US009735958B2

(12) **United States Patent**
Alness et al.

(10) **Patent No.: US 9,735,958 B2**
(45) **Date of Patent: Aug. 15, 2017**

(54) **KEY CEREMONY OF A SECURITY SYSTEM FORMING PART OF A HOST COMPUTER FOR CRYPTOGRAPHIC TRANSACTIONS**

(71) Applicant: **Coinbase, Inc.**, San Francisco, CA (US)

(72) Inventors: **Andrew E. Alness**, Santa Cruz, CA (US); **James Bradley Hudon**, San Francisco, CA (US)

(73) Assignee: **Coinbase, Inc.**, San Francisco, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/716,100**

(22) Filed: **May 19, 2015**

(65) **Prior Publication Data**

US 2016/0344543 A1 Nov. 24, 2016

(51) **Int. Cl.**

H04L 9/32	(2006.01)
H04L 9/08	(2006.01)
G06Q 20/06	(2012.01)
G06Q 20/38	(2012.01)
G06F 21/00	(2013.01)

(52) **U.S. Cl.**

CPC ***H04L 9/0819*** (2013.01); ***G06Q 20/065*** (2013.01); ***G06Q 20/3823*** (2013.01)

(58) **Field of Classification Search**

CPC H04L 63/0428; H04L 2209/24; H04L 63/061; H04L 63/065; H04L 63/067; H04L 63/068; H04L 63/0846; H04L 9/0822

USPC 713/170, 171, 175, 168; 380/227, 282

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,855,318	B1 *	10/2014	Patnala	H04L 9/0822 380/277
9,071,429	B1 *	6/2015	Roth	H04L 9/3268
2002/0116611	A1 *	8/2002	Zhou	H04L 9/004 713/156
2005/0138374	A1 *	6/2005	Zheng	H04L 9/0894 713/166
2007/0223706	A1 *	9/2007	Gantman	G06F 21/34 380/286
2008/0263363	A1 *	10/2008	Jueneman	G06F 21/32 713/184
2009/0254750	A1 *	10/2009	Bono	H04L 63/0428 713/170
2010/0054458	A1 *	3/2010	Schneider	H04L 9/085 380/28
2010/0175061	A1 *	7/2010	Maeda	G06F 8/65 717/173
2010/0235588	A1 *	9/2010	Maeda	H04L 9/085 711/147

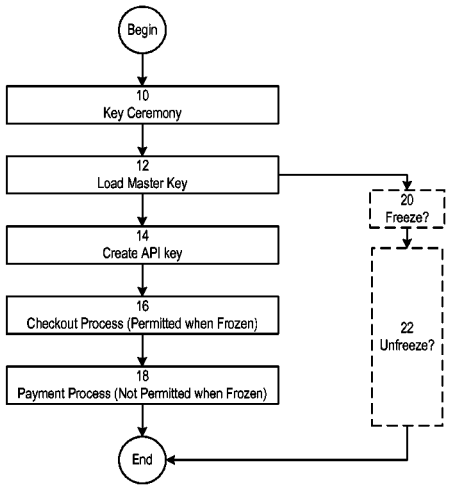
(Continued)

Primary Examiner — Gary Gracia

(74) *Attorney, Agent, or Firm* — Stephen M. De Klerk

(57) **ABSTRACT**

A key ceremony application creates bundles for custodians encrypted with their passphrases. Each bundle includes master key share. The master key shares are combined to store an operational master key. The operational master key is used for private key encryption during a checkout process. The operational private key is used for private key decryption for transaction signing in a payment process. The bundles further include TLS keys for authenticated requests to create an API key for a web application to communicate with a service and to unfreeze the system after it has been frozen by an administrator.

5 Claims, 8 Drawing Sheets

Sequential Setup and Operation