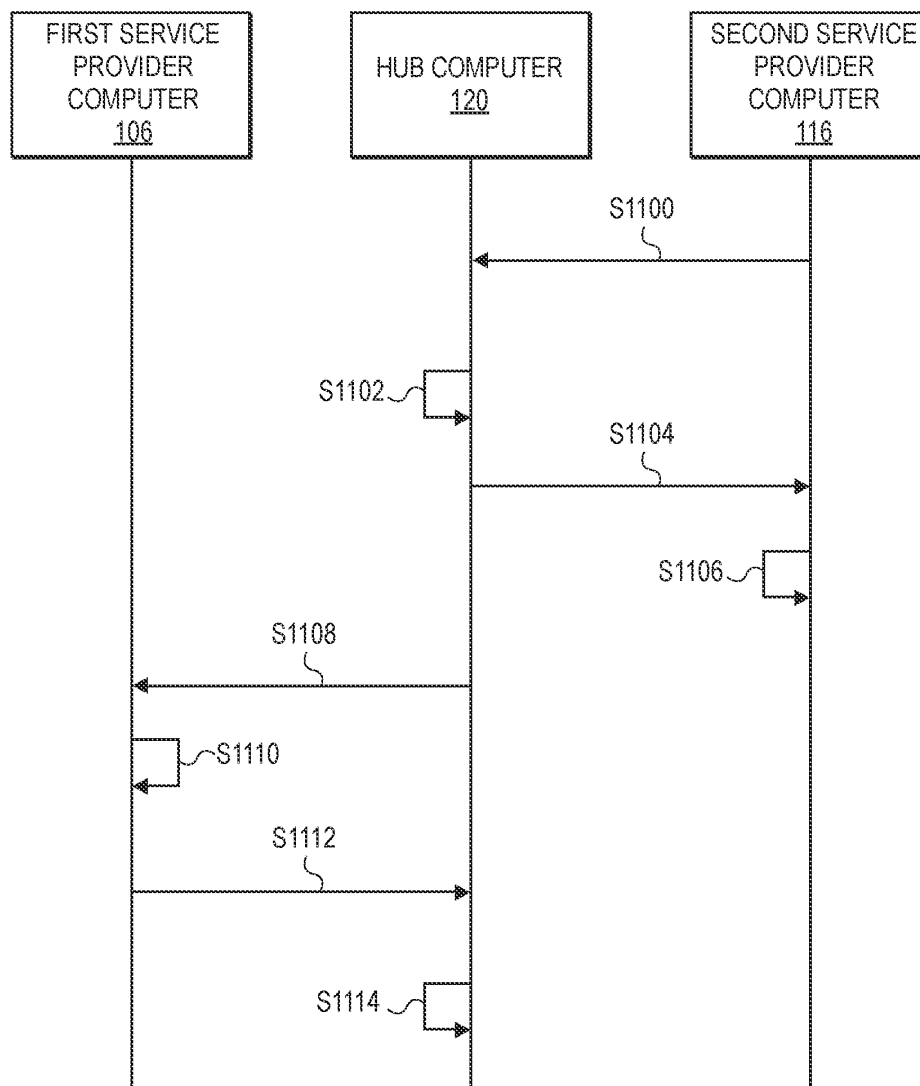


FIG. 9

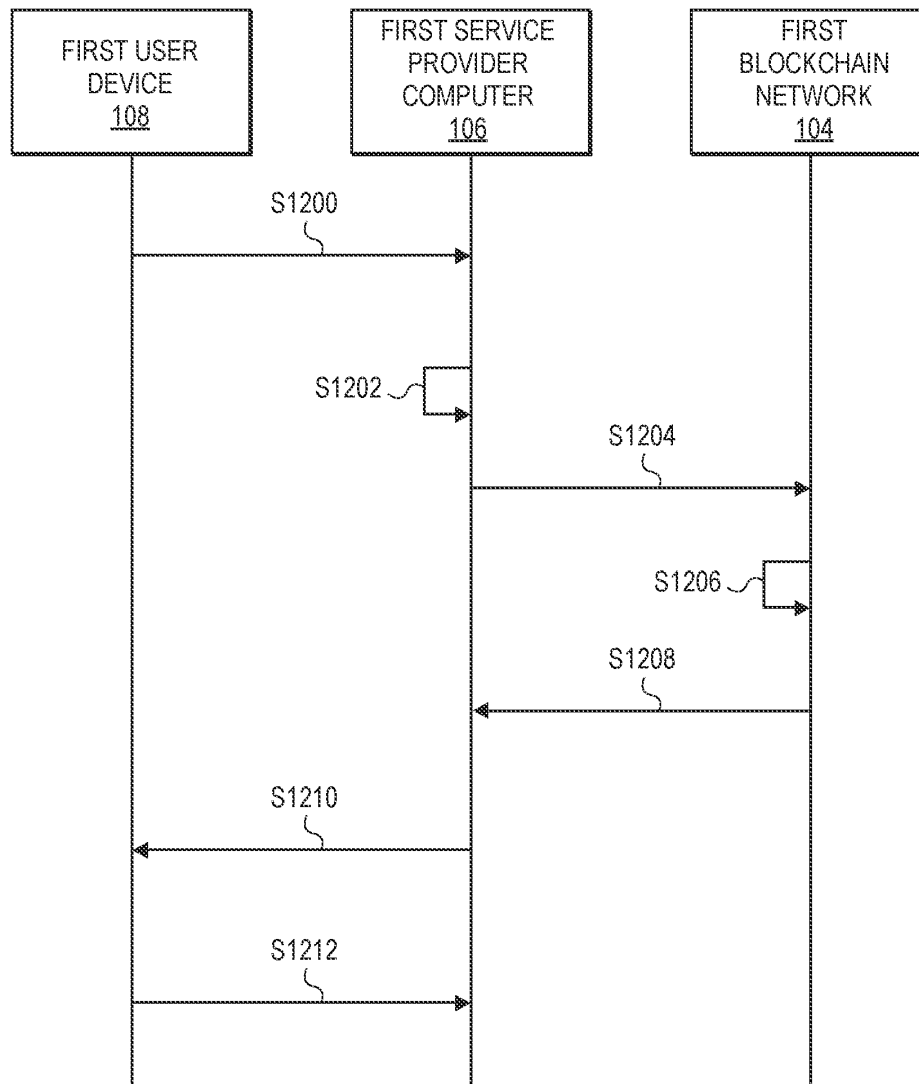
10/15

**FIG. 10**

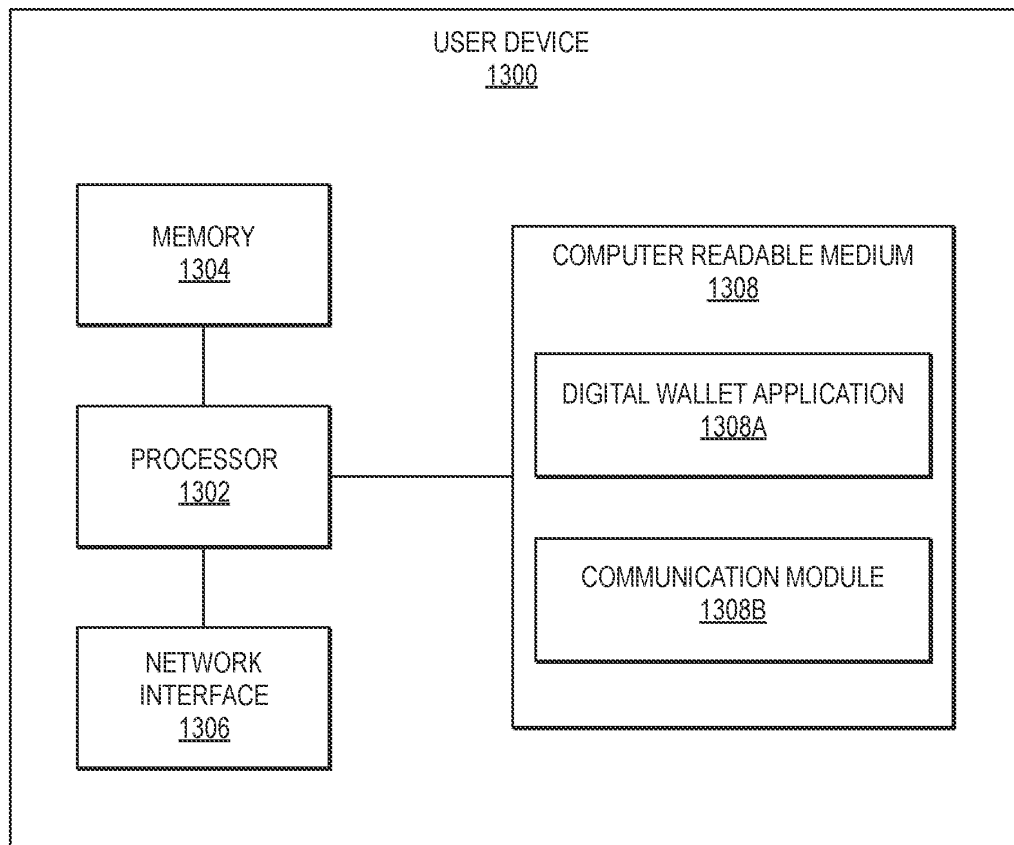
11/15

**FIG. 11**

12/15

**FIG. 12**

13/15

**FIG. 13**

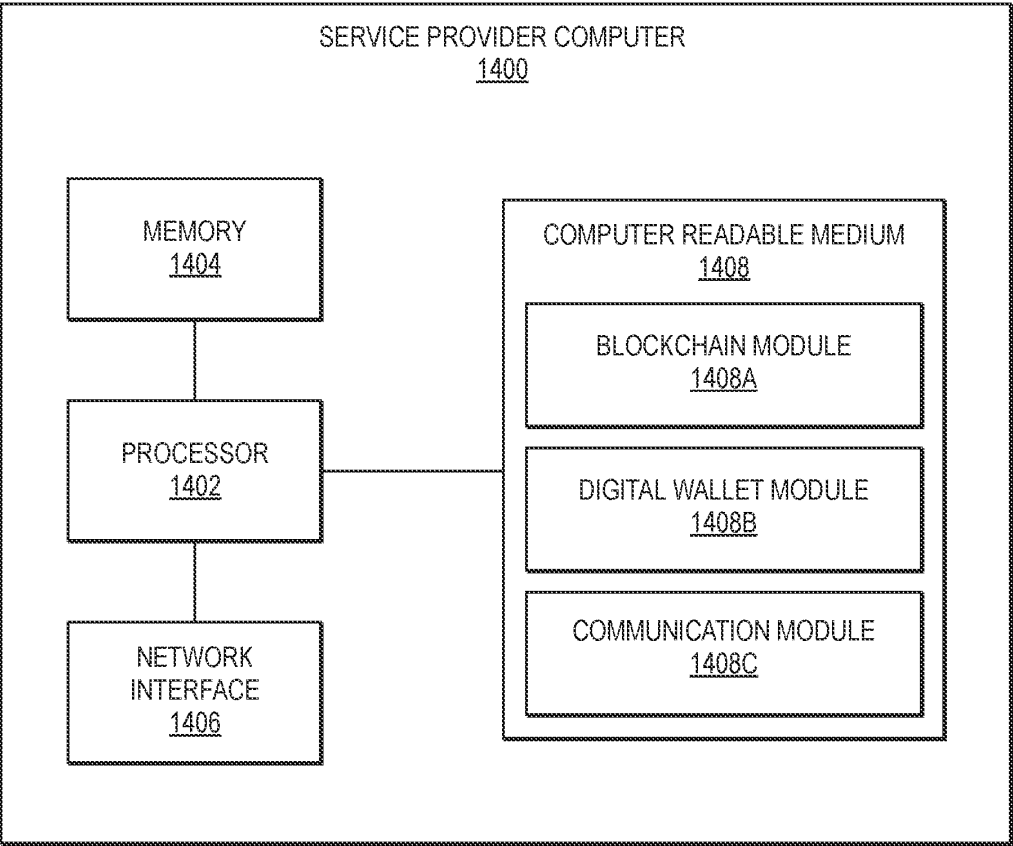
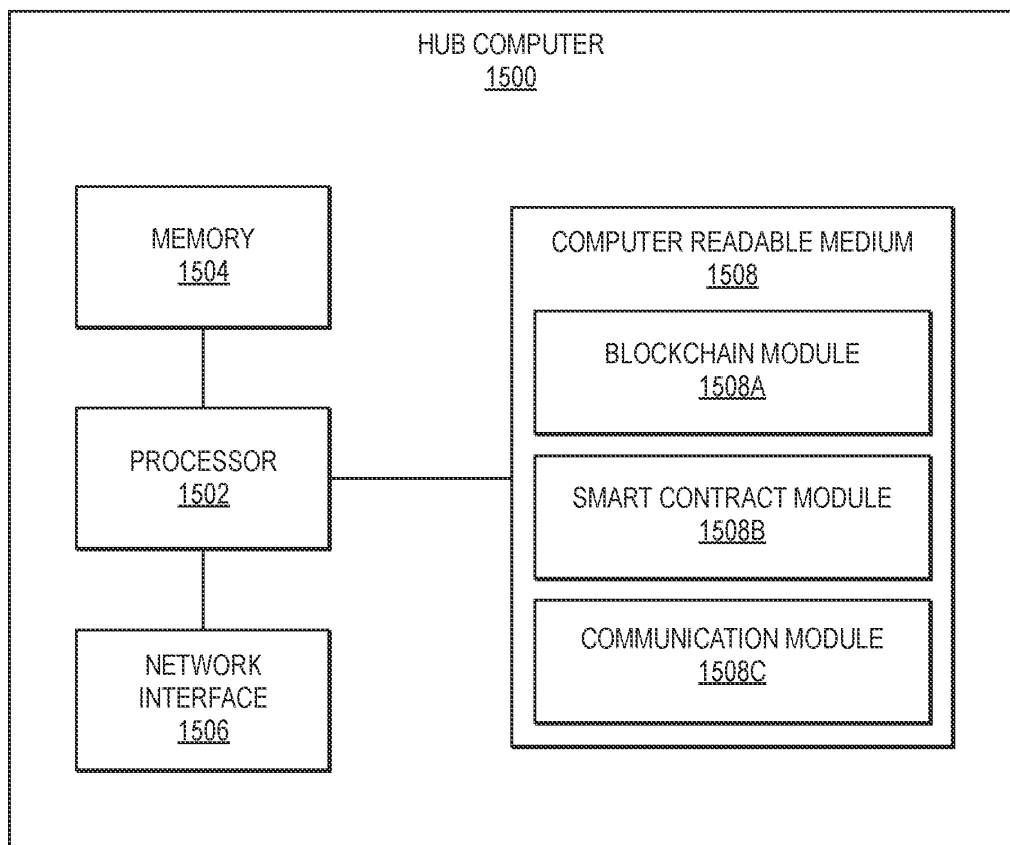


FIG. 14

15/15

**FIG. 15**