1. The following commitments $\{t_1, t_2, t_3\}$ are computed:

$$t_1 = g^u \bmod p$$

$$t_2 = g^v \bmod p$$

$$t_3 = (D_{12a})^u \cdot \beta^{-v} \bmod p$$

Net verifies transaction correctness by verifying the following identities

$$g^r = a^h \cdot t_1 \bmod p$$ // A proves that she knows her PrK = x

$$g^s = (D_{34\beta})^h \cdot t_2 \bmod p$$ // A proves that she knows her random parameter i_{34} used for encryption

$$(E_{34\beta})^h \cdot (E_{12a})^{-h} \cdot (D_{12a})^r \cdot \beta^{-s} = t_3 \bmod p$$

A proves that based on her knowledge of x and i_{34}, the ciphertexts C_{12a} and $C_{34\beta}$ are equivalent.

$g^r = g^{xh+u} = g^{xh} \cdot g^u = (g^x)^h \cdot g^u = a^h \cdot t_1$ mod p; $\qquad a = g^x \bmod p$

$g^s = g^{i34*h+v} = g^{i34*h} \cdot g^v = (g^{i34})^h \cdot g^v = (D_{34\beta})^h \cdot t_2$ mod p; $\qquad (\underbrace{n_{34} \cdot \beta^{i_{34}}}_{E_{34\beta}}, \underbrace{g^{i_{34}}}_{D_{34\beta}}) = C_{34\beta}$

$(E_{34\beta})^h = (n34 \cdot \beta^{i34})^h = (n34)^h \cdot (D_{34\beta})^h$ mod p.

$(E_{12a})^{-h} = (n12 \cdot a^{i12})^{-h} = (n12)^{-h} \cdot a^{-(i12*h)}$ mod p;

$(D_{12a})^r = (g^{i12})^r = (g^{i12*x*h+i12*u}) = (g^x)^{i12*h} \cdot (g^{i12})^u = a^{h*i12} \cdot (g^{i12})^u = a^{i12*h} \cdot (D_{12a})^u$ mod p;

$$(E_{12a}, D_{12a}) = (n_{12} \cdot a^{i_{12}}, g^{i_{12}}) = C_{12a}$$

$$r = (x \cdot h + u) \bmod (p-1)$$

$$s = (i_{34} \cdot h + v) \bmod (p-1)$$

$\beta^{-s} = \beta^{-i34*h-v} = \beta^{-i34*h} \cdot \beta^{-v} = (D_{34\beta})^{-h} \cdot \beta^{-v}$ mod p;

$(E_{34\beta})^h \quad \cdot \quad (E_{12a})^{-h} \quad \cdot \quad (D_{12a})^r \quad \cdot \quad \beta^{-s}$ mod p ===

$$=== (n34)^h \cdot (D_{34\beta})^h \cdot (n12)^{-h} \cdot a^{-(i12*h)} \cdot a^{i12*h} \cdot (D_{12a})^u \cdot (D_{34\beta})^{-h} \cdot \beta^{-v} \mod p ===$$

If balance equation is valid, then $n34 = n12 = n \mod p$ then $(n34)^h = (n12)^{-h} = n^{-h} \mod p$ and $(n34)^h \cdot (n12)^{-h} = n \cdot n^{-h} = 1 \mod p$.

$$=== (n34)^h \cdot (n12)^{-h} \cdot (D_{12a})^u \cdot \beta^{-v} \mod p ===$$

$$=== \underbrace{(n34)^h \cdot (n12)^{-h}}_{1} \cdot (D_{12a})^u \cdot \beta^{-v} === (D_{12a})^u \cdot \beta^{-v} = \boldsymbol{t_3}.$$

The correctness of (30), (31) is proved by the following identities:

$$g^r = g^{xh+u} = g^{xh} \cdot g^u = (g^x)^h \cdot g^u = a^h \cdot t_1; \quad (33)$$

$$g^s = g^{lh+v} = g^{lh} \cdot g^v = (g^l)^h \cdot g^v = (\delta_{\beta,E})^h \cdot t_2. \quad (34)$$

The correctness of (32) is proved by considering every multiplier separately:

$$(\varepsilon_{\beta,E})^h = (E \cdot \beta^l)^h = E^h \cdot \beta^{lh}; \quad (35)$$

$$(\varepsilon_{a,I})^{-h} = (I \cdot a^k)^{-h} = I^{-h} \cdot a^{-kh}; \quad (36)$$

$$(\delta_{a,I})^r = (g^k)^r = (g^{kxh+ku}) = (g^x)^{hk} \cdot (g^k)^u = a^{hk} \cdot (g^k)^u = a^{hk} \cdot (\delta_{a,I})^u; \quad (37)$$

$$\beta^{-s} = \beta^{-lh-v} = \beta^{-lh} \cdot \beta^{-v}. \quad (38)$$

Notice that k is not known to Alice and is included in $(\delta_{a,I})$. If the transaction is honest, then the transaction balance (1) is satisfied and $I=E$ since. Then $E^h \cdot I^{-h} = 1 \mod p$, and putting it all together, we obtain:

$$E^h \cdot \beta^{lh} \cdot I^{-h} \cdot a^{-kh} \cdot a^{hk} \cdot (\delta_{a,I})^u \cdot \beta^{-lh} \cdot \beta^{-v} = (\delta_{a,I})^u \cdot \beta^{-v} = t_3. \quad (39)$$

This is the proof to the Net that the balance equation (1) is valid.