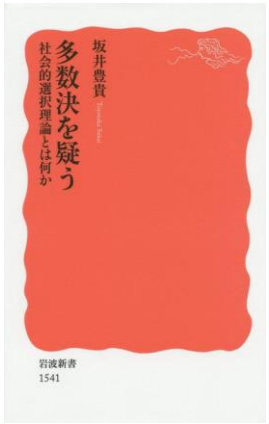
制度設計の観点から見た、ビットコインの面白さ

坂井豊貴
慶應義塾大学経済学部
tsakai@keio.jp

自己紹介



- 慶應義塾大学経済学部 教授、 Ph.D. in Economics (Rochester 05)
- 専攻　ゲーム理論や実験を用いた制度設計（メカニズムデザイン）
- 株式会社 デューデリ＆ディール　チーフエコノミスト、不動産オークションに従事
- オークション設計の学知を、土地の売却に活用（オークションの仕組みしだいで変わる値段。コインを売るのにも使える）

分散管理

- しばしば「管理者が存在しない」と説明されるビットコインだが
- 管理者は存在するし、必要
- 特定少数の主体による管理（中央管理）ではなく、不特定多数の主体による管理（分散管理）
- キーワードは “decentralization”（分権、分散、脱中央）。経済学では馴染みのある言葉。ミクロ経済学系の”Decentralization Conference”は日本でも毎年開催

分散管理

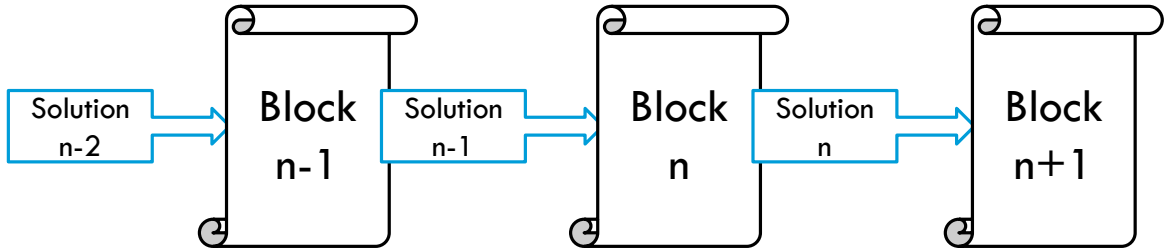
- 不特定多数の主体（マイナー、ノード、コア開発者など）は、ひとつの同じ目的を共有しているとは限らない
- 一つひとつの主体は、生態系の構成要素のようなもの
- 各自は、各自の目的のために行動（局所最適化）する。その結果、ビットコインの生態系が安定的に稼働する（大域最適化）
- 制度設計の研究者としては、ビットコインのプロトコルは制度に見える。その制度のもとで各自が行動する結果、社会がうまく行くといったように
- その制度と行動について、いくつか考えていきたい。とくにマイナー。あの仕組みはなぜ上手くいくのか？　これからの懸念材料は？

これからする話

ビットコインのブロックチェーンの概要

1. Proof of Workとコンドルセ陪審定理
2. いろんな攻撃（51%攻撃と、51%以下での攻撃）
3. ブロック報酬の減少が変えるゲーム
4. ルソー流の社会契約論との親和性

ブロックチェーン

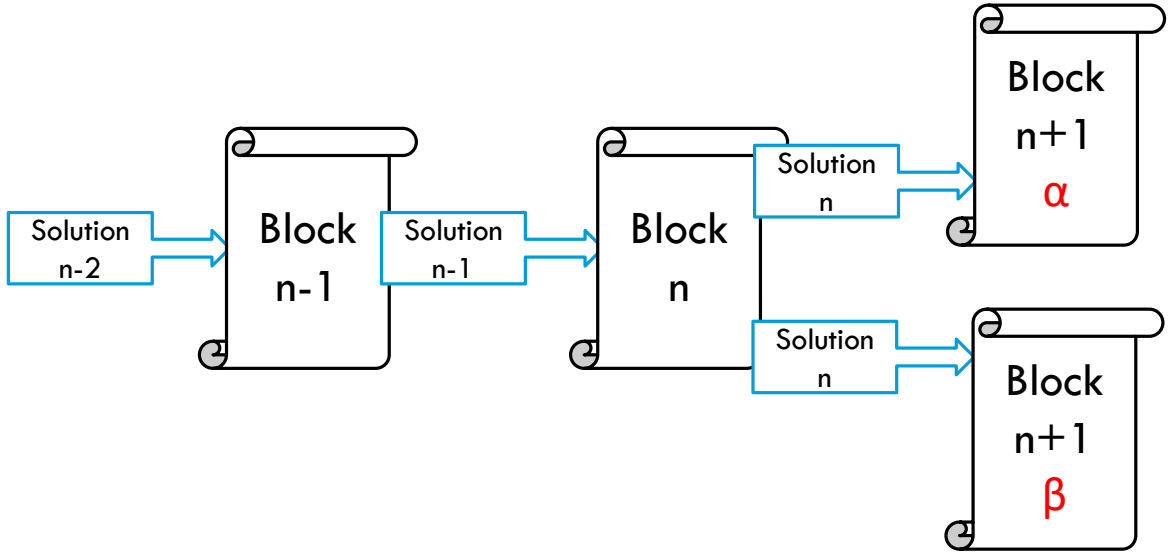


Block
n

送金者	受金者	金額(BTC)
None	Miner X	12.5
User A	User B	1.0
User C	User D	2.5
User E	User F	0.42
・・・	・・・	・・・
User P	User Q	5.32
・・・	・・・	・・・

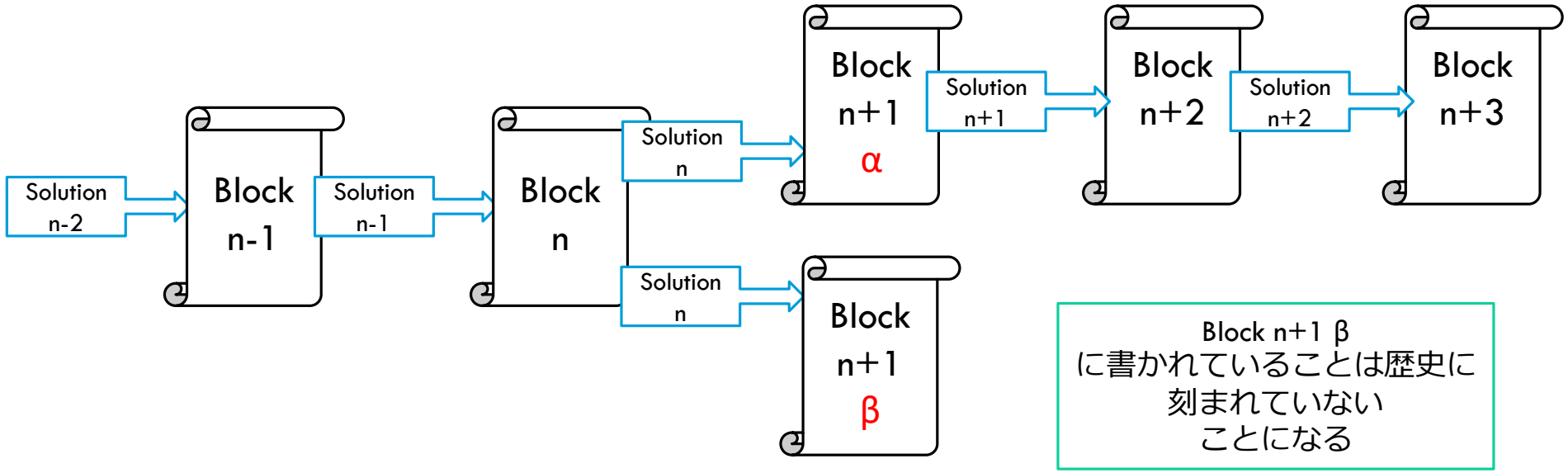
- すべての金銭移転を記録した一続きの台帳
- 既存の先頭ページに、新たな１ページを接続
- 「先頭ページと新たな１ページ」が計算パズルを出題
- 計算パズルを解くと、その答えが鍵となり、新たなページをガチッと接続できる
- これをするのがマイナー、その作業がマイニング（採掘）
- 解くのに電力と時間がかかる（接続コスト）

ブロックチェーンの枝分かれ（フォーク）



- ２つの新ブロックが接続されることもある。２つの異なる台帳は、両方は認められない
- どちらを正統とするか？
- 長く伸びるほうを正統とするのがプロトコルの鉄則。Proof of Work（労力による証明）

ブロックチェーンの枝分かれ（フォーク）



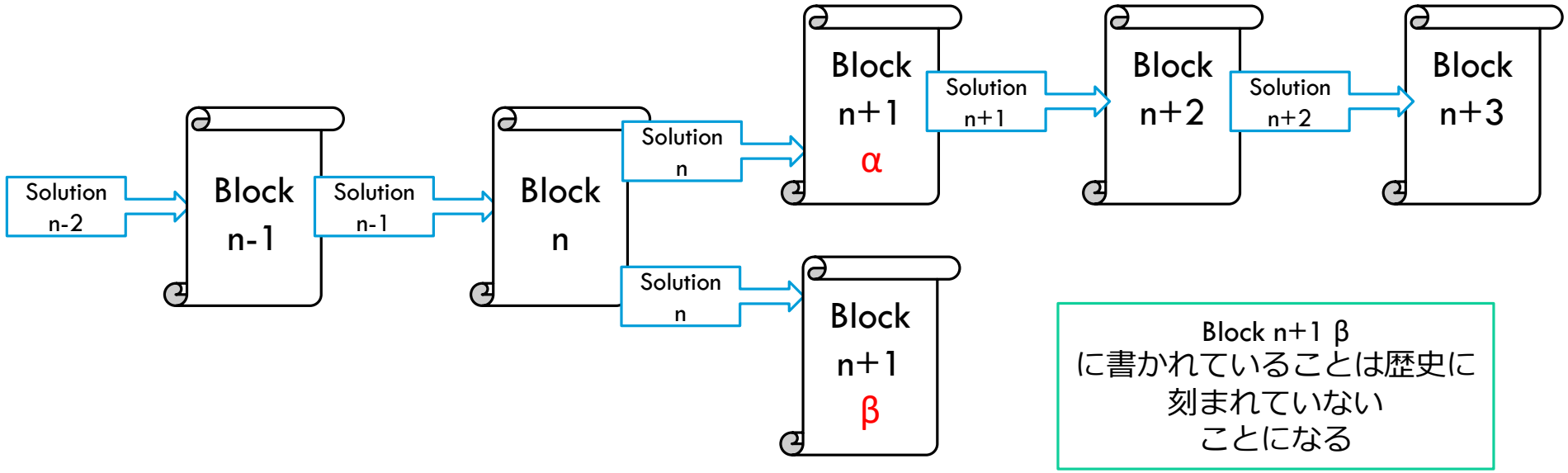
正統な台帳として扱われる「正しい歴史」

Block n+1 β
に書かれていることは歴史に刻まれていない
ことになる

- ２つの新ブロックが接続されることもある。２つの異なる台帳は、両方は認められない
- どちらを正統とするか？
- 長く伸びるほうを正統とするのがプロトコルの鉄則。Proof of Work（労力による証明）

“1 CPU, 1 VOTE”のもとでの

一種の多数決で「正しい歴史」を決定



正統な帳簿として扱われる「正しい歴史」

Block n+1 β に書かれていることは歴史に刻まれていないことになる

- ２つの新ブロックが接続されることもある。２つの異なる台帳は、両方は認められない
- どちらを正統とするか？
- 長く伸びるほうを正統とするのがプロトコルの鉄則。Proof of Work（労力による証明）

１．PROOF OF WORKとコンドルセ陪審定理

- コンドルセ侯　旧体制からフランス革命の時代にかけて活躍した、数学出身の学者・政治家
- 自由主義者。奴隷解放や、女性参政権を主張した先駆者
- 革命前の1785年に『多数決論』を公刊
- 「社会数学」を構想。現在でいう数理社会科学の先駆者
- おそらく最初の目立った応用は、20世紀のノイマン

Condorcet, Image from Public Domain

ノイマンによる、コンドルセ陪審定理の応用

Image from Wikimedia Commons

- 20世紀を代表する天才科学者フォン・ノイマン（1903-1957）
- 現代のコンピュータの父の一人
- 信頼性の低い電気回路から、いかに信頼性の高いマシンを作るか
- 一つひとつの電気回路は、ときにエラーを起こし、誤った信号を送る
- 本来なら「A」と信号を送るべきところを、「not A」と送る
- そこでノイマンは「電気回路の多数決」を考えた

- 電気回路１ → A
- 電気回路２ → A
- 電気回路３ → not A
  - マシンは多数意見のAを採用。ただし前提として、「ボス」がいたらダメ（１の命令を２が必ずきくとか）
  - ふたつの電気回路が同時にエラーを起こす確率はとても低い（＝多数決の結果が正しい確率はとても高い）

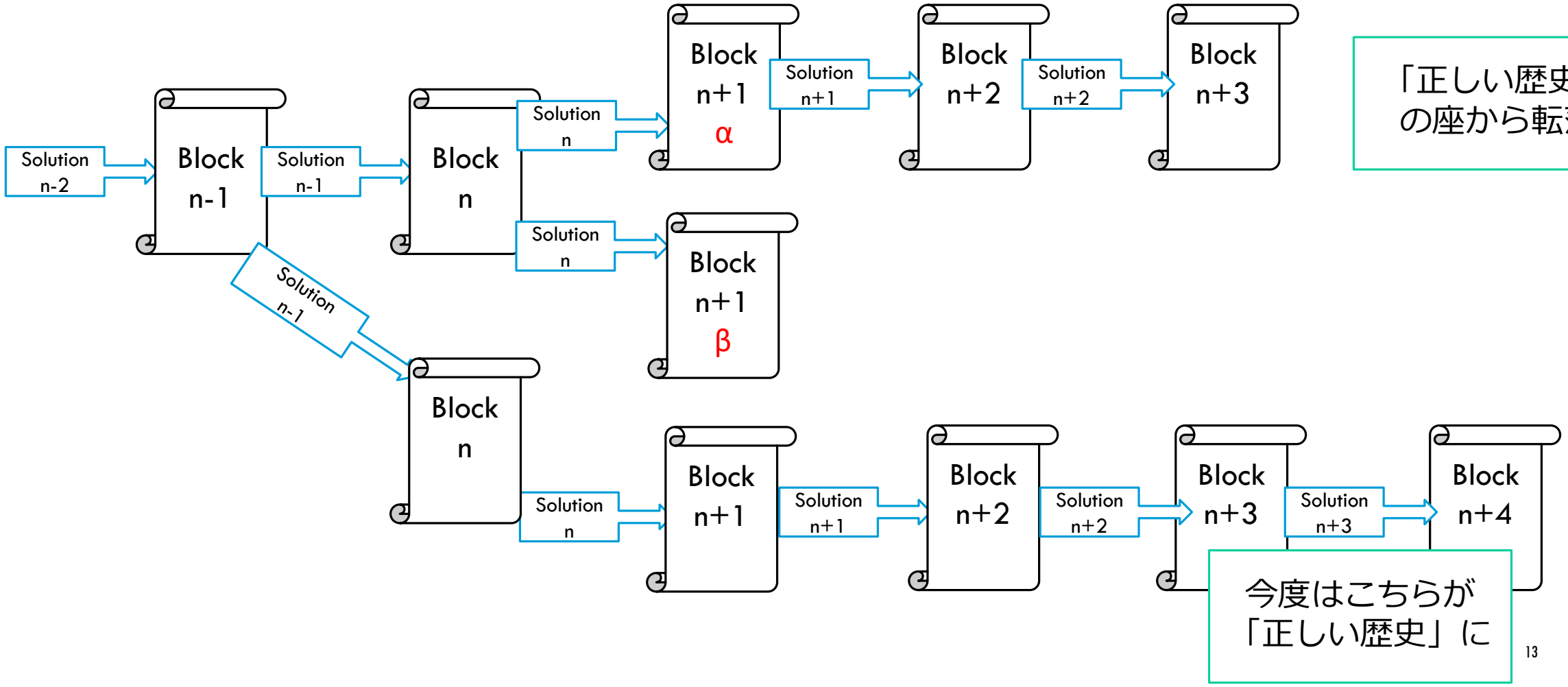
コンドルセ陪審定理
（CONDORCET JULY THEOREM, CJT）

- PoWの多数決では、CJT（のようなもの）が成り立っているか
- ハッシュパワーが、マイナー間でそれなりに分散していることが必要。

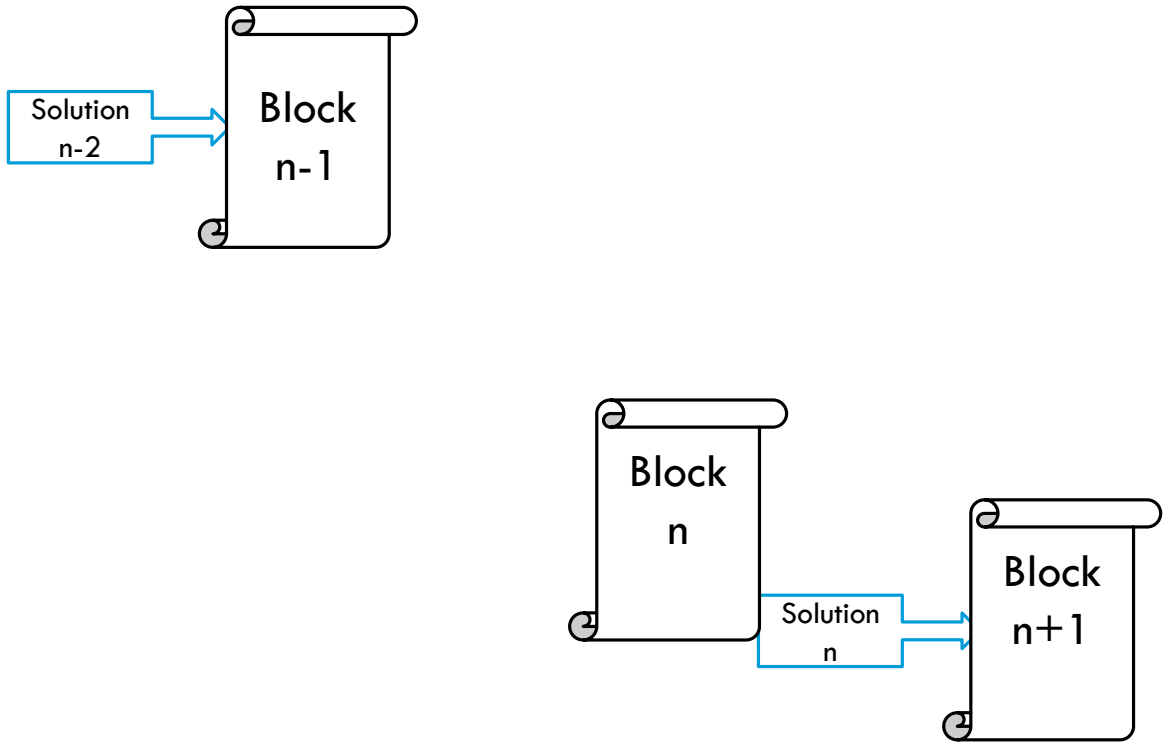
このとき「1 cpu, 1 vote」が「1 person, 1 vote 」と似通ってくるので、CJTが成り立つ

- すなわち分散化は、ビットコインの思想としてだけでなく、機能として重要。多数決のメリットを引き出すために

２．いろんな攻撃：　まず有名なのは「５１%攻撃」



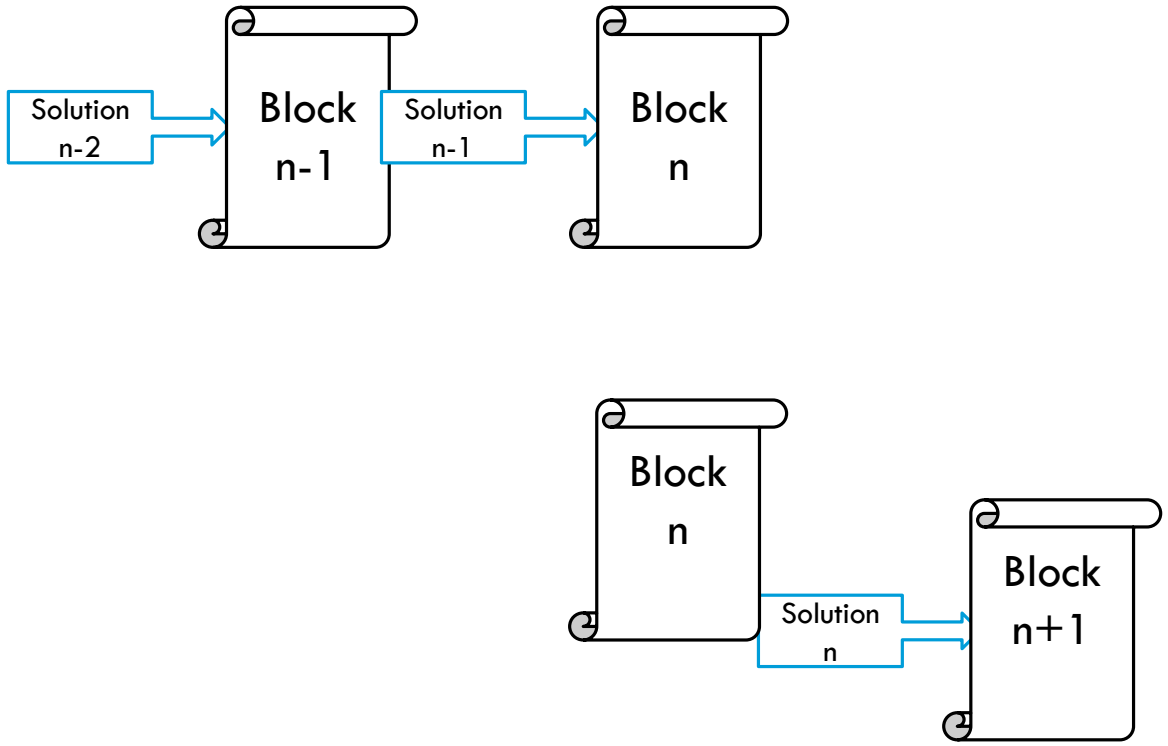
AYEL AND SIRERの「ブロック秘匿攻撃（BLOCK WITHHOLDING ATTACK）」



マイニングに成功したブロックを隠しもって、その後にブロックを接続し続ける。他のマイナーは、他のブロックを接続し続ける。期待利得を計算すると、意外とこれが有利になる。他人の労力をムダ使いさせる

Eyal and Sirer “Majority is not enough”
Communications of the ACM, 2018

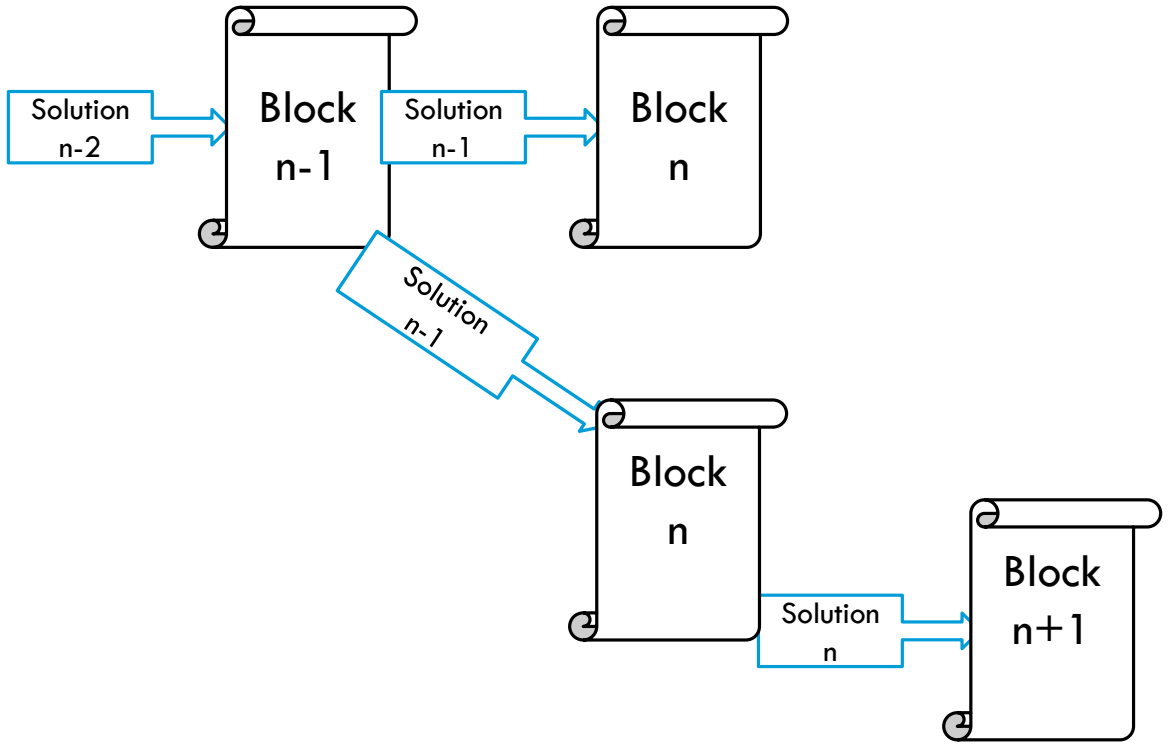
AYEL AND SIRERの「ブロック秘匿攻撃（BLOCK WITHHOLDING ATTACK）」



マイニングに成功したブロックを隠しもって、その後にブロックを接続し続ける。他のマイナーは、他のブロックを接続し続ける。期待利得を計算すると、意外とこれが有利になる。他人の労力をムダ使いさせる

Eyal and Sirer “Majority is not enough”
Communications of the ACM, 2018

AYEL AND SIRERの「ブロック秘匿攻撃（BLOCK WITHHOLDING ATTACK）」

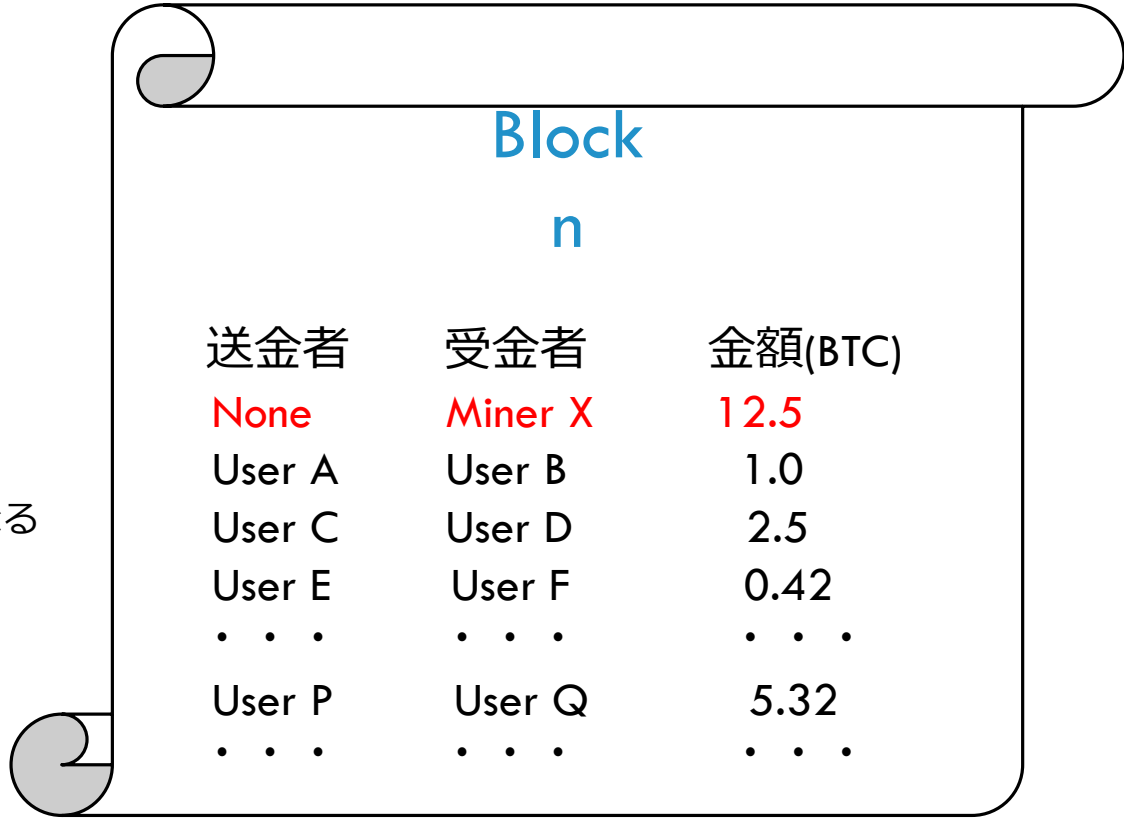


マイニングに成功したブロックを隠しもって、その後にブロックを接続し続ける。他のマイナーは、他のブロックを接続し続ける。期待利得を計算すると、意外とこれが有利になる。他人の労力をムダ使いさせる

Eyal and Sirer “Majority is not enough”
Communications of the ACM, 2018

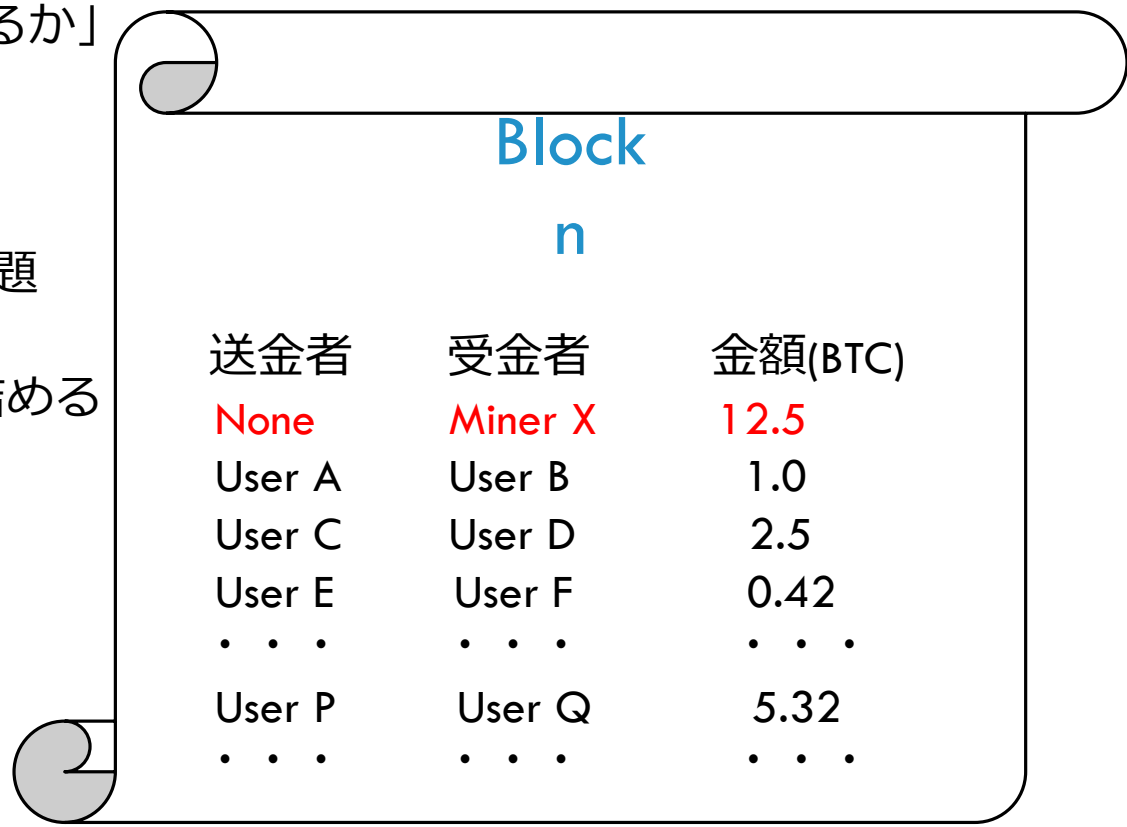
3．ブロック報酬の減少が変えるゲーム

- 現在のマイナーの報酬
  - ブロック報酬＝12.5 BTC（出所はナシ）
  - 少額の手数料＝計 0.7～1.5 BTC 程度（出所はユーザーたち）
- マイナーは１ブロックに２千数百件の記録を詰める
- ブロック報酬は今後、半減していく
  - よく言われること：手数料が上がらないと、マイナーが儲からなくなる
  - 問題はそれだけではない。マイナーが直面する「ゲーム」が変わる

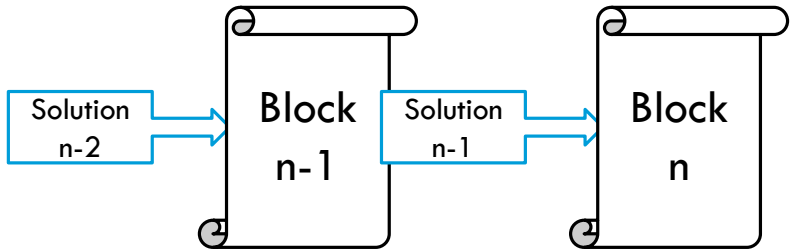


ブロック報酬の減少が変えるゲーム

- マイナーは１つのブロックに「どの記録をいくつ詰めるか」
- おそらく、いまその意思決定は問題とされていない
- ブロック報酬 12.5 BTC が大きいので、わりと小さい問題
- なので、たぶんそんなに考えず、2千数百件の記録を詰める
- では、12.5 BTC が無くなったら？



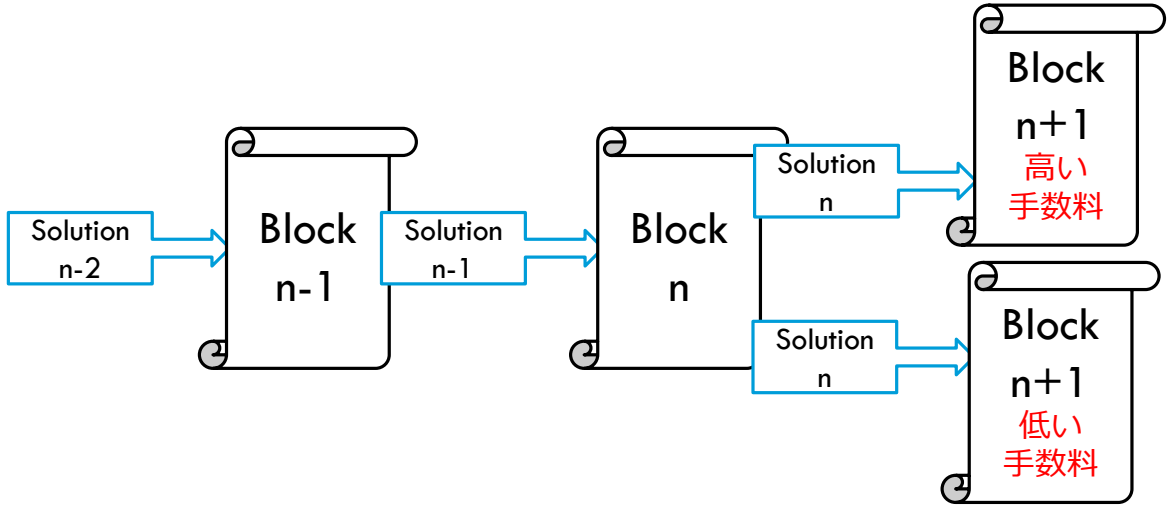
どの記録を自分のブロックに詰めるか？



プールに手数料がとても高い記録があるとしよう。この記録を自分は、これから接続したい Block n+1 に入れるべきか？

- 普通に考えると「入れる」べき。だって手数料が高いのだから
- でも、あえて残したほうがよいかもしれない。そのほうが、フォークしたときに後ろにブロックが続きやすいだろうから

どの記録を自分のブロックに詰めるか？



低い手数料の記録たちがプールに少数残っている

マイナーはどちらを延伸したがるか？

高い手数料の記録たちがプールに多数残っている

- 「どの記録をいくつブロックに詰めるか」という新たな変数
- このとき実際にマイナーがどう行動するかは分からない
- たぶん、けっこう複雑なゲームになる。一般論として、複雑な制度ほど、悪さはしやすい
- Budish “The economic limits of bitcoin and the blockchain” NBER working paper, 2018

４．ルソー流の社会契約との親和性

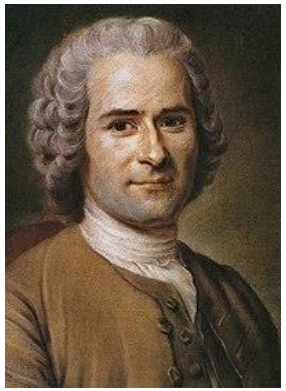


Image from Public Domain

- ルソー『社会契約論』（1762）
- 人間が自由でいられる社会の範型を構築（ここでの主な自由概念は moral freedom=自ら定めた法に従う自由）

よくある批判：　実際には社会契約はなされていない。ただしルソーは事実ではなく、原理を説明したかったので、べつにそれでよい

- ルソーの社会契約論では、社会は契約で作られ、その後、続けるかどうか再契約の機会がある（誰でもそのとき自由に離脱できる）。これも現実的でないと評されがち（ただし自由な社会の範型なのでべつによい）。しかし！

けっこう暗号通貨のコミュニティは、ルソーの社会契約論っぽい

- The DAO 事件。詳細はさておき、コードのエラーを衝いた攻撃が起き、イーサが「盗まれた」
- コードが悪いのか、エラーを衝くのが悪いのか。前者が少数派の「code is law」派で、後者が多数派。コミュニティは信念の違いにより分裂
- ツォルト・フォルフォルディ（イーサリアムのコア開発者のひとりだった）
  - 「イーサリアムのプログラムより高いレベルの「正義」などあるべきでないことに、僕は皆が賛成してくれていると考えていたんだ。その「盗まれた」とされるイーサは、「泥棒」と呼ばれている人の正当な所有物だ。僕たちがクリエイトしているのは、どんなに公衆が憤慨しようとその人の所有権が守られる仕組みだ。そのことに誇りをもつべきなんだ」Zsolt Felföldi “A Tale for Two Coins” Decentralize Today, https://decentralize.today/a-tale-of-two-chains-3f6d58a9df4a
- こういう分裂は、否定的に評されやすいが、むしろルソー流の自由の観点からは良い点
- ルソー流の社会契約のようなことが、通貨については、ついに人間社会で可能になった

おわりに

- よく「マイナーの金銭インセンティブ設計が特徴」のように言われるが
- 金銭インセンティブだけで生態系は動いていない
- おそらく金銭インセンティブだけでは、コミュニティのようなものは作れない
- ひとつの暗号通貨のコミュニティは、ひとつの実験社会。文化人類学的な考察の対象
- そのうえで、金銭インセンティブの設計は重要で、メカニズムデザインの知見が活用できる
  - とくに12.5 BTC のブロック報酬は、永遠に出続けるようにしては。そうすると、非常に弱いインフレが起こり続ける。そのコストは、ビットコインユーザー全員の負担となる（まっとうな負担の仕方であろう）。また、完全に予期できるインフレなので、法定通貨の突然のインフレのような混乱は起こらない
- このような話やコイン売却オークションの話などを、非営利の月例ワークショップ「Auction Lab」でやっています。関心ある方は、坂井のツイッター（@toyotaka_sakai）まで

おわりに

- よく「マイナーの金銭インセンティブ設計が特徴」のように言われるが
- 金銭インセンティブだけで生態系は動いていない
- おそらく金銭インセンティブだけでは、コミュニティのようなものは作れない
- ひとつの暗号通貨のコミュニティは、ひとつの実験社会。文化人類学的な考察の対象
- そのうえで、金銭インセンティブの設計は重要で、メカニズムデザインの知見が活用できる
  - とくに12.5 BTC のブロック報酬は、永遠に出続けるようにしては。そうすると、非常に弱いインフレが起こり続ける。そのコストは、ビットコインユーザー全員の負担となる（まっとうな負担の仕方であろう）。また、完全に予期できるインフレなので、法定通貨の突然のインフレのような混乱は起こらない
- このような話やコイン売却オークションの話などを、非営利の月例ワークショップ「Auction Lab」でやっています。関心ある方は、坂井のツイッター（@toyotaka_sakai）まで

Thanks !