Kỷ yếu Hội nghị Quốc gia lần thứ X về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR), Đà Nẵng, ngày 17-18/08/2017
DOI: 10.15625/vap.2017.00016

ĐỀ XUẤT CHỮ KÝ SỐ ỦY NHIỆM VÀ ỨNG DỤNG CHO ỦY NHIỆM CHI TRONG HỆ THỐNG BITCOIN

Đặng Minh Tuấn[1], Nguyễn Văn Căn[2], Nguyễn Ánh Việt[3], Nguyễn Tiến Xuân[2]

[1]Infinity Blockchain Lab

[2] Trường Đại học Kỹ thuật-Hậu cần CAND

[3]Cục CNTT/BTTm Bộ Quốc phòng

dangtuan@vietkey.vn, cannv@truongt36.edu.vn, nguyenanhviet@hcmpreu.edu.vn,xuantn@vietkey.vn

TÓM TẮT: *Chữ ký số ủy nhiệm cho phép một người có thể ủy quyền cho một người khác ký thay cho mình khi vắng mặt. Đã có một số tác giả đề xuất lược đồ chữ ký ủy nhiệm dựa trên hệ mật trên đường cong elliptic, tuy nhiên một số trong đó hiện có những hạn chế hoặc chưa đáp ứng được nhu cầu. Tác giả đề xuất một lược đồ chữ ký số ủy nhiệm mới dựa trên đường cong elliptic và cụ thể là dựa trên chuẩn thuật toán chữ ký số ECDSA (Elliptic Curve Digital Signature Algorithm) là lược đồ được ứng dụng trong hệ thống Bitcoin (là hệ thống tiền mật mã phổ biến nhất hiện nay) và đồng thời cũng đã được phê duyệt trong nhiều tiêu chuẩn quốc tế, đồng thời cũng đề xuất mô hình ủy nhiệm chi cho hệ thống Bitcoin.*

Từ khóa*: Chữ ký số, chữ ký số ủy nhiệm, hệ mật đường cong elliptic, Bitcoin..*

I. GIỚI THIỆU

Ngày 14-10-2015 Chính phủ Việt Nam đã có Nghị quyết số 36a/NQ-CP về Chính phủ điện tử trong đó có đề cập đến việc cần phải triển khai các giao dịch điện tử không chỉ cho các hoạt động của Chính phủ mà còn cho các giao dịch thanh toán điện tử. Để bảo đảm tính pháp lý của các giao dịch điện tử thì chữ ký số có một vai trò rất quan trọng trong việc xác thực, định danh người giao dịch cũng như tính toàn vẹn của giao dịch.

Chữ ký số có nhiều loại hình ứng dụng khác nhau và một trong số có nhu cầu ứng dụng khá lớn là chữ ký số ủy nhiệm. Chữ ký số ủy nhiệm (proxy signature) cho phép một người có thể ủy quyền cho một người khác ký thay cho mình khi vắng mặt hoặc để ủy quyền ký cho cấp dưới trong những mảng công việc được phân công. Chữ ký số ủy nhiệm lần đầu tiên được đề xuất bởi Mambo và cộng sự trong [1]. Từ đó đến nay đã có rất nhiều công trình công bố liên quan đến chữ ký số ủy nhiệm, từ năm 2009, Das đã liệt kê có hơn 20 công bố về chữ ký số ủy nhiệm [2], tuy nhiên có nhiều lược đồ đề xuất trong thời điểm đó và cho đến nay đã bị phá vỡ hoặc có lỗi trong thiết kế.

Hệ mật dựa trên đường cong elliptic (ECC – Elliptic Curve Cryptography) là một hệ mật tiên tiến hơn hẳn hệ mật RSA do có độ dài khóa nhỏ 160-bit của ECC tương đương với 1024-bit đối với RSA (nguồn: NSA [3]) và sử dụng tài nguyên cũng như ít bộ nhớ hơn so với RSA. ECC đã được đưa vào nhiều tiêu chuẩn quốc tế như IEEE 1363, ANSI X9.62 và X9.63, FIPS 186.4, SECG, ISO 15946-2, RFC 3278…

Chữ ký số dựa trên ECC cũng được đưa vào nhiều tiêu chuẩn ISO 15946-2, FIPS 186.4 và thuật toán chữ ký số dựa trên ECC là ECDSA (Elliptic Curve Digital Signature Algorithm) cũng được sử dụng khá rộng rãi: trong hệ thống tiền mật mã Bitcoin, có thể được lựa chọn sử dụng trong các giao thức HTTPS, TLS, SSL, SSH…

ECDSA nguyên thủy không có khả năng ký ủy nhiệm do đó đã có một số biến thể để có thể sử dụng ECDSA làm nền tảng cho lược đồ chữ ký số ủy nhiệm, tiêu biểu là lược đồ Chang-Chen-Chen [4], Bin-Chenhui [5] và Yanlin-Xiaoping [6]. Tuy nhiên các lược đồ này có một số hạn chế là có nhiều điều chỉnh (thêm thành phần) vào lược đồ gốc ECDSA, đa phần phức tạp hơn. Đặc biệt lược đồ Chang-Chen-Chen [4] không đáp ứng yêu cầu của lược đồ ủy nhiệm được mô tả bởi Lee và cộng sự [7] do lược đồ này không có sự giới hạn về các điều kiện ủy nhiệm, một khi đã được ủy nhiệm thì người được ủy nhiệm sẽ sử dụng mãi mãi quyền ký thay này. Lược đồ Bin-Chenhui [5] còn có lỗi trong thiết kế: công thức (2) trong [5] là $s_oG = r_o y_o h(m_w, r_o, ID_p) + IP_p r_o$ trong đó không thể nhân 02 điểm trên đường cong elliptic là $r_o = k_o G$ với $y_o = x_o G$.

Từ thực tế trên, tác giả đề xuất một lược đồ ký ủy nhiệm mới đơn giản hơn và gần hơn với ECDSA so với một số lược đồ ủy nhiệm trước đây dựa trên ECDSA cũng như trên ECC. Phần còn lại của bài báo được cấu trúc như sau: Phần II: khái lược kiến thức nền tảng đường cong Elliptic và thuật toán ký số dựa trên ECC (ECDSA). Phần III là đề xuất lược đồ chữ ký số ủy nhiệm mới dựa trên ECDSA và phần IV là ứng dụng lược đồ mới vào các bút toán ủy nhiệm chi trong Bitcoin là hệ thống tiền mật mã lâu đời và có giá trị lớn nhất cho đến thời điểm này. Cuối cùng phần V là kết luận của bài báo.

II. HỆ MẬT ECC VÀ CHỮ KÝ SỐ ỦY NHIỆM DỰA TRÊN ECDSA

II.1. Đường cong Elliptic

Đường cong Elliptic là một đường cong đại số được định nghĩa bằng phương trình sau:

$$y^2 = x^3 + ax + b \quad (1)$$

Đường cong này không kỳ dị (không có các điểm tự cắt nhau hoặc các điểm lùi) khi và chỉ khi định thức của đường cong đó khác không: $4a^2 + 27b^2 \neq 0$. Phương trình trên còn gọi là phương trình Weierstrass của đường cong Elliptic. Coi a, b, x và y là các phần tử của các trường số thực, số hữu tỷ, số phức hoặc trường hữu hạn $\mathbb{F}_q$ trong đó $q = p^n$ với p là số nguyên tố và $n \geqq 1$. Nếu K là một trường với $a, b \in K$, thì ta nói đường cong Elliptic được định nghĩa trên K. Điểm (x, y) trên đường cong với $(x, y) \in K$ được gọi là điểm K-hữu tỷ. Trong bài báo này chúng ta không xét phương trình tổng quát Weierstrass cũng như đường cong Elliptic trong trường $\mathbb{F}_{2^m}$ với m là số nguyên.

Vì lý do kỹ thuật, chúng ta thêm "điểm vô cùng" (∞) vào đường cong Elliptic và cho nó là điểm trung hòa với ký hiệu $\mathcal{O}$. Điểm trung hòa có thể nằm trên cùng hoặc dưới cùng của trục y. Một trong những thuộc tính quan trọng nhất của đường Elliptic là tồn tại phép tính cộng cho các điểm trên đường cong. Xét hai điểm $P_1 = (x_1, y_1)$ và $P_2 = (x_2, y_2); P_1 \neq P_2$ trên đường cong Elliptic với ký hiệu là $E: y^2 = x^3 + ax + b$.

Định nghĩa phép cộng như sau: $P_3 = P_1 + P_2$, ở đó $P_3 = (x_3, y_3)$ là điểm đối xứng qua trục hoành của điểm P_3' trên đường cong E và P_3', P_1, P_2 cũng cùng nằm trên một đường thẳng. Theo [8], ta có các công thức để tính cho điểm P_3 như sau:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right) \times (x_1 - x_3)$$

Định lý 2.1: Với các điểm P, P_1, P_2, P_3 trên đường cong E, phép cộng các điểm trên đường cong Elliptic E thỏa mãn các thuộc tính sau:

Tính giao hoán: $P_1 + P_2 = P_2 + P_1$;

Tồn tại điểm trung hòa sao cho: $P + \mathcal{O} = P$;

Tồn tại điểm đối lập: với mọi P trên E, luôn tồn tại điểm P' cũng trên E sao cho $P' + P = \mathcal{O}$;

Tính kết hợp: $P_1 + (P_2 + P_3) = (P_1 + P_2) + P_3$.

Chứng minh chi tiết định lý được trình bày trong [9], [10]. Phép nhân vô hướng trên E được định nghĩa như những phép cộng liên tiếp, ví dụ $Q = kP$ có nghĩa là điểm Q được tạo thành do k lần phép cộng chính điểm $P, Q = \underbrace{P + P + \cdots + P}_{k}$. Bài toán cho trước P, Q tìm điểm k là bài toán rất khó và nó được gọi là bài toán Logarit rời rạc của đường cong Elliptic. Cơ sở toán học của phép mã hóa hay chữ ký số dựa trên đường cong Elliptic đều xuất phát từ bài toán Logarit rời rạc này.

II.2. Thuật toán ECDSA (Elliptic Curve Digital Signature Algorithm)

Đường cong Elliptic E có điểm cơ sở G có bậc là n. Thuật toán ký số ECDSA được dùng trong Bitcoin, người ký có cặp khóa bí mật và công khai là (d, Q). Với văn bản m tính giá trị băm $e = SHA256(m)$.

Hình thành chữ ký số ECDSA:

1- Chọn 1 số ngẫu nhiên lớn 256-Bit gọi là k.

2- Tính điểm trên đường cong Elliptic: $R(x_R, y_R) = kG$, và chọn $r = x_R \mod n$.

3- Tính giá trị $s = (e + d \times r)k^{-1} \bmod n$. Chữ ký số của văn bản m sẽ là cặp giá trị (r, s). Nếu $k = 0$ hoặc $s = 0$ thì phải thực hiện lại bước 1.

Xác thực chữ ký số ECDSA:

1- Sau khi nhận được văn bản m' và chữ ký số (r, s) và biết khóa công khai Q của người ký chúng ta phải kiểm tra: có đúng văn bản nhận được m' có chữ ký là (r, s) hay không. Tính giá trị băm của văn bản m': $e' = SHA256(m')$.

2- Xác thực bằng các tính điểm $V(x_V, y_V) = s^{-1}e'G + s^{-1}rQ$, kiểm tra nếu $r = x_V$ thì chữ ký số hợp lệ.

III. ĐỀ XUẤT CHỮ KÝ SỐ ỦY NHIỆM DỰA TRÊN ECDSA

Ký hiệu:

Or	Người ủy nhiệm ký (Original Signer) có cặp khóa bí mật và khóa công khai là (d_O, Q_O).
Pr	Người được ủy nhiệm ký (Proxy Signer) có cặp khóa bí mật và khóa công khai là (d_P, Q_P).
Vr	Người xác thực chữ ký ủy nhiệm (Verifier).
$\bar{x}(R)$	Hàm lấy giá trị x_R của điểm $R = (x_R, y_R)$ trên đường cong Elliptic nghĩa là $x_R = \bar{x}(R)$.
p	Số nguyên tố lớn.
E	Đường cong Elliptic trên trường hữu hạn $\mathbb{F}_p$.
n	Số điểm trên đường cong E.
G	Điểm cơ sở trên E có bậc n.
$h(m)$	Hàm băm chuỗi bit m, với Bitcoin hàm này sẽ là SHA-256.
h_w	Điều kiện ủy nhiệm.
$A \to B$	Người *A* gửi dữ liệu đến cho người *B*.

III.1. Hình thành khóa ủy nhiệm

Người được ủy nhiệm Pr ở bước đầu tiên sẽ gửi khóa công khai Q_P cho người ủy nhiệm và người xác thực chữ ký số ủy nhiệm (bước 1). Ở bước 2 người ủy nhiệm Or sẽ chọn số nguyên k_O và tính theo các công thức (2), (3). Ở bước 3. Người ủy nhiệm Or sẽ gửi các giá trị m_w và (r_O, s_O) tới người được ủy quyền và người xác thực chữ ký số. Ở bước 4, người xác thực Pr sẽ kiểm tra tính hợp lệ của chữ ký số của người ủy nhiệm Or nếu không thỏa mãn thì yêu cầu cấp lại chữ ký số của người ủy nhiệm, nếu hợp lệ sẽ tiến hành tính khóa bí mật và khóa công khai mới là d_{Pr}, Q_{Pr}.

Ở bước 2 giá trị m_w là điều kiện để ủy nhiệm, có thể là một biểu thức regular expression tổng hợp nhiều điều kiện ủy nhiệm khác nhau như: khoảng thời gian ủy nhiệm kết hợp với giá trị ủy nhiệm, hoặc lĩnh vực (mảng) được ủy nhiệm…

1.	$Pr \to (Or, Vr)$:	Q_P.
2.	Or:	Or có cặp khóa bí mật và khóa công khai là (d_O, Q_O) với $Q_O = d_O G$. Chọn k_O với điều kiện $(1 < k_O < q)$. Tính: $r_P = \bar{x}(Q_P)$, $R_O = k_O G$ và $r_O = \bar{x}(R_O) \mod n$ (2) $s_O = k_O^{-1}(h(m_w, r_P) + r_O d_O) \mod n$ (3)
3.	$Or \to (Pr, Vr)$:	m_w và (r_O, s_O).
4.	*Pr:*	*Pr* có cặp khóa bí mật và khóa công khai là (d_P, Q_P) với $Q_P = d_P G$. Tính:

		$w_O = s_O^{-1} \bmod n$, $z = h(m_w, r_P)$, $u_{1_O} = zw_O \bmod n$, $u_{2_O} = r_O w_O \bmod n$ $R_{OP} = u_{1_O} G + u_{2_O} Q_O$, $r_{OP} = \bar{x}(R_{OP})$ (4) Kiểm tra: $r_O \overset{?}{=} r_{OP}$, chấp nhận nếu thỏa mãn. Tính khóa bí mật và công khai ủy nhiệm theo công thức: $d_{Pr} = s_O + zd_P$ và $Q_{Pr} = d_{Pr} G$.

III.2. Ký văn bản được ủy nhiệm

1.	*Pr*:	Chọn k với điều kiện $(1 < k < q)$. Tính: $R = kG$ và $r = \bar{x}(R) \bmod n$ (5) $s = k^{-1}(h(m) + rd_{Pr}) \bmod n$ (6)
2.	$Pr \rightarrow Vr$:	m, Q_{Pr} và chữ ký số (r, s).

III.3. Xác thực văn bản được ủy nhiệm

1.	*Vr*:	Tính: $z = h(m_w, r_P)$. Kiểm tra: $Q_{Pr} \overset{?}{=} s_O G + zQ_P$ nếu đúng chấp nhận chữ ký của *Pr* đúng là được ủy nhiệm bởi *Or* và tiếp tục thực hiện bước xác thực tiếp theo: Tính: $w = s^{-1} \bmod n$, $u_1 = h(m)w \bmod n$, $u_2 = rw \bmod n$ $R_{Vr} = u_1 G + u_2 Q_{Pr}$, $r_{Vr} = \bar{x}(R_{Vr}) \bmod n$ Kiểm tra: $r \overset{?}{=} r_{Vr}$, chấp nhận nếu thỏa mãn.

III.4. Chứng minh tính đúng đắn của lược đồ chữ ký số ủy nhiệm

Định lý 3.1: Với giá trị $h(m_w, r_P)$ và r_O, s_O, r_{OP} được tính theo các công thức (2),(3),(4) ở mục III.1 thì $r_O = r_{OP}$.

Chứng minh: Vì r_{OP}, r_O là các giá trị x của 02 điểm trên đường cong Elliptic là R_{OP} và R_O, ta chỉ cần chứng minh 2 điểm này bằng nhau, thực vậy:

$$\begin{aligned} R_{OP} &= u_{1_O} G + u_{2_O} Q_O \\ &= zw_O G + r_O w_O Q_O \\ &= s_O^{-1}(z + r_O d_O) G \\ &= k_O (z + r_O d_O)^{-1} (z + r_O d_O) G \\ &= k_O G \\ &= R_O \end{aligned}$$

Định lý 3.2: Với giá trị $h(m)$ và r, s, r_{Vr} được tính theo các công thức (5), (6), (7) ở mục III.2 thì $r = r_{Vr}$.

Chứng minh: Vì r_{Vr}, r là các giá trị x của 02 điểm trên đường cong Elliptic là R_{Vr} và R, ta chỉ cần chứng minh 2 điểm này bằng nhau, thực vậy:

$$\begin{aligned} R_{Vr} &= u_1 G + u_2 Q_{Pr} \\ &= h(m) wG + rwQ_{Pr} \\ &= s^{-1}(h(m) + rd_{Pr}) G \\ &= k(h(m) + rd_{Pr})^{-1} (h(m) + rd_{Pr}) G \\ &= kG \\ &= R \end{aligned}$$

III.5. Phân tích độ an toàn của lược đồ đề xuất

Trong cả 2 phần III.1 và III.2 có thể thấy bài báo sử dụng 02 lược đồ chuẩn ECDSA trong quá trình xây dựng giao thức ủy nhiệm do đó có thể sử dụng các thư viện và phần mềm hiện có cho ECDSA để xây dựng thành công cụ cho chữ ký số ủy nhiệm. Ngoài ra, có thể khẳng định độ an toàn của lược đồ chữ ký số ủy nhiệm đề xuất dựa trên độ an toàn của lược đồ ECDSA, về độ an toàn của lược đồ chuẩn ECDSA đã có nhiều công trình công bố và đã được đưa vào nhiều chuẩn cũng như thực tế sử dụng, đặc biệt là trong hệ thống Bitcoin.

Lược đồ chữ ký số ủy nhiệm được đề xuất cũng có khả năng chịu được 03 kịch bản tấn công như được mô tả trong [4].

IV. ÁP DỤNG CHỮ KÝ SỐ ỦY NHIỆM CHO ỦY NHIỆM CHI TRONG HỆ THỐNG BITCOIN

Trong mục này chúng ta áp dụng lược đồ chữ ký số ủy nhiệm đã được đề xuất ở phần III. để áp dụng cho các bút toán ủy nhiệm chi trong hệ thống tiền mật mã Bitcoin. Ủy nhiệm chi là việc một người có thể ủy quyền cho một người khác hoặc một cơ quan khác để chi trả cho bên thứ 3 khi người đó đi vắng hoặc không có điều kiện chi trả trực tiếp với các điều kiện giới hạn nào đó, tương tự như ở phần trên các điều kiện ủy nhiệm được thể hiện qua chuỗi bit m_w tương tự như đã mô tả ở mục III.1.

Trong hệ thống Bitcoin, các dữ liệu được tổ chức thành các khối (block), mỗi khối lại chứa nhiều dữ liệu nhỏ hơn là các giao dịch (transaction), mỗi giao dịch lại có một hoặc nhiều đầu vào (input) và một hay nhiều đầu ra (output). Input của một giao dịch sẽ là Output của một giao dịch được thực hiện ở thời gian trước đó. Khi có một bút toán giao dịch chi trả thì trong đầu ra sẽ chứa đoạn mã *locking script* và nguồn vào input được lấy từ một output trước đó gửi đến và chứa đoạn mã *unlocking script.* Các đoạn mã script này là mã lệnh dạng stack-based có nghĩa là các tham số đầu vào và kết quả trả về sẽ được đẩy vào ngăn xếp (stack). Ngôn ngữ script bao gồm 80 lệnh được liệt kê tại [11], bao gồm các lệnh về xử lý chuỗi, phép tính số học, mã hóa, hàm băm…

Các giao dịch trong hệ thống Bitcoin được thực hiện thông qua các transaction được mô tả trong [12], [13]. Khi hình thành các giao dịch thì người tạo ra giao dịch cần phải ký số thông qua ECDSA toàn bộ dữ liệu của transaction (hình 1). Sau khi hình thành transaction, người tạo ra nó sẽ phát tán transaction đó đến tất cả các mode trong mạng thông qua mạng ngang hành peer-to-peer. Ở mỗi node, transaction sẽ được kiểm tra tính hợp lệ, nếu hợp lệ thì sẽ tiếp tục phát tán, nếu không sẽ dừng không chuyển tiếp và transaction sẽ không được lưu thông trong hệ thống.

Trong quá trình kiểm tra tính hợp lệ của transaction, với mỗi input, phần mềm client sẽ lấy các mã lệnh locking script trong ouput của transaction được trỏ tới bởi input. Phần mềm client sẽ thực hiện mã unlocking script trong input ngay sau đó là mã locking script của output được input trỏ tới. Kết quả thực hiện 2 đoạn mã này nếu trả về giá trị TRUE trên stack thì transaction đó hợp lệ. Các locking script và unlocking script mặc định được liệt kê ở mục IV.2 và IV.1.

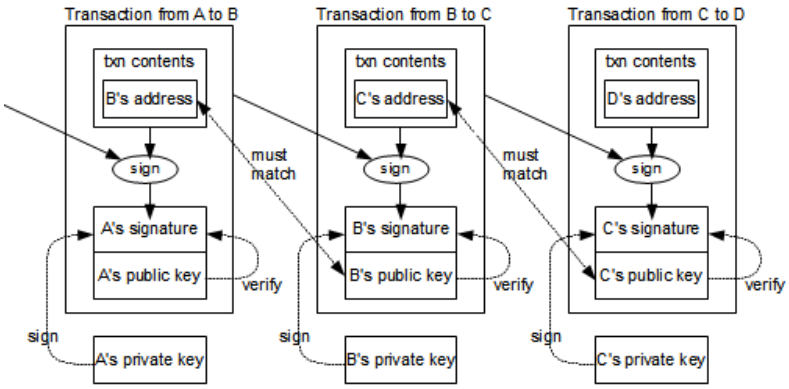
Lệnh <OP_PUSHDATA1> là đẩy chuỗi bytes sau mã lệnh vào ngăn xếp. Lệnh <OP_DUP> là copy đúp giá trị trên đỉnh ngăn xếp sẽ tạo ra 2 giá trị giống nhau trên đỉnh stack. Lệnh <OP_HASH160> là băm SHA-256 và sau đó băm tiếp theo RIPEMD-160 giá trị nằm trên đỉnh stack. Lệnh <OP_EQUALVERIFY> là kiểm tra 2 giá trị trên đỉnh stack có trùng nhau không, nếu trùng trả về giá trị TRUE. Lệnh <OP_CHECKSIG> là kiểm tra chữ ký số của chữ ký số và kháo công khai được lưu trên đỉnh stack. Lệnh ><OP_CHECKMULTISIG> là lệnh kiểm tra chữ ký số tập thể (có ít nhất 02 chữ ký thì transaction mới hợp lệ). Lệnh <OP_DROP> xóa đỉnh ngăn xếp.

IV.1. Unlocking script mặc định

```
a.1.    <OP_PUSHDATA1><chữ ký số Sig và SIGHASH_ALL>
a.2.    <OP_PUSHDATA1><khóa công khai PubK>
```

IV.2. Locking script mặc định

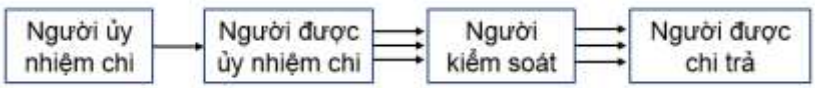
```
b.1.    <OP_DUP>
b.2.    <OP_HASH160>
b.3.    <OP_PUSHDATA1><Bitcoin address (public key hash)>
b.4.    <OP_EQUALVERIFY>
b.5.    <OP_CHECKSIG>
```



Hình 1. Ký số các giao dịch transaction trong hệ thống Bitcoin

IV.3. Đề xuất mô hình ủy nhiệm chi

Hình 2 là mô hình đề xuất cho ủy nhiệm chi trong Bitcoin. Các mã script cũng được điều chỉnh để người kiểm soát có thể kiểm tra tính hợp lệ của chữ ký ủy nhiệm. Các điều chỉnh mã lệnh này không phá vỡ tính đúng đắn của kiểm tra chữ ký trong mô hình truyền thống. Các mã điều chỉnh



Hình 2. Mô hình ủy nhiệm chi trong Bitcoin

Mô hình ủy nhiệm chi được mô tả khái lược ở hình 2:

Người ủy nhiệm chi sẽ thực hiện 01 transaction với số Bitcoin sẽ ủy nhiệm cho người được ủy nhiệm với *locking script ủy nhiệm* (xem mục IV.5).

Người được ủy nhiệm mỗi khi chi trả cho người được chi trả sẽ thực hiện một transaction với số Bitcoin nhỏ hơn hoặc bằng số Bitcoin được ủy nhiệm với *unlocking script ủy nhiệm* (xem mục IV.4) đến người kiểm soát. Người được ủy nhiệm không thể chi trả cho người được chi trả do các transaction này đòi hỏi phải có chữ ký của người kiểm soát nữa.

Người kiểm soát sau khi kiểm tra các điều kiện ủy nhiệm như được mô tả ở phần III, sẽ ký tiếp vào transaction để đủ 02 chữ ký và chuyển tiếp transaction này đến người được chi trả. Lúc này do có đủ 02 chữ ký nên điều kiện kiểm tra <OP_CHECKMULTISIG> sẽ được thỏa mãn và người được chi trả sẽ nhận được số Bitcoin do người được ủy nhiệm chi trả. Vai trò người kiểm soát ở đây có thể được thực hiện bởi một phần mềm được thiết kế tự động kiểm tra các điều kiện ủy nhiệm được mô tả ở phần III.

IV.4. Unlocking script ủy nhiệm

c.1. <OP_0>
c.2. <OP_PUSHDATA1><chữ ký số Sig_C và SIGHASH_ALL>
c.3. <OP_PUSHDATA1><chữ ký số Sig và SIGHASH_ALL>
c.4. <OP_PUSHDATA1><khóa công khai PubK>

IV.5. Locking script ủy nhiệm

d.1. <OP_DUP>
d.2. <OP_HASH160>
d.3. <OP_PUSHDATA1><Bitcoin address (public key hash)>
d.4. <OP_EQUALVERIFY>
d.5. <OP_PUSHDATA1>< Q_C >
d.6. <2><OP_CHECKMULTISIG>
d.7. <OP_PUSHDATA1>< m_w >
d.8. <OP_PUSHDATA1>< Q_P >
d.9. <OP_PUSHDATA1>< Q_O >

d.10. <OP_PUSHDATA1><(r_O, s_O)>

d.11. <OP_PUSHDATA1><Q_{Pr}>

d.12. <OP_PUSHDATA1><Q_C>

d.13. <OP_PUSHDATA1><m>

d.14. <OP_PUSHDATA1><(r, s)>

d.15. <OP_DROP><OP_DROP><OP_DROP><OP_DROP>

d.16. <OP_DROP><OP_DROP><OP_DROP><OP_DROP>

V. KẾT LUẬN

Trong bài báo này, tác giả đã đề xuất một lược đồ chữ ký số ủy nhiệm mới dựa trên thuật toán chuẩn ECDSA, so với một số đề xuất trước đó cũng dựa trên ECDSA hoặc dựa trên đường cong Elliptic thì lược đồ mới đơn giản hơn và gần với ECDSA hơn vì vậy không phải thay đổi nhiều vào thuật toán và chương trình ký số ECDSA có sẵn, độ an toàn của thuật toán cũng dựa trên độ an toàn của ECDSA đã được chứng minh và công nhận sử dụng trong nhiều chuẩn và thực tiễn. Dựa trên ý tưởng của lược đồ mới đề xuất có thể dễ dàng điều chỉnh để có thể xây dựng các lược đồ chữ ký số ủy nhiệm tập thể hoặc ủy nhiệm ký mù. Ngoài ra bài báo cũng đề xuất một giao thức áp dụng lược đồ đề xuất để thực hiện các giao dịch ủy nhiệm chi cho hệ thống tiền mật mã lâu đời và phổ biến nhất hiện nay là Bitcoin.

TÀI LIỆU THAM KHẢO

[1] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: delegation of the power to sign messages," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E79–A, no. 9, pp. 1338–1353, 1996.

[2] M. L. Das, A. Saxena, and D. B. Phatak, "Algorithms and approaches of proxy signature: A survey," *International Journal of Network Security*, vol. 9, no. 3, pp. 264–284, 2009.

[3] "The Case for Elliptic Curve Cryptography," 2009. [Online]. Available: http://www.nsa.gov/business/programs/elliptic_curve.shtml.

[4] M.-H. Chang, I.-T. Chen, and M.-T. Chen, "Design of Proxy Signature in ECDSA," *2008 Eighth International Conference on Intelligent Systems Design and Applications*, pp. 17–22, 2008.

[5] H. Bin and J. Chenhui, "A Secure Proxy Signature Scheme Based On Elliptic Curve Cryptosystem," *JOURNAL OF ELECTRONICS*, vol. 23, no. 1, pp. 54–57, 2006.

[6] Q. Yanlin and W. Xiaoping, "A New Digital Multilevel Proxy Signature Scheme Based on Elliptic Curve Cryptography," *University Journal of Natural Sciences*, vol. 11, no. 6, pp. 1704–1706, 2006.

[7] B. Lee, H. Kim, and K. Kim, "Strong Proxy Signature and its Applications," *SCIS2001*, vol. 2, pp. 603–608, 2001.

[8] I. Blatcher, *Cryptography and Elliptic Curves*. 2010.

[9] J. H. Silverman, *The Arithmetic of Elliptic Curves*. Springer, 2009.

[10] Đ. M. Tuấn, "Hệ mật mã khóa công khai dựa trên đường cong Elliptic - Một số ứng dụng (1)," *Epsilon Magazine*, vol. 9, pp. 17–35, 2016.

[11] "Bitcoin Script." [Online]. Available: https://en.bitcoin.it/wiki/Script.

[12] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Www.Bitcoin.Org*, pp. 1–9, 2008.

[13] H. Kuzuno and C. Karam, "Blockchain Explorer/: An Analytical Process and Investigation Environment for Bitcoin," *Electronic Crime Research (eCrime)*, 2017.

A NEW PROXY SIGNATURE SCHEME BASED ON ECDSA AND ITS APPLICATION FOR AUTHORIZED PAYMENTS IN BITCOIN

Dang Minh Tuan, Nguyen Van Can, Nguyen Anh Viet, Nguyen Tien Xuan

ABSTRACT: *Proxy signature is a special digital signature which enables a proxy signer to sign messages on behalf of the original signer. In this paper, we propose a new proxy signature scheme based on ECDSA (Elliptic Curve Digital Signature Algorithm), which has been approved in many standard and then we also describe it's application for authorized payments in Bitcoin, which is the largest and most popular cryptocurrency system today.*