(12) **Translation of European patent specification**

(11) **NO/EP 3257191 B1**

NORWAY

(19) NO

(51) Int Cl.

H04L 9/00 (2006.01)
G06Q 20/02 (2012.01)
G06Q 20/36 (2012.01)
G06Q 30/06 (2012.01)

Norwegian Industrial Property Office

(21)	Translation Published	2018.09.24
(80)	Date of The European Patent Office Publication of the Granted Patent	2018.04.11
(86)	European Application Nr.	17708587.5
(86)	European Filing Date	2017.02.16
(87)	The European Application's Publication Date	2017.12.20
(30)	Priority	2016.02.23, GB, 201603114 2016.02.23, GB, 201603117 2016.02.23, GB, 201603123 2016.02.23, GB, 201603125 2016.04.01, GB, 201605571 2016.11.15, GB, 201619301
(84)	Designated Contracting States:	AL ; AT ; BE ; BG ; CH ; CY ; CZ ; DE ; DK ; EE ; ES ; FI ; FR ; GB ; GR ; HR ; HU ; IE ; IS ; IT ; LI ; LT ; LU ; LV ; MC ; MK ; MT ; NL ; NO ; PL ; PT ; RO ; RS ; SE ; SI ; SK ; SM ; TR
(73)	Proprietor	Nchain Holdings Limited, Fitzgerald House 44 Church Street, St. John's, AG-Antigua og Barbuda
(72)	Inventor	WRIGHT, Craig Steven, c/o Urquhart-Dykes&Lord LLP7th Floor Churchill HouseChurchill Way, Cardiff CF10 2HH, GB-Storbritannia SAVANAH, Stephane, c/o Urquhart-Dykes&Lord LLP7th Floor Churchill HouseChurchill Way, Cardiff CF10 2HH, GB-Storbritannia
(74)	Agent or Attorney	TANDBERG INNOVATION AS, Postboks 1570 Vika, 0118 OSLO, Norge

(54) Title **REGISTRY AND AUTOMATED MANAGEMENT METHOD FOR BLOCKCHAIN-ENFORCED SMART CONTRACTS**

(56) References Cited:

US-A1- 2015 206 106, Andreas M. Antonopoulos: "Mastering Bitcoin - Unlocking Digital Cryptocurrencies" In: "Mastering bitcoin : [unlocking digital cryptocurrencies]", 20 December 2014 (2014-12-20), O'Reilly Media, Beijing Cambridge Farnham Köln Sebastopol Tokyo, XP055306939, ISBN: 978-1-4493-7404-4 page 22 - page 25 page 113 - page 117, Jeff Herbert ET AL: "A Novel Method for Decentralised Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology", , 27 January 2015 (2015-01-27), XP055358639, Retrieved from the Internet: URL:http://crpit.com/confpapers/CRPITV159H erbert.pdf [retrieved on 2017-03-24]

Enclosed is a translation of the patent claims in Norwegian. Please note that as per the Norwegian Patents Acts, section 66i the patent will receive protection in Norway only as far as there is agreement between the translation and the language of the application/patent granted at the EPO. In matters concerning the validity of the patent, language of the application/patent granted at the EPO will be used as the basis for the decision. The patent documents published by the EPO are available through Espacenet (http://worldwide.espacenet.com) or via the search engine on our website here: https://search.patentstyret.no/

Patentkrav

1. Datamaskinimplementert fremgangsmåte for å kontrollere synligheten og/eller ytelsen til en kontrakt, idet fremgangsmåten er omfattende trinnene:
(a) å lagre en kontrakt på eller i et databasert lager;
(b) å kringkaste en transaksjon til en blokkjede, idet transaksjonen omfatter:
i) minst én ubrukt utgangsverdi (UTXO); og
ii) metadata som omfatter en identifikator som indikerer plasseringen der kontrakten er lagret;
(c) å tolke kontrakten som åpen eller gyldig inntil den ubrukte utgangsverdien (UTXO) brukes på blokkjeden;
og
(d) å fornye eller rulle kontrakten på ved:
å generere en ny nøkkel ved hjelp av data knyttet til en tidligere nøkkel forbundet med kontrakten;
å generere et skript som omfatter den nye nøkkelen, plasseringen til kontrakten og en rute til kontrakten; og
å betale et valutabeløp til skriptet.

2. Fremgangsmåte ifølge krav 1, hvori transaksjonen videre omfatter en deterministisk innløsningsskriptadresse, fortrinnsvis hvori innløsningsskriptadressen er en betal-for-skript-rute-adresse (P2SH).

3. Fremgangsmåte ifølge krav 2 og videre omfattende trinnet med å avslutte kontrakten ved å kringkaste en ytterligere transaksjon til blokkjeden for å bruke den ubrukte utgangsverdien (UTXO).

4. Fremgangsmåte ifølge krav 3, hvori den videre transaksjonen omfatter:
en inngang som er den ubrukte utgangsverdien (UTXO); og
et opplåsingsskript omfattende en signatur; metadataene; og en offentlig nøkkel.

5. Fremgangsmåte ifølge ett foregående krav, hvori kontrakten definerer:
i) minst én tilstand; og
ii) minst én handling hvis ytelse avhenger av evalueringen av tilstanden; og/eller
hvori metadataene omfatter:

i) en adresse eller representasjon av en adresse på hvor kontrakten er lagret i det databaserte lageret; og/eller
ii) en rute til kontrakten.

6. Fremgangsmåte ifølge ett foregående krav, og omfattende trinnet:
å kontrollere om kontrakten er avsluttet ved å avgjøre om ubrukt transaksjon UTXO er i listen over ubrukte transaksjonsutgangsverdier for blokkjeden.

7. Fremgangsmåte ifølge ett foregående krav, hvori
i) kontrakten er lagret i en distribuert rutetabell (DHT); og/eller
ii) fremgangsmåten omfatter trinnet:
å kringkaste en transaksjon til blokkjeden som omfatter en instruksjon for å bruke den ubrukte utgangsverdien på en spesifisert dato og/eller tid, fortrinnsvis hvori instruksjonen er en CheckLockTimeVerify-instruksjon.

8. Fremgangsmåte ifølge ett foregående krav, hvori:
i) tilgang til noe eller alt innholdet i kontrakten er begrenset til minst én utpekt autorisert part; og/eller
ii) kontrakten omfatter en Deterministic Finite Automaton (DFA) for å implementere kontrakten;
fortrinnsvis hvori Deterministic Finite Automaton defineres ved anvendelse av et kodifikasjonsskjema.

9. Fremgangsmåte ifølge krav 8, hvori Deterministic Finite Automaton implementeres ved anvendelse av:
i) minst én blokkjedetransaksjon, fortrinnsvis ved anvendelse av et skriptspråk;
ii) et databehandlingsmiddel anordnet for å overvåke tilstanden til blokkjeden; og/eller
iii) et sett med instruksjoner for en digital lommebok.

10. Datamaskinimplementert fremgangsmåte for å kontrollere synligheten og/eller ytelsen til en kontrakt, idet fremgangsmåten er omfattende trinnene:
(a) å lagre en kontrakt på eller i et databasert lager;
(b) å kringkaste en transaksjon til en blokkjede, idet transaksjonen omfatter:
i) minst én ubrukt utgangsverdi (UTXO); og
ii) metadata som omfatter en identifikator som indikerer plasseringen der kontrakten er lagret;

(c) å tolke kontrakten som åpen eller gyldig inntil den ubrukte utgangsverdien (UTXO) brukes på blokkjeden;
og
(d) å generere en underleverandør avledet av kontrakten, hvori underleverandøren er forbundet med en deterministisk adresse og genereres ved:
iii) å anvende en ny offentlig nøkkel avledet ved hjelp av et frø;
iv) å lagre underkontrakten i eller på lageret med henvisning til kontrakten, og kringkaste en transaksjon til blokkjeden som omfatter et skript som inkluderer referansen; og/eller
v) å legge til en referanse til underkontrakten til metadataene i den eksisterende kontrakten.

11. Fremgangsmåte ifølge krav 10, hvori transaksjonen videre omfatter en deterministisk innløsningsskriptadresse, fortrinnsvis hvori innløsningsskriptadressen er en betal-for-skript-rute-adresse (P2SH).

12. Fremgangsmåte ifølge krav 11 og videre omfattende trinnet med å avslutte kontrakten ved å kringkaste en videre transaksjon til blokkjeden for å bruke den ubrukte utgangsverdien (UTXO).
fortrinnsvis hvori den videre transaksjonen omfatter:
en inngang som er den ubrukte utgangsverdien (UTXO); og
et opplåsingsskript omfattende en signatur; metadataene; og en offentlig nøkkel.

13. Fremgangsmåte ifølge ett av kravene 10 til 12 hvori:
i) kontrakten definerer:
i) minst én tilstand; og
b) minst én handling hvis ytelse avhenger av evalueringen av tilstanden;
og/eller
ii) metadataene omfatter:
a) en adresse eller representasjon av en adresse på hvor kontrakten er lagret i det databaserte lageret; og/eller
b) en rute til kontrakten.

14. Fremgangsmåte ifølge ett av kravene 10 til 13 og omfattende trinnet:
å kontrollere om kontrakten er avsluttet ved å avgjøre om ubrukt transaksjon UTXO er i listen over ubrukte transaksjonsutgangsverdier for blokkjeden.

15. Fremgangsmåte ifølge ett av kravene 10 til 14, hvori kontrakten er lagret i en distribuert rutetabell (DHT).

16. Fremgangsmåte ifølge ett av kravene 10 til 15 og omfatter trinnet:
å kringkaste en transaksjon til blokkjeden som omfatter en instruksjon for å bruke den ubrukte utgangsverdien på en spesifisert dato og/eller tid, fortrinnsvis hvori instruksjonen er en CheckLockTimeVerify-instruksjon.

17. Fremgangsmåte ifølge ett av kravene 10 til 16 hvori:
i) tilgang til noe eller alt innholdet i kontrakten er begrenset til minst én utpekt autorisert part; og/eller
ii) kontrakten omfatter en Deterministic Finite Automaton (DFA) for å implementere kontrakten;
fortrinnsvis hvori:
Deterministic Finite Automaton defineres ved anvendelse av et kodifikasjonsskjema; og/eller
Deterministic Finite Automaton implementeres ved anvendelse av:
i) minst én blokkjedetransaksjon, fortrinnsvis ved anvendelse av et skriptspråk;
ii) et databehandlingsmiddel anordnet for å overvåke tilstanden til blokkjeden; og/eller
iii) et sett med instruksjoner for en digital lommebok.

18. System anordnet til å utføre fremgangsmåten ifølge ett foregående krav.