

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号  
特許第7464334号  
(P7464334)

(45)発行日 令和6年4月9日(2024.4.9)

(24)登録日 令和6年4月1日(2024.4.1)

(51)国際特許分類	F I
G 0 6 Q 50/10 (2012.01)	G 0 6 Q 50/10
G 0 6 Q 30/0207(2023.01)	G 0 6 Q 30/0207 3 2 8
G 0 6 Q 20/06 (2012.01)	G 0 6 Q 20/06

請求項の数 8 (全42頁)

(21)出願番号	特願2020-150023(P2020-150023)	(73)特許権者	516002521
(22)出願日	令和2年9月7日(2020.9.7)		谷本 広志
(62)分割の表示	特願2020-517617(P2020-517617)		東京都千代田区麹町5 - 2 - 1 K - W
	)の分割		I N G 9階
原出願日	令和2年1月21日(2020.1.21)	(74)代理人	100079108
(65)公開番号	特開2021-28827(P2021-28827A)		弁理士 稲葉 良幸
(43)公開日	令和3年2月25日(2021.2.25)	(74)代理人	100109346
審査請求日	令和4年12月21日(2022.12.21)		弁理士 大貫 敏史
(31)優先権主張番号	特願2019-147695(P2019-147695)	(74)代理人	100117189
(32)優先日	令和1年8月9日(2019.8.9)		弁理士 江口 昭彦
(33)優先権主張国・地域又は機関	日本国(JP)	(74)代理人	100134120
			弁理士 内藤 和彦
		(72)発明者	谷本 広志
			東京都千代田区麹町5 - 2 - 1 K - W
			I N G 9階

最終頁に続く

(54)【発明の名称】 プログラム、チャレンジ支援システム、チャレンジ支援方法、端末

(57)【特許請求の範囲】

【請求項1】

プログラムであって、  
インターネットに接続される端末に、  
第1のユーザ及び第2のユーザを含む複数のユーザのうち前記第1のユーザが達成すべきチャレンジを達成するための条件及び前記チャレンジを達成する期限を含む前記チャレンジに関する契約条件、前記チャレンジのために預けるトークンの量、少なくとも前記第2のユーザへの前記チャレンジの成功時における前記トークンの配分設定、及び前記チャレンジの失敗時における前記トークンの配分設定を含むコントラクト情報を生成する処理と、

前記契約条件が満たされたか否かを、前記契約条件及び前記契約条件の判定に用いる判定用データに基づいて判定し、前記契約条件の判定結果に基づいて、前記トークンを配分するトランザクションを生成する第1のスマートコントラクトを、前記インターネットに接続されるブロックチェーンネットワークに生成するために、前記コントラクト情報に基づくコントラクト生成トランザクションを、前記ブロックチェーンネットワークへ送信する処理と、を実行させる、プログラム。

【請求項2】

請求項1に記載のプログラムであって、  
前記端末に、  
前記チャレンジの中断を示す情報を生成する処理と、

前記第1のスマートコントラクトに、前記チャレンジが中断された場合の前記トークンの配分設定に従って前記トークンを配分するトランザクションを生成させるために、前記チャレンジの中断を示す情報を前記第1のスマートコントラクトへ送信する処理と、を実行させる、プログラム。

【請求項3】

請求項1又は2に記載のプログラムであって、

前記第1のスマートコントラクトは、前記契約条件及び前記判定用データに基づいて前記チャレンジの達成度を算出し、算出した前記達成度に基づいて、前記トークンを配分するトランザクションを生成する、プログラム。

【請求項4】

請求項1から3のいずれか一項に記載のプログラムであって、

前記判定用データは、

前記チャレンジの終了を判定する終了判定データ、を含む、プログラム。

【請求項5】

請求項4に記載のプログラムであって、

前記終了判定データは日時に関するデータを含む、プログラム。

【請求項6】

チャレンジ支援システムであって、

インターネットに接続される第1の端末と第2の端末を備え、

前記第1の端末は、

第1のユーザ及び第2のユーザを含む複数のユーザのうち前記第1のユーザが達成すべきチャレンジを達成するための条件及び前記チャレンジを達成する期限を含む前記チャレンジに関する契約条件、前記チャレンジのために預けるトークンの量、少なくとも前記第2のユーザへの前記チャレンジの成功時における前記トークンの配分設定、及び前記チャレンジの失敗時における前記トークンの配分設定を含むコントラクト情報を生成するコントラクト情報生成部と、

前記契約条件が満たされたか否かを、前記契約条件及び前記契約条件の判定に用いる判定用データに基づいて判定し、前記契約条件の判定結果に基づいて、前記トークンを配分するトランザクションを生成するスマートコントラクトを、前記インターネットに接続されるブロックチェーンネットワークに生成するために、前記コントラクト情報に基づくコントラクト生成トランザクションを、前記ブロックチェーンネットワークへ送信する第1のトランザクション生成部と、を備え、

前記第2の端末は、

前記判定用データを取得する判定用データ取得部と、

前記判定用データを前記スマートコントラクトへ送信する第2のトランザクション生成部と、を備える、チャレンジ支援システム。

【請求項7】

チャレンジ支援方法であって、

インターネットに接続される第1の端末が、

第1のユーザ及び第2のユーザを含む複数のユーザのうち前記第1のユーザが達成すべきチャレンジを達成するための条件及び前記チャレンジを達成する期限を含む前記チャレンジに関する契約条件、前記チャレンジのために預けるトークンの量、少なくとも前記第2のユーザへの前記チャレンジの成功時における前記トークンの配分設定、及び前記チャレンジの失敗時における前記トークンの配分設定を含むコントラクト情報を生成するステップと、

前記第1の端末が、前記契約条件が満たされたか否かを、前記契約条件及び前記契約条件の判定に用いる判定用データに基づいて判定し、前記契約条件の判定結果に基づいて、前記トークンを配分するトランザクションを生成するスマートコントラクトを、前記インターネットに接続されるブロックチェーンネットワークに生成するために、前記コントラクト情報に基づくコントラクト生成トランザクションを前記ブロックチェーンネットワー

10

20

30

40

50

クへ送信するステップと、

前記インターネットに接続される第2の端末が、

前記判定用データを取得するステップと、

前記第2の端末が、前記判定用データを前記スマートコントラクトへ送信するステップと、を含むチャレンジ支援方法。

【請求項8】

端末であって、

第1のユーザ及び第2のユーザを含む複数のユーザのうち前記第1のユーザが達成すべきチャレンジを達成するための条件及び前記チャレンジを達成する期限を含む前記チャレンジに関する契約条件、前記チャレンジのために預けるトークンの量、少なくとも前記第2のユーザへの前記チャレンジの成功時における前記トークンの配分設定、及び前記チャレンジの失敗時における前記トークンの配分設定を含むコントラクト情報を生成するコントラクト情報生成部と、

10

前記契約条件が満たされたか否かを、前記契約条件及び前記契約条件の判定に用いる判定用データに基づいて判定し、前記契約条件の判定結果に基づいて、前記トークンを配分するトランザクションを生成するスマートコントラクトを、ブロックチェーンネットワークに生成するために、前記コントラクト情報に基づくコントラクト生成トランザクションを、前記ブロックチェーンネットワークへ送信するトランザクション生成部と、を備える、端末。

【発明の詳細な説明】

20

【技術分野】

【0001】

本発明は、プログラム、チャレンジ支援システム、チャレンジ支援方法、及び端末に関する。

【背景技術】

【0002】

人々は、達成したいと思いつながらなかなか実現できないチャレンジを持っていることがある。チャレンジには、例えば、健康維持・増進のためにウォーキングをすること、健康診断に行くこと、禁煙すること、英会話の勉強をすること等が含まれる。

【0003】

30

この種のチャレンジの場合、チャレンジを行う本人以外の方が、本人の健康のためや技能習得のために、本人がチャレンジを達成することを期待していることも多い。例えば、不健康な生活を送っている人の父親は、何とかしてその人にウォーキング等の健康的な活動をさせたいと願い、また、その人の妻や子は、その人が長く健康であることを願い、その人の健康的な活動への取り組みを応援したいと思っている。

【発明の概要】

【発明が解決しようとする課題】

【0004】

この種のチャレンジを行う本人は自分自身に、チャレンジの実行に対するモチベーションを適切に与える必要がある。また、チャレンジが達成されないことは、本人のみならず、本人がチャレンジを達成することに期待する他の人々にとっても、望ましいことではない。本人がチャレンジを達成することに期待する他の人々は、本人に対してチャレンジの実行についてモチベーションを与えることができる。

40

【0005】

しかし、本人がチャレンジを達成することに期待する他の人々も、本人がチャレンジを達成するというメリットに加えて、すぐに顕在化する他の人々自身にとっての何らかのメリットがない状況で本人を積極的に応援し続けることは難しい。

【0006】

本人自身によるモチベーション維持・増進あるいは他の人々の応援による本人のモチベーション維持・増進が不十分な場合、本人がチャレンジの達成に対して消極的となり、チ

50

チャレンジが達成されない可能性が高くなる。

【0007】

そこで、本発明は、ユーザがチャレンジを達成する可能性を高めるチャレンジ支援システムを実現可能なプログラムを提供することを目的とする。

【課題を解決するための手段】

【0008】

本発明の一態様に係るプログラムは、インターネットに接続される端末に、第1のユーザが達成すべきチャレンジを達成するための条件及びチャレンジを達成する期限を含むチャレンジに関する契約条件が満たされたか否かを判定し、契約条件の判定結果に基づいて、第1のトークンを配分するトランザクションを生成する第1のスマートコントラクトと、第1のスマートコントラクトから第1のトークンが配分され、第1のユーザから第2のユーザに対して配分可能な第2のトークンの残高を管理し、第2のユーザの第2のトークンの残高に基づいて、第1のトークンを第2のユーザに配分するトランザクションを生成する第2のスマートコントラクトと、を有し、前記インターネットに接続されるブロックチェーンネットワークにおいて、契約条件の判定に用いる判定用データを取得する処理と、判定用データを第1のスマートコントラクトへ送信する処理と、第2のスマートコントラクトによる第1のユーザから第2のユーザに対する第2のトークンの配分に用いられるトランザクションを生成する処理と、第1のユーザから第2のユーザに対する第2のトークンの配分に用いられるトランザクションを第2のスマートコントラクトへ送信する処理と、を実行させる。

10

20

【0009】

この態様によれば、チャレンジが達成された場合に第1のスマートコントラクトが配分する第1のトークンを、第1のユーザが配分する第2のトークンの残高に基づいて、第2のユーザへ配分することが可能となる。第1のユーザは、チャレンジ開始前、チャレンジの達成過程又はチャレンジ達成の前後において、第2のトークンを第2のユーザに対して配分することが可能となる。

【0010】

第2のユーザは、第2のトークンを保有することにより、第1のトークンの配分を得ることができる。よって、第2のユーザに、第1のトークンを獲得するために第1のユーザのチャレンジに対して積極的な応援を行い、第1のユーザから応援の対価である第2のトークンを得ようという動機が与えられる。第1のユーザは第2のユーザから応援されることによって、チャレンジの実行についてモチベーションを獲得する。第1のユーザ単独ではなく、第2のユーザを巻き込んでチャレンジの達成に挑む状況が作られることによって、第1のユーザがチャレンジを達成する可能性が高まる。

30

【0011】

上記態様において、プログラムは、端末に、第2のトークンを発行するために用いるトークン発行情報を生成する処理と、トークン発行情報をブロックチェーンネットワークに送信する処理と、を実行させてもよい。

【0012】

この態様によれば、第1のユーザが端末を操作することによって、第2のトークンの発行が可能となる。第1のユーザが第2のトークンを自由に発行できるようにすることで、第2のユーザへの配分の割合を適切に調整することができる。より第1のユーザを応援してくれた貢献度の高いユーザが第2のトークンの配分をより多く受けるような割合に調整される。よって、第1のユーザは、第2のユーザ及び他のユーザに対して、自身を応援するように働きかけやすくなる。よって、より多くの応援を獲得し、第1のユーザがチャレンジを達成する可能性が高まる。

40

【0013】

上記態様において、プログラムは、端末に、第2のユーザから第3のユーザに対する第2のトークンの配分に用いられるトランザクションを生成する処理と、第2のユーザから第3のユーザに対する第2のトークンの配分に用いられるトランザクションを第2のスマ

50

ートコントラクトに送信する処理と、を実行させてもよい。

【 0 0 1 4 】

この態様によれば、第2のユーザは第2のトークンを第3のユーザに対して送付することができる。第2のトークンは転々流通可能となる。第1のユーザが選択したユーザとは異なるユーザに対しても第2のトークンが配分されるようになる。よって、より多くのユーザから応援を受けることが可能となり、第1のユーザがチャレンジを達成する可能性が高まる。

【 0 0 1 5 】

上記態様において、プログラムは、端末に、第3のトークンの残高を管理する第3のスマートコントラクト、をさらに有するブロックチェーンネットワークにおいて、第3のスマートコントラクトによる第2のトークンの残高に基づく第3のトークンの配分に用いられるトランザクションを生成する処理と、第2のトークンの残高に基づく第3のトークンの配分に用いられるトランザクションを第3のスマートコントラクトへ送信する処理、を実行させてもよい。

10

【 0 0 1 6 】

この態様によれば、第3のトークンの残高は、第2のトークンの残高に基づいて管理されることとなる。第2のトークンを、第1のユーザのチャレンジ毎の応援に対する一時的なトークンとし、第3のトークンを、第1のユーザの複数のチャレンジに対する長期的なトークンとすることで、第1のユーザは長期的な応援を獲得することが可能となる。長期的な応援を獲得しているという安心感を持つ第1のユーザは、チャレンジに対する安定したモチベーションを獲得する。よって、第1のユーザがチャレンジを達成する可能性が高まる。

20

【 0 0 1 7 】

上記態様において、プログラムは、端末に、第3のスマートコントラクトによる、第2のトークンの残高及びチャレンジの難易度に基づく第3のトークンの配分に用いられるトランザクションを生成する処理と、第2のトークンの残高及びチャレンジの難易度に基づく第3のトークンの配分に用いられるトランザクションを第3のスマートコントラクトへ送信する処理と、を実行させてもよい。

【 0 0 1 8 】

チャレンジの難易度に基づいて、第3のトークンを配分するようにすることで、各チャレンジにおいて、一律に第2のトークンの残高から第3のトークンを配分するのではなく、第3のチャレンジの難易度に応じて、適切に第3のトークンを配分することが可能となる。

30

【 0 0 1 9 】

上記態様において、プログラムは、端末に、チャレンジの中断を示す情報を生成する処理と、第1のスマートコントラクトに、チャレンジが中断された場合の第1のトークンの配分設定に従った第1のトークンの配分に用いられるトランザクションを生成させるために、チャレンジの中断を示す情報を第1のスマートコントラクトへ送信する処理と、を実行させてもよい。

【 0 0 2 0 】

この態様によれば、チャレンジを中断することが可能となり、システムとしての利便性が向上する。

40

【 0 0 2 1 】

上記態様において、プログラムは、端末に、第1のユーザのチャレンジに関する情報を送信するための送信先を取得する処理と、ブロックチェーンネットワークの所定のユーザから、第1のユーザに対するブロックチェーンネットワークにおける所定のトークンの配分に用いられるトランザクションを生成させるために、第1のユーザのチャレンジに関する情報を送信先に対して送信する処理と、を実行させてもよい。

【 0 0 2 2 】

この態様によれば、ブロックチェーンネットワークの所定のユーザは、第1のユーザに

50

対して所定のトークンを配分することが可能となる。第1のユーザが自身のチャレンジに関する情報に基づいて、所定のユーザからトークンを受け取るようにして、第1のユーザは所定のユーザから応援されることができ、第1のユーザがチャレンジを達成する可能性が高まる。

【0023】

本発明の他の態様に係るプログラムは、インターネットに接続される端末に、第1のユーザが達成すべきチャレンジを達成するための条件及びチャレンジを達成する期限を含むチャレンジに関する契約条件、チャレンジのために預ける第1のトークンの量、チャレンジの成功時における第1のトークンの配分設定、及びチャレンジの失敗時における第1のトークンの配分設定を含むコントラクト情報を生成する処理と、契約条件が満たされたか否かを、契約条件及び契約条件の判定に用いる判定用データに基づいて判定し、契約条件の判定結果に基づいて、第1のトークンを配分するトランザクションを生成する第1のスマートコントラクトを、インターネットに接続されるブロックチェーンネットワークに生成するために、コントラクト情報に基づくコントラクト生成トランザクションをブロックチェーンネットワークへ送信する処理と、を実行させる。

10

【0024】

この態様によれば、インターネットに接続される端末から、チャレンジ達成のための第1スマートコントラクトを生成することができる。インターネットに接続される端末であれば、自由にチャレンジに関する第1のスマートコントラクトを生成することができるので、ユーザ毎の目的に沿ったチャレンジの達成が可能となる。ユーザの目的に沿うチャレンジとすることで、ユーザのチャレンジに対するモチベーションを増し、ユーザがチャレンジを達成する可能性が高まる。

20

【0025】

上記態様において、プログラムは、端末に、チャレンジの中断を示す情報を生成する処理と、第1のスマートコントラクトに、チャレンジが中断された場合の第1のトークンの配分設定に従って第1のトークンを配分するトランザクションを生成させるために、チャレンジの中断を示す情報を第1のスマートコントラクトへ送信する処理と、を実行させてもよい。

【0026】

チャレンジに関する第1のスマートコントラクトの作成者が、チャレンジを中断することが可能となり、システムとしての利便性が向上する。

30

【0027】

上記態様において、第1のスマートコントラクトは、契約条件及び判定用データに基づいてチャレンジの達成度を算出し、算出した達成度に基づいて、第1のトークンを配分するトランザクションを生成してもよい。

【0028】

この態様によれば、チャレンジが中断あるいは失敗したような場合であっても、達成度に基づいて、第1のトークンが配分される。チャレンジの難易度を高く設定した場合に、チャレンジが中断あるいは失敗する可能性が高くなることもある。この場合にチャレンジが中断したとしても、第1のトークンが配分されるので、ユーザのチャレンジに対するモチベーションを保ち、チャレンジの達成を促進することができる。

40

【0029】

上記態様において、判定用データは、チャレンジの終了を判定する終了判定データ、を含んでもよい。

【0030】

この態様によれば、第1のスマートコントラクトが外部から、チャレンジの終了を判断するための情報（オラクル）を取得することが可能となり、確実にチャレンジを終了させることができる。

【0031】

上記態様において、終了判定データは日時に関するデータを含んでもよい。

50

## 【 0 0 3 2 】

この態様によれば、第1のスマートコントラクトがインターネットやブロックチェーンネットワークから自動的に日時に関する情報を取得できない場合に、第1のスマートコントラクトに対して日時に関する情報を送信することができる。よって、チャレンジの期限が過ぎた場合に、確実にチャレンジを終了させることができる。

## 【 0 0 3 3 】

本発明の他の態様に係るプログラムは、インターネットに接続される端末に、第1のユーザが達成すべきチャレンジを達成するための条件及びチャレンジを達成する期限を含むチャレンジに関する契約条件が満たされたか否かを判定し、契約条件の判定結果に基づいて、第1のトークンを配分するトランザクションを生成し、第1のユーザから第2のユーザに対して配分可能であり、判定がなされた後に有効となる第2のトークンの残高を管理し、契約条件の判定結果に基づいて、第2のトークンを第2のユーザに配分するトランザクションを生成する、スマートコントラクトをブロックチェーンネットワークに生成するために、コントラクト生成トランザクションをブロックチェーンネットワークへ送信する処理を実行させる。

10

## 【 0 0 3 4 】

この態様によれば、チャレンジに関する契約条件が満たされたか否かが判定された後に有効となる第2のトークンを第1のユーザが第2のユーザに対して配分することが可能となる。よって、第2のユーザに、第2のトークンを有効にするために、第1のユーザのチャレンジに対して応援を行う動機が与えられる。第1のユーザは第2のユーザから応援されることによって、チャレンジの実行についてモチベーションを獲得する。第1のユーザ単独ではなく、第2のユーザを巻き込んでチャレンジの達成に挑む状況が作られることによって、第1のユーザがチャレンジを達成する可能性が高まる。

20

## 【 0 0 3 5 】

本発明の他の態様に係るプログラムは、インターネットに接続される端末に、所定のユーザが達成すべきチャレンジを達成するための条件とチャレンジを達成する期限と、を含むチャレンジに関する契約条件が満たされたか否かを、契約条件及び契約条件の判定に用いる判定用データに基づいて判定する第1のスマートコントラクトと、第1のスマートコントラクトから送信された判定結果に基づいて、インターネットに接続されるブロックチェーンネットワークにおけるトークンの残高を管理する第2のスマートコントラクトと、を有するブロックチェーンネットワークからトークンが集積され、第1のスマートコントラクトから送信された判定結果に基づいて、集積されたトークンを配分する第2のスマートコントラクトと、を有するブロックチェーンネットワークにおいて、トークンを判定結果の予想に対して賭けるトランザクションを生成する処理と、トークンを判定結果の予想に対して賭けるトランザクションを第2のスマートコントラクトへ送信する処理と、を実行させる。

30

## 【 0 0 3 6 】

この態様によれば、第2のスマートコントラクトは、第1のユーザのチャレンジの判定結果について、トークンを賭けさせ、判定結果に基づいてトークンの残高を管理することで、トークンを配分する。よって、より多くのユーザが、自身のトークンを増やそうとするために、第1のチャレンジに対して関心を有する。第1のユーザは、自身のチャレンジが多くに関心を集めていると、その関心に応えるべくチャレンジの達成に挑む。よって、第1のユーザがチャレンジを達成する可能性が高まる。

40

## 【 0 0 3 7 】

本発明の他の態様に係るチャレンジ支援システムは、インターネットに接続される第1の端末と第2の端末を備え、第1の端末は、第1のユーザが達成すべきチャレンジを達成するための条件及びチャレンジを達成する期限を含むチャレンジに関する契約条件、チャレンジのために預ける第1のトークンの量、チャレンジの成功時における第1のトークンの配分設定、及びチャレンジの失敗時における第1のトークンの配分設定を含むコントラクト情報を生成するコントラクト情報生成部と、契約条件が満たされたか否かを、契約条

50

件及び契約条件の判定に用いる判定用データに基づいて判定し、契約条件の判定結果に基づいて、第1のトークンを配分するトランザクションを生成するスマートコントラクトを、インターネットに接続されるブロックチェーンネットワークに生成するために、コントラクト情報に基づくコントラクト生成トランザクションを、ブロックチェーンネットワークへ送信する第1のトランザクション生成部と、を備え、第2の端末は、契約条件の判定に用いる判定用データを取得する判定用データ取得部と、判定用データをスマートコントラクトへ送信する第2のトランザクション生成部と、を備える。

【0038】

この態様によれば、第1の端末によって生成されるコントラクト情報によってブロックチェーンネットワーク上にスマートコントラクトが生成される。スマートコントラクトには、第1のトークンが預けられる。ユーザは、チャレンジに関する契約条件が満たされるか否かに応じて配分される第1のトークンを得るために、チャレンジの実行についてモチベーションを獲得する。契約条件の判定に用いる判定用データは、第2の端末によって、スマートコントラクトに送信される。スマートコントラクトは、判定用データに従って契約条件が満たされたか否かを判定する。

10

【0039】

スマートコントラクトを介したチャレンジの判定を行うことにより、チャレンジの結果に応じた第1のトークンの配分が管理者不在で確実に履行される。よって、ユーザは、スマートコントラクトをブロックチェーンネットワークに生成することによって、チャレンジ結果に対する報酬が配分されることが約束されているチャレンジを作成することができる。チャレンジ支援システムは、チャレンジの結果に対する報酬の獲得についての信頼性を高くすることによって、ユーザにチャレンジの実行についてモチベーションを与え、ユーザがチャレンジを達成する可能性を高める。

20

【発明の効果】

【0040】

本発明によれば、ユーザがチャレンジを達成する可能性を高めるチャレンジ支援システムを実現可能なプログラムを提供することができる。

【図面の簡単な説明】

【0041】

【図1】第1実施形態に係るチャレンジ支援システムの構成を示す図である。

30

【図2】第1実施形態に係る資金提供者端末のブロック図である。

【図3】第1実施形態に係る挑戦者端末のブロック図である。

【図4】第1実施形態に係る応援者端末のブロック図である。

【図5】第1実施形態に係る運営者端末のブロック図である。

【図6】第1実施形態に係る運営者端末に記憶されるデータ構造である。

【図7】第1実施形態に係るブロックチェーンネットワークにおけるスマートコントラクトを示す図である。

【図8】第1実施形態に係る判定用データ送信端末のブロック図である。

【図9】第1実施形態に係るチャレンジ支援システムのシーケンス図である。

【図10】第1実施形態に係るチャレンジ支援システムのシーケンス図である。

40

【図11】第1実施形態に係るチャリングトークンコントラクトを説明する図である。

【図12】第1実施形態に係るチャリングトークンコントラクトを説明する図である。

【図13】第1実施形態に係るサングストークンコントラクトを説明する図である。

【図14】第1実施形態に係る資金提供者端末に記憶されるデータ構造の図である。

【図15】第1実施形態に係る資金提供者端末により作成されるコントラクト情報の一例である。

【図16】第1実施形態に係るチャレンジコントラクトを説明する図である。

【図17】第1実施形態に係る運営者端末に記憶されるデータ構造である。

【図18】第1実施形態に係る運営者端末に記憶されるデータ構造である。

【図19】第1実施形態に係る判定用データのデータ構造である。

50

【図 2 0】第 1 実施形態に係るチャレンジコントラクトに記録される判定用データのデータ構造である。

【図 2 1】第 1 実施形態に係る挑戦者端末に記憶されるデータ構造である。

【図 2 2】第 1 実施形態に係るサクストークンコントラクトを説明する図である。

【図 2 3】第 1 実施形態に係る他のチャレンジの一例である。

【図 2 4】第 1 実施形態に係る他のチャレンジの一例である。

【図 2 5】第 1 実施形態に係る他のチャレンジの一例である。

【図 2 6】第 1 実施形態に係る他のチャレンジの一例である。

【図 2 7】第 1 実施形態に係るチャレンジアプリにより表示される画面である。

【図 2 8】第 1 実施形態に係るチャレンジアプリにより表示される画面である。

10

【図 2 9】第 1 実施形態に係るチャレンジアプリにより表示される画面である。

【図 3 0】第 1 実施形態に係るチャレンジアプリにより表示される画面である。

【図 3 1】第 1 実施形態に係るチャレンジアプリにより表示される画面である。

【図 3 2】第 1 実施形態に係るチャレンジアプリにより表示される画面である。

【図 3 3】第 1 実施形態に係るチャレンジアプリにより表示される画面である。

【図 3 4】第 2 実施形態に係るチャレンジ支援システムの構成を示す図である。

【図 3 5】第 3 実施形態に係るブロックチェーンネットワークにおけるスマートコントラクトを示す図である。

【図 3 6】第 3 実施形態に係るサクストークンコントラクトを説明する図である。

【図 3 7】第 3 実施形態に係るサクストークンコントラクトを説明する図である。

20

【図 3 8】第 3 実施形態に係るサクストークンコントラクトを説明する図である。

【図 3 9】第 3 実施形態に係るサクストークンコントラクトを説明する図である。

【図 4 0】第 4 実施形態に係るブロックチェーンネットワークにおけるスマートコントラクトを示す図である。

【図 4 1】第 4 実施形態に係るブロックチェーンネットワークにおけるトークンの管理を説明する図である。

【図 4 2】第 4 実施形態に係るブロックチェーンネットワークにおけるトークンの管理を説明する図である。

【図 4 3】第 4 実施形態に係るブロックチェーンネットワークにおけるトークンの管理の他の一例を説明する図である。

30

【図 4 4】第 5 実施形態に係るブロックチェーンネットワークにおけるスマートコントラクトを示す図である。

【発明を実施するための形態】

【0042】

添付図面を参照して、本発明の好適な実施形態について説明する。なお、各図において、同一の符号を付したものは、同一又は同様の構成を有する。

【0043】

第 1 実施形態について説明する。図 1 に第 1 実施形態に係るチャレンジ支援システムを示す。チャレンジ支援システム 1 は、資金提供者端末 10、挑戦者端末 20、応援者端末 30、30A、運営者端末 40、インターネット 50、ブロックチェーンネットワーク 55 及び判定用データ送信端末 60 を備える。

40

【0044】

資金提供者端末 10、挑戦者端末 20、応援者端末 30、30A、運営者端末 40、及び判定用データ送信端末 60 がネットワーク N を介して接続されるようにして、インターネット 50 が構成される。ブロックチェーンネットワーク 55 はインターネット 50 に繋がっている。

【0045】

ブロックチェーンネットワーク 55 は、トランザクションが記録された台帳を複数の端末が共有して管理するシステムである。ブロックチェーンは、時系列にそって複数のブロックがチェーン状に繋がったデータであり、各ブロックは、一定期間におけるトランザク

50

ションのデータを含む。ブロックチェーンの技術では、複数のブロックが過去の情報を保持した状態で追加されるので、履歴の改ざんが困難であるという特徴がある。

【0046】

本実施形態では、ブロックチェーンネットワーク55として、スマートコントラクトを実現することが可能なイーサリアム(Ethereum)を用いるものとする。スマートコントラクトを実現できる他のブロックチェーンネットワークを用いてもよい。

【0047】

図2に、資金提供者端末10のブロック図を示す。資金提供者端末10は、ネットワークNを介して運営者端末40、インターネット50及びブロックチェーンネットワーク55と通信を行う機能を備えた情報処理端末である。例えば、スマートフォン、PC、タブレット等が挙げられるが、これらに限られない。

10

【0048】

資金提供者端末10は、入力部111、表示部112、通信部113、制御部114、記憶部115、及び撮像部116を備える。

【0049】

入力部111は、ユーザからの操作を受け付ける。表示部112は、ユーザに対して情報を表示する。入力部111及び表示部112は、タッチパネル等のように一体となってもよい。通信部113は、ネットワークNを介して外部の端末と通信を行う。記憶部115にはチャレンジアプリ80が記憶される。撮像部116は、画像の取得などに用いられる。

20

【0050】

入力部111を通じて入力された情報に基づいて、チャレンジアプリ80のユーザアカウント及びパスワードが記憶部115に保存される。資金提供者端末10は、保存されたユーザアカウントに関するユーザ識別情報を運営者端末40へと送信する。

【0051】

ユーザ識別情報は、例えばチャレンジアプリ80のインストール時や起動時にユーザに入力させることで取得した会員情報の一部又は全部を使用して生成した情報である。ユーザ識別情報には、氏名、性別、生年月日、アカウント名、ユーザが使用する判定用データ送信端末の公開アドレス等が含まれる。

【0052】

制御部114は、CPU及びメモリを含む。制御部114は、記憶部115に記憶されているチャレンジアプリ80(プログラム)がRAMに読み出され、CPUによって実行されることで、鍵生成部121、アドレス生成部122、アドレス取得部123、ウォレット部124、トランザクション生成部125、チャレンジ設定部126、及びコントラクト情報生成部127として機能する。

30

【0053】

鍵生成部121は、資金提供者端末10のユーザ毎に一意的な秘密鍵と公開鍵のペアを生成する。生成された秘密鍵は、記憶部115に保存される。秘密鍵はトランザクションをブロックチェーンネットワーク55に送信する際の電子署名に用いられる。秘密鍵は、オフライン時に生成され、通常はオフラインで保存され、必要に応じて接続可能とされることが望ましい。

40

【0054】

アドレス生成部122は、鍵生成部121により生成された公開鍵に基づいて、ブロックチェーンネットワーク55における公開アドレスを生成する。生成された資金提供者の公開アドレスは記憶部115に保存される。公開アドレスは、ブロックチェーンネットワーク55のユーザを識別するために用いられる。ブロックチェーンネットワーク55において、イーサリアムにおける仮想通貨であるイーサ及び他のトークンのトランザクションによる送付先は公開アドレスとなる。以降、イーサをETHERと表記する。ETHERの略称はETHである。

【0055】

50

アドレス生成部 1 2 2 は、生成された公開アドレスをユーザ識別情報と対応付けて、後述する運営者端末 4 0 へと送信する。公開アドレスとユーザ識別情報とを対応付けることによって、ブロックチェーンネットワーク 5 5 における、ある公開アドレスが、チャレンジ支援システム 1 の利用者であることを確認できる。

【 0 0 5 6 】

アドレス取得部 1 2 3 は、ブロックチェーンネットワーク 5 5 における他の公開アドレスを、運営者端末 4 0 又は他の端末から取得する。運営者端末 4 0 から他の公開アドレスを取得する場合、アドレス取得部 1 2 3 は、ネットワーク N を介して運営者端末 4 0 と通信を行い、運営者端末 4 0 に記憶された他の公開アドレスを取得する。

【 0 0 5 7 】

他の端末から他の公開アドレスを取得する場合は、例えば、公開アドレスを示す二次元バーコード等の画像を撮像部 1 1 6 により読み取ることで取得する。あるいは、他の端末が生成した画像やテキストによって表された公開アドレスを、ネットワーク N を介して取得することによって、他の公開アドレスを取得する。アドレス取得部 1 2 3 により取得された公開アドレスは記憶部 1 1 5 に保存される。

【 0 0 5 8 】

アドレス取得部 1 2 3 は、運営者端末 4 0 又は他の端末から取得した公開アドレスに、他の端末に記憶されたチャレンジアプリ 8 0 と同種のアプリによって生成されたユーザ識別情報がある場合は、ユーザ識別情報も取得可能である。取得されたユーザ識別情報は記憶部 1 1 5 に保存される。

【 0 0 5 9 】

アドレス取得部 1 2 3 は、ブロックチェーンネットワーク 5 5 におけるチャレンジに関連するスマートコントラクトのコントラクトアドレスを、運営者端末 4 0 又は他の端末から取得可能である。

【 0 0 6 0 】

ウォレット部 1 2 4 は、仮想通貨の残高を管理する機能を有する。第 1 実施形態における仮想通貨は、E T H E R や、ブロックチェーンネットワーク 5 5 にて独自に発行されるトークンである。ウォレット部 1 2 4 は、仮想通貨の残高を、ブロックチェーンネットワーク 5 5 に記録されるトランザクションの履歴から取得する。取得された残高は表示部 1 1 2 に表示されることでユーザが確認可能である。

【 0 0 6 1 】

ウォレット部 1 2 4 は、送金先の公開アドレス又は送金先の公開アドレスに対応するアカウント名と、送金額と、を含む資金支払データを生成する。例えば、ウォレット部 1 2 4 は、入力部 1 1 1 を介してユーザから指定されたアカウントと送金額とを含む資金支払データを生成する。なお、送金及び資金という言葉は、仮想通貨の移動に関する意味で用いており、移動する対象は、E T H E R に限られず、他のトークンも含まれる。

【 0 0 6 2 】

トランザクション生成部 1 2 5 は、記憶部 1 1 5 に保存された秘密鍵により署名したトランザクションを生成し、ブロックチェーンネットワーク 5 5 に送信する。例えば、トランザクション生成部 1 2 5 はウォレット部 1 2 4 によって生成された資金支払データに基づいて、記憶部 1 1 5 に保存された秘密鍵で署名したトランザクションを生成し、ブロックチェーンネットワーク 5 5 に送信する。トランザクションがブロックチェーンネットワーク 5 5 において承認されると、そのトランザクションに基づいた資金の移動がブロックチェーンネットワーク 5 5 に保存される。

【 0 0 6 3 】

ウォレット部 1 2 4 は、運営者端末 4 0 から、後述するチャレンジコントラクトの一覧を取得して、ユーザに選択可能な形式で表示してもよい。また、チャレンジコントラクトの一覧を取得する際、ウォレット部 1 2 4 が記憶部 1 1 5 の公開アドレスを送信することで、当該ユーザが資金提供者として運営者端末 4 0 に登録されているチャレンジコントラクトのコントラクトアドレスの一覧を取得できるようにしてもよい。

10

20

30

40

50

## 【 0 0 6 4 】

チャレンジ設定部 1 2 6 は、資金提供者が作成するチャレンジに関する設定をユーザから取得し、設定データを生成する。設定データには、資金提供者の公開アドレス、チャレンジに挑戦する挑戦者の公開アドレス、運営者の公開アドレス、資金額、チャレンジ開始期限、チャレンジ期間等の情報が含まれる。また、チャレンジを達成するためのチャレンジの具体的な内容、チャレンジの達成条件、チャレンジ成功時の資金の配分設定、及びチャレンジ失敗時の資金の配分設定等の契約条件が含まれる。

## 【 0 0 6 5 】

コントラクト情報生成部 1 2 7 は、チャレンジ設定部 1 2 6 が生成した設定データに基づいて、Solidity 言語で記述された、コントラクト・コードを solc によりコンパイルし、コンパイル済コントラクト・コードを生成する。

10

## 【 0 0 6 6 】

トランザクション生成部 1 2 5 が、コントラクト情報生成部 1 2 7 によって生成されたコンパイル済コントラクト・コードを、ブロックチェーンネットワーク 5 5 にトランザクションとして送信する。トランザクションがブロックチェーンネットワーク 5 5 において承認されると、図 7 に示すように、スマートコントラクトであるチャレンジコントラクト 5 0 1 がブロックチェーンネットワーク 5 5 に生成される。チャレンジコントラクト 5 0 1 については後述する。なお、資金提供者端末 1 0 が用いる言語は Solidity 言語に限定されず、スマートコントラクトをブロックチェーンネットワーク 5 5 に生成可能な他の言語を用いることができる。

20

## 【 0 0 6 7 】

ブロックチェーンネットワーク 5 5 に生成されたチャレンジコントラクト 5 0 1 は、ブロックチェーンネットワーク 5 5 におけるコントラクトアドレスを有する。チャレンジコントラクト 5 0 1 のコントラクトアドレスに資金提供者が供託する資金が送付され保持される。チャレンジコントラクト 5 0 1 のコントラクトアドレスは、チャレンジコントラクト 5 0 1 が生成された際に、ブロックチェーンネットワーク 5 5 から資金提供者端末 1 0 へと送信され取得するか、資金提供者端末 1 0 がブロックチェーンネットワーク 5 5 から取得する。取得されたチャレンジコントラクト 5 0 1 のコントラクトアドレスは、チャレンジ設定部 1 2 6 が生成した設定データと共に、資金提供者端末 1 0 から運営者端末 4 0 へと送信される。

30

## 【 0 0 6 8 】

図 3 に挑戦者端末 2 0 のブロック図を示す。挑戦者端末 2 0 は、ネットワーク N を介して運営者サーバ及びブロックチェーンネットワーク 5 5 と通信を行う機能を備えた情報処理端末である。例えば、スマートフォン、PC、タブレット等が挙げられるが、これらに限られない。

## 【 0 0 6 9 】

挑戦者端末 2 0 は、入力部 2 1 1、表示部 2 1 2、通信部 2 1 3、制御部 2 1 4、記憶部 2 1 5、及び撮像部 2 1 6 を備える。

## 【 0 0 7 0 】

入力部 2 1 1、表示部 2 1 2、通信部 2 1 3、及び撮像部 2 1 6 に関しては、入力部 1 1 1、表示部 1 1 2、通信部 1 1 3、及び撮像部 1 1 6 と同様である。挑戦者端末 2 0 は、自身のユーザ識別情報を運営者端末 4 0 へと送信する。記憶部 2 1 5 には、チャレンジアプリ 8 0 が記憶される。

40

## 【 0 0 7 1 】

制御部 2 1 4 は、CPU 及びメモリを含む。制御部 2 1 4 は、記憶部 2 1 5 に記憶されているチャレンジアプリ 8 0 (プログラム) が RAM に読み出され、CPU によって実行されることで、鍵生成部 2 2 1、アドレス生成部 2 2 2、アドレス取得部 2 2 3、ウォレット部 2 2 4、トランザクション生成部 2 2 5、判定用データ取得部 2 2 6、及びトークン発行情報生成部 2 2 7 として機能する。

## 【 0 0 7 2 】

50

鍵生成部 2 2 1、アドレス生成部 2 2 2、アドレス取得部 2 2 3、ウォレット部 2 2 4、及びトランザクション生成部 2 2 5 は、鍵生成部 1 2 1、アドレス生成部 1 2 2、アドレス取得部 1 2 3、ウォレット部 1 2 4、及びトランザクション生成部 1 2 5 と同様の機能を有する。

【 0 0 7 3 】

鍵生成部 2 2 1 によって生成される秘密鍵は、記憶部 2 1 5 に保存される。アドレス生成部 2 2 2 によって生成される挑戦者の公開アドレスは、記憶部 2 1 5 に保存される。

【 0 0 7 4 】

判定用データ取得部 2 2 6 は、契約条件が満たされたか否かを判定するために用いる判定用データを、入力部 2 1 1 にて入力された情報あるいは挑戦者端末 2 0 にて記憶部 2 1 5 に記録される情報から取得する。記憶部 2 1 5 に記録される情報には、例えば、スマートフォンの歩数計機能によって集計され、記憶部 2 1 5 に記録された歩数等の運動情報がある。あるいは、通信部 2 1 3 を介して外部の歩数を計測可能な端末から記憶部 2 1 5 に記録される歩数等の運動情報がある。

【 0 0 7 5 】

判定用データには、チャレンジを達成するための活動のエビデンスとなるデータや、チャレンジの「成功」又は「失敗」のいずれかを含むデータ等、任意のデータを用いることができる。

【 0 0 7 6 】

判定用データは、チャレンジの「中断」を示すデータを含むことができる。チャレンジの「中断」を示すデータが、ブロックチェーンネットワーク 5 5 に送信された場合には、チャレンジコントラクト 5 0 1 が所定の処理を行うように設定することができる。

【 0 0 7 7 】

判定用データは、チャレンジの成功、失敗を決定づける終了判定データを含む。終了判定データとは、例えば、複数日にまたがるチャレンジにおいて、最終日の結果である。また、終了判定データとは、チャレンジの期限を徒過したかを判定するための日時に関する情報でもよい。

【 0 0 7 8 】

トランザクション生成部 2 2 5 は、判定用データをスマートコントラクトに送信するために、記憶部 2 1 5 に保存された秘密鍵で署名されたトランザクションを生成する。トランザクション生成部 2 2 5 は、判定用データに関するトランザクションをスマートコントラクトに送信する。トランザクションがブロックチェーンネットワーク 5 5 において承認されると、トランザクションの宛先であるスマートコントラクトのデータが更新される。宛先は、例えば、チャレンジコントラクト 5 0 1 のコントラクトアドレスである。

【 0 0 7 9 】

判定用データ取得部 2 2 6 によって取得した判定用データが、スマートコントラクトへと送信される場合、トランザクション生成部 2 2 5 は、運営者端末 4 0 からスマートコントラクトのコントラクトアドレスを取得し、トランザクションの宛先として、ユーザに選択可能な形式で表示してもよい。

【 0 0 8 0 】

また、スマートコントラクトのコントラクトアドレスを取得する際、アドレス取得部 2 2 3 が、挑戦者の公開アドレスを送信することで、当該ユーザが挑戦者として運営者端末 4 0 に登録されているスマートコントラクトのコントラクトアドレスの一覧を取得できるようにしてもよい。

【 0 0 8 1 】

なお、判定用データを裏付ける画像等のコンテンツについては、判定用データ取得部 2 2 6 は、コンテンツを一意に識別するハッシュ値を生成し、当該生成したハッシュ値だけをトランザクションとしてブロックチェーンネットワーク 5 5 に送信する。実際のコンテンツについては、ハッシュ値と共に運営者端末 4 0 に送信する。画像には、例えば、挑戦者が撮影した食事画像、挑戦者が撮影した身体測定結果画像等が含まれる。ハッシュ値を

10

20

30

40

50

用いることで、ブロックチェーンネットワーク 5 5 に直接サイズが大きく、コスト（G A S 代）が多く発生するようなコンテンツを記録する必要がなくなる。

【 0 0 8 2 】

トークン発行情報生成部 2 2 7 は、ブロックチェーンネットワーク 5 5 におけるトークンを発行するためのトークン発行情報を生成する。

【 0 0 8 3 】

トークン発行情報には、トークンの総発行数、トークンの名称、トークンの単位表記等が含まれる。トークン発行情報生成部 2 2 7 は入力部 2 1 1 からのユーザの入力に基づいて、これらの情報を取得しトークン発行情報を生成する。

【 0 0 8 4 】

トランザクション生成部 2 2 5 がトークン発行情報に基づいて、ブロックチェーンネットワーク 5 5 へトランザクションを送信する。トランザクションがブロックチェーンネットワーク 5 5 において承認されると、ブロックチェーンネットワーク 5 5 に、トークンコントラクトが生成される。トークンの残高を管理するためのスマートコントラクトであるトークンコントラクトが生成されるということが、トークンが発行されるということである。

【 0 0 8 5 】

トークンコントラクトは、ブロックチェーンネットワーク 5 5 におけるコントラクトアドレスを有する。トークンコントラクトは、発行されたトークンを所有する公開アドレスとその公開アドレスに対するトークンの残高の状態を記録することによって、ブロックチェーンネットワーク 5 5 におけるトークンの残高を管理する。

【 0 0 8 6 】

第 1 実施形態では、図 7 に示されるように、トークンコントラクトとしてサックストークンコントラクト 5 0 2 が生成される。サックストークンコントラクト 5 0 2 については後述する。

【 0 0 8 7 】

挑戦者端末 2 0 におけるチャレンジアプリ 8 0 は、資金提供者端末 1 0 におけるチャレンジ設定部 1 2 6 及びコントラクト情報生成部 1 2 7 を実現可能であってもよい。資金提供者端末 1 0 におけるチャレンジアプリ 8 0 は挑戦者端末 2 0 における判定用データ取得部 2 2 6 及びトークン発行情報生成部 2 2 7 を実現可能であってもよい。すなわち、資金提供者端末 1 0 と挑戦者端末 2 0 は資金提供者という立場と挑戦者という立場によって区別されているが、両者の区別は任意に入れ替えることが可能である。また、資金提供者と挑戦者が同一人物であってもよい。

【 0 0 8 8 】

図 4 に応援者端末 3 0 のブロック図を示す。応援者端末 3 0 は、ネットワーク N を介して運営者サーバ及びブロックチェーンネットワーク 5 5 と通信を行う機能を備えた情報処理端末である。例えば、スマートフォン、P C、タブレット等が挙げられるが、これらに限られない。

【 0 0 8 9 】

応援者端末 3 0 は、入力部 3 1 1、表示部 3 1 2、通信部 3 1 3、制御部 3 1 4、記憶部 3 1 5、撮像部 3 1 6 を備える。

【 0 0 9 0 】

入力部 3 1 1、表示部 3 1 2、通信部 3 1 3、及び撮像部 3 1 6 に関しては、入力部 1 1 1、表示部 1 1 2、通信部 1 1 3、及び撮像部 1 1 6 と同様である。応援者端末 3 0 は、自身のユーザ識別情報を運営者端末 4 0 へと送信する。記憶部 3 1 5 には、チャレンジアプリ 8 0 が記憶される。

【 0 0 9 1 】

制御部 3 1 4 は、C P U 及びメモリを含む。制御部 3 1 4 は、記憶部 3 1 5 に記憶されているチャレンジアプリ 8 0（プログラム）が R A M に読み出され、C P U によって実行されることで、鍵生成部 3 2 1、アドレス生成部 3 2 2、アドレス取得部 3 2 3、ウォレ

10

20

30

40

50

ット部 3 2 4、トランザクション生成部 3 2 5 として機能する。

【 0 0 9 2 】

鍵生成部 3 2 1、アドレス生成部 3 2 2、アドレス取得部 3 2 3、ウォレット部 3 2 4、及びトランザクション生成部 3 2 5 は、鍵生成部 1 2 1、アドレス生成部 1 2 2、アドレス取得部 1 2 3、ウォレット部 1 2 4、及びトランザクション生成部 1 2 5 と同様の機能を有する。

【 0 0 9 3 】

アドレス生成部 3 2 2 によって生成される応援者の公開アドレスは、記憶部 3 1 5 に保存される。応援者端末 3 0 は、ブロックチェーンネットワーク 5 5 において、仮想通貨の送受信が可能な端末として機能する。応援者端末 3 0 A については、応援者端末 3 0 と同様である。

10

【 0 0 9 4 】

応援者端末 3 0 におけるチャレンジアプリ 8 0 は、資金提供者端末 1 0 におけるチャレンジ設定部 1 2 6 及びコントラクト情報生成部 1 2 7 又は、挑戦者端末 2 0 における判定用データ取得部 2 2 6 及びトークン発行情報生成部 2 2 7 を実現可能であってもよい。すなわち、資金提供者端末 1 0、挑戦者端末 2 0、及び応援者端末 3 0 は、チャレンジに応じて互いの区別を任意に入れ替えることが可能である。

【 0 0 9 5 】

運営者端末 4 0 は、入力部 4 1 1、通信部 4 1 3、制御部 4 1 4、及び記憶部 4 1 5 を備える。例えば、運営者端末 4 0 はサーバ装置である。入力部 4 1 1 及び通信部 4 1 3 に関しては、入力部 1 1 1 及び通信部 1 1 3 と同様である。

20

【 0 0 9 6 】

記憶部 4 1 5 には、データベース (DB) としてチャレンジ DB 4 1 5 1、会員 DB 4 1 5 2、コンテンツ DB 4 1 5 3 が保存される。

【 0 0 9 7 】

制御部 4 1 4 は、CPU 及びメモリを含む。制御部 4 1 4 は、記憶部 4 1 5 に記憶されているプログラムが RAM に読み出され、CPU によって実行されることで、鍵生成部 4 2 1、アドレス生成部 4 2 2、アドレス取得部 4 2 3、ウォレット部 4 2 4、トランザクション生成部 4 2 5、チャレンジ設定部 4 2 6、コントラクト情報生成部 4 2 7、トークン発行情報生成部 4 2 8、サイト提供部 4 3 1、会員登録部 4 3 2、及びコンテンツ受信部 4 3 3 として機能する。

30

【 0 0 9 8 】

チャレンジ DB 4 1 5 1 には、チャレンジに関する情報が保存されている。第 1 実施形態では、チャレンジ DB 4 1 5 1 には、チャレンジ支援システム 1 のユーザが挑戦するチャレンジに関する情報が各チャレンジ毎に保存される。チャレンジに関する情報には、チャレンジを規定するチャレンジコントラクト 5 0 1 のコントラクトアドレス、契約条件等が含まれる。

【 0 0 9 9 】

会員 DB 4 1 5 2 には、チャレンジ支援システム 1 の会員に関する情報が保存されている。第 1 実施形態では、図 6 に示されるように、会員 DB 4 1 5 2 には、氏名、性別、生年月日、アカウント名等のユーザ識別情報、各ユーザの公開アドレス、会員が関連する関連チャレンジ情報等が登録されていることが望ましい。なお、図 6 に示す各公開アドレスは、説明のための架空のアドレスであり、イーサリアムで使用される実際のアドレスとはアドレスの桁数が異なっている。他の図においても同様である。

40

【 0 1 0 0 】

ユーザがブロックチェーンネットワーク 5 5 にサンクストークンコントラクト 5 0 2 を有している場合は、サンクストークンコントラクト 5 0 2 のコントラクトアドレスが登録されていてもよい。

【 0 1 0 1 】

関連チャレンジ情報には、ユーザが関連付けられているチャレンジを規定するスマート

50

コントラクトのコントラクトアドレスと、キャンペーンへの参加属性とが保存される。参加属性には、例えば、チャレンジの作成者であることを示す「資金提供者」、チャレンジの挑戦者であることを示す「挑戦者」等が設定される。なお、関連チャレンジ情報には、ユーザが関連付けられている任意のチャレンジに関する情報を保存することができる。

【0102】

コンテンツDB4153には、チャレンジ支援システム1のチャレンジを達成するための活動のエビデンスとなる画像や音声等のコンテンツに関する情報が保存されている。第1実施形態では、コンテンツDB4153にはコンテンツ、コンテンツから生成したハッシュ値が保存されていることが望ましい。ハッシュ値は、コンテンツを一意に識別する情報である。ハッシュ値を用いることで、ブロックチェーンネットワーク55に画像ファイル等を記録する必要がなくなる。よって、コンテンツそのものはブロックチェーンネットワーク55によって公開されることなく、秘匿される。なおブロックチェーンネットワーク55に記録されるデータからコンテンツを一意に識別可能であれば、ハッシュ値とは異なるデータを用いてもよい。

10

【0103】

鍵生成部421、アドレス生成部422、アドレス取得部423、ウォレット部424及びトランザクション生成部425は、鍵生成部121、アドレス生成部122、アドレス取得部123、ウォレット部124、及びトランザクション生成部125と同様の機能を有する。

【0104】

鍵生成部421によって生成される秘密鍵は、記憶部415に保存される。アドレス生成部422によって生成される運営者の公開アドレスは、記憶部415に保存される。運営者の公開アドレスは、資金提供者端末10のアドレス取得部123によって、資金提供者端末10が取得可能である。

20

【0105】

チャレンジ設定部426及びコントラクト情報生成部427は、チャレンジ設定部126及びコントラクト情報生成部127と同様である。チャレンジ設定部426及びコントラクト情報生成部427は、運営者によるチャレンジの作成を可能とする。なお、チャレンジの作成にあたって、運営者端末40が、外部で生成されたコントラクト情報を受信し、コントラクト生成トランザクションをブロックチェーンネットワーク55に送信することで、チャレンジを作成してもよい。

30

【0106】

トークン発行情報生成部428は、トークン発行情報生成部227と同様に、運営者によるブロックチェーンネットワーク55におけるトークンの発行を可能とする。なお、トークンの発行にあたって、運営者端末40が、外部で生成されたトークン発行情報を受信し、ブロックチェーンネットワーク55に送信することで、トークンを発行してもよい。

【0107】

サイト提供部431は、チャレンジ支援システム1を利用するためのウェブサイトをネットワークN上で提供する。当該サイトにおいて、資金提供者や挑戦者、資金の還付先となる還付者が会員登録をしたりすることができる。このためにサイト提供部431は、HTML(HyperText Markup Language)等で記述されたウェブページを、ユーザの使用する端末へ送信すると共に、ユーザによる入力結果等を、端末から受信する。

40

【0108】

会員登録部432は、ユーザの端末からユーザ識別情報を受信して、会員DB4152に登録する。第1実施形態では、サイト提供部431が提供する会員登録画面でのユーザの操作に応じて端末から会員情報が送信されると、会員登録部432は、受信したユーザ識別情報に基づいて会員DB4152にデータを登録する。

【0109】

会員登録部432は、チャレンジアプリ80をダウンロードした端末から公開アドレス

50

をユーザ識別情報と共に受信すると、ユーザ識別情報によって特定された会員DB4152に公開アドレスを保存する。

【0110】

コンテンツ受信部433は、挑戦者端末20又は後述する判定用データ送信端末60から、画像データや音声データ等のコンテンツを受信してコンテンツDB4153に保存する。コンテンツ受信部433は、コンテンツを一意に識別するハッシュ値をコンテンツと共に受信して、受信したハッシュ値及びコンテンツをコンテンツDB4153に保存する。

【0111】

ブロックチェーンネットワーク55には、チャレンジコントラクト501、サンストークンコントラクト502、及びチアリングトークンコントラクト503が設けられる。

【0112】

チャレンジコントラクト501は、資金提供者端末10のコントラクト情報生成部127又は運営者端末40のコントラクト情報生成部427が生成したコントラクト情報に基づいて生成されるスマートコントラクトである。

【0113】

サンストークンコントラクト502は、挑戦者端末20のトークン発行情報生成部227が生成したトークン発行情報に基づいて生成されるスマートコントラクトである。

【0114】

チアリングトークンコントラクト503は、運営者端末40のトークン発行情報生成部428が生成したトークン発行情報に基づいて生成されるスマートコントラクトである。

【0115】

ブロックチェーンネットワーク55上に設けられるチャレンジコントラクト501、サンストークンコントラクト502、及びチアリングトークンコントラクト503によって、あるチャレンジをユーザに達成させる可能性を高めるという機能を持つdapp(Decentralized application)が構成される。ユーザは、資金提供者端末10、挑戦者端末20等のクライアント端末を経由し、所定の使用料を支払うことで、dappを利用する。イーサリアムにおける使用料はGASである。

【0116】

判定用データ送信端末60は、入力部611、表示部612、通信部613、制御部614、記憶部615、及び撮像部616を備える。

【0117】

入力部611、表示部612、通信部613、及び撮像部616に関しては、入力部111、表示部112、通信部113、及び撮像部116と同様である。判定用データ送信端末60は、保存されたユーザ識別情報を運営者端末40へと送信する。記憶部615には、チャレンジアプリ81が記憶される。

【0118】

制御部614は、CPU及びメモリを含む。制御部614は、記憶部615に記憶されているチャレンジアプリ81(プログラム)がRAMに読み出され、CPUによって実行されることで、鍵生成部621、アドレス生成部622、アドレス取得部623、ウォレット部624、トランザクション生成部625、判定用データ取得部626、及び鍵秘匿部627として機能する。

【0119】

鍵生成部621、アドレス生成部622、アドレス取得部623、及びトランザクション生成部625は、鍵生成部121、アドレス生成部122、アドレス取得部123、及びトランザクション生成部125と同様の機能を有する。判定用データ取得部626は、判定用データ取得部226と同様の機能を有する。

【0120】

鍵秘匿部627は、判定用データ送信端末60のユーザが鍵生成部621によって生成される秘密鍵を、他の端末に移転できないようにする機能を有する。仮想通貨の一般的なウォレットは、秘密鍵の移転やバックアップのために必要な情報をユーザに対して表示す

10

20

30

40

50

る機能を有する。例えば、ウォレットは秘密鍵を画像として表示したり、ニーモニック ( Mnemonic ) を表示する。鍵秘匿部 627 は、秘密鍵の移転や、秘密鍵のバックアップのために必要な情報をユーザに対して表示する機能を制限することによって、秘密鍵の移転を制限する。

#### 【0121】

秘密鍵の移転を制限する理由について説明する。ブロックチェーンネットワーク 55 において送信者が本当に送ったトランザクションであるかどうかの識別は、トランザクションが送信者の秘密鍵により署名されているかどうかをブロックチェーンネットワーク 55 の各ノードが検証されることにより行われる。送信者の秘密鍵によってトランザクションに署名を行うということが、そのトランザクションの送信が所有者本人によってなされたということを示すことになる。

10

#### 【0122】

秘密鍵を移転すれば、判定用データを、他の端末やソフトウェアを使ってチャレンジコントラクト 501 に送ることができる。他の端末やソフトウェアを使って、自身の秘密鍵で署名をした判定用データを送れば、チャレンジコントラクト 501 において、判定用データは、ユーザが保有する端末からのデータなのか、他の端末やソフトウェアからのデータなのかという区別がつかない。

#### 【0123】

判定用データ送信端末 60 では、鍵秘匿部 627 によって秘密鍵の移転を制限することによって、判定用データが判定用データ送信端末 60 以外の端末から送信されるような事態を避けることが可能となる。よって、判定用データ送信端末 60 の秘密鍵を用いて署名された判定用データは、判定用データ送信端末 60 から送られることをスマートコントラクトが確認できる。

20

#### 【0124】

図 9 及び図 10 のシーケンス図と図 11 から図 21 を参照しつつ、チャレンジ支援システム 1 の動作について説明する。

#### 【0125】

ステップ S101 において、運営者端末 40 がブロックチェーンネットワーク 55 へ、チャリングトークンコントラクト 503 を生成するトランザクションを送信する。

#### 【0126】

ステップ S102 にて、ブロックチェーンネットワーク 55 によってトランザクションが承認され、ブロックチェーンネットワーク 55 にチャリングトークンコントラクト 503 が生成される。

30

#### 【0127】

ステップ S103 において、ブロックチェーンネットワーク 55 は、チャリングトークンコントラクト 503 のコントラクトアドレス CA3 を運営者端末 40 へと送信する。

#### 【0128】

ブロックチェーンネットワーク 55 に生成されたチャリングトークンコントラクト 503 の初期の例を図 11 に示す。チャリングトークンの通貨単位は「CT」とする。「0x69d...」の公開アドレスはチャリングトークンコントラクト 503 のコントラクトアドレス CA3 である。「0xe33...」の公開アドレスは運営者端末 40 に保存される秘密鍵に対応する運営者の公開アドレスである。

40

#### 【0129】

チャリングトークンコントラクト 503 は、他のユーザに対して、ETHER と交換するようにして、チャリングトークンを配分する。チャリングトークンの配分が行われた場合、チャリングトークンコントラクト 503 は図 12 に示すように、チャリングトークンの保有者の公開アドレスを追加し、その公開アドレスについてチャリングトークンの残高を管理する。

#### 【0130】

ステップ S104 において、挑戦者端末 20 が、ブロックチェーンネットワーク 55 へ

50

、サンクストークンコントラクト502を生成するトランザクションを送信する。

【0131】

ステップS105において、ブロックチェーンネットワーク55によりトランザクションが承認され、ブロックチェーンネットワーク55にサンクストークンコントラクト502が生成される。

【0132】

ブロックチェーンネットワーク55に生成されたサンクストークンコントラクト502の初期の例を図13に示す。チャリングトークンの通貨単位は「TT」とする。「0x202...」の公開アドレスはサンクストークンコントラクト502のコントラクトアドレスCA2である。「0xb2f...」の公開アドレスは、挑戦者端末20に保存される秘密鍵に対応する挑戦者の公開アドレスA2である。ここでは、「0xb2f...」の公開アドレスを有するユーザをユーザAとする。

10

【0133】

ステップS106において、ブロックチェーンネットワーク55は、サンクストークンコントラクト502のコントラクトアドレスCA2を挑戦者端末20へと送信する。

【0134】

ステップS107において、挑戦者端末20は、コントラクトアドレスCA2、挑戦者のユーザ識別情報、及び挑戦者の公開アドレスA2を運営者端末40へ送信する。

【0135】

ステップS108において、運営者端末40は、コントラクトアドレスCA2、挑戦者のユーザ識別情報及び公開アドレスA2を、資金提供者端末10へ送信する。この処理により、資金提供者端末10が、サンクストークンコントラクト502のコントラクトアドレスCA2と挑戦者の公開アドレスA2を対応付けて記憶することができる。資金提供者端末10には、図14に示すようにアカウント名と公開アドレスが対応付けて記憶される。図14では、公開アドレスに対応するサンクストークンコントラクトがない場合は、サンクストークンコントラクトの公開アドレスは空欄となっている。

20

【0136】

ステップS109において、資金提供者端末10は、コントラクトアドレスCA2、挑戦者のユーザ識別情報、公開アドレスA2、契約条件等に基づいて、コントラクト情報を生成する。この時生成されるコントラクト情報の一例を図15に示す。

30

【0137】

図15に示されるコントラクト情報は、ユーザAが、自身で一日に一定以上の歩数を歩くチャレンジであるチャレンジAを作成した場合のコントラクト情報である。コントラクト情報の内容は以下の通りである。

【0138】

挑戦者は、2019年7月1日から2019年7月31日までの期間にチャレンジを行うことができる。目標歩数は、一日あたり8000歩である。挑戦者は、期間の中から任意の20日間を選ぶ。挑戦者が、そのうち連続でも断続的でもよい10日以上の日数において一日あたり8000歩を歩くことでチャレンジが達成される。供託金額は1ETHである。

40

【0139】

チャレンジの成功、失敗の判定には、歩数データが用いられる。歩数データは、スマートコントラクトに保存される。

【0140】

コントラクト情報には、「判定用データ送信端末公開アドレス」の項目が設けられる。この項目に対応する公開アドレスは、判定用データ送信端末60の公開アドレスに対応する。判定用データ送信端末60の公開アドレスは、挑戦者のユーザ識別情報に含まれている場合や、資金提供者のユーザ識別情報に含まれる場合等がある。判定用データ送信端末60を用いない場合は、特段の設定は行われない。

【0141】

50

チャレンジ情報には、「チャレンジ開始日」及び「チャレンジ終了期限」の項目が設けられる。チャレンジ開始日とは、挑戦者がチャレンジにとりかかった日である。チャレンジ開始日は、例えば、判定用データの最初の送信が行われた日などとすることができる。

【0142】

チャレンジ終了期限は、チャレンジを終了しなければならない期限である。図15では、チャレンジ開始日から20日でチャレンジを達成しなければならない。仮に2019年7月5日がチャレンジ開始日である場合、チャレンジ終了期限は、2019年7月24日となる。

【0143】

コントラクト情報には、「チャレンジ達成度」の項目が設けられる。この項目は、チャレンジコントラクト501が、チャレンジ過程において、歩数データ及び目標歩数からチャレンジの達成度を算出し、記憶するために設けられる。達成度は、例えば、チャレンジにおいて達成すべき目標歩数に対する現在の歩数の割合として算出することができる。

10

【0144】

チャレンジが成功した場合、失敗した場合のそれぞれに対して決められた配分先に、供託金が配分設定に基づいて配分される。配分先や配分量は自由に設定できる。配分量は供託金額に対するパーセンテージで設定してもよい。配分量は配分するETHERの量を直接設定してもよい。運営者の手数料は、例えば供託金の2パーセントのようにして、差し引かれる。

【0145】

20

配分先を指定する際は、配分先の公開アドレスを直接指定することができる。例えば、資金提供者端末10の撮像部116によって読み取った画像から公開アドレスを取得し、配分先とすることができる。図14に示されるように資金提供者端末10の記憶部115に記憶される公開アドレスを用いることも可能である。

【0146】

資金の配分状態にはそれぞれ、還付、寄付及び没収が含まれ、資金提供者端末10からは、還付、寄付及び没収で指定した金額の合計が資金額と一致するように指定された配分設定が送られる。還付には、イーサリアムの公開アドレスを保持している任意の還付先及び任意の金額を指定することができる。寄付には、イーサリアムの公開アドレスを保持している任意の寄付先及び任意の金額を指定することができる。チャレンジ成功時・失敗時・中断時に運営者には運営者手数料が支払われるようにしてもよい。

30

【0147】

記憶部115に記憶される公開アドレスは、運営者端末40に記憶されるユーザ識別情報と同期可能であり、他のユーザのアドレスが変わった場合には、自動的にその新しいアドレスを取得することができる。

【0148】

チャレンジ作成時に、チャレンジの中断を示す情報に基づいてチャレンジを中断することが可能か否かを定めることができる。

【0149】

チャレンジの中断には、ギブアップによる中断と自己解体による中断がある。ギブアップによる中断は、資金提供者や挑戦者がチャレンジの達成を諦め、チャレンジの中断を示す情報をトランザクションとしてスマートコントラクトに送信することによる中断である。

40

【0150】

自己解体による中断は、何らかの事情でチャレンジコントラクト501から資金が出ない等のトラブルが発生し、運営者が利用者からのリクエストによりチャレンジコントラクト501を自己解体させる場合や、警察、法令、裁判所又は政府機関の命令、要求又は要請があった場合、又は運営者が独自に必要と判断した場合がある。自己解体による中断の場合、運営者はチャレンジコントラクト501を自己解体させるトランザクションをチャレンジコントラクト501に送信する。

【0151】

50

ギブアップした場合において、供託金の配分は、運営者の手数料を差し引いた残りが事前に決められた配分先に供託金が配分されるギブアップパターンAや、ギブアップするまでのチャレンジの達成度を考慮し、チャレンジ成功時と同じ配分先に供託金が配分され、運営者の手数料を差し引いた残りが資金提供者に戻されるギブアップパターンB等がある。

【0152】

チャレンジコントラクト501を自己解体させる場合において、供託金の配分は、資金提供者に資金を一部返還する自己解体モードAや、運営者に全額送金される自己解体モードB等がある。

【0153】

ステップS110において、資金提供者端末10は、ブロックチェーンネットワーク55へ、コントラクト情報に基づいて、チャレンジコントラクト501を生成するためのコントラクト生成トランザクションを送信する。

【0154】

ステップS111において、ブロックチェーンネットワーク55によってコントラクト生成トランザクションが承認され、ブロックチェーンネットワーク55にチャレンジコントラクト501が生成される。生成されたチャレンジコントラクト501は、図15で説明したコントラクト情報に加えて、図16において「0x202...」で示されるチャレンジコントラクト501のコントラクトアドレスCA1及びチャレンジ結果のデータを含む。チャレンジ結果は、成功、失敗、ギブアップパターンA、ギブアップパターンB、自己解体モードA、又は自己解体モードBのいずれの結果に従って供託金の配分が行われるかを示す情報である。

【0155】

ステップS112-1において、ブロックチェーンネットワーク55はチャレンジコントラクト501のコントラクトアドレスCA1を資金提供者端末10へ送信する。ステップS112-2において、資金提供者端末10は、コントラクトアドレスCA1を宛先として、チャレンジコントラクト501に供託金額を送金する。チャレンジコントラクト501は、供託金額をコントラクトアドレスCA1に紐づいた残高として保持する。

【0156】

ステップS113において、資金提供者端末10は運営者端末40へコントラクト情報及びコントラクトアドレスCA1を送信する。運営者端末40は、図17に示されるように、各チャレンジについての情報をチャレンジDB4151へと記録する。なお、「配分金受取者」の項目に記憶される情報には、チャレンジコントラクト501等のスマートコントラクトが含まれていてもよい。また、「配分金受取者公開アドレス」の項目に記憶される情報には、スマートコントラクトのコントラクトアドレスが含まれていてもよい。また、運営者端末40は、図18に示されるように、ユーザ毎に、ユーザのユーザ識別情報及びユーザが関連するチャレンジを、会員DB4152へと記録する。

【0157】

ステップS114において、運営者端末40は挑戦者端末20へ、コントラクト情報及びコントラクトアドレスCA1を含むチャレンジ情報を送信する。これにより、挑戦者は、チャレンジの内容や、どのコントラクトアドレスへと判定用データを送信すべきかについての情報を得ることができる。

【0158】

図10に示されるステップS121にて、挑戦者はチャレンジ期間中に、挑戦者端末20からチャレンジコントラクトへと判定用データを送信する。判定用データの送信には、必ずしも挑戦者端末20を用いなくともよい。ステップS122のように、判定用データ送信端末60を用いて判定用データをチャレンジコントラクトへ送信してもよい。

【0159】

挑戦者端末20からチャレンジコントラクトに送信される判定用データの一例は図19に示される。図20には、挑戦者端末20からチャレンジコントラクトに送信される判定用データ、送信されたトランザクションにより、チャレンジコントラクト501に保存さ

10

20

30

40

50

れるデータ構造が示されている。データの投稿日時として、トランザクションが格納されるブロックチェーンネットワーク55のブロックの生成日時が、図19のデータに加えられている。また、チャレンジコントラクト501によって達成日数の数が記録されている。

【0160】

ステップS123において、挑戦者は、自身のチャレンジに対する応援を行う応援者に対して、サンクストークンを配分するトランザクションをサンクストークンコントラクトへ送信する。

【0161】

挑戦者は、図21に示されるように、応援者端末30にチャレンジアプリ81をインストールしているチャレンジ支援システム1の利用者のアドレスを運営者端末40から取得し、記憶している。挑戦者は、各アドレスに対してサンクストークンを配分することができる。

10

【0162】

ステップS124において、ブロックチェーンネットワーク55によってトランザクションが承認されることで、サンクストークンコントラクト502の残高が更新される。サンクストークンコントラクト502の残高の更新によってサンクストークンの応援者への配分が行われる。

【0163】

挑戦者からサンクストークンを配分された応援者は、他の応援者に対して、サンクストークンを再配分することができる。サンクストークンを再配分する場合は、再配分を行う元の応援者のみが再配分送付先の公開アドレスを知っていればよい。つまり、サンクストークンは転々流通することが可能である。

20

【0164】

サンクストークンの配分並びに再配分が行われた後のサンクストークンコントラクト502の残高の一例を示す。挑戦者であるユーザAの残高は0となっている。図22に示されるように、挑戦者端末20はユーザD、ユーザE、ユーザFについて、それぞれの公開アドレスを取得しており、それぞれに対してサンクストークンを配分した。ユーザAはユーザDに20TT、ユーザEに50TT、ユーザFに30TTの配分を行った。その結果、サンクストークンの残高は、図22にてサンクストークン残高(1)で示されるようになる。その後、ユーザAが当初は把握していない応援者端末30Aを有するユーザGに、ユーザFから10TTが再配分された結果が図22のサンクストークン残高(2)である。

30

【0165】

ステップS125において、挑戦者端末20はチャレンジコントラクト501へ終了判定データを送信する。終了判定データは、ステップS126のように判定用データ送信端末60から送信されてもよい。また、ステップS127のように運営者端末40から送信されてもよい。

【0166】

終了判定データはチャレンジコントラクト501がチャレンジの成功、失敗を判断するために用いられる。例えば、図15のコントラクト情報に従って、7月5日から7月24日までの20日間のうち10日間、一日あたり8000歩以上歩くというチャレンジがあるとすると、この時7月5日から7月13日までの9日間は8000歩以上歩いているとする。この場合、7月14日の歩数データとして10000歩を送ったときにチャレンジ成功が終了判定となる。

40

【0167】

7月14日の10000歩のデータが、「終了判定歩数データ」となる。終了判定歩数データを送信するトランザクションがブロックチェーンネットワーク55に承認された時点でチャレンジ成功が確定する。

【0168】

また、上記と同じ条件のチャレンジにおいて、7月5日から7月13日までの9日間は8000歩以上歩いているとする。その後、7月14日から7月23日までは8000歩

50

未満しか歩いていない場合、挑戦者が7月24日の歩数として5000歩を送ると、この5000歩が、「終了判定歩数データ」となり、チャレンジ失敗が終了判定となる。

【0169】

挑戦者が、7月24日の5000歩のデータを送ることをためらったり、忘れてりする場合、チャレンジコントラクト501はチャレンジの成功、失敗を判断できない。

【0170】

スマートコントラクトが、ブロックチェーンネットワーク55におけるブロックをマイニングしたマイナーが記録するブロックタイムによる日付情報を取り込んでもよい。その他のブロックチェーンネットワークが有する機能を用いて日付情報を取り込んでもよい。第1実施形態におけるスマートコントラクトは、外部からの何らかの日付に関する情報を必要とする。そのため、チャレンジコントラクト501において、7月24日を過ぎても歩数データが送られてこない場合はチャレンジ失敗とみなすという設定は行えないからである。資金提供者や運営者等の関係者がスマートコントラクトに対して日付に関する情報をトランザクションとして送ってもよい。

10

【0171】

前述の例で、7月24日の5000歩のデータが送られない場合、7月25日や26日に運営者が資金提供者や挑戦者等に対して、歩数データが送られていないことをメールやアプリ上のお知らせ等によって知らせてもよい。運営者は、チャレンジコントラクト501におけるデータの状態をアプリからの情報又はチャレンジコントラクト501を直接参照することによって知ることができる。挑戦者は、本来チャレンジ期間中の歩数を適切なタイミングで全部送信することが求められるが、それを履行しない場合は、チャレンジ期間終了後一定の猶予期間を経た後、後述のようにその未送信の歩数はゼロであるとチャレンジコントラクト501に取り扱いされることになる。前述のお知らせメールを受け取った資金提供者が、チャレンジコントラクト501に対して「本日は7月26日」という日付データをトランザクションとして送ると、チャレンジコントラクト501は挑戦者からの未送信の7月24日の歩数をゼロとして取り扱うので、チャレンジコントラクト501は、チャレンジ失敗と判定する。この場合、資金提供者からの日付に関する情報が、「終了判定日付データ」となっている。

20

【0172】

上記のように誰かが「終了判定データ」を送信し、「終了判定データ」がブロックチェーンネットワーク55に取り込まれると、自動的にチャレンジコントラクト501が事前に決められた通りに動き始める。

30

【0173】

終了判定データがチャレンジコントラクト501へ送られることでチャレンジ達成判定が可能となる。ステップS128において、ブロックチェーンネットワーク55のチャレンジコントラクト501がチャレンジ達成判定処理を行う。

【0174】

ステップS129において、判定結果に基づいて、チャレンジコントラクト501がETHERの配分処理を行う。

【0175】

チャレンジコントラクト501によるETHERの配分処理は、イーサリアムでは、インターナルトランザクションをチャレンジコントラクト501が生成することによって行われる。イーサリアムにおけるインターナルトランザクションは、挑戦者等から受け取ったトランザクションをトリガーにしてスマートコントラクトが生成するトランザクションである。

40

【0176】

ステップS130において、チャレンジコントラクト501からETHERが配分されたサンクストークンコントラクト502によって、サンクストークンの残高に基づいた、応援者へのETHERの配分処理が行われる。

【0177】

50

サックストークンの残高に基づいた E T H E R の配分について、図 2 2 のサックストークン残高 ( 2 ) に基づく場合を例に説明する。チャレンジコントラクト 5 0 1 が供託金を 1 E T H 保有するとする。1 E T H の供託金のうち、0 . 8 E T H がサックストークンコントラクト 5 0 2 へと配分されるとする。この場合、ユーザ D、ユーザ E、ユーザ F、ユーザ G それぞれのサックストークンの持分に従って 0 . 8 E T H が配分される。ユーザ D に対しては、0 . 1 6 E T H、ユーザ E に対しては 0 . 4 E T H、ユーザ F に対しては 0 . 1 6 E T H、ユーザ G に対しては 0 . 0 8 E T H が配分される。

【 0 1 7 8 】

サックストークンコントラクト 5 0 2 は、E T H E R だけでなく、各種トークンがサックストークンコントラクト 5 0 2 に送られてきたときも同様に配分してよい。

【 0 1 7 9 】

資金提供者がチャレンジコントラクト 5 0 1 へと供託する仮想通貨ベースの供託金額の価格変動リスクヘッジのため、チャレンジコントラクト 5 0 1 の作成に当たり、常に同じレートで法定通貨に交換できる、価値が変動しない仮想通貨を用いて今回のチャレンジ支援システム 1 を作ってもよい。

【 0 1 8 0 】

チャレンジコントラクト 5 0 1 が規定するチャレンジは、歩数に関するチャレンジとは異なる他の種類のチャレンジとしてもよい。図 2 3 から図 2 6 を参照して、チャレンジのバリエーションについて説明する。

【 0 1 8 1 】

図 2 3 には、安全運転チャレンジについての、スマートコントラクトの内容が示される。判定用データは、自動車や、運転者が保有するスマートフォンから、自動車の速度、シートベルト着用の有無、急ブレーキ、急発進の情報である。判定用データの取得及び送信に、ウォレット機能を持った I o T デバイスを使ってもよい。I o T デバイスからスマートフォン等に情報を転送し、スマートフォンに内蔵するアプリのウォレットの秘密鍵で署名したトランザクションをブロックチェーンネットワークに送ってもよい。運送会社が、トラックドライバーに対して、1 日の運転で判定条件が満たされたら E T H E R やトークンを自動的に送るチャレンジに関するスマートコントラクトを作ってもよい。

【 0 1 8 2 】

図 2 4 には、血糖値スパイク予防チャレンジについての、スマートコントラクトの内容が示される。血糖値が急激に上昇する血糖値スパイクが問題となっている。例えば朝食を抜いて、昼食に大量の糖質を摂取すると血糖値スパイクが起こる。野菜や海藻などを食事の最初に食べる、長時間空腹が続くようにしない等の工夫を行うことで血糖値スパイクを予防することができる。腕に取り付けることで継続的に血糖値を測定することができる機器からの血糖値データを、スマートフォン等に転送し、スマートフォンに内蔵するアプリのウォレットの秘密鍵で署名したトランザクションをブロックチェーンネットワークに送ってもよい。保険会社が保険加入者に対して、血糖値を急激に上昇させないライフスタイルを勉強してもらうために図 2 4 のようなスマートコントラクトを作ってもよい。加入者は短期的に経済的な見返りがないと真剣にやらない。まず、血糖値スパイクを起こさない方法のレクチャーを行いチャレンジを開始するとよい。

【 0 1 8 3 】

図 2 5 には、子供勉強チャレンジについての、スマートコントラクトの内容が示される。子供が I o T デバイスを取り付けたえんぴつを使用して勉強をすると、I o T デバイスからスマートコントラクトに対して一定時間勉強した情報が送信され、I o T デバイスのウォレット又は、子供専用のウォレットにご褒美として E T H E R やオンラインゲームで使用できるトークン等が送られる。I o T デバイスに E T H E R が送られた場合、貯まった E T H E R に応じて I o T デバイスの色が変化し、子供はその色の変化を見て勉強を沢山するとお小遣いが増えることを意識し、勉強に対するモチベーションが高まる。親の経済レベルに合わせて、ご褒美の金額は調整するとよい。成功時に兄弟にも一部 E T H E R を送ることで、勉強の邪魔をしなくなる。

10

20

30

40

50

## 【 0 1 8 4 】

図 2 6 には、禁煙チャレンジについての、スマートコントラクトの内容が示される。保険適用の治療ではなく、自費治療を想定する。禁煙を希望する患者に対して、医師が 6 0 万円の禁煙チャレンジを院内処方する。患者は、病院に対して 6 0 万円を支払う。病院は、利益と経費 5 万円を差し引いた、5 5 万円分の E T H E R を使って禁煙チャレンジスマートコントラクトを作る。患者の禁煙が達成されたかどうかは、呼気中の C O を測定する機器を使って医師が判定してもよい。C O 測定の I o T デバイスで呼気中の C O を測定し、そのデータを I o T デバイスに内蔵したウォレットからスマートコントラクトに送ってスマートコントラクトが禁煙チャレンジの成功・失敗を判定してもよい。より高額な禁煙チャレンジを処方してもよい。

10

## 【 0 1 8 5 】

チャレンジ支援システム 1 が稼働するにあたって、ブロックチェーンネットワーク 5 5 における、チャレンジコントラクト 5 0 1 等の各種スマートコントラクトの生成及び各種トランザクションの送信、供託金の供託には、仮想通貨が必要となる。資金提供者等は仮想通貨取引所等から仮想通貨を購入する。仮想通貨の購入方法の他の例について説明する。

## 【 0 1 8 6 】

資金提供者、挑戦者、応援者等は仮想通貨やトークンを、コンビニ等で購入してもよい。購入者は、仮想通貨やトークンの情報を持つギフト券を購入する。そのギフト券の一部を削ると、二次元バーコードが出てくる。二次元バーコードは、ギフト券ウォレットの秘密鍵である。ギフト券の発行者は、あらかじめこのギフト券ウォレットの公開アドレスにギフト券に記載されたものと同額の仮想通貨やトークンを送付しておく。ギフト券の発行者はギフト券の秘密鍵情報は一切保管せず、ギフト券の公開アドレスのみを保管して管理するものとする。

20

## 【 0 1 8 7 】

購入者は自身のアプリで二次元バーコードを読み取り、アプリ内にギフト券ウォレットを取り込む。ユーザはギフト券ウォレットの秘密鍵の情報を取得することとなるので、ギフト券ウォレットを自由に使うことができる。

## 【 0 1 8 8 】

又は、購入者がコンビニの A T M 画面でギフト券を選択し、入金すると、上記と同じ秘密鍵である二次元バーコードが発行される。その場でアプリを使用し、二次元バーコードを読み取ることで、アプリ内にギフト券ウォレットを取り込んでよい。

30

## 【 0 1 8 9 】

この場合、ギフト券発行者は、A T M からリクエストされたときだけ秘密鍵を作成し、それに対応する公開アドレスに送金すればよい。紙等のギフト券の場合は、事前にギフト券ウォレットに送金しておかなければならない。二次元バーコードには、秘密鍵情報が入っており実質的に金券と同じような価値があるので取り扱いに注意が必要である。

## 【 0 1 9 0 】

ギフト券ウォレットの秘密鍵を読み取った時点で、購入者のアプリ内には、元々所有していたウォレットと、ギフト券ウォレットの 2 つが存在することになる。言い換えると、仮想通貨を管理する秘密鍵を 2 つ所有するということである。購入者は、ギフト券ウォレットの残高を全て元々所有していたウォレットに送信し、ギフト券ウォレットを削除する。

40

## 【 0 1 9 1 】

又は、購入者がコンビニのレジに行き、仮想通貨、トークンが欲しいと店員に伝える。現金を支払うと、店員は購入者のアプリの中に元々あったウォレットの二次元バーコードを読み取る。これは、購入者の公開アドレスである。コンビニが自身の仮想通貨、トークンをその公開アドレスに直接送るようにしてもよい。

## 【 0 1 9 2 】

又は、ギフト券発行者が作成したスマートコントラクトに対して、コンビニ端末から仮想通貨と購入者の公開アドレスをトランザクションとして送ると、スマートコントラクトから直接購入者のウォレットに仮想通貨やトークンが送信されるようにしてもよい。

50

## 【0193】

チャレンジアプリ80によるチャレンジコントラクトの生成における、チャレンジアプリ80がインストールされる端末に表示される画面の遷移について、図27から図33を参照しつつ説明する。

## 【0194】

図27の画面801には、チャレンジ欄8011、資金提供者欄8012、挑戦者欄8013、供託金額欄8014が設けられる。チャレンジ欄8011には、チャレンジ名が入力される。資金提供者欄8012、挑戦者欄8013には、資金提供者のアカウント名が表示される。資金提供者欄8012、挑戦者欄8013がそれぞれ有するボタンBT1又はBT2が選択されると、図28に示される画面802が表示される。

10

## 【0195】

画面802には、端末に記憶されるアカウント名と公開アドレスが対応付けられて表示される。ユーザは、各行を選択することによって、資金提供者及び挑戦者を選択することができる。ユーザは図28のボタンBT4を選択することによって、アカウント名及びアドレスの組を追加可能である。

## 【0196】

図27の供託金額欄8014には、資金提供者が供託する供託金額が入力される。ユーザが画面801のボタンBT3を選択することで、図29の画面803が表示される。

## 【0197】

画面803には、期限欄8031及び条件欄8032が設けられる。期限欄8031にはチャレンジの開始可能期間及び終了可能期間が入力される。条件欄8032には、チャレンジの種類、チャレンジ実行日数、歩数、達成すべき日数が入力される。

20

## 【0198】

ユーザが画面803のボタンBT5を選択することによって、図30の画面804が表示される。

## 【0199】

画面804には成功時配分欄8041、失敗時配分欄8042、GAS手数料欄8043が設けられる。

## 【0200】

成功時配分欄8041には、成功時に資金を受け取るユーザのアカウント名及び、受け取る額が入力される。また、供託金額の2パーセントの資金が運営者手数料として配分される。運営者手数料は自由に設定してよい。失敗時配分欄8042についても同様である。挑戦者宛GAS手数料欄には、挑戦者が歩数情報をスマートコントラクトに送信するときに必要なGAS手数料を補助する金額が入力される。

30

## 【0201】

ユーザが画面804のボタンBT6を選択すると、図31の画面805が表示される。画面805は、ギブアップ選択欄8051及びギブアップパターン選択欄8052を有する。ユーザは、ギブアップ選択欄8051の項目を選択することで、ギブアップを可能とするかを選択できる。ユーザは、ギブアップパターン選択欄8052の項目を選択することで、ギブアップ時の供託金の配分方法を選択できる。

40

## 【0202】

ユーザが画面805のボタンBT6を選択すると、図32の画面806が表示される。画面806には、ここまでに設定した条件が一覧として表示される。

## 【0203】

ユーザは画面805のボタンBT7を選択することによって、当該チャレンジを管理するチャレンジコントラクトをブロックチェーンネットワーク55に生成するトランザクションがブロックチェーンネットワーク55へと送信される。

## 【0204】

また、画面805のボタンBT8を選択することによって、図33に示されるような、作成するチャレンジの情報を他の端末で読み取折り可能とするための画面806を生成す

50

ることができる。生成された画像を他の端末が読み取ることによって、チャレンジに関する情報を他の端末が取得可能となる。

【0205】

第1実施形態において説明してきたプログラムは、記憶媒体に格納することができる。当該プログラムを格納した記憶媒体は、非一時的な記憶媒体(Non transitory computer readable medium)であってもよい。非一時的な記憶媒体は特に限定されないが、例えば、USBメモリ又はCD-ROM等の記憶媒体であってもよい。

【0206】

第1実施形態では、資金提供者端末10は、チャレンジコントラクト501を生成する  
としたが、チャレンジ支援にあたって作成されるスマートコントラクトは複数であっても  
よい。複数のスマートコントラクトが連携した処理を行うようにスマートコントラクトを  
構築し、より複雑な条件が設定されたチャレンジを作成することができる。

10

【0207】

第2実施形態について説明する。第2実施形態以降の実施形態では第1実施形態と共通  
の事柄についての記述を省略し、異なる点についてのみ説明する。

【0208】

第2実施形態に係るチャレンジ支援システム1Aは、図34に示されるように協賛企業  
端末70をさらに備える。協賛企業端末は、ブロックチェーンネットワーク55Aにおけ  
るアカウント及び公開アドレスを有する。

20

【0209】

協賛企業は例えば、飲料メーカーであるとする。挑戦者は、協賛企業の飲料メーカーの  
飲料を購入する。飲料にはウェブサイトのアドレスを示す画像が添付される。飲料に添付  
された画像を読み取り、運営者又は協賛企業のウェブサイトにアクセスが可能となる。ウ  
ェブサイトにおいて、挑戦者に関する情報として、氏名、年齢、居住地、自身の公開アド  
レス、チャレンジコントラクトのコントラクトアドレス、サンクストークンコントラクト  
のコントラクトアドレス等を入力する。

【0210】

協賛企業は、チャレンジコントラクトに対して、ETHERや、協賛企業がブロックチ  
ェーンネットワーク55Aにおいて発行する製品交換トークン、チアリングトークン等を  
送付する。チャレンジコントラクトに送られた製品交換トークン等は、チャレンジの達成  
度に応じて段階的に有効化されてもよい。

30

【0211】

製品交換トークンは、協賛企業の飲料と交換できる。製品交換トークンの価値は、製品  
交換トークンと交換可能な本数、有効期限、利用可能地域を自由に設計できる。例えば、  
交換は1対1でなくても良く、1つの製品交換トークンに対して5本の飲料と交換しても  
よい。

【0212】

製品交換トークンの実際の使われ方について一例を説明する。製品交換トークンはユー  
ザのウォレットで管理される。ユーザはコンビニに行き、レジ横に置かれたコンビニが保  
有するトークン受け取り用公開アドレスをアプリで読み取る等して取得する。ユーザは、  
そのアドレス宛に製品交換トークンを送付する。コンビニは、コンビニが保有するトー  
クン受け取り用公開アドレスで受けとった製品交換トークンが有効かどうかを確認する。

40

【0213】

コンビニは受け取った製品交換トークンの対価として飲料をユーザに渡す。コンビニは  
後日製品交換トークンを運営者又は協賛企業との間で清算する。ユーザに手間をかけさせ  
ないために、コンビニは、自身の端末によって、コンビニがユーザの製品交換トークンの  
ウォレットの公開アドレスを取得し、ユーザからコンビニへ製品交換トークンを送付する  
トランザクションを生成する。生成されたトランザクションの確認画面をユーザのアプリ  
内に表示させ、ユーザがその内容を承認し、トランザクションとして送信するとユーザの

50

製品交換トークンはコンビニに渡される。

【0214】

第2実施形態のように、チャレンジコントラクト501、サンクストークンコントラクト502、及びチアリングトークンコントラクト503によるトークンの配分に加えて、製品交換トークンを組み合わせることによって構成されるd a p pによって、家族や友人だけでなく、企業の支援を受けながらユーザがチャレンジを達成する可能性をより高めることができる。

【0215】

第3実施形態について説明する。第3実施形態に係るチャレンジ支援システム1Bでは、図35に示されるように、ブロックチェーンネットワーク55Bに、サンクストークンコントラクト502A、サンクストークンコントラクト502B、及びサンクストークンコントラクト502Cが設けられる点が異なる。

10

【0216】

サンクストークンコントラクト502A及びサンクストークンコントラクト502Cは、第1実施形態におけるサンクストークンコントラクト502と同様にチャレンジ毎に挑戦者が応援者の応援に対して配分するトークンの残高を管理するスマートコントラクトである。

【0217】

また、サンクストークンコントラクト502Cは、サンクストークンコントラクト502Aが関係するチャレンジとは別のチャレンジに関係する。

20

【0218】

サンクストークンコントラクト502Bは、挑戦者に対する継続的な応援の貢献を表すものである。サンクストークンコントラクト502Bは、サンクストークンコントラクト502Aに基づいて残高が更新される。サンクストークンコントラクト502Bはサンクストークンコントラクト502Aとは異なるトークンの残高を管理する。トークンの通貨単位は、サンクストークンコントラクト502AはTTA、サンクストークンコントラクト502BはTTB、サンクストークンコントラクト502CはTTCとする。

【0219】

図36に示されるように、TTBの初期の残高はユーザAからユーザDまで0であるとする。あるチャレンジに対する、サンクストークンコントラクト502Aによるトークンの配分が図37に示されるようになったとする。サンクストークンコントラクト502Bの残高の加算量は、サンクストークンコントラクト502Aのトークンの残高に基づいて決定される。

30

【0220】

サンクストークンコントラクト502Bにおける加算量は、サンクストークンコントラクト502Aの各ユーザについて、発行済みトークンに対する割合に難易度係数をかけ合わせた量である。サンクストークンコントラクト502Aが関係するチャレンジの難易度は難易度係数が0.8である。

【0221】

あるチャレンジに対する、サンクストークンコントラクト502Cによるトークンの配分が、図38に示されるようになったとする。サンクストークンコントラクト502Aにおける場合と同様に、サンクストークンコントラクト502Bの残高の加算量は、サンクストークンコントラクト502Cの残高に基づいて決定される。

40

【0222】

サンクストークンコントラクト502Bにおける加算量は、サンクストークンコントラクト502Cの各ユーザについて、発行済みトークンに対する割合に難易度係数をかけ合わせた量である。サンクストークンコントラクト502Cが関係するチャレンジの難易度は難易度係数が0.2である。

【0223】

サンクストークンコントラクト502A及びサンクストークンコントラクト502Cに

50

よるトークンの配分に基づいて決定された加算量によって、サンクストークンコントラクト502Bの残高が図39のように更新される。

【0224】

あるチャレンジだけの応援者の貢献度を管理するサンクストークンコントラクト502A又はサンクストークンコントラクト502Cによるトークンの管理に基づいて、サンクストークンコントラクト502Bのように挑戦者の一生ものの応援者の貢献度を管理することで、長期的な応援が可能となる。

【0225】

健康保険組合や保険会社等が、一時的な応援者に対するサンクストークンコントラクト502Aではなく、サンクストークンコントラクト502Bに対して、インセンティブを支払う方が、組合員・加入者に対する継続的な応援が行われる可能性がある。また、サンクストークンコントラクト502Bが管理するトークンは他の人に譲渡できないようにトークン設計をしてもよい。

10

【0226】

第4実施形態について説明する。第4実施形態では、図40に示されるように、ブロックチェーンネットワーク55Cが、チャレンジアンドサンクストークンコントラクト504を有する点が第1実施形態とは異なる。

【0227】

チャレンジアンドサンクストークンコントラクト504は、第1実施形態におけるチャレンジコントラクト501とサンクストークンコントラクト502を兼ねるものである。チャレンジアンドサンクストークンコントラクト504は、図41に示されるトークン残高5041のように、それぞれのチャレンジ結果に対応した3種類のトークンをチャレンジ開始時に各関係者に配分する。

20

【0228】

各トークンは、チャレンジ結果が成功、失敗又はギブアップのいずれか一つに決定した後結果に対応するトークンが有効になるものとする。

【0229】

挑戦者は図42に示されるように、自身の成功に期待して、自己のトークンを下請けに対して送付できる。チャレンジ成功時の配分金受取者も同様に、下請けに対してトークンを配分できる。

30

【0230】

チャレンジが成功すれば、成功時のトークンが有効になるので、トークンを配分された下請けは挑戦者をより積極的に応援する。

【0231】

チャレンジが失敗した場合は、成功時トークンは無効となり、失敗時のトークンが有効となる。ギブアップ時も同様である。

【0232】

チャレンジアンドサンクストークンコントラクト504は、図43に示されるトークン残高5041Aのように、1種類のトークンについて管理するものであってもよい。

【0233】

1種類のトークンについて管理する場合、チャレンジ開始時に初期配分として各関係者にトークンが配布される。トークンを受け取った人は、それを下請けに出して協力を得ることができる。例えば、挑戦者が下請けに0.2トークン渡したとする。チャレンジが成功した場合、下請けは、成功時配分に従うと、挑戦者のトークンが60倍されるため、0.2トークンの60倍の12トークンを保有することになる。

40

【0234】

第4実施形態では、チャレンジ中に挑戦者や配分金受取者等の手元にトークンを与え、チャレンジ結果に応じて、トークンに価値が生じる。これによって、サンクストークンが分配用の媒介物として機能するのではなく、トークンそれ自体に価値を与えつつ、チャレンジが行われるようにすることができる。

50

## 【0235】

第5実施形態について説明する。第5実施形態では、図44に示されるように、ブロックチェーンネットワーク55Dが、予想コントラクト505を有する点が、第1実施形態と異なる。予想コントラクト505は挑戦者によるチャレンジの過程、成功、失敗に対して、予想を行い、チアリングトークンで賭金を支払う。

## 【0236】

予想コントラクト505は、応援者等からのチアリングトークンを受け取り次第、自動的に予想コントラクトの作成者に一定の手数料を支払う。また、チャレンジコントラクト501に対してもチアリングトークンを送付する。チャレンジコントラクト501に集積され、保持されたチアリングトークンは、例えば、チャレンジが成功したときに、チャレンジ成功の配分と同じ条件で関係者に配分される。チャレンジコントラクト501に送られるこのチアリングトークンは、自分や人のお金を供託してまでリスクを取って自身の歩行等のチャレンジに挑戦することに対するインセンティブとなる。

10

## 【0237】

以上説明した実施形態は、本発明の理解を容易にするためのものであり、本発明を限定して解釈するためのものではない。実施形態が備える各要素並びにその配置、材料、条件、形状及びサイズ等は、例示したものに限定されるわけではなく適宜変更することができる。また、異なる実施形態で示した構成同士を部分的に置換し又は組み合わせることが可能である。

## 【符号の説明】

20

## 【0238】

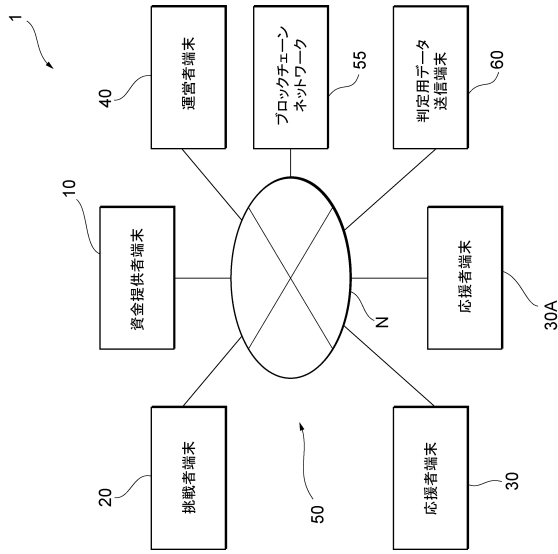
1, 1A, 1B...チャレンジ支援システム、10...資金提供者端末、20...挑戦者端末、30, 30A...応援者端末、40...運営者端末、55, 55A, 55B, 55C, 55D...ブロックチェーンネットワーク、60...判定用データ送信端末、70...協賛企業端末、80...チャレンジアプリ、501...チャレンジコントラクト、502, 502A, 502B, 502C...サンクストークンコントラクト、503...チアリングトークンコントラクト

30

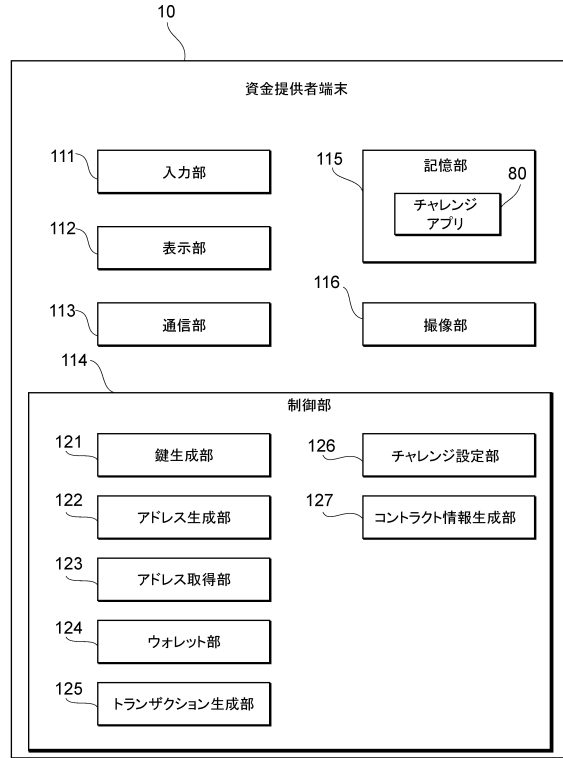
40

50

【図面】  
【図 1】



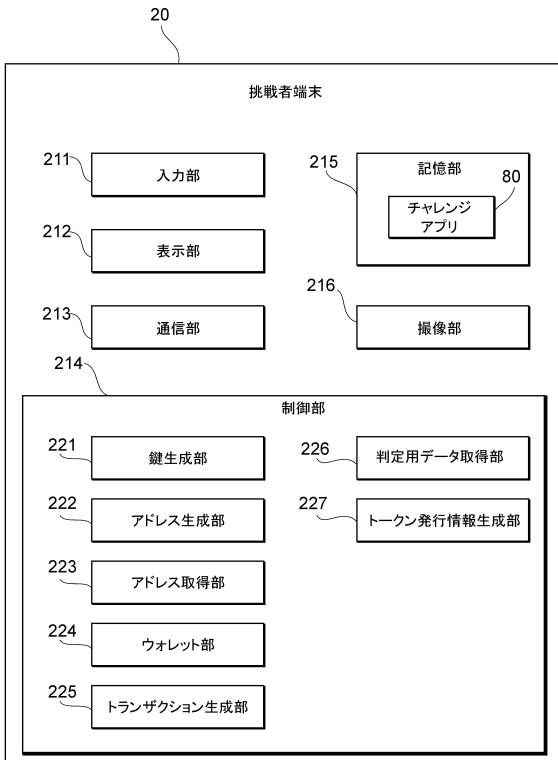
【図 2】



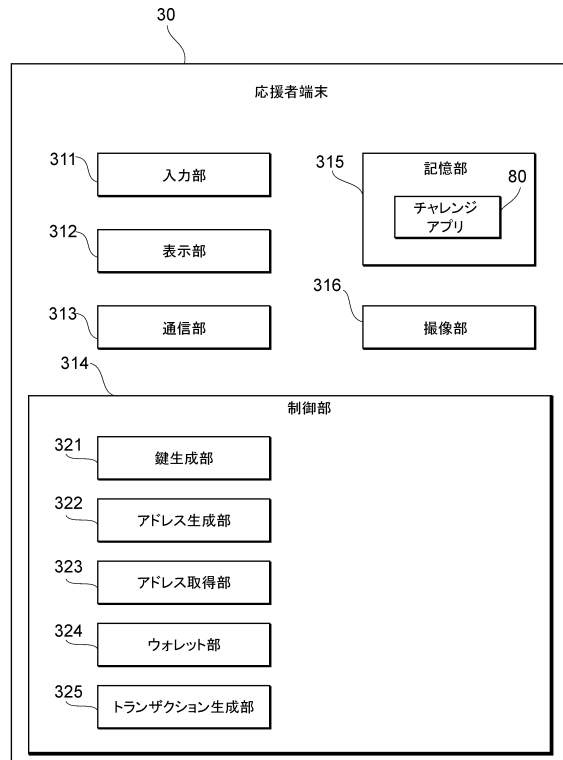
10

20

【図 3】



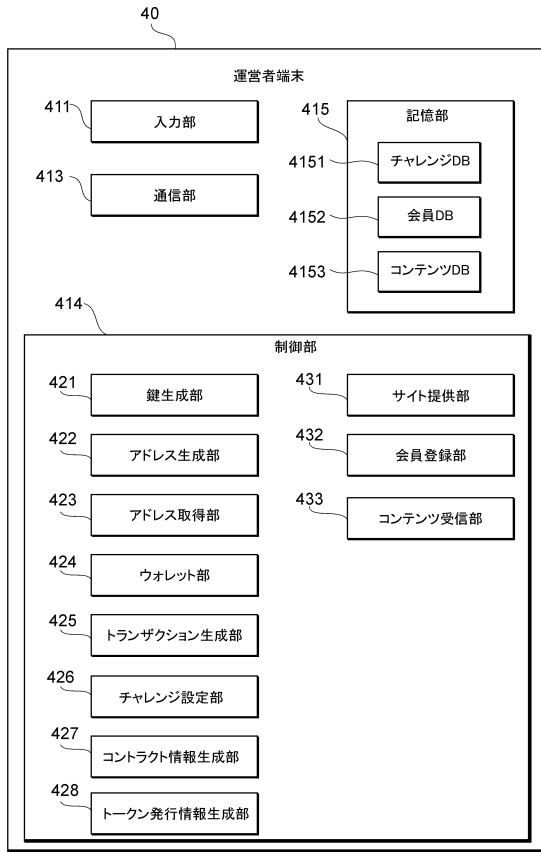
【図 4】



30

40

【図5】



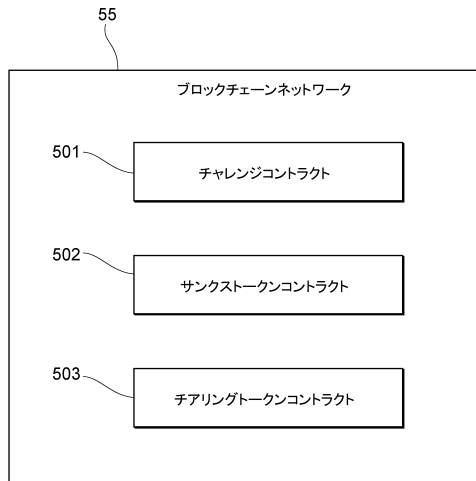
【図6】

アカウント名	氏名、性別 生年月日等	公開アドレス	サンクストーン コントラクトの コントラクトアドレス	関連チャレンジ 情報
ユーザA	...	0xb2f7795b723 ee66aec54	0x20204df9d 503df62d989	...
ユーザB	...	0x4a594f9d008 5819d2904		...
ユーザC	...	0x978730379 d0592ceb6e3		...
ユーザD	...	0x461e3f5a96b 9baa0e161	0x1fc291f95b 1071a91664	...
ユーザE	...	0x2f46e1688cf 78ba364a3		...
ユーザF	...	0x461e3f5a96b 9baa0e161		...
ユーザG	...	0x0b957cf975 c131196984		...

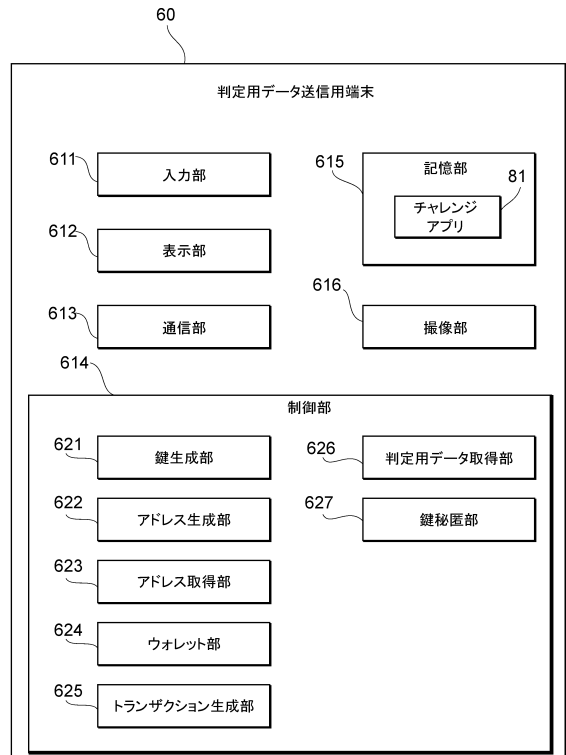
10

20

【図7】



【図8】



30

40

50



【図 1 3】

CA2		502
コントラクトアドレス		
0x20204df9d503df62d989		
公開アドレス	サンクストークン残高	
A2 0x4a594f9d0085819d2904 (ユーザA)	100TT	
トークン総発行数	100TT	

【図 1 4】

アカウント名	公開アドレス	サンクストークンコントラクトのコントラクトアドレス
運営者	0xe33b915ac221b530e8f0	
ユーザ A	0xb2f7795b723ee66aec54	0x20204df9d503df62d989
ユーザ B	0x4a594f9d0085819d2904	
ユーザ C	0x978730379d0592ceb6e3	
ユーザ D	0x461e3f5a96b9baa0e161	
ユーザ E	0x5919d8120d1a3ea05e18	
ユーザ F	0x461e3f5a96b9baa0e161	

10

【図 1 5】

チャレンジA	
チャレンジ作成日	2019年6月30日
資金提供者公開アドレス	0xb2f7795b723ee66aec54(ユーザA)
挑戦者公開アドレス	0xb2f7795b723ee66aec54(ユーザA)
運営者公開アドレス	0xe33b915ac221b530e8f0
判定用データ送信端末公開アドレス	0x3bf49d9dbb306c41b2ea03
供託金額	1 ETH
目標歩数	8,000 歩/日
チャレンジ開始可能	2019年7月1日
チャレンジ終了可能	2019年7月31日
設定チャレンジ日数	20日
設定達成日数	10日
チャレンジ開始日	
チャレンジ終了期限	
歩数データ	
チャレンジ達成度	
成功時配分	0xb2f7795b723ee66aec54(ユーザA) 供託金額の80%(0.8 ETH)
	0x20204df9d503df62d989 (ユーザAのチャレンジトークンコントラクト)供託金額の18%(0.18 ETH)
失敗時配分	0xe33b915ac221b530e8f0(運営者) 供託金額の2%(0.02 ETH)
	0xb2f7795b723ee66aec54(ユーザA) 供託金額の98%(0.98 ETH)
ギブアップ	0xe33b915ac221b530e8f0(運営者) 供託金額の2%(0.02 ETH)
	無し/パターン1/パターン2
ギブアップ情報送信者	資金提供者/挑戦者
ギブアップパターンA	0xb2f7795b723ee66aec54(ユーザA) 供託金額の98%(0.98 ETH)
	0xe33b915ac221b530e8f0(運営者) 供託金額の2%(0.02 ETH)
ギブアップパターンB	0xb2f7795b723ee66aec54(ユーザA) (供託金額の80%) × 達成率
	0x20204df9d503df62d989 (ユーザAのチャレンジトークンコントラクト) (供託金額の18%) × 達成率
	0xb2f7795b723ee66aec54(ユーザA) 供託金額の残額
自己解体モード A	0xe33b915ac221b530e8f0(運営者) 供託金額の2%(0.02 ETH)
	0xb2f7795b723ee66aec54(ユーザA) 供託金額の98%(0.98 ETH)
自己解体モードB	0xe33b915ac221b530e8f0(運営者) 供託金額の100%(1 ETH)

【図 1 6】

CA1		501
コントラクトアドレス		
0x20204df9d503df62d989		
コントラクト情報		
チャレンジ結果	成功/失敗 ギブアップ/パターンA/ギブアップ/パターンB 自己解体モードA/自己解体モードB	

20

30

40

50

【 図 1 7 】

チャレンジ名	チャレンジA	チャレンジB
チャレンジコントラクトアドレス	0x20204df9d503df62d989	0x1fc291f95b1071891664
挑戦者名	ユーザA	ユーザA
挑戦者公開アドレス	xb2f7795b723ee66aec54	xb2f7795b723ee66aec54
判応用データ送信用公開アドレス	0x3b40db309c41b2ea03	0x3b40db309c41b2ea03
配分金受取者	ユーザA	ユーザB
配分金受取者公開アドレス	0x4e594f9d008581942904	0x4e594f9d008581942904
運営者公開アドレス	0x33915ac221b5306e0	0x33915ac221b5306e0

【 図 1 8 】

ユーザA	
e-mail	A
携帯番号	+81-AA-AAAA-AAA
公開アドレス	0xb2f7795b723ee66aec54
関連チャレンジ 1	
立場	資金提供者
チャレンジ名	チャレンジA
チャレンジ作成日	2019年7月30日
コントラクトアドレス	0x20204df9d503df62d989
資金提供者名	ユーザA
資金提供者e-mail	A
資金提供者公開アドレス	0xb2f7795b723ee66aec54
資金提供者残高	5.5 ETH
挑戦者名	ユーザA
挑戦者e-mail	A
挑戦者公開アドレス	0xb2f7795b723ee66aec54
挑戦者残高	2.2 ETH
資金提供額	1 ETH
目標歩数	8,000 歩/日
チャレンジ開始可能	2019年7月1日
チャレンジ終了可能	2019年7月31日
設定チャレンジ日数	20日
設定達成日数	10日
チャレンジ開始日	2019年7月5日
チャレンジ終了期限	2019年7月24日
歩数データ	2019年7月5日 8,900 歩 2019年7月6日 5,500 歩 ..... 2019年7月14日 2,000 歩
チャレンジ達成度	50%
成功時配分s1	
成功時配分s2	
失敗時配分f1	
失敗時配分f2	
ギブアップ	無し/パターン 1/パターン 2
ギブアップ送信者	資金提供者/挑戦者
ギブアップパターン1	
ギブアップパターン2	
.....	
チャレンジ結果	成功/失敗/ギブアップパターンA/ギブアップパターンB/自己解体モードA/自己解体モードB
関連チャレンジ 2	
立場	挑戦者
チャレンジ名	チャレンジB
.....	.....
関連チャレンジ 3	
立場	応援者
チャレンジ名	チャレンジC
.....	.....

10

20

【 図 1 9 】

歩数データ [0]	データ開示可否 (初回のみ)	可
	歩行日	2019年7月5日
	歩数	8900歩
	Evidence ハッシュ値[0]	xxxxxx
歩数データ [1]	Evidence ハッシュ値[1]	Xxxxxx
	歩行日	2018年7月6日
	歩数	5500歩
	Evidence ハッシュ値[2]	xxxxxx
	Evidence ハッシュ値[3]	Xxxxxx

【 図 2 0 】

歩数データ [0]	データ開示可否	可
	歩行日	2019年7月5日
	歩数	8900歩
	投稿日時	block.timestamp (2019年7月6日 11:05:33)
歩数データ [1]	Evidence ハッシュ値[0]	Xxxxxx
	Evidence ハッシュ値[1]	Xxxxxx
	達成日数累積	1
	歩行日	2019年7月6日
	歩数	5500歩
	投稿日時	block.timestamp (2019年7月7日 13:41:32)
	Evidence ハッシュ値[2]	xxxxxx
	Evidence ハッシュ値[3]	xxxxxx
	達成日数累積	1

30

40

【図 2 1】

アカウント名	公開アドレス
運営者	0xe33b915ac221b530e8f0
ユーザ A	0xb2f7795b723ee66aec54
ユーザ B	0x4a594f9d0085819d2904
ユーザ C	0x978730379d0592ceb6e3
ユーザ D	0x5919d8120d1a3ea05e18
ユーザ E	0x2f46e1688cf78ba364a3
ユーザ F	0x461e3f5a96b9baa0e161

【図 2 2】

コントラクトアドレス		
0x20204df9d503df62d989		
公開アドレス	サンクストーン残高(1)	サンクストーン残高(2)
0xb2f7795b723ee66aec54 (ユーザA)	0TT	0TT
0x5919d8120d1a3ea05e18 (ユーザD)	20TT	20TT
0x2f46e1688cf78ba364a3 (ユーザE)	50TT	50TT
0x461e3f5a96b9baa0e161 (ユーザF)	30TT	20TT
00x0b957cf975c131196984 (ユーザG)	0TT	10TT
トークン総発行数	100TT	100TT

10

【図 2 3】

チャレンジコントラクトアドレス	0xxxxxxxxxxxxxxxxx
チャレンジ名	安全運転チャレンジ
チャレンジ期間	1か月
資金提供者	運送会社
挑戦者運送会社	運転手
条件	1日の運転で下記を全て満たす。 (最高速度)80km/時 (シートベルト)運転中は常に着用 (急ブレーキ)2回以下 (急発進)2回以下
成功時	運転手 1,000円/日相当のETH
	運転手妻 500円/日相当のETH
失敗時	運送会社 全額

【図 2 4】

チャレンジコントラクトアドレス	0xxxxxxxxxxxxxxxxx
チャレンジ名	血糖値スバイク予防チャレンジ
チャレンジ期間	1か月
資金提供者	生命保険会社
挑戦者	生命保険加入者
内容	(最高血糖値) 1日の空腹時血糖値+ 30 mg/dL以内
成功時	加入者 1,000円/日相当のETH
	加入者妻(弁当協力) 500円/日相当のETH
失敗時	保険会社 全額

20

30

40

50

【図 2 5】

チャレンジコントラクトアドレス	0xxxxxxxxxxxxxxxxx	
チャレンジ名	子供勉強チャレンジ	
チャレンジ期間	1年間	
資金提供者	親	
挑戦者	勉強しなければいけない子供	
内容	子供は、IoTデバイスを取り付けたえんぴつを使って勉強する。	
成功時	子供	20円/時相当のETH
	子供の兄弟 (邪魔せず 応援する婆美)	2円/時相当のETH
失敗時	親	全額

【図 2 6】

チャレンジコントラクトアドレス	0xxxxxxxxxxxxxxxxx	
チャレンジ名	禁煙チャレンジ	
チャレンジ期間	3カ月	
資金提供者	病院(元々は患者が支払ったもの)	
挑戦者	禁煙を希望する患者	
内容	患者は、日々保険適用のアプリやニコチンパッチ等 を利用しながら禁煙にチャレンジする。定期的 (例えば毎日)CO測定 IoTデバイスで呼気中のCOを 測定し、そのデータをIoTデバイスに内蔵したウォレット からスマートコントラクトに送信する。	
成功時	患者	1カ月成功する毎に15万円相当の ETH、3カ月間成功すると45万円相当 のETH
	病院 (または医師)	3カ月間成功したら10万円相当の ETH
失敗時	寄付先	ユニセフ等に寄付。 ただし、患者が成功した月は、患者 に15万円相当のETH

10

20

【図 2 7】

801

<

8011

チャレンジ名

チャレンジID

8012

8013

資金提供者

ABC

挑戦者

DEF

BT1

BT2

供託金額

0.5 ETH JPY

8014

BT3

次へ

【図 2 8】

802

<

アカウント名

公開アドレス

ABC

0x7c0418189623d9ed8471

BT4

ユーザ追加

30

40

50

【図 29】

803

<

8031 期限

参照時刻	Tokyo(JST/UTC+900)
開始日	📅
終了日	📅

8032 条件

種類	実行日数	歩数	達成すべき日数
ウォーキング	30	10000	15

BT5

次へ

【図 30】

804

<

8041 成功時配分 Edit

受取人	%	金額
ABC	97%	0.485 ETH
+ユーザ追加		
手数料	2%	0.01 ETH

8042 失敗時配分 Edit

受取人	%	金額
DEF	97%	0.485 ETH
+ユーザ追加		
手数料	2%	0.01 ETH

8043 挑戦者宛 GAS手数料

	%	金額
手数料	1%	0.005 ETH

BT6

次へ

10

20

【図 31】

805

<

8051 ギブアップ選択

<input type="radio"/> ギブアップ不可	<input checked="" type="radio"/> ギブアップ可
-------------------------------	---

ギブアップパターン選択

<input checked="" type="radio"/> 供託金額を資金提供者に全て返還
<input type="radio"/> チャレンジ達成度に応じて資金を配分

BT6

次へ

【図 32】

806

<

チャレンジの確認

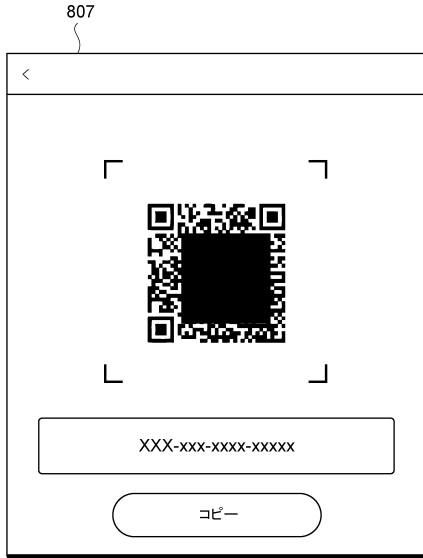
チャレンジ名	
チャレンジID	
資金提供者	挑戦者
ABC	DEF
供託金額	
0.5 ETH    1 JPY	
期限	
参照時刻	Tokyo(JST/UTC+0900)
開始日	26/07/2019
終了日	26/07/2019
条件	
種類	ウォーキング
実行日数	30
歩数	10000
達成すべき日数	15
成功時配分	
受取人	%    金額
ABC	97    0.485 ETH
手数料	2    0.01 ETH
成功時配分	
受取人	%    金額
DEF	97    0.485 ETH
手数料	2    0.01 ETH
GAS手数料	
	%    金額
手数料	1    0.005 ETH
ギブアップ可否	
ギブアップ可	
BT7	
送信	
BT8	
スマートコントラクト確認	
チャレンジ出力	

30

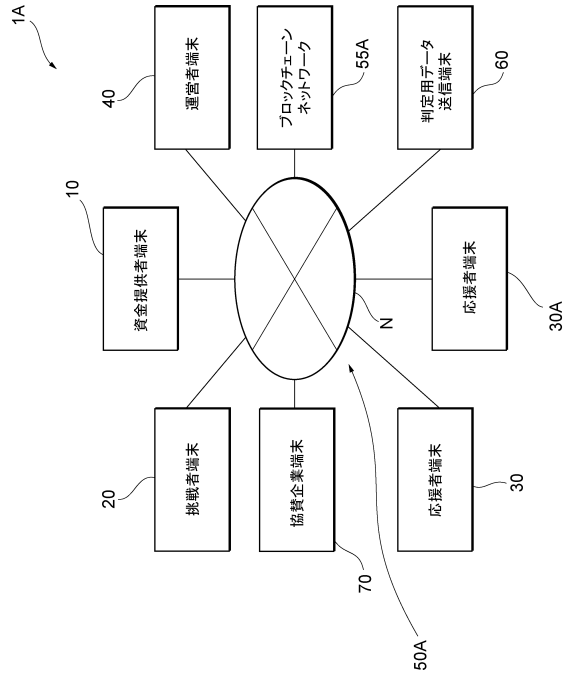
40

50

【図 3 3】



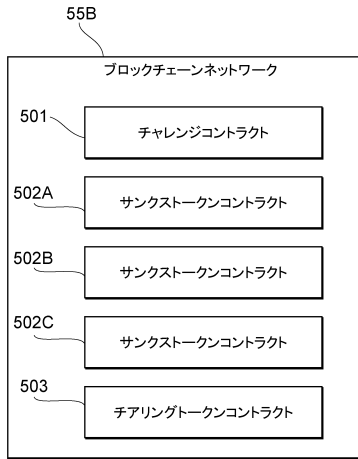
【図 3 4】



10

20

【図 3 5】



【図 3 6】

502B

サンクストーンコントラクト	
応援者	TTB残高
ユーザA	0 T T B
ユーザB	0 T T B
ユーザC	0 T T B
ユーザD	0 T T B
合計	0 T T B

30

40

50

【図 3 7】

502A

サンクストーンコントラクト		
応援者	TTA残高	TTBへの加算(難易度係数)
ユーザA	200 TTA	200/400 × 0.8 TTB
ユーザB	100 TTA	100/400 × 0.8 TTB
ユーザC	50 TTA	50/400 × 0.8 TTB
ユーザD	50 TTA	50/400 × 0.8 TTB
発行済みTTA合計	400 TTA	

【図 3 8】

502C

サンクストーンコントラクト		
応援者	TTC残高	TTBへの加算(難易度係数)
ユーザ A	300TTC	300/800 × 0.2 TTB
ユーザ B	200TTC	200/800 × 0.2 TTB
ユーザ C	200TTC	200/800 × 0.2 TTB
ユーザ D	100TTC	100/800 × 0.2 TTB
発行済みTTC合計	800TTC	

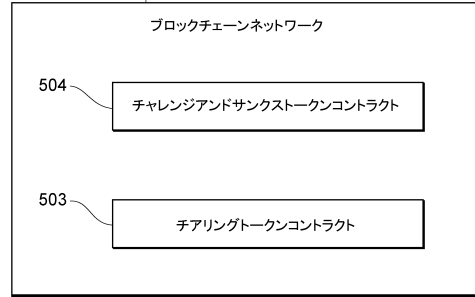
【図 3 9】

502B

TTBコントラクト	
応援者	TTB残高
ユーザA	0.475TTB
ユーザB	0.25TTB
ユーザC	0.15TTB
ユーザD	0.125TTB
合計	1TTB

【図 4 0】

55C



10

20

【図 4 1】

5041

	成功時 トークン	失敗時 トークン	ギブアップ時 トークン
運営者	5	5	5
資金提供者	0	85	95
挑戦者	60	0	0
配分金受取者1	15	0	0
配分金受取者2	10	0	0
寄付先1	5	5	0
寄付先2	5	5	0
TOTAL	100	100	100

【図 4 2】

5041

	成功時 トークン	失敗時 トークン	ギブアップ時 トークン
運営者	5	5	5
資金提供者	0	85	95
挑戦者	50	0	0
挑戦者下請け	10	0	0
配分金受取者1	10	0	0
配分金受取者1下請け	5	0	0
配分金受取者2	10	0	0
寄付先1	5	5	0
寄付先2	5	5	0
TOTAL	100	100	100

30

40

50

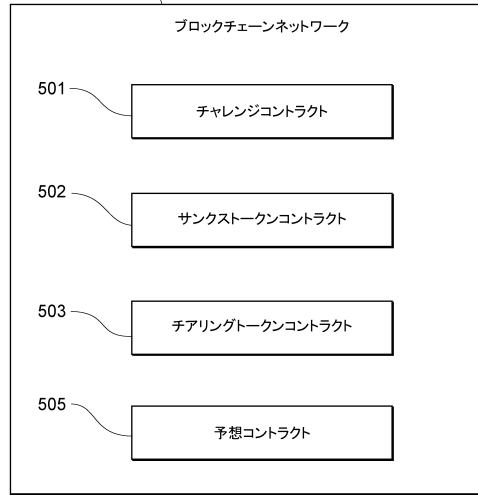
【図43】

5041A

	初期 トークン	成功時 トークン	失敗時 トークン	ギブアップ時 トークン
運営者	1	5	5	5
資金提供者	1	0	85	95
挑戦者	1	60	0	0
配分金受取者1	1	15	0	0
配分金受取者2	1	10	0	0
寄付先1	1	5	5	0
寄付先2	1	5	5	0
未配布	93	0	0	0
TOTAL	100	100	100	100

【図44】

55D



10

20

30

40

50

## フロントページの続き

審査官 関 博文

- (56)参考文献 特開2011-034544(JP,A)  
特開2019-133630(JP,A)  
特開2019-091402(JP,A)  
特許第5806428(JP,B1)
- (58)調査した分野 (Int.Cl., DB名)  
G06Q 10/00-99/00