Децентрал зоване сусп льство: пошук душ Web3[1]

Е. Глен Вейл, [2] Пуджа Олхавер,[3] В тал к Бутер н[4]

травень 2022 року

«Дао — це вогнище д м

з десяти тисяч речей.

Добр душ ц нують його,

заблукан знаходять у ньому притулок».

— Лаоцзи, № 62

Анотац я

Сьогодн Web3 зосереджується на вираженн переданих ф нансових актив в, а не на кодуванн соц альних в дносин дов ри. Проте багато основних вид в економ чної д яльност — наприклад, беззаставне кредитування та створення особистих бренд в — будуються на пост йних в дносинах, як не п длягають передач . У ц й статт ми про люструємо, як непередаван «прив'язан до душ » токени (SBT), що представляють зобов'язання, повноваження та зв'язки «Souls», можуть кодувати мереж дов ри реальної економ ки для встановлення походження та репутац ї. Що ще важлив ше, SBT дають змогу використовувати нш амб ц йн застосування, так як в дновлення гаманця сп льноти, ст йке до сиб л в управл ння, механ зми децентрал зац ї та нов ринки з розкладними сп льними правами. Ми називаємо цю багатшу, плюрал стичну екосистему «Децентрал зоване сусп льство» (DeSoc) — сп льнодетерм новану соц альн сть, де душ та сп льноти об'єднуються знизу вгору, як виникл властивост один одного для сп льного створення множинних мережевих товар в та нтелекту на певн й в дстан . ваги. Ключем до ц єї соц альност є права власност , що розкладаються, вдосконален механ зми управл ння, так як квадратичне ф нансування з дисконтуванням за результатами кореляц ї, як винагороджують дов ру та сп впрацю, одночасно захищаючи мереж в д захоплення, вилучення та дом нування. Завдяки так й розширен й соц альност , web3 може уникати сьогодн шньої г пер-нанс ал зац ї на користь б льш трансформуючого, плюрал стичного майбутнього, що п двищить прибуток через соц альну дистанц ю.

---

[1] Ми вдячн Одр Тан, Ф лу Даяну, Дан ель Аллен, Леону Ер хсену, Меттью Прев тту, Д в'ї С ддарт, Джарону Ланьє та Роберту М ллеру за їхн вдумлив в дгуки та коментар . Ус помилки та погляди наш власн .

[2] Корпорац я Microsoft RadicalXChange Foundation, glen@radicalxchange.org. Glen vinicula este documento a su Alma.

[3] Flashbots Ltd., puja@ashbots.net. Пуджа присвячує цей пап р своїй бабус Сать , чия любов св тло завжди будуть сяяти багатьом душам.

[4] Ethereum Foundation, vitalik.buterin@ethereum.org.

§1. ВСТУП

Web3 приголомшив св т, створивши паралельну систему ф нансування безпрецедентної гнучкост та творчост менш н ж за десятил ття. Криптограф чн та економ чн прим тиви, так як криптограф я з в дкритим ключем, смарт-контракти, п дтвердження роботи та п дтвердження участ , привели до складної та в дкритої екосистеми для вираження ф нансових транзакц й.

Але економ чну ц нн сть, якою торгує ф нансування, створюють люди та їхн стосунки. Оск льки web3 не вистачає прим тив в для репрезентац ї такої соц альної дентичност , в н став фундаментально залежним в д дуже централ зованих структур web2, як в н прагне перевершити, в дтворюючи їх обмеження.

Приклади цих залежностей включають:

1. Б льш сть виконавц в NFT покладаються на централ зован платформи, так як OpenSea Twitter, щоб взяти на себе зобов'язання деф цит початкове походження.

2. DAO, як намагаються вийти за рамки простого голосування за монети, часто покладаються на нфраструктуру web2, таку як соц альн мед а, для опору сиб лам.

3. Багато учасник в web3 покладаються на кастод альн гаманц , якими керують централ зован орган зац ї, наприклад Coinbase або Binance. Децентрал зован системи керування ключами не є зручними для користувач в, а є найскладн шими.

Кр м того, в дсутн сть нативної дентичност web3 робить сьогодн шню екосистему DeFi нездатною п дтримувати д яльн сть, повсюдно поширену в реальн й економ ц , таку як кредитування з недостатньою заставою або прост контракти, як-от оренда квартири. У ц й статт ми про люструємо, як нав ть невелик та поетапн кроки до репрезентац ї соц альної дентичност за допомогою токен в, пов'язаних з душею, можуть подолати ц обмеження та наблизити екосистему до регенерац ї ринк в з їхн ми людськими стосунками у р дному контекст web3.

Ще б льш багатооб цяючим, ми п дкреслюємо, як р дна соц альна дентичн сть web3 з багатим соц альним компонуванням, може дати великий прогрес у вир шенн ширших давн х проблем у мереж 3, пов'язаних з концентрац єю багатства та вразлив стю управл ння до ф нансових атак, одночасно стимулюючи кембр йський вибух нновац йних пол тичних, економ чних та соц альних застосувань. Ми називаємо ц вар анти використання та багатшу плюрал стичну екосистему, яку вони забезпечують, «децентрал зоване сусп льство» (DeSoc).

§2 КОНТР

Ми починаємо з пояснення прим тив в DeSoc, зосереджених на обл кових записах (або гаманцях), що м стять непередаван (спочатку загальнодоступн) «прив'язан до душ » токени (SBT), що представляють зобов'язання, обл ков дан та права власност . Так токени будуть схож на розширене резюме, випущене ншими гаманцями, як п дтверджують ц соц альн в дносини.

Пот м ми описуємо «сходи» все б льш амб тних додатк в через соц альний стек, як так прим тиви можуть розширити, зокрема:

- встановлення походження
- розблокування ринк в кредитування з недостатньою заставою через репутац ю
- забезпечення децентрал зованого керування ключами
- перешкоджання та компенсац я скоординованої стратег чної повед нки
- вим рювання децентрал зац ї
- створення нових ринк в з сп льними правами та дозволами

Цей опис завершується баченням DeSoc — сп льно визначеної соц альност , де душ та сп льноти об'єднуються знизу вгору, як виникл властивост один одного для сп льного створення множинних мережевих товар в, включаючи множинний нтелект, у р зних соц альних масштабах.

Нарешт , ми в дпов даємо на к лька потенц йних проблем заперечень проводимо пор вняння з ншими парадигмами дентичност , знайомими в простор web3, часто визнаючи, що наше бачення є лише першим кроком, але тим не менш прогресом у програмован й конф денц йност та комун кац ї. Пот м ми розглядаємо техн чн шляхи для запуску бачення, яке ми уявляємо. Розробляючи це, ми з б льшою ф лософ єю спод ваємося на потенц ал DeSoc перенаправити web3 на б льш глибокий, законний трансформац йний шлях.

§3 ДУШІ

Наш ключовий прим тив — це обл ков записи або гаманц , як м стять загальнодоступн токени, як не п длягають передач (але, можливо, в дкликаються ем [5] Ми називаємо рахунки «Душами», а токени (SBT), якими волод є припускаємо публ чн сть, незважаючи на нашу глибоку зац кавлен сть у конф денц йност , тому що техн чно прост ше перев рити як п дтвердження концепц ї, нав ть якщо обмежена п дмножиною маркер в, якими люди готов под литися публ чно. Дал в статт ми вводимо концепц ю «програмованої конф денц йност » для б льших вар ант в використання.

Уяв ть соб св т, де б льш сть учасник в мають Душ , як збер гають SBT, в дпов дн сер ї ал менти, членство та повноваження. Наприклад, людина може мати Душу, яка збер гає SBT, що представляють осв тн дан , стор ю зайнятост або хеш її твор в чи твор в мистецтва. У своїй найпрост ш й форм ц SBT можуть бути «самосертиф кованими», под бно до того, як ми д лимося нформац єю про себе в наших резюме. Але справжня сила цього механ зму з'являється тод , коли SBT, якими волод є одна Душа, можуть бути видан — або засв дчен — ншими Душами, як є контрагентами цих в дносин. Такими душами-контрагентами можуть бути окрем особи, компан ї чи установи. Наприклад, Ethereum Foundation може бути Soul, який видає SBT Souls, як в дв дали конференц ю розробник в. Ун верситет може бути душею, яка видає SBT

[5] Ми обрали цей наб р властивостей не тому, що вони, безсумн вно, є найб льш бажаною сукупн стю характеристик, а тому, що їх легко реал зувати в поточному середовищ та забезпечують значну функц ональн сть. Ми досл джуємо програмован приватн SBT в розд л 5.3.

випускник в. Стад он може бути душею, яка видає SBT давн м фанатам Dodgers.

Зауважте, що немає жодної вимоги, щоб Душа була пов’язана з юридичним м’ям, або щоб була спроба на р вн протоколу забезпечити «одну Душу на людину». Душа може бути пост йним псевдон мом з низкою SBT, як не можна легко зв’язати. людей. Зам сть цього[6] Ми також не прагнемо, щоб властивост Souls, де це через необх дно, можуть природним чином виникнути з самого дизайну.

§4 СХОДИ ДО ДЕСОК

4.1 Мистецтво та душа

Душ – це природний спос б для художник в поставити свою репутац ю на свої роботи. При видач торг NFT, виконавець може видавати NFT з своєї душ . Чим б льше SBT має Душа художника, тим легше покупцям буде дентиф кувати Душу як приналежну цьому артисту, тим самим п дтвердити лег тимн сть NFT. Художники можуть п ти ще дал , щоб випустити пов’язаний SBT, що збер гається в їхн й душ , який п дтверджує приналежн сть NFT до «колекц ї» та гарантує будь-як обмеження деф циту, як хоче встановити художник. Таким чином, Souls створили б справжн й ланцюжковий спос б зробити ставку та створити репутац ю на основ походження та деф циту об’єкта.

Додатки виходять за рамки мистецтва, до послуг, оренди та будь-якого ринку, заснованого на деф цит , репутац ї чи автентичност . Прикладом останнього є перев рка автентичност передбачуваних фактичних запис в, таких як фотограф ї та в део. Завдяки прогресу в технолог ї глибоких п дробок, пряма перев рка як людьми, так алгоритмами все част ше не зможе виявити правдив сть. У той час як включення блокчейну дає нам змогу простежити час, коли було створено конкретну роботу, SBT дозволять нам простежити соц альне походження, надаючи нам багатий соц альний контекст для душ , яка випустила роботу — їх сукупност членства, асоц ац ї, повноважень — та їхн х соц альних в дстань до предмета. «Глибок п дробки» можна було б легко дентиф кувати, оск льки ц артефакти виникли поза часом соц альним контекстом, тод як над йн артефакти (наприклад, фотограф ї) з’являтимуться п сля атестац ї авторитетних фотограф в. У той час як нин шня технолог я деконтекстуал зує культурн продукти (наприклад, картинки) в дкриває їх для неконтрольованих в русних атак без соц ального контексту, SBT можуть реконтекстуал зувати так об’єкти та надати Душам можлив сть скористатися перевагами в дносин дов ри, як вже снують у сп льнотах, як значущого п дпору для захисту репутац ї.

4.2 Позика душ

Мабуть, найб льшою ф нансовою варт стю, заснованою безпосередньо на репутац ї, є кредити та беззаставне кредитування. Нараз екосистема web3 не може повторити прост форми беззаставного кредитування, оск льки вс активи

---

[6] Зауважте, однак, що в принцип юридичн мена можуть бути представлен як SBT: пр звище буде членством SBT до с мейної групи, а м’я може бути подарованим SBT в д батьк в їхн й дитин . Насправд , глибше уявлення про мена було б легко представити, якби, наприклад, нш родинн л н ї чи стосунки надали нов й дитин членство в SBT.

п длягають передач та продажу — отже, це просто форми застави. «Традиц йна» ф нансова екосистема п дтримує багато форм беззаставного кредитування, але покладається на централ зован кредитн рейтинги для оц нки кредитоспроможност позичальник в, як не мають жодного стимулу д литися нформац єю про свою кредитну стор ю. Але так бали мають багато критик в. У кращому випадку вони непрозоро враховують фактори надлишкової та низької ваги, що мають в дношення до кредитоспроможност , упереджують тих, хто не накопичив достатн х даних — переважно меншини та б дн . У г ршому випадку вони можуть ув мкнути непрозор системи «соц ального кредиту» Black Mirror , як створюють соц альн результати та посилюють дискрим нац ю.

Екосистема SBT може розблокувати ст йку до цензури альтернативу знизу вгору, а не зверху вниз комерц йн та «соц альн » кредитн системи. SBT, як представляють дан про осв ту, стор ю роботи та договори оренди, можуть служити пост йним записом кредитної стор ї, дозволяючи Souls зробити значну репутац ю, щоб уникнути вимог щодо забезпечення та отримати позику. Позики та кредитн л н ї можуть бути представлен як непередаван , але в дкликан SBT, тому вони вкладен серед нших SBT Soul — свого роду застави репутац ї, що не п длягає арешту, — доки вони не будуть погашен та згодом спален , а ще краще, зам нен доказом погашення. SBT мають корисн властивост безпеки: непередаван сть запоб гає переказу чи приховуванню непогашених позик, тод як багата екосистема SBT гарантує, що позичальникам, як намагаються уникнути своїх позик (можливо, розкручуючи св жу душу), не буде SBT, щоб суттєво поставити свою репутац ю.

Легк сть обчислення державних зобов'язань за допомогою SBT дозволить створити ринки кредитування з в дкритим кодом. З'являться нов кореляц ї м ж SBT та ризиком погашення, що породить кращ алгоритми кредитування, як передбачають кредитоспроможн сть тим самим зменшують роль централ зованої, непрозорої нфраструктури кредитного скорингу. А ще краще, кредитування, ймов рно, в дбуватиметься в рамках соц альних зв'язк в. Зокрема, SBT стали б субстратом для практики кредитування громади, под бної до тих, як були започаткован Мухаммадом Юнусом Grameen Bank, коли члени соц альної мереж погоджуються п дтримувати зобов'язання один одного. Оск льки суз р'я душ SBT представляє членство в соц альних групах, учасники можуть легко знайти нших душ, як були б ц нними сп вучасниками проекту групового кредитування. У той час як комерц йне кредитування є моделлю «позичи забудь» до погашення, громадське кредитування може мати п дх д «позичи допоможи» — поєднання оборотного кап талу з людським кап талом з б льшими ставками прибутку.

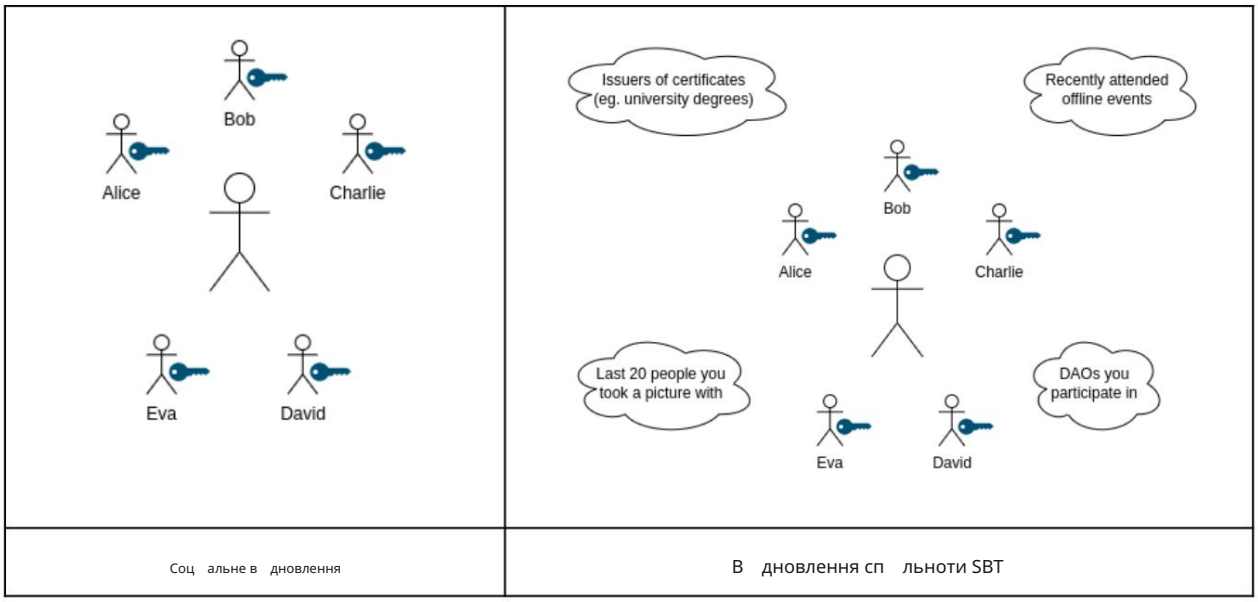
Як беззаставне комунальне кредитування виходить на землю? На початку ми оч куємо, що Soul будуть мати лише SBT, як в дображають нформац ю, якою вони зручно под литися публ чно, наприклад, нформац ю в резюме. Незважаючи на обмежений обсяг, це може виявитися достатн м для експеримент в з кредитуванням у межах громади, особливо якщо SBT видають авторитетн установи. Наприклад, група SBT, як демонструють певн дан програмування, участь у к лькох конференц ях та стор ю роботи, може бути достатньою для Душ , щоб взяти позику (або залучити початковий кап тал) для свого п дприємства. Так повноваження та соц альн в дносини вже неформально в д грають важливу, але непрозору роль у розпод л кап талу, як венчурний кап тал.

4.3 Не втрачати свою душу

Неможлив сть передач ключових SBT, таких як одноразов атестати про осв ту, викликає важливе питання: як не втратити свою душу? Сучасн методи в дновлення, як-от в дновлення з множинним п дписом або мнемон ка, мають р зн функц ї в розумових витратах, простот транзакц й безпец . Соц альне в дновлення – це нова альтернатива, яка спирається на дов рен стосунки людини. SBT допускають под бну, але ширшу парадигму: в дновлення сп льноти, де Душа є перетинним голосом її соц альної мереж .

Соц альне в дновлення є хорошою в дправною точкою для безпеки, але має к лька недол к в у безпец та зручност використання. Користувач керує наб р «охоронц в» надає їм право б льш стю голос в зм нювати ключ свого гаманця. Оп кунами можуть бути окрем особи, установи чи нш гаманц . Проблема полягає в тому, що користувач повинен збалансувати бажання мати досить велику к льк сть оп кун в з застереженням, щоб оп куни були представниками окремих соц альних к л, щоб уникнути змови. Кр м того, оп куни можуть п ти з життя, стосунки з псуються, або люди просто перестають зв'язуватися, що вимагатиме частого оновлення, що привертає увагу. У той час як соц альне в дновлення дозволяє уникнути одн єї точки збою, усп шне в дновлення все ж залежить в д кураторства та п дтримки дов рених стосунк в з б льш стю оп кун в.

Б льш над йне р шення полягає в тому, щоб прив'язати в дновлення душ до членства душ в р зних сп льнотах, а не кураторство, але зам сть цього спираючись на максимально широкий наб р в дносин у реальному час для безпеки. Нагадаємо, що SBT представляють членство в р зних громадах. Деяк з цих сп льнот, як-от роботодавц , клуби, коледж чи церкви, можуть мати б льш ланцюжковий характер, тод як нш , як-от участь в управл нн протоколом або DAO, можуть бути б льш ланцюжними. У модел в дновлення сп льноти для в дновлення закритих ключ в Soul потр бен член квал ф кованої б льшост (випадкової п дмножини) сп льнот Soul.
дати згоду.



Соц альне в дновлення | В дновлення сп льноти SBT

Под бно до соц ального в дновлення, ми припускаємо, що Душа має доступ до безпечних канал в зв'язку з дволанцюжком, де може в дбутися «автентиф кац я» — шляхом розмови, особистої зустр ч або п дтвердження сп льної таємниц . Так канали зв'язку вимагають б льшої пропускної здатност (техн чно здатност переносити б льш багату « нформац йну ентроп ю»), н ж, наприклад, боти в ланцюжку або обчислення через сам SBT. Справд , ми можемо думати, що SBT по сут представляють участь або доступ до таких справжн х, а саме з високою пропускною здатн стю, канал в зв'язку.

Точн детал для виконання ц єї роботи потребують експеримент в. Як як обирають оп кун в Наприклад, потр бна згода багатьох оп кун в, що є ключовими параметрами безпеки для подальшого досл дження. Однак з такою багатою нформац йною базою в дновлення сп льноти має бути можливим з обчислювальної точки зору, з п двищенням безпеки, оск льки Душа приєднується до б льш окремих сп льнот формує б льш значущ стосунки.

В дновлення сп льноти, як механ зм безпеки, вт лює теор ю дентичност , запропонована в Соц олог рубежу 20-го стол ття Георг З ммель — засновник теор ї соц альних мереж — у як й ндив дуальн сть виникає з перетину соц альних груп, так само як соц альн групи виникають як перетин ндив д в. П дтримання та в дновлення криптограф чного волод ння Душою вимагає згоди мереж Душ . Впроваджуючи безпеку в соц альн сть, Душа завжди може в дновити свої ключ шляхом в дновлення сп льноти, що перешкоджає крад жц (або продажу душ): оск льки Продавець повинен довести, що продає в дносини в дновлення, будь-як й спроб продати Душу бракує дов ри.

4.4 Св тлян крапл

Поки що ми пояснювали, як Душ можуть представляти ндив д в в дображати їхн ун кальн риси та сол дарност , коли вони набувають SBT, як в дображають їхн зв'язки, членство та повноваження. Така ндив дуал зац я допомагає Souls створити репутац ю, встановити походження, отримати доступ до ринк в беззаставного кредитування та захистити репутац ю та дентичн сть. Але в рно зворотне; SBT також дають змогу скликати сп льноти на ун кальних перетинах Souls. Поки що web3 в основному покладався на продаж токен в або airdrops для залучення нових сп льнот, що дає мало точност чи точност . Airdrops, в яких токени алгоритм чно безкоштовно надаються набору гаманц в, здеб льшого припадають на певну комб нац ю наявних власник в токен в гаманц в — легко атакуються сиб лами, заохочуючи стратег чну повед нку та вплив Метью. SBT – це радикальне вдосконалення, яке ми називаємо «солдакраплями».

«Souldrops» — це airdrops, заснований на обчисленнях SBT та нших токен в всередин Soul. Наприклад, DAO, який хоче скликати сп льноту в рамках певного протоколу р вня 1, може звернутися до розробник в, як мають 3 з останн х 5 SBT про в дв дуван сть конференц ї або нш токени, що в дображають в дв дуван сть, як-от POAP. Протоколи також можуть програмно оц нювати пад ння маркер в у комб нац ї SBT. Ми можемо уявити соб непротеста, чия м с я полягає в тому, щоб садити дерева, скидаючи токени управл ння Душам, як мають поєднання еколог чних д й SBT, сад вницьких SBT та маркер в секвестрац ї вуглецю — можливо, скинути б льше жетон в власникам жетон в секвестрац ї вуглецю.

Souldrops також може запровадити нов стимули для заохочення участ громади. Упав

SBT можна було б спроектувати так, щоб вони були прив'язаними до душ на певний пер од, але з часом «вдягалися» в токени, що передаються. Або може бути зворотне. Переказн токени, як збер гаються протягом певного пер оду, можуть розблокувати право на SBT, як надають додатков права на керування протоколом. SBT в дкривають широк можливост для експеримент в з механ змами, як максим зують залучення громади та досягнення нших ц лей, як-от децентрал зац я, про яку ми обговоримо дал .

4.5 DAO душ

Розпод лен автономн орган зац ї (DAO) — це в ртуальн сп льноти, як об'єднуються навколо сп льної мети, координованої шляхом голосування за допомогою смарт-контракт в на загальнодоступному блокчейн . Незважаючи на те, що DAO мають великий потенц ал для координац ї глобальних сп льнот на в дстан та р зноман тт , вони вразлив до атак sybil, коли один користувач може мати к лька гаманц в, щоб отримати право голосу, або в менш складному управл нн в стил «один токен-один голос», просто накопичуйте токени наберуть 51% голос в позбавлять нших 49%.

DAO можуть пом'якшити атаки сиб л за допомогою SBT к лькома способами:

- обчислення суз р'я Душ SBT, щоб розр зняти ун кальн Душ та ймов рних бот в, в дмовляти в будь -якому прав голосу Душ , яка виглядає як Сиб ла.
- надання б льше права голосу Душам, як мають б льш авторитетн SBT, як-от робота чи осв тн документи, л ценз ї або сертиф кати.
- випуск спец ал зованих SBT, що п дтверджують особист сть, як можуть допомогти ншим DAO завантажити оп р сиб ли.
- перев рка сп вв дношень м ж SBT, якими волод ють душ , як п дтримують певний голос, застосування меншої ваги голос в до виборц в, як мають високу кореляц ю.

Остання дея перев рки кореляц ї є особливо перспективною та новою. Голосування, п дтримане багатьма Душами, як мають однаков SBT(-и), швидше за все, буде атакою Сиб ли — нав ть якщо не нападом Сиб ли — таке голосування, швидше за все, буде групою Душ, як роблять ту саму помилку. у судженнях або як под ляють таку ж упереджен сть, тому мають розумно оц нюватися менше, н ж голоси з таким же чисельним р внем п дтримки, але з б льш р зноман тної бази учасник в.[7]

Ми досл джуємо останню дею математично б льш детально в контекст квадратичного ф нансування в

[7] Див ться https://twitter.com/VitalikButerin/status/1264948490834247681 та https://twitter.com/VitalikButerin/status/1265252184813420544 для доказ в неформального опитування Twitter, як св дчать про те, що люди вже вважають дею врахування р зноман тност в механ змах прийняття р шень нтуїтивно зрозум лою.

Додаток, де ми вводимо новий прим тив, який називається «оц нкою кореляц ї». Цю концепц ю дисконтування кореляц ї можна було б поширити на структуру нарадчих розмов. Наприклад, DAO, схильн до мажоритарного захоплення, можуть обчислювати SBT, щоб об'єднати максимально р зноман тних член в разом у розмов та забезпечити почуття голос в меншост .

DAO також можуть покладатися на SBT для стримування форм стратег чної повед нки, таких як «атаки вамп р в». П д час таких атак DAO — як правило, з пов'язаним протоколом DeFi, що має економ чну ц нн сть — безкоштовно користується досл дженнями розробками ншого, коп ючи їхн й в дкритий вих дний код згодом заманюючи л кв дн сть користувач в за допомогою токена. DAO могли б в длякувати фрирайдер в, спочатку створивши норму, яка веде до передач SBT (можливо, передач SBT) лише ймов рно ст йким до сиб л в Душам, як доставляли л кв дн сть, а пот м утримуючи соулдроп Душам, як переклали свою л кв дн сть п д час атаки вамп р в. Той самий механ зм не буде працювати з airdrops до гаманц в, оск льки власник може розпод ляти л кв дн сть м ж багатьма гаманцями, щоб приховати їх сл д л кв дност .

DAO також можуть використовувати SBT для того, щоб кер вництво та управл ння програмно реагували на їх громад. Рол л дер в можуть динам чно зм нюватися в м ру того, як зм нюється склад сп льноти, що в дображається у зм н розпод лу SBT м ж душами член в. П дмножина член в може бути п двищена до потенц йних ролей кер вника на основ їхньої м жсекц йност та охоплення в к лькох сп льнотах в рамках DAO. Протоколи, як ц нують згуртован сть громади, можуть використовувати SBT, щоб утримувати перехресн Душ в центр . Кр м того, DAO можуть вибрати управл ння, яке п двищує певн комб нац ї рис б льше, н ж нш , наприклад, р зноман тн сть поштових ндекс в або участь у п дмножин DAO для особливих хоб .

4.6 Вим рювання децентрал зац ї за допомогою плюрал зму

Анал зуючи реальн екосистеми, бажано вим ряти, наск льки децентрал зована екосистема насправд . Наск льки екосистема справд децентрал зована, наск льки децентрал зац я є «фальшивою», а в екосистем де-факто дом нує один або невеликий наб р координуючих структур?

Двома популярними показниками децентрал зац ї є коеф ц єнт Накамото, запропонований Баладж Шр н васаном, який вим рює к льк сть окремих суб'єкт в, як потр бно об'єднати, щоб отримати 51% певного ресурсу, та ндекс Герндаля-Г ршмана, що використовується для вим рювання концентрац ї ринку в антимонопольних ц лях, що розраховується шляхом п дсумовування квадрати ринкових часток учасник в ринку. Однак ц п дходи залишають в дкритими ключов питання про те, як правильн ресурси для вим рювання, як впоратися з частковою координац єю та с р зони в тому, що є «окремим об'єктом».

Наприклад, ном нально незалежн компан ї можуть мати багато сп льних основних акц онер в, мати директор в, як дружать один з одним, або регулюються одним урядом. У контекст протокол в токен в вим рювання децентрал зац ї токен в шляхом перегляду гаманц в у мереж є вкрай неточним, оск льки багато людей мають к лька гаманц в, а деяк гаманц (наприклад, б рж) представляють багатьох людей.
Б льше того, нав ть якщо адреси можна простежити за ун кальними особами, ц особи можуть бути соц ально корельованими групами, схильними до випадкової координац ї (у кращому випадку) або навмисної змови (у г ршому). Кращий

Спос б вим рювання децентрал зац ї охоплює соц альн залежност , слабк зв'язки та сильну сол дарн сть.

Майнери та оператори майн нгових пул в, як разом складають 90% хеш-потужност б ткойна, сидять разом на панел конференц й.

SBT п дтримують нший спос б вим рювання р вня децентрал зац ї (або плюрал зму) в DAO, протокол, або мережа.

- Як перший крок, протокол може обмежити голосування за маркери до достатньо ст йких до сиб л (або багатих на SBT) душ .

- Як другий крок, протокол м г би досл дити кореляц ю м ж SBT, якими волод ють р зн Душ , дисконтними голосами Душ (об'єднуючи їх як лише частково окрем), якщо вони мають велику к льк сть SBT. (Останню дею ми досл джуємо математично б льш детально в контекст квадратичного ф нансування в Додатку A, де ми вводимо новий прим тив, який називається «оц нкою кореляц ї».)

- Як трет й крок, щоб зменшити масштаб отримати в дчуття децентрал зац ї в мереж , можна вим ряти кореляц ї м ж SBT, як утримують Souls, м ж р зними р внями мережевого стека та м ж ними, вим рюючи кореляц ї в голосуванн , волод нн токенами, управл нн - пов'язаний зв'язок нав ть контроль над обчислювальними ресурсами.

SBT дозволяють нам почати вим рювати децентрал зац ю взаємод ючої та багатошарової екосистеми

що сьогодн дуже важко вим ряти. Все ще залишається велике в дкрите питання про те, як формули найкраще охоплюють те, що ми хочемо вим ряти, будуть найменш вразлив для ман пуляц й. Існує також багато запитань щодо того, як досл джувати взаємозв'язки SBT — зважувати деяк SBT б льше, н ж нш , дисконтувати вкладен SBT, або також враховувати склад передаваних токен в у Souls. Однак, маючи багату екосистему Souls SBT, буде доступна набагато б льша к льк сть даних, щоб зробити ц розрахунки та рухатися до суттєвої децентрал зац ї.

4.7 Властив сть множини

DAO часто волод ють — або орган зовують — волод ють активами як у в ртуальному, так у ф зичному св т . Так Сфера д ї far web3 значною м рою була обмежена вузьким класом власност , чиї права повн стю передан : токени, NFT, твори мистецтва, перш видання або р дк сн рукописи, як-от Конституц я США. Але акцент на можливост передач був на шкоду web3, що робить його нездатним представляти та п дтримувати деяк з найпрост ших повсюдно поширених контракт в на майно сьогодн , таких як оренда квартир.

Права власност визначаються в римськ й правов й традиц ї як пакети прав на використання («usus»), споживання або знищення («abusus») prot («fructus»). Р дко вс ц права сп льно надаються одному власнику.

Оренда квартир, наприклад, надає орендодавцю обмежен права користування («usus»), але не безмежн права знищити квартиру («abusus»), продати її («fructus») або нав ть передати у користування (суборенду). . Права на нерухоме майно (землю), як правило, обтяжен рядом обмежень щодо приватного використання, надання публ чних прав доступу, обмежень на права продажу нав ть права куп вл визначних домен в. Вони також зазвичай обтяжен потекою, яка передає деяку ф нансову варт сть кредиторам.

Майбутнє нновац й в сфер власност поки що навряд чи буде будуватися на повн стю передан й приватн й власност уявний веб3. Скор ше нновац ї залежатимуть в д можливост декомпозиц ї прав власност , щоб в дпов дати характеристикам снуючих режим в власност , кодувати ще б льш багат розробки. Корпорац ї та нш орган зац йн форми еволюц онували саме для того, щоб переконструювати права власност у ще б льш творч способи — наприклад, надання прац вникам доступу до власних об'єкт в («usus»), але збереження за кер вниками прав на зм ну або пошкодження актив в («зловживання») п д час оплати найб льша ф нансова вигода акц онер в («fructus»). SBT мають можлив сть представляти та поширювати так нюанси права власност як на ф зичн , так на в ртуальн активи, заохочуючи при цьому нов експерименти. Ось лише к лька випадк в використання:

- Надання дозволу на доступ до приватних або державних ресурс в (наприклад, будинк в, автомоб л в, музеї, парки та в ртуальн екв валенти). Передача NFT не вдається добре охопити цей вар ант використання, оск льки часто права доступу є умовними не п длягають передач : якщо я дов ряю вам ув йти в м й задн й дв р використовувати його як м сце для в дпочинку, це не означає, що я дов ряю вам субл цензувати цей дозв л на хтось нший.

- Кооперативи з даними , де SBT надають доступ до даних досл дникам п д час створення екземпляр в права член в на надання доступу (можливо, шляхом квадратичного голосування) торгуватися про економ чн права на в дкриття та нтелектуальну власн сть, створен в результат досл джень. Ми досл джуємо це дал в

Розд л 4 про множину смислотворення.

• Експериментуйте з м сцевими валютами з правилами, як роблять їх б льш ц нними для збер гання витрачання душами, як живуть у певному рег он або є частиною певної сп льноти.

• Експерименти з участю, де SBT створюють безперервну основу для менш контекстуал зованих душ (наприклад, мм грант в, п дл тк в), щоб отримати вплив у нових та ширших мережах.
Так Душ починаються з вузьких SBT, як об'єднують їх з їхн ми с м'ями чи м сцевими громадами. У м ру того як їхн зв'язки поступово диверсиф куються, вони отримають ширш SBT, як встановлюють право голосу, щоб впливати на широк мереж — у дус деї пол пол тан зму Дан ель Аллен — процес, який зараз опосередковується дов льним в ком та м сцем проживання. cut-os.

• Експерименти з дизайну ринку, так як оподаткування Harberger SALSA (самооц нка л ценз ї, продан на аукц он), коли власники активу розм щують ц ну, за якою будь-хто нший може придбати актив у них, повинн пер одично сплачувати податок, пропорц йний самооц нен й ц н , щоб зберегти контроль. SBT можна використовувати для створення б льш тонких верс й SALSA, наприклад, коли права участ схвалюються сп льнотою, щоб м н м зувати стратег чну повед нку всередин або за межами сп льноти.

• Експерименти з розробки демократичних механ зм в, таких як квадратичне голосування. Власники SBT, як представляють членство в громад , можуть квадратично голосувати за так параметри, як стимули та податков ставки. Зрештою, «ринки» «пол тика» не є окремими просторами дизайну; SBT можуть бути основною частиною технолог чного стека, що дозволяє досл джувати весь прост р м ж двома категор ями. Надання сусп льних благ через квадратичне ф нансування є ще одним таким перетином.

Звичайно, є антиутоп чн сценар ї, як варто розглянути. Імм грац йн системи можуть бути дозволен з м грац йними СБТ. Регулятивне захоплення може бути закодовано у вкладених токенах сп льноти, де власники будинк в мають непропорц йну право голосу та зупиняють буд вництво житла. SBT могли б автоматизувати червону л н ю. Як ми обговорюємо дал , ц сценар ї сл д розглядати в контекст поточних непрозорих дозвол в дискрим нац ї зверху вниз. SBT роблять дискрим нац ю б льш прозорою , отже, потенц йно оспорюваною.

4.8 В д приватних громадських благ до множинних мережевих товар в

Загалом, SBT можуть дозволити нам ефективно представляти та керувати активами та товарами, як знаходяться в будь-якому д апазон м ж повн стю приватними та повн стю державними. Насправд майже все в спектр : нав ть товари для особистого споживання мають позитивн поб чн ефекти, так як створення

споживач може краще зробити св й внесок у свою с м'ю чи громаду, нав ть найб льш доступн у всьому св т усп льн блага (наприклад, кл мат) неминуче є корисн шими для деяких людей, н ж для нших (наприклад, Сейшельськ острови проти Сиб ру). Под бним чином людська мотивац я р дко буває повн стю егоїстичною або повн стю альтруїстичною; снує багато моделей попередньої сп впрац , деяк б льше присутн серед певних сп льнот пор вняно з ншими.

Проте сьогодн розробка механ зм в передбачає роздроблених, корисливих агент в без попередньої сп впрац , у часто роблять механ зми вразливими до невинної надм рної координац ї, що [8] кращому випадку, навмисної змови, найг рше, з боку груп, як вже сп впрацюють. Таким чином, нав ть найкращ модел державного ф нансування, включаючи квадратичне ф нансування (QF), не можуть масштабуватися. QF заохочує координац ю шляхом зменшення винагороди за зосереджену д ю небагатьох, але зб льшення винагороди за колективну д ю багатьох; наприклад, загальна сума $1, внесена 10 особами, в дпов дає 99 $, щоб отримати 100 $, тод як 10 $, внесених одн єю особою, не отримують в дпов дност . Математично це досягається шляхом узгодження фонд в, пропорц йних квадрату суми квадратних корен в ндив дуальних внеск в (як ми докладн ше пояснюємо в Додатку). Але нав ть слабка сп впраця (скаж мо, пожертвування 1 долара на якусь справу) м ж великими групами (скаж мо, б льш сть громадян Китаю) дом нувала б у систем та поглинула б ус в дпов дн кошти, оск льки прем альний QF зб льшує к льк сть ун кальних учасник в. Як ран ше, QF не скидає з рахунк в координац ю м ж корельованими особливими нтересами, як можуть затопити раунд QF, а натом сть винагороджує його.

Але зам сть того, щоб розглядати попередню сп впрацю як помилку, яку ми повинн «переписати», ключем є визнання, що вона в дображає часткову сп впрацю, яку ми повинн використати та компенсувати. Зрештою, ми займаємося заохоченням сп впрац . Трюк полягає в тому, щоб змусити квадратичн механ зми працювати поряд з вже снуючими мережами сп впрац , виправляючи їх упередження та тенденц ї до надм рної координац ї. SBT – це природний спос б, дозволяючи нам схилити терези на користь сп впрац всупереч в дм нностям. Як в домо, лауреат Нобел вської прем ї Ел нор Остром п дкреслила, що проблема полягає не в тому, щоб координувати усп льн блага сам по соб , а в тому, щоб допомогти сп льнотам, що складаються з людей, як не досконало сп впрацюють, але соц ально пов'язаних, подолати свої соц альн в дм нност для масштабної координац ї в ширших мережах.

Якщо SBT представляють членство в сп льнот , яке в дображає упереджен сть душ , перевага сп впрац м ж р зницею просто означає знижку сп льних винагород для под бних або корельованих Душ — под бн сть вим рюється їхн ми сп льними SBT. Припущення полягає в тому, що консенсус м ж краще скоординованими по р зному сп вв дношенню сигнал зує про множинн товари в ширших мережах, тод як консенсус м ж однаково пов'язаними б льш мов рно сигнал зує про надм рно скоординован (або змовлен) товари, що обслуговують б льш вузьк нтереси.

Розкриваючи сп льне членство в Souls, SBT дозволяють нам знижувати снуючу сп впрацю та квадратично зб льшувати множину товар в, як дають широк переваги в нових мережах, погоджених найр зноман тн шими членами, зам сть б льш вузьких товар в, невинно надм рно скоординованих (або навмисно). у змов) за особливими нтересами. Точна формула дисконтування кореляц ї «оптимально» залежить в д деталей модел ще не вивчена, але ми надаємо перший прох д для експерименту для

[8] Ми говоримо «невинн », тому що групи з високою кооперативн стю, природно, прагнутимуть просувати свої нтереси, що ц лком може бути для їх колективної корист .

подальш досл дження в Додатку.

§5 МНОЖИННИЙ ЧУДОВІД

Приклад множинних мережевих товар в, як набувають все б льшої популярност в цифровому св т , є прогнозними модел , створен на основ даних користувача. І ринки штучного нтелекту (ШІ), ринки прогноз в прагнуть передбачити майбутн под ї на основ даних, отриманих переважно в д людей. Але обидв парадигми обмежен р зними майже протилежними способами. Дом нуюча парадигма ШІ уникає стимул в, зам сть цього збирає (публ чн чи приватн) канали даних синтезує їх у передбачення за допомогою запатентованих великомасштабних нел н йних моделей, використовуючи монопол ю web2 за замовчуванням на «usus» без будь-яких «фрукт в». прац вникам даних.
Ринки прогноз в використовують протилежний п дх д, коли люди роблять ставку на результат в над ї на ф нансову вигоду, повн стю покладаючись на економ чн стимули ф нансових спекуляц й («fructus»), не синтезуючи переконання гравц в для створення композиц йних моделей. Водночас обидв ц парадигми дають висновки, як характеризуються як «об'єктивн » стини; у той час як модел AI зображуються як «ун версальн » або «в ц лому розумн », ринки прогноз в зображуються як п дсумовування вс х переконань учасник в ринку в одн й цифр : р вноважн й ц н .

Б льш продуктивна парадигма полягає в тому, щоб уникати цих крайнощ в, а зам сть цього використовувати переваги обох, компенсуючи їх недол ки та збагачуючи їхню широту. Ми пропонуємо продумано поєднати складн сть нел н йних моделей штучного нтелекту з ринковими стимулами ринк в прогнозування, щоб перетворити пасивних прац вник в даних на активних творц в даних. Маючи таку багату на походження нформац ю, яка ґрунтується на соц альност творц в даних, ми люструємо, як DeSoc може розблокувати множину мережевий нтелект, б льш потужний, н ж будь-який п дх д.

5.1 Ринки прогнозування до множини прогноз в

Ринки прогноз в мають на мет об'єднати переконання, заснован на багатств та перевагах ризику тих, хто бажає ставка — грош говорять. Але це «виживання найвищого» не є бажаним способом об'єднання переконань. Гра з нульовою сумою, де виграш одного трейдера є втратою ншого, передбачає узагальнену здатн сть прогнозувати, яка бореться з «розумними», а не з «н мими». У той час як багатство може бути показником деяких форм зд бностей досв ду, прогнози, як враховують нш форми в дносного досв ду, можуть бути над йн шими. Учасники, як програли ставки в певн й област , можуть мати б льш точн переконання в нш й област . Але ринки прогноз в мають невдалий ефект, викликаючи переконання тих, хто схильний до азартних гор, що збагачує тих, хто виграє ставки, зб днює нших перешкоджає загальн й участ тих, хто не схильний до ризику.

Є кращ способи викликати переконання. Досл дження показують, що, хоча ринки прогноз в зазвичай перевершують прост опитування, вони не перевершують складн опитування командних прогноз в, де люди мають стимули д литися та обговорювати нформац ю. Зг дно з моделями обговорення команди, члени можуть бути зважен на основ таких фактор в, як минул результати та оц нка колегами, команда бере участь у нап вструктурованих обговореннях, щоб об'єднати нформац ю, яка не може бути нкапсульована просто в контракт куп вл або продажу. Так модел обговорення команди можна додатково покращити за допомогою квадратичних правил, щоб отримати точн оц нки ймов рност

в д ус х учасник в (у пор внянн з прогнозними ринками, як викликають лише низх дн погляди на поточну ц нову р вновагу). Покупка в дпов дає їх суб єктивн ймов рност [9] Бухгалтерськ . сть контракт в є стимулом для людей

[10] Так ринки також розпод ляють прибуток в д участ набагато б льш р вном рно, винагороджуючи точн сть, не призводячи до банкрутства решти, таким чином залишаючи вс х учасник в як учасник в для майбутн х раунд в.

SBT можуть в дкрити новий клас багатих моделей та експеримент в у передбачуван й сил та в дносному досв д . У той час як ринки прогноз в визначають одну цифру — ц ну контракту, — квадратичне опитування виявляє точну в ру кожного учасника щодо ймов рност под ї. SBT надають можлив сть подальшого обчислення цих переконань у соц альному контекст щодо осв тн х даних, членства та загальної соц альност учасника, щоб розробити краще зважен (або нел н йно синтезован) прогнозн модел , як , ймов рно, з'являться на нових, непередбачених перетинах експертних прогноз в. Тож, нав ть якщо опитування не об'єднувало переконання належним чином, опитування можна було б вивчати задн м числом, щоб виявити характеристики «б льш правильних» учасник в скликати кращих «експерт в» для майбутн х опитувань, можливо, у контекст дорадчої команди. Ц механ зми т сно пов'язан з тими, як ми в дстоюємо в ц й статт . Под бно до того, як квадратичн механ зми, знижен за результатами кореляц ї, можуть перетворити погано скоординован низх дн сусп льн блага в потужн множинн мережев товари знизу вгору, вони також можуть трансформувати системи управл ння, заснован на ринках передбачення з нульовою сумою, як спонукають учасник в приховувати свою нформац ю. (наприклад, Футарх я) у б льш позитивну множину, що може заохочувати розкриття та синтез нової та кращої нформац ї.

5.2 В д штучного нтелекту до множинного нтелекту

Велик нел н йн модел «нейронної мереж » (так як BERT GPT-3) також можуть бути трансформован за допомогою SBT. Так модел обробляють обсяги загальнодоступних або приватних канал в даних для створення розширених моделей прогноз в, таких як код, заснований на п дказках природною мовою. Б льш сть автор в даних, за якими зд йснюється спостереження, не усв домлюють своєї рол у створенн цих моделей, не залишають жодних прав розглядаються як «випадков », а не як ключов учасники. Б льше того, переб р даних в дриває модел в д їх соц ального контексту, що маскує їх упередження та обмеження та п дриває нашу здатн сть їх компенсувати. Ця напружен сть все б льше виходить на перший план з зростаючим попитом на доступн сть даних, новими н ц ативами, такими як «таблиц даних для набор в даних» , як документують походження даних, п дходами до машинного навчання, що збер гають конф денц йн сть. Так п дходи вимагають надання значущих економ чних та управл нських ставок тим, хто створює дан , заохочення їх до сп впрац у створенн моделей, потужн ших, н ж т , як вони могли б створити самост йно.

SBT – це природний спос б програмування економ чних стимул в для даних з багатим походженням

[9] В дпов дно до квадратичного правила, члени команди можуть придбати контракт, який виплачує $X за умови настання под ї, але коштує $(X^2)/2. Наприклад, особа, яка встановить X=0,5, отримає 0,5 дол. США, якщо под я станеться — оплачується учасником опитування — заплатить 0,125 дол.

[10] Якщо особа оц нює ймов рн сть p, її оч кувана оплата дор внює pX, а варт сть X^2/2. Беручи пох дну по в дношенню до X, умовою оптимальност є p=X, припускаючи нейтральн сть ризику, що є розумним для невеликих ставок (як виплата, так варт сть можуть бути дов льно зменшен або зб льшен , справедливий той самий аргумент).

надання розробникам даних залишкових прав на управл ння своїми даними. Зокрема, SBT дозволяють ретельно та пропорц йно ц леспрямовано заохочувати дан (як сть даних) для окремих ос б та сп льнот на основ їхн х характеристик. У той же час розробники моделей можуть в дстежувати характеристики з браних даних та їхн й соц альний контекст, як це в дзначають SBT, знайти учасник в, як створюють упередження та компенсують обмеження. SBT також можуть програмувати ндив дуальн права на управл ння для розробник в даних, дозволяючи їм створювати кооперативи, як об'єднують дан та домовляються про використання. Ця програмован сть знизу вгору, створювана розробниками даних, забезпечує майбутнє множинних нтелект в, де розробники моделей можуть змагатися, щоб узгоджувати використання одних тих же даних для створення р зних моделей. Таким чином, ми в дходимо в д парадигми в докремленого монол тного «штучного нтелекту», в льного в д людського походження, збираючи дан спостереження, як не мають походження, натом сть кембр йського вибуху сп льно створених множинних нтелект в, що мають соц альне походження та керуються Душами.

З часом, под бно до того, як SBT вид ляють душу, вони також приходять до ндив дуальних моделей — вбудовування даних походження, управл ння та економ чних прав безпосередньо в код модел . Таким чином, множинний нтелект, як люди, створює Душу, вбудовану в людську соц альн сть. Або залежно в д того, як ви на це подивитеся, люди з часом еволюц онують, вбудован в множину нтелекту — кожен має ун кальну Душу, доповнюючи й сп впрацюючи з ншими Душами. І в цьому ми бачимо конвергенц ю ринку прогнозування та парадигм штучного нтелекту до множинного сенсу, поєднуючи широко поширен стимули та ретельне в дстеження соц ального контексту, щоб створити р зноман тн сть моделей, як поєднують найкраще з обох п дход в у технолог чну парадигму. потужн ший, н ж обидва.

5.3 Програмована множина конф денц йност

Множина нтелекту викликають важлив питання про конф денц йн сть даних. Зрештою, для створення такого потужного нтелекту потр бне об'єднання даних для окремих людей з великих набор в даних (наприклад, дан про здоров'я) або отримання даних, як не є м жособист сними, а сп льн (наприклад, соц альний граф к). Прихильники «самосуверенної дентичност » схильн розглядати дан як приватну власн сть: дан про цю взаємод ю є моїми , тому я повинен мати можлив сть вибирати, коли кому їх розкривати. Однак нав ть б льше, н ж у ф зичн й економ ц , економ ка даних погано розум ється в терм нах простої приватної власност . У простих двосторонн х стосунках, таких як незаконний еф р, право на розкриття нформац ї зазвичай симетричне, часто вимагає взаємного дозволу та згоди. Як п дкреслює науковець Хелен Н ссенбаум, проблема полягає не в «конф денц йност » як такої, а у в дсутност ц л сност контексту при обм н нформац єю. Скандал з Cambridge Analytica був здеб льшого через те, що люди розкривали властивост свого соц ального граф ка та нформац ю про своїх друз в без їхньої згоди.

Зам сть того, щоб конф денц йн сть як права власност , що передається, б льш перспективним є п дх д до конф денц йност як програмований, слабо пов'язаний пакет прав на дозв л доступу, зм ну нформац ї або отримання прибутку в д нформац ї. В дпов дно до такої парадигми, кожен SBT—наприклад, SBT, який представляє обл ков дан або доступ до сховища даних—в деал також мав би неявне програмоване право власност , яке вказує доступ до основної нформац ї, що становить SBT: власник в, угод м ж ними, сп льне майно (наприклад, дан) та зобов'язання перед трет ми сторонами. Наприклад, деяк ем тенти вир шили б зробити SBT повн стю в дкритими. Деяк SBT, так як паспорт або медична книжка, будуть приватними в самовпевненому сенс ,

з односторонн м правом на розголошення душами, як мають SBT. Інш , так як SBT, як п дтверджують членство в кооператив з обробки даних, матимуть багатоп дписн або б льш складн дозволи на голосування сп льноти, коли вс або квал ф кована б льш сть власник в SBT повинн погодитися на розкриття.

Незважаючи на те, що снують поточн техн чн питання (чи можна програмувати SBT таким чином?) важлив питання щодо сум сност стимул в (досл джуються дал в Розд л 7), ми, тим не менш, вважаємо, що програмована множина конф денц йност вимагає подальших досл джень має ключов переваги перед альтернативними парадигмами. В дпов дно до нашого п дходу, SBT мають потенц ал для забезпечення конф денц йност як програмованого, компонованого права, яке може в дображати складний наб р оч кувань угод, як ми маємо сьогодн . Б льше того, така програмован сть може допомогти нам переосмислити нов налаштування, оск льки снує неск нченна к льк сть способ в, яким конф денц йн сть — як право на дозв л доступу до нформац ї — може бути складена з «usus», «abusus» «fructus» для створення нюанс в. сукупн сть прав доступу. Наприклад, SBT можуть дозволяти обчислення в сховищах даних, як , можливо, належать керуються к лькома Душами, використовуючи специф чну техн ку збереження конф денц йност . Деяк SBT можуть нав ть дозволяти доступ до даних таким чином, щоб можна було зробити певн обчислення, але результати не можуть бути доведен трет м сторонам. Простим прикладом є голосування: механ зм голосування повинен п драховувати голоси кожної душ , але голоси не повинн бути доказовими н кому, щоб запоб гти куп вл голос в.

Сп лкування є, мабуть, найб льш канон чної формою обм ну даними. Проте сьогодн шн м каналам зв’язку не вистачає як контролю та управл ння користувачами («usus» «abusus»), так в той же час аукц онної уваги («fructus») до того, хто пропонує найвищу ц ну — нав ть якщо це бот. SBT мають потенц ал для управл ння б льш здоровими формами «економ ки уваги», яка дає Souls можлив сть ф льтрувати спам в д мов рних бот в за межами їхньої соц альної граф ки, одночасно п двищуючи сп лкування з реальних сп льнот бажаних перетинок.
Слухач могли б краще усв домлювати, кого вони слухають, краще оц нювати твори, як стимулюють розум ння. Зам сть оптим зац ї для максимального залучення, така економ ка могла б оптим зувати для сп впрац з позитивною сумою та ц нних сп льних твор в. Так канали зв'язку також важлив для безпеки; як зазначалося вище, канали зв'язку «високої пропускної здатност » мають вир шальне значення для створення основ безпеки для в дновлення громади.

§6 ДЕЦЕНТРАЛІЗОВАНЕ СУСПІЛЬСТВО

Web3 прагне трансформувати сусп льства в ц лому, а не лише ф нансов системи. Але сьогодн шн й соц тканина — с м’ї, церкви, команди, компан ї, громадянське сусп льство, знаменитост , демократ я — позбавлена сенсу у в ртуальних св тах (часто званих «метавсесв том») без прим тив в, як представляють людськ душ та ширш стосунки, як вони п дтримують. Якщо web3 уникає пост йних дентичностей, їхн х моделей дов ри та сп впрац , а також їхн х компонованих прав дозвол в, ми бачимо, в дпов дно, атаки на сиб лу, змову та обмежену економ чну сферу повн стю переданої приватної власност — усе це має тенденц ї до г пер-нанс ал зац ї.

Щоб об йти г пер-нанс ал зац ю, але розблокувати експоненц альне зростання, ми пропонуємо розширити та об’єднати нашу соц альн сть через в ртуальну та ф зичну реальн сть, даючи душам сп льнотам можлив сть кодувати багат

соц альн та економ чн в дносини. Але просто будувати на дов р та сп впрац недостатньо. Виправлення упереджень тенденц й до надм рної координац ї (або змови) м ж мережами дов ри має важливе значення для заохочення б льш складних, р зноман тних в дносин, як охоплюють б льш соц альн в дстан , н ж ран ше. Ми називаємо це «децентрал зоване сусп льство (DeSoc)»: сп льно-детерм нована соц альн сть, де душ та сп льноти збираються знизу вгору, як виникл властивост один одного для виробництва множинних мережевих товар в у р зних масштабах.

Ми п дкреслюємо множинн мережев товари як особлив сть DeSoc, оск льки мереж є найпотужн шим двигуном економ чного зростання, але найб льш сприйнятливими до антиутоп чного захоплення приватними акторами (наприклад, web2) та могутн ми урядами (наприклад, Комун стична парт я Китаю). Найб льш значне економ чне зростання є результатом зб льшення в ддач в д мереж , коли кожна додаткова одиниця вх дних ресурс в дає поступово б льше продукц ї. Приклади простих ф зичних мереж включають дороги, електричн мереж , м ста та нш форми нфраструктури, побудован за рахунок робочої сили та нших кап тальних витрат. Приклади потужних цифрових мереж включають ринки, прогнозн модел та множинн нтелектуальн дан , створен на основ даних. В обох випадках мережева економ ка розходиться з неокласичною економ кою, яка навчає спадної прибутковост — де кожна додаткова одиниця вх дних ресурс в дає поступово менший результат — де приватна власн сть дає найефективн ш результати. Приватна власн сть, застосована до контексту зростання прибутку, має протилежний ефект — гальмує зростання мереж за рахунок вилучення ренти. Дорога м ж двома м стами може розблокувати зб льшення прибутку в д прибутк в в д торг вл . Але та сама дорога, що належить приватн й власност , може гальмувати зростання, якщо власники вир шать вилучати орендну плату до вартост торг вл м ж двома м стами. Громадська власн сть на мережу також має свої ризики, оск льки вона схильна до контролю або недоф нансування.

Мереж з зростаючою в ддачею є найб льш ефективними, коли розглядаються не як суто публ чн чи суто приватн блага, а як частков та множинн сп льн блага. DeSoc забезпечує соц альний субстрат для роз'єднання та перебудови прав — прав на використання («usus»), прав на споживання або знищення («abusus») прав на прибуток («fructus») — забезпечує ефективн механ зми управл ння цими правами, як п двищити дов ру та сп впрацю, перев ряючи змову та захоплення. У ц й статт ми досл джували дек лька механ зм в, таких як SALSA на основ сп льноти та квадратичне ф нансування (голосування), дисконтован за результатами кореляц ї. Цей трет й спос б часткової та множинної власност уникає Харибди приватного видобутку ренти та Сцилли державного регулювання.

Багато в чому DeFi сьогодн є парадигмою приватної власност , яка зменшується, в дновлюється в мережах, що зростають. Побудований на передумов бездов р'я , DeFi за своєю суттю обмежений сферою повн стю переданої приватної власност (наприклад, переданих токен в), яка здеб льшого об'єднує «usus», «abusus» «fructus». У кращому випадку DeFi ризикує гальмувати зростання мереж за рахунок вилучення ренти, а в г ршому ризикує започаткувати антиутоп чн монопол ї нагляду, де дом нують «кити», як збирають збирають дан в гонц до дна — так само, як web2.

DeSoc перетворює змагання DeFi щодо контролю та спекуляц й на ц нност мереж у координац ю знизу вгору для створення, участ та керування ними. Як м н мум, соц альний субстрат DeSoc може зробити DeFi

ст йкий до sybil (забезпечує управл ння громадою), ст йкий до вамп р в (нтернал зує позитивн зовн шн ефекти для побудови мереж з в дкритим кодом) ст йкий до змов (збер гає децентрал зац ю мереж). Завдяки структурним виправленням DeSoc DeFi може п дтримувати та розширювати множинн мереж , як надають переваги в широких межах — за згодою найр зноман тн ших член в — зам сть того, щоб ще б льше закр плювати мереж , захоплен вузькими нтересами.

Проте найб льшою перевагою DeSoc є його мережева компоновка. Пост йна зростаюча в ддача зростання мереж – це не просто уникнення ризик в вилучення ренти, а й заохочення поширення та перетину вкладених мереж. Дорога може утворювати мережу м ж двома м стами. Але в д рвавшись в д ширшого сп вроб тництва, два м ста, як сп впрацюють, зрештою досягнуть меж зменшення прибутку — або через затори (дороги та житло), або через виснаження (досягаючи обмежень к лькост людей, яким вони можуть обслуговувати). Лише завдяки технолог чним нновац ям та розширенню, хоча й в льне, сп впрац з сус дн ми мережами для нових джерел зб льшення прибутку варт сть може продовжувати зростати в геометричн й прогрес ї. Деяка сп впраця буде ф зичною, поступово розширюючи ф зичну торг влю в космос . Але набагато б льше з'єднань буде нформац йно-цифровими. З часом ми побачимо нов матриц сп впрац м ж ф зичними та цифровими мережами, як залежать в д соц альних взаємозв'язк в, на яких вони побудован , розширюють їх. Саме ця перетинається, частково вкладена структура пост йно зростаючого мережевого сп вроб тництва в цифровому та ф зичному св тах забезпечує DeSoc.

Завдяки створенню мереж та координац ї DeSoc виявляється на перетин пол тики та ринки, доповнюючи обидва соц альн стю. DeSoc розширює бачення JCR Licklider — засновника ARPANET, який створив Інтернет — «симб озу людини та комп'ютера» у «м жгалактичн й комп'ютерн й мереж » з р зко зб льшеною сусп льною динам змом , побудованою на дов р . Зам сть того, щоб будувати на основ бездов рної передумови DeFi, DeSoc кодує мереж дов ри, як лежать в основ реальної економ ки сьогодн , дозволяє нам використовувати їх для створення множинних мережевих товар в, ст йких до захоплення, вилучення або дом нування. Завдяки так й розширен й соц альност , web3 може уникати короткострокової г пер-нанс ал зац ї на користь безмежного майбутнього, що зростаюча в ддача через соц альну дистанц ю.

6.1 Душ можуть потрапити в рай... або в пекло

Хоча ми виб рково вид лили потенц ал, розкритий DeSoc, який ми знаходимо багатооб цяючим, це важливо пам'ятати, що майже будь-яка технолог я з таким трансформац йним потенц алом матиме под бний потенц ал до деструктивної трансформац ї: повторне спалювання; колесо котиться парою; телебачення промиває м зки; автомоб л забруднюють; кредитн картки потрапили в борг тощо. Тут т сам SBT, як можна було б використовувати для компенсац ї внутр шньогрупової динам ки та досягнення сп впрац м ж р зними напрямками, також можна було б використовувати для автоматизац ї «червоної л н ї» несприятливих соц альних груп або нав ть для нац лювання на них для к бер- або ф зичних атак, застосування обмежувальної м грац йної пол тики або брати граб жницьк кредити. Багато з цих можливостей менш пом тн в поточн й екосистем web3, оск льки вони не є значущими поняттями з огляду на поточний субстрат. Включення переваг DeSoc також уможливлює цю шкоду. Так само, як недол ком серце є те, що його можна розбити, недол ком душ є те, що воно може потрапити до пекла, а недол ком сусп льства є те, що сусп льства часто оживлен ненавистю,

упередження, насильство та страх. Людство – це великий часто траг чний експеримент.

Коли ми розм рковуємо про можлив антиутоп ї DeSoc, ми також повинн контекстуал зувати ц можливост в рамках нших технолог чних антиутоп й. Web2 — це арх тектура для непрозорого авторитарного спостереження та соц ального контролю. У той час як web2 часто покладається на штучну бюрократ ю зверху вниз для надання дентиф кац ї ("посв дчення вод я"), DeSoc покладається на горизонтальн ("р вний-р вному") соц альн атестац ї. У той час як DeSoc надає Souls можлив сть кодувати власн стосунки та сп льно створювати множинн властивост , web2 виступає пром жною ланкою в соц альних зв'язках або монетизує їх за допомогою непрозорих алгоритм в, як можуть поляризувати, розд ляти та дез нформувати. DeSoc обходить низх дн , непрозор системи соц ального кредитування. В основ їх лежить Web2. DeSoc розглядає Souls як агент в, тод як web2 розглядає Souls як об'єкти.

Ризик соц ального контролю за допомогою DeFi — без будь-якого субстрату дентичност — менший, принаймн , у найближчим часом. Але у DeFi є своя антиутоп я. Хоча DeFi долає явн форми централ зац ї, коли конкретн суб'єкти мають величезний р вень формальної влади в систем , у нього немає вбудованого способу подолати неявну централ зац ю через змову та ринкову владу. Монопол ї не завжди з'являються як стандартн масла минулого. Змова може статися нав ть на вищих в ддалених р внях екосистеми. Сьогодн ми бачимо це з зростанням класу нституц йних управл нц в активами (наприклад, Vanguard, BlackRock, State Street, Fidelity тощо), як є найб льшими акц онерами вс х найб льших банк в, ав акомпан й, автомоб льних компан й та нших великих галузей промисловост . Оск льки так менеджери актив в мають частку в ус х конкурентах у галуз (тобто частки в кожн й велик й ав акомпан ї), їх стимул полягає в тому, щоб компан ї, якими вони волод ють, виглядали як конкуруюча галузь, але д яли як монопол ст, який максим зує прибуток у вс й галуз та закр плення за споживч та загальнодержавн кошти.

У DeFi також одн й т сам «кити» та венчурн компан ї накопичують б льш частки на кожному р вн стеку та серед конкурент в у стеку, можливо, голосуючи в управл нн токенами або делегуючи його одному класу делегат в, як також однаково корелюють м ж собою. мереж . Без будь-якого соц ального субстрату для опору сиб ли та кореляц йних знижок до примусової децентрал зац ї, ми також повинн оч кувати зб льшення монопол й, як ф нансуються китами, оск льки монопол сти все б льше стають найб льшим пулом доступного нвестиц йного кап талу. Оск льки «грошовий клас» користувач розходяться, ми повинн оч кувати (вже бачимо) все б льший б льший р вень неузгодженост стимул в вилучення ренти. Якщо з'являться програми DeFi, як мають справу з приватними даними, ми ц лком можемо побачити под бну динам ку, наприклад, програми стимулюють в йни м ж к лькома людьми, як «волод ють» даними, як насправд є м жособист сними (наприклад, їхн й соц альний граф к), щоб створити монол тний приватний ШІ, який конкурує з людей, уникаючи майбутнього конкуруючих множинних штучних нтелект в, як доповнюють людей.

Таким чином, DeSoc не обов'язково повинен бути деальним, щоб пройти тест на прийнятно не антиутоп ю; щоб бути парадигмою, яку варто досл джувати, вона просто повинна бути кращою за наявн альтернативи. У той час як DeSoc має можлив антиутоп чн сценар ї, в д яких варто захищатися, web2 снуючий DeFi потрапляють у модел , як неминуче є антиутоп чними, концентруючи владу серед ел ти, яка вир шує соц альн результати або волод є б льшою частиною

[11] Див. Познер, Е. та Вейл, Е. Г., «Розчленування восьминога», Радикальн ринки: викор нення кап тал зму та демократ ї для a Just Society, Princeton University Press, 2018.

багатство. Напрям web2 є детерм нованим авторитарним, що прискорює можливост спостереження зверху та ман пулювання повед нкою. Напрямок сьогодн шнього DeFi ном нально є анархо-кап тал стичним, але в н уже потрапляє п д вплив мереж та монопольний тиск, що ризикує, що його середньостроковий шлях стане авторитарним приблизно так само.

На в дм ну в д цього, DeSoc — це стохастичний соц альний плюрал зм — мережа ндив д в сп льнот, як об'єднуються, будучи нев д'ємними властивостями один одного, сп льно визначають власне майбутнє. Дивлячись на web2, вир ст DeSoc можна пор вняти з п днесенням популярних уряд в, як брали участь у багатов ков й монарх ї. Уряди за участ не неминуче породжували демократ ю; це також призвело до п днесення комун зму та фашизму. Аналог чно, SBT не роблять цифрову нфраструктуру за своєю суттю демократичною, але є демократично сум сною залежно в д того, що Душ та сп льноти сп льно визначають. В дкриття такого простору можливостей є пом тним покращенням у пор внянн з авторитаризмом web2 та анархо-кап тал змом DeFi.

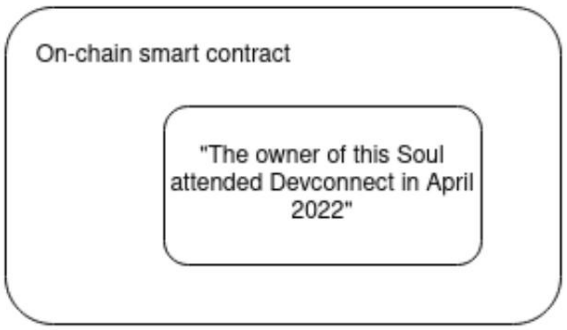
§7 ПРОБЛЕМИ РЕАЛІЗАЦІЇ

Конф денц йн сть є ключовою проблемою для DeSoc. З одного боку, занадто багато публ чних SBT також може виявити багато нформац ї про Душу, що робить її вразливою для соц ального контролю. З ншого боку, занадто багато суто приватних SBT може також призвести до приватних канал в зв'язку, як уникають дисконтування кореляц ї для управл ння та соц альної координац ї, що створює важлив питання сум сност стимул в. З проблемою конф денц йност т сно пов'язана проблема обману: душ можуть нев рно представляти свою соц альну сол дарн сть, координуючи через приватн або поб чн канали. Ми не можемо прагнути знати вс можливост та в дпов д , а натом сть досл джуємо природу виклику й накидаємо к лька перспективних шлях в для майбутн х досл джень.

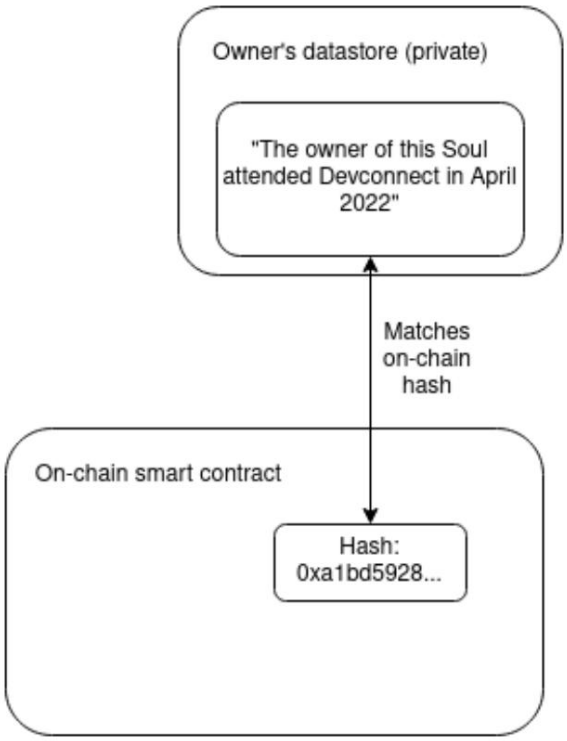
7.1 Приватн душ

Системи на основ блокчейну загальнодоступн за замовчуванням. Будь-як стосунки, як записан в ланцюжку, одразу видно не лише учасникам, а й будь-кому в усьому св т . Певну конф денц йн сть можна зберегти, маючи к лька псевдон м в: с мейна душа, медична душа, профес йна душа, пол тична душа, кожна з яких має р зн SBT. Але якщо зробити це наївно, можна дуже легко сп вв днести ц Душ один з одним.
Насл дки такої в дсутност конф денц йност є серйозними. Справд , без явних заход в, вжитих для захисту конф денц йност , «наївне» бачення простого розм щення вс х SBT в ланцюжку ц лком може оприлюднити занадто багато нформац ї для багатьох додатк в.

Для боротьби з надм рною публ чн стю снує ряд р шень з р зними р внями техн чної складност та функц ональност . Найпрост ший п дх д полягає в тому, що SBT може збер гати дан о-ланцюга, залишаючи лише хеш даних у ланцюжку.



Дан в мереж (повн стю загальнодоступн)



Дан О-ланцюга, хеш-посилання на ланцюжку (Власник вибирає, коли розкривати)

Виб р способу збер гання даних о-ланцюга залишається за людиною; Можлив р шення включають (i) їхн власн пристрої, (ii) хмарну службу, як й вони дов ряють, або (iii) децентрал зован мереж , так як м жпланетна файлова система (IPFS). Збер гання даних o-chain дозволяє нам продовжувати мати смарт-контракти, як надають право записувати дан SBT, але в той же час мають окрем дозволи на читання цих даних. Боб може розкрити вм ст будь-якого з своїх SBT (або сховищ даних, як вони дозволяють) лише тод , коли забажає. Це вже заведе нас досить далеко має додатков переваги у покращенн техн чної масштабованост , оск льки б льш сть даних має оброблятися лише дуже невеликою к льк стю стор н. Але щоб повн стю досягти таких властивостей, як множина конф денц йност , а також б льш ч тких форм розкриття нформац ї, нам потр бно п ти дал . На щастя, багато криптограф чних технолог й дозволяють нам це зробити.

Один потужний наб р буд вельних блок в, який дає нов способи часткового розкриття даних, — це галузь криптограф ї, яка називається «докази нульових знань». Хоча докази з нульовим знанням найчаст ше використовуються сьогодн , щоб забезпечити передачу актив в з збереженням конф денц йност , вони також можуть дозволити людям доводити дов льн твердження, не розкриваючи додаткової нформац ї, кр м самого заяви. Наприклад, у св т , де державн документи та нш атестац ї п ддаються криптограф чному п дтвердженню, хтось може п дтвердити твердження на кшталт «Я громадянин Канади, якому б льше 18 рок в, я маю вищу економ чну осв ту та понад 50 000 п дписник в у Twitter, який ще не претендував на обл ковий запис у ц й систем ».

Докази з нульовим знанням можуть бути обчислен за допомогою SBT, щоб довести характеристики душ (наприклад, що має певн членства). Цю техн ку можна розширити дал , запровадивши багатосторонн обчислювальн методи, так як спотворен схеми, як могли б зробити так тести подв йно приватними: дов дник не розкриває вер єру, хто вони, а вер єр не розкриває св й механ зм перев рки дов рювачу. . Натом сть обидв сторони виконують обчислення разом вивчають лише результат.

Ще одна потужна техн ка - це п дтвердження призначених вериф катор в. Загалом «дан » слизьк : якщо я в дправлю а ф льм для вас, я не можу технолог чно заборонити вам записувати та надсилати його трет й сторон .
Обх дн шляхи, так як керування цифровими правами (DRM), у кращому випадку мають обмежену ефективн сть часто коштують користувачам великих витрат. Проте докази не так ж слизьк . Якщо Амма хоче довести Бобу деяку властив сть X про свої SBT, вона може зробити нульовий доказ твердження «Я волод ю SBT, як задовольняють властив сть X, АБО я маю ключ доступу до душ Боба». Боб знайшов би це твердження переконливим: в н знає, що в н не зробив докази, тому Амма насправд повинна мати SBT, як задовольняють властив сть X. Але якщо Боб передасть доказ Куйфену, Кейфен не буде переконаний: незважаючи на все, що в н знає, Боб м г би зробити доказ за допомогою власного ключа. Це можна зробити ще сильн ше за допомогою перев рених функц й затримки (VDF): Амма може зробити та представити докази, як можна зробити лише за допомогою необх дних SBT прямо зараз, але будь-хто нший зможе зробити через п'ять хвилин. Це означає, що можна представляти складн дозволи доступу до над йних доказ в даних , незважаючи на неможлив сть надати так ж виборч дозволи до самих необроблених даних, як можна просто скоп ювати та вставити. Проте це може завести нас досить далеко. Под бно до того, як блокчейни забезпечують можлив сть в дстеження в транзакц ях, що не дозволяє комусь клацнути правою кнопкою миш , скоп ювати та вставити ц нний NFT (sybil, атакуючи ориг нального власника), так само SBT можуть забезпечувати в дстеження в соц альному запоб ганн , що як м н мум може знизити ц нн сть коп ювання. вставлен дан з неперев реним походженням.

Ц дан о-ланцюга та методи нульового знання сум сн з негативом репутац я — SBT, як стають видимими, нав ть якщо власник не хоче , щоб вони були видимими. Важливими прикладами негативної репутац ї є кредитна стор я, дан про непогашен кредити, негативн в дгуки та скарги в д б знес-партнер в, а також SBT, що п дтверджують соц альн зв'язки, що мають значення для координац ї.
Блокчейни в поєднанн з такою ж криптограф єю можуть стати потенц йним р шенням: лог ка розумних контракт в може змусити Souls включати негативн SBT в структуру даних, як-от дерево Меркла , яке збер гається я о-ланцюжком, будь-як докази нульових знань або спотворен обчислення ланцюга вимагатимуть їм ввести цю нформац ю, тому що в ншому випадку в наданих даних була б видима «д рка», яку б розп знавав вер єр. Протокол Unirep є прикладом того, як це можна реал зувати.

Сенс цих приклад в не в тому, щоб показати, як саме можна використовувати криптограф чн технолог ї вир шити вс проблеми з конф денц йн стю та дозволами на дан за допомогою SBT. Скор ше, це накреслити к лька приклад в, щоб показати силу таких технолог й. Важливим напрямком майбутн х досл джень є визначення точних меж р зних вид в дозвол в на дан та специф чних комб нац й метод в, як працюють.

найкраще досягти бажаного р вня дозвол в. Інше питання полягає в тому, як типи режим в множинної власност бажан для управл нння даними як правильно розд лити права доступу (“usus”), редагування (“abusus”) та грошових кошт в (“fructus”).

7.2 Обман душ

Якщо SBT є соц альним субстратом, на якому координується множинна власн сть, мережев товари та нтелект, можна занепокоїтися тим, що Souls спробують обдурити або обдурити св й шлях до сп льнот, щоб отримати доступ до управл нння чи прав власност , як , як ми уявляємо, дозволять SBT. Наприклад, якщо багато заявок залежать в д SBT, як представляють участь у конференц ї, недобросов сн конференц ї можуть отримати так SBT в обм н на хабар . Маючи достатню к льк сть хабар в, люди (боти) можуть створити фальшивий соц альний граф к, який зробить обл ковий запис схожим на справжню людську душу, багато диференц йовану (п дробленими) SBT. Так само, як DAO можна п дкупити, так само можна п дкупити душ та механ зми голосування в мереж , як вони використовують. І навпаки, якщо SBT використовуються для зниження координац ї, Душ можуть уникати SBT, щоб максим зувати їх вплив. Чому ми повинн в рити, що SBTs a Soul волод ють точно в дображають свої справжн соц альн зобов’язання, а не просто те, як вони вибирають грати в цю гру?

Один з аргумент в полягає в тому, що р зн стимули до шахрайства можуть «збалансувати». Душ можуть в дсортувати та само дентиф куватися в мережах, як важлив для них, у правильному масштаб , под бно до того, як податки Harberger вр вноважують стимули до завищеної та заниженої вартост актив в, щоб отримати приблизно точн ринков оц нки. Душ захочуть мати б льше SBT, щоб отримати вплив у своїх сп льнотах, але, з ншого боку, будуть уникати SBT в д сп льнот, про як вони не п клуються, щоб отримати нижч результати за показниками кореляц ї та зб льшити св й вплив на управл нння б льш широкими мережами.

Але було б наївно вважати, що два стимули — отримати доступ максим зувати вплив—завжди р вном рно скасовується або нав ть наближається до скасування, як за допомогою маг ї. Може бути багато сп льнот, як використовують нш системи, н ж SBT, для доступу та управл нння. Або ж громади можуть — всупереч нашим основним припущенням про публ чн сть — роздавати приватн SBT для захисту прав управл нння, але спонукати член в сп льноти збер гати ц SBT в таємниц п д час прийняття б льш широких р шень.

Не варто недооц нювати проблему « гор». Це важлива проблема, її вир шення є одним з найважлив ших напрямк в майбутн х досл джень. Справд , це головна причина, чому в дкрити багато снуючих алгоритм в, як визначають пр оритети або ф льтрують для людей-користувач в, дуже складно. Щоб пом’якшити стримувати SBT гри, ми пропонуємо к лька норм криптограф чних напрямк в:

1. Екосистема SBT може завантажити «товст » канали сп льноти, де сигнал SBT справжнє членство в сп льнот o-chain з м цними соц альними зв’язками та повторюваними взаємод ями. Це полегшило б сп льнотам ф льтрац ю та скасування SBT м татор в бот в. Так товст канали, як ми часто знаходимо в церквах, на робочих м сцях, у школах, групах зустр чей та в орган зац ях у громадянському сусп льств , стали б б льш ст йким до сиб л соц альним субстратом для пол цейських гор.

(наприклад, через бот в, хабар , видавання себе за ншу особу) у б льш «тонких» соц альних каналах.

2. Вкладен сп льноти можуть вимагати, щоб SBT нав'язували контекст потенц йним векторам змови «просто нижче» ними. Наприклад, якщо штат проводить раунд ф нансування або голосування, держава може вимагати в д кожного громадянина, який бере участь, також мати SBT округу та мун ципал тету.

3. В дкрит сть криптограф чна доказов сть екосистеми SBT сама по соб може бути використана для активного виявлення шаблон в змови та покарання за неавтентичну повед нку — можливо, зневажаючи право голосу Душ, як змовилися, або зобов'язуючи Душ приймати SBT, що представляють негативн атестац ї. Наприклад, якщо одна Душа засв дчує людян сть ншої Душ , яка виявляється ботом, справу можна розширити та публ чно перев рити, що призведе до того, що ця Душа має велику к льк сть негативних п дтверджень. Це вже певною м рою в дбувається в екосистем GitCoin QF, де використовується ряд сигнал в для виявлення «груп змови».

4. Технолог я ZK (наприклад, MACI) може криптограф чно запоб гти деяким атестац ям, зробленим душою в д доказовост . Це зробило б спроби продати певн види атестат в недостов рними, оск льки хабарник не мав би можливост визначити, чи виконував одержувач хабара на їхньому боц угоди. Було проведено велику к льк сть досл джень щодо використання таких метод в для голосування, але в к нцевому п дсумку будь-який неф нансований соц альний механ зм може в к нцевому п дсумку отримати користь в д под бних дей.

5. Ми могли б заохочувати викривач в як спос б зробити змову значного розм ру нестаб льною.
Зам сть того, щоб виявляти та карати неправильну чи образливу повед нку, ми виявляємо та караємо образи зловживань . Цю техн ку ризиковано зловживати через можлив сть отримання хабар в фальшивого п дходу, але вона, тим не менш, є частиною набору нструмент в.

6. Ми могли б використовувати механ зми з теор ї прогнозування однол тк в, щоб заохочувати зв тн сть бути чесною у вс х випадках, кр м випадк в, коли змова надзвичайно велика. Зам сть того, щоб конференц я п дтверджувала присутн сть учасник в, учасники могли засв дчувати присутн сть один одного , тому к льк сть учасник в, яких потр бно було б п дкупити, щоб п дтвердити неправдиву заяву, стає дуже великою. Винагороди не обов'язково мають бути ф нансовими, але можуть бути SBT, що робить винагороду б льш корисною для справжн х член в сп льноти, н ж для зловмисник в.

7. Ми могли б використовувати показники кореляц ї, як зосереджуються на кореляц ї, де є великий стимул бути чесним, якщо група душ под ляє сп льн нтереси. Наприклад, техн ка кореляц ї, яка використовується в обмеженому попарному квадратурному ф нансуванн , використовує сам квадратичн ф нансов пожертвування, щоб визначити, наск льки корелюють два учасники, , отже, на ск льки знижувати їх перетин. Якщо два учасники мають багато сп льних нтерес в, їх стимул висловлювати цей факт механ зму QF, безумовно, зменшується з дисконтуванням кореляц ї, але в н н коли не стає нульовим або негативним.

§8 ПОРІВНЯННЯ ТА ОБМЕЖЕННЯ

Хоча д апазон пропонованих структур дентичност майже безмежний, є чотири особливо пом тн та сум жн парадигми, як широко обговорюються в простор web3, як заслуговують на пор вняння: дом нуюча «спадкова» екосистема дентичност , псевдон мна економ ка, п дтвердження особистост та справжн дан .
Кожна парадигма висв тлює важливий внесок виклики для майбутнього розвитку парадигми соц альної дентичност , яку ми в дстоюємо, ми використовуємо так обмеження як плацдарм для вивчення майбутн х напрямк в.
Враховуючи все це, ми також пояснюємо, чому вважаємо, що наш прим тиви соц альної дентичност , так як Souls soulbound токени, є б льш перспективним шляхом для режим в конф денц йност .

8.1 Спадщина

Застар л системи дентиф кац ї покладаються на папери або посв дчення особи, видан та за посередництвом третьої сторони (уряд, ун верситет, роботодавець тощо). Походження встановлюється шляхом виклику третьої сторони для п дтвердження.
Незважаючи на те, що застар ла система має ц кавий наб р властивостей, як ми повинн зрозум ти глибше, так системи вкрай неефективн не п ддаються компонування або обчислення для швидкої та ефективної координац ї. Б льше того, цим системам не вистачає соц ального контексту, тому Souls покладається на централ зовану третю сторону для п дтвердження членства в сп льнот , а не на вбудовану сп льноту. Наприклад, б льш сть виданих державою посв дчень особи в к нцевому п дсумку простежуються за св доцтвом про народження, виданим за дорученням л каря та член в с м'ї, як є остаточним джерелом стини не враховують багато однаково значущих соц альних зв'язк в, як , разом узят , мають набагато сильн ше п дтвердження. .
Насправд , коли центри зосередженої влади прагнуть достов рної дентиф кац ї (наприклад, отримати дозв л в д великого уряду), вони р дко покладаються на так документи, зам сть цього звертаються до нтерв'ю в соц альних мережах. Таким чином, так застар л системи дентиф кац ї мають тенденц ю зосереджувати владу в ем тент та в тих, хто може провести належну ретельн сть, щоб отримати б льш над йну перев рку, як , у свою чергу, стають розпачливою та ненад йною бюрократ єю.
Важливою метою дизайну DeSoc є забезпечення того, щоб вимоги безпеки державних дентиф катор в могли бути виконан та перевищен , дозволяючи горизонтальним мережам зробити б льший р вень безпеки доступним для вс х користувач в через низку соц альних субстрат в.

8.2 Псевдон мна економ ка

Бачення сусп льства, засноване на поєднанн систем репутац ї з нульовим доказом знань
Механ зми збереження конф денц йност найб льш широко пропагував Баладж Ср н васан, який придумав популяризував фразу «псевдон мна економ ка». Його рання верс я наголошує на використанн псевдон м в, щоб уникнути дискрим нац ї та уникнути «культури скасування» соц альними натовпами, як прагнуть зашкодити репутац ї людини та роз рвати їхн соц альн зв'язки. В н передбачає, що люди накопичують у своїх гаманцях атестац ї з нульовою нформац єю (ZK), як можна передати, ухилятися в д репутац йних атак шляхом перенесення певної к лькост атестац й на нов гаманц або розд лення атестац й м ж к лькома гаманцями, мов рно, без в дстеження . Вибравши атестац ї на перенесення, людина вибирає бажаний р вень псевдон мност в новому обл ковому запис , зважуючи м ж б льшою анон мн стю (перенесення меншої к лькост атестац й) або б льшим поширенням у своїй соц альн й мереж (перенесення б льшої

атестац ї).

Практична р зниця м ж типовими псевдон мними економ чними пропозиц ями та DeSoc полягає в тому, що ми не прид ляємо уваги под лу дентичностей як основного способу захисту учасник в в д зловживань та скасування культури. Певний р вень под лу (наприклад, р зн Душ м ж с м'єю, роботою, пол тикою тощо) може бути здоровим, але загалом покладатися на здатн сть створювати нов особистост як основну милицю проти напад в має велик недол ки. Це ускладнює ставку на репутац ю для позик походження, а також погано поєднує механ зми управл ння, як намагаються виправити кореляц ї або Сиб ли.

Зам сть того, щоб захищати жертв, дозволяючи їм знову виходити з атак з новою (якщо зменшеною) особист стю, DeSoc дозволить використовувати нш п дходи, наприклад, контекстуал зац ю нападника. «Скасування» часто виникає саме через те, що заяви та д ї вирван з контексту, а в русн сигнали проходять через неконтекстуальн мереж , коли людина або бот не мають соц ального зв'язку чи контексту з жертвою. Под бно до того, як SBT забезпечують походження для захисту в д глибоких п дробок, карта SBT соц ально в дображає походження «х т-частини». «Х тов фрагменти» по сут — це артефакти, що виникають за межами сп льнот жертви (як показують сп льн членства в SBT) або не мають сертиф кат в SBT в д сп льнот жертви — що має поставити п д сумн в правдив сть твору. SBT також дають можлив сть жертвам почати захисну в дпов дь для протид ї удару, куратором поширеним з їхньої мереж дов ри (представлено тут моделями сп льного утримання SBT). Збер гаючи соц альний контекст, люди можуть п дтримувати дов ру, нав ть якщо їм загрожує скасування, притягувати зловмисник в до в дпов дальност . Пол пшення походження покращує соц альну основу стини.

8.3 Доказ особи (PoP)

Протоколи Proof of Personhood (PoP) мають на мет надати маркери ндив дуальної ун кальност , щоб запоб гти Sybil атакує та дозволяє неф нансован програми. Для цього вони покладаються на так п дходи, як глобальний анал з соц альних граф к в, б ометричн дан , одночасн глобальн ключов сторони або їхня комб нац я . Однак, оск льки протоколи PoP прагнуть представляти ндив дуальн дентичност — зосереджен на досягненн глобальної ун кальност — зам сть того , щоб соц альн дентичност в дображали в дносини та сол дарн сть, протоколи PoP обмежен додатками, як однаково ставляться до вс х людей. Б льш сть додатк в, як нас ц кавлять, наприклад, репутац я, є реляц йними виходять за меж ун кальност людини до диференц йованої людини.

Кр м того, протоколи PoP не захищен в д атак сиб ли. Майже у вс х передбачуваних на найближчу перспективу програмах PoP системи ефективно в дкрит для атак Sybil, лише за трохи вищою ц ною. Якщо б льш сть людей на планет не зареєстрован в служб PoP не беруть участь у певн й перев рц , зловмисник завжди може завербувати незац кавлених людей, як ще не беруть участ , щоб д яти як Сиб ли. Хоча так найманц не зовс м боти, в дм нност є надважливими, кр м, можливо, невеликих додаткових витрат.

Багато протокол в PoP мають на мет створити основу для ун версального базового доходу або глобальної демократ ї. Поки

ми не под ляємо однаков амб ц ї, так протоколи спонукали нас, тим не менш, подумати про те, як поступово розвиватися до координац ї множинних мережевих товар в. На в дм ну в д б нарної, ндив дуал стичної та глобальної природи PoP, наш п дх д має на мет створити багатий, контекстуальний багатошаровий субстрат для репутац ї знизу вгору, власност та управл ння, що дозволяє брати участь у низц сп льнот мереж, малих великих.

8.4 Істинн обл ков дан

Veriable credentials (VC) — це стандарт W3C, де обл ков дан (або атестац ї) доступн для сп льного використання zk на розсуд власника. VC п дкреслюють основн обмеження нашої базової парадигми конф денц йност та мотивують наше обговорення розширень конф денц йност вище. До тих п р, поки SBT не мають розширення конф денц йност , як звужують публ чн сть, VC SBT можна розглядати як природн доповнення: зокрема, SBT спочатку є загальнодоступними, що робить їх непридатними для конф денц йної нформац ї, як-от державна дентиф кац я, тод як реал зац ї VC боролися з парадигмою в дновлення, яку можна було б вир шується шляхом в дновлення громади.
Об'єднан два п дходи в найближч й перспектив можуть бути сильн шими, н ж будь-який окремо. Але венчурн компан ї також мають ключове обмеження: принаймн у своїй стандартизован й форм венчурн компан ї не п дтримують б льш сть перерахованих нами програм через їх односторонню конф денц йн сть.

Односторонн й сп льний доступ до zk не сум сний з заохоченнями з нашими випадками використання, а також не в дпов дає нашим нормам щодо конф денц йност . Б льш сть наших програм залежить в д певного р вня публ чност . Але в рамках zk-sharing Souls не можуть знати, що нша Душа волод є SBT, якщо вона не надається їм, що робить неможливим отримання репутац ї, над йних зобов'язань, управл ння, ст йкого до сиб лл, простих договор в оренди (наприклад, оренди квартири). п дстава, оск льки нш зобов'язання та обтяження не обов'язково видно. Б льш глибоко, ми скептично ставимося до того, що одностороння можлив сть сп льного використання зазвичай є правильною парадигмою конф денц йност . Р дко одна сторона у багатосторонн х в дносинах має одностороннє право розкривати в дносини без згоди ншої. Под бно до того, як приватна власн сть, що передається в односторонньому порядку, не є режимом багатої власност , спрощена одностороння сп льна власн сть не є дуже багатим режимом конф денц йност . Якщо дв сторони сп льно волод ють активом вир шують представляти свої стосунки через венчурний кап тал, так обл ков дан не допускають взаємної згоди та взаємних дозвол в.
Ця проблема стосується б льш складних випадк в множинної власност та складних орган зац йних форм дозвол в, як є особлив стю DeSoc.

§9 НАРОДЖЕННЯ ДУШІ

Шлях в д нин шньої екосистеми web3 до розширеної соц альност , опосередкованої SBT, стикається з класичною проблемою холодного старту. З одного боку, SBT не п длягають передач . З ншого боку, сьогодн шнє поєднання гаманц в не може бути к нцевим домом для SBT, оск льки в них в дсутн механ зми в дновлення сп льноти. Але для того, щоб гаманц для в дновлення сп льноти працювали, їм потр бен широкий виб р SBT в окремих сп льнотах, щоб бути безпечними. Що перше: SBT або в дновлення громади? Хто так сп льноти ранн х усиновлювач в? Як взаємод ють SBT в р зних ланцюгах? Ми не можемо прагнути знати вс можливост та в дпов д , але

натом сть намалюйте к лька перспективних шлях в для подальшого вивчення читача в рамках поточної арх тектури web3 нав ть web2.

9.1 Прото SBT

Хоча в дм нною рисою SBT є непередаван сть, SBT також можуть мати ншу властив сть, яка може виявитися б льш корисним для завантаження: в дкликання. Ц лком можливо, що SBT спочатку зароджуються як токени, що можуть бути в дкликан , а пот м переростають у непередаван . Токен можна в дкликати, якщо ем тент може спалити токен повторно випустити його на новий гаманець. Спалювання та повторна видача матиме сенс, якщо, наприклад, ключ втрачен або зламан , а ем тент зац кавлений у тому, щоб токени не були ф нансован та не продан сторон — ншими словами, коли токен сигнал зує про справжнє членство в сп льнот . . Роботодавц , церкви, групи зустр чей, клуби з повторюваними взаємод ями о-chain мають хорош можливост для запису та перевипуску токен в, оск льки вони мають стосунки з особою, можуть легко перев рити, чи не видають себе за ншу особу за допомогою телефонного дзв нка, в деоконференц ї або проста зустр ч особисто. Поодинок взаємод ї, так як в дв дування концерту чи конференц ї, погано п дходять, оск льки зв'язки з громадою слабк ш .

В дкликан , передан токени — це свого роду прото-SBT, як виконують п дтримуючу функц ю плаценти до народження Душ . Ц токени виграють час як для гаманц в, щоб започаткувати безпечн механ зми в дновлення сп льноти, так для того, щоб людина могла накопичити прото-SBT, як в к нцевому п дсумку можуть бути спален та повторно видан в непередаван SBT. П д цим шляхом не виникає питання: «Що станеться спочатку: SBT чи в дновлення громади?» Швидше, SBT в дновлення сп льноти створюються одночасно, народжуючи Душу.

9.2 Гаманц для в дновлення сп льноти

Хоча сучасним гаманцям бракує в дновлення сп льноти, кожен з них має в дносн сильн та слабк сторони у тому, що вони є дом вками — або, можливо, гестац йними матками — для SBT. Протоколи Proof of Personhood (PoP) мають перевагу, оск льки вже експериментують з механ змами вир шення соц альних суперечок, як є основою в дновлення громади. Кр м того, багато DAO використовують PoP для полегшення управл ння, що робить їх першими ем тентами SBT. Однак, незважаючи на природну перевагу PoP, протоколи PoP ще не заслужили широкої дов ри до розм щення ц нних токен-актив в, в той час як кастод альн гаманц мають.

Таким чином, кастод альн гаманц , незважаючи на їх страхи централ зац ї, можуть бути природною платформою для менших витрат. досв дчен роздр бн користувач . Так кастод альн гаманц також можуть створювати нструменти для роздр бних сп льнот для випуску в дкликаних токен в, як згодом перетворюються (або записуються та перевидаються) у SBT або нав ть нструменти для б льш «корпоративних» ем тент в, багато з яких шукають способи створити базу лояльних кл єнт в у web3, але в дсутн сть досв ду в утриманн . П сля того, як механ зми в дновлення сп льноти будуть формал зован та випробуван в бою, ц гаманц збер гання можуть децентрал зуватись у в дновленн сп льноти, тод як збер гач перейдуть до надання нших ц нних послуг у DeSoc (наприклад, управл ння сп льнотою, випуск SBT тощо).

Для б льш досв дчених користувач в Web3 децентрал зован гаманц без збер гання (або соц альн гаманц в дновлення, так як Argent Loopring) є природною в дправною точкою для сп льноти завантаження

механ зми в дновлення. Незалежн гаманц мають перевагу в тому, що вони є в дкритим вих дним кодом web3, а також мають можлив сть попередньо оголошувати та експериментувати з механ змами поступово до п дгрупи добров льних, досв дчених користувач в, щоб протестувати стимули та зм шувати механ зми (наприклад, к лька п дпис в). Ус ц п дходи — PoP, збер гання та не утримання — в д грають важливу роль у експериментуванн та адаптац ї користувач в з р зним ступенем витонченост та терпимост до ризику.

9.3 Прото-души

Норми також можуть спонукати Душ до снування. Коли ми переосмислюємо токени та гаманц , ми також можемо зм нити своє уявлення про певн класи NFT та токен в, як призначен для сигналу про членство. Зокрема, ми можемо запровадити норму не передавати NFT та POAP, виданих авторитетними установами, як залежать в д в дв дування конференц ї, досв ду роботи чи осв тн х документ в. Так передач токен в членства — якщо їх торгувати за варт стю — можуть зменшити репутац ю гаманця , можливо, в дбити охоту ем тент в в д подальшої видач токен в членства або POAP для цього гаманця. Вже в екосистем без збер гання значна к льк сть користувач в досягли значної ф нансової репутац ї та частки у своїх гаманцях, як могли б стати ефективним забезпеченням для них, щоб не зловживати оч куваннями щодо непередаваност .

Хоча вс ц шляхи мають в дпов дн проблеми, ми спод ваємося, що р зноман тн сть п дход в зб льшується шанс зближення до нашого кваз р вноважного стану в середньостроков й перспектив через невеликий наб р крок в.

§10 ВИСНОВОК

Як би ми не були амб тними в уяв , що DeSoc може дати, багато в чому вищенаведене т льки перш кроки. Існує б льше н ж одна дорога до DeSoc, включаючи ряд фреймворк в, не заснованих на блокчейн , таких як Spritely, ACDC Backchannel , як покладаються на сховища даних, прив'язан до локальних машин, а не до глобальних реєстр в. Згодом ц структури можуть викликати ще б льшу дов ру через соц альну дистанц ю, оск льки вони можуть використовувати транзитивн сть дов рчих стосунк в — наприклад, дов рене знайомство — зам сть того, щоб покладатися на SBT, видан в домими, високостатусними установами (наприклад, ун верситетами чи DAO). Б льше того, програми, як ми описуємо вище, є лише початком того, що може надати DeSoc, не торкаючись в ртуальних св т в: їх ф зики, усп льства та їх складного перетину з ф зичним св том. Усе це говорить про те, що нав ть т широк амб ц ї, як ми малюємо вище, — це лише початок того, чим може стати DeSoc.

Однак на цьому шляху залишається багато виклик в в дкритих питань. Наведен вище еск зи вимагають велика к льк сть червоних команд, багато з них є б льше натякаючими, н ж повн стю наказовими. Як DAO можуть п дтримувати публ чн сть свого стану, вдумливо пор внюючи шаблони душ кореляц ї в SBT, щоб забезпечити захист децентрал зац ю Сиб ли? Наск льки сум сним є стимулювання придбання SBT в умовах р зних схем кореляц йного дисконтування? Наск льки конф денц йн сть узгоджується з кореляц йним дисконтуванням та ншими механ змами DeSoc? Як ми можемо вим ряти нер вн сть соц альним водночас належним чином приватним (контекстуально ц л сним) способом? Як має працювати спадкування в рамках в дновлення громади? Чи снують червон л н ї, як можна провести або нав ть записати в протоколи, щоб уникнути антиутоп чних сценар їв?
Або ми повинн просто змагатися за створення найкращих сценар їв для початку? Ц питання лише початок того, що ми

Оч кується, що це програма досл джень, що охоплюють роки, як будуть розвиватися разом з екосистемою DeSoc.

Проте потенц ал, який має DeSoc, здається, не просто вартий ц ни нав гац ї в цих складних викликах, але, можливо, необх дний для забезпечення нашого виживання. Альберт Ейнштейн сказав на конференц ї з роззброєння 1932 року, що невдач «орган зуючої сили людини» йти в ногу з «його техн чними досягненнями» поклали «бритву в руки 3-р чної дитини». У св т , де його спостереження здається б льш прозорливим, н ж будь-коли, навчитися програмувати майбутнє, яке кодує соц альн сть, — а не писати над дов рою — здається необх дним курсом для збереження людського життя на ц й планет .

ДОДАТОК

Коригування квадратичних механ зм в для попередньої сп впрац

Оск льки квадратичн механ зми спонукають до сп впрац з базової л н ї егоїзму, вони вразлив для груп, як вже сп впрацюють. Якщо SBT в дгукуються про членство в сп льнот , яке визначає душу, щоб в дображати її упереджен сть, SBT можуть допомогти нам в дмовитися в д попередньої сп впрац схилити ваги на користь сп впрац через в дм нност . Тут ми надаємо люстрац ю першої спроби оновленої квадратичної модел та подальш напрямки досл джень. Цей механ зм не оптим зований , безсумн вно, має вразлив м сця; в н призначений як люстративний приклад для стимулювання експеримент в майбутн х досл джень. Хоча ми люструємо квадратичне ф нансування (QF), т сам принципи та формули також застосовуються до квадратичного голосування (де окрем внески просто зам нюються голосовими кредитами).

У QF сп льнота сп вставляє ндив дуальн внески в сп льн проекти з коштами пропорц йно до квадрата суми квадратних корен в ндив дуальних внеск в. Для ф ксованих р вн в внеск в в дпов дн фонди ростуть як квадрат к лькост ндив дуальних внеск в, але мають спадну в ддачу в д ндив дуальних внеск в. В ддача в д концентрованих ндив дуальних д й зменшується, але в д колективних д й зростає. Наприклад, якщо Абду, Шоу та Белль були особами, як не сп впрацювали — в дпов дно внески та грошов одиниц — QF (наприклад, Gitcoin Grants) кошти, що в дпов дають їм, мають бути пропорц йним у програм (з масштабуванням, визначеним наявними коштами). до квадрата суми квадратних корен в ндив дуальних пожертв.

$$h \sim (\sqrt{\ } + \sqrt{\ } + \sqrt{\ })^2 \quad (+ +)$$

Єдине членство

Тепер припустимо спрощену модель, де Абду, Шоу Белль в др зняються одним членством — робочим м сцем — в дпов дн кошти доступн для стартап в, компан й проект в з в дкритим кодом (знову ж таки, в дус Gitcoin). Оск льки люди з одного робочого м сця мають сильний стимул робити внесок у власне робоче м сце, щоб максим зувати в дпов дн кошти для своєї компан ї, ми повинн оч кувати, що вони координуватимуть. Крайн м п дходом було б вважати, що прац вники повн стю под ляють ц л та повн стю координують свою повед нку. Але нав ть у цьому простому випадку снує к лька способ в компенсац ї у формул .

Простий п дх д, який ми називаємо «кластеризац єю», пом стить двох сп вроб тник в «п д той самий квадратний кор нь» у квадратичн й формул , щоб виявити їх тенденц ю до вже координац ї. Якби Абду Шоу були колегами (але не Белль), внесок Абду Шоу був би п дсумований квадратний кор нь разом, тод як внесок Боба мав би квадратний кор нь окремо, ефективно даючи його внесок б льше

вага:

$$h \sim \sqrt{(+)}^{2}$$

Якщо Абду Шоу деально скоординован , для них завжди оптимально розд лити св й сп льний внесок однаково, тому ми можемо вважати = , дозволяючи нам спростити:

$$= (2\sqrt{+}) \quad \sqrt{}^{2} \quad (2+)$$

У цьому випадку легко побачити, як кластеризац я призводить до оптимальност (або максим зац ї добробуту) тим самим аргумент щодо QF у б льш загальному вигляд : якщо Абду Шоу деально скоординован , вони ефективно д ють як один агент формула кластеризац ї є формулою QF для двох агент в — сп льного Абду-Шоу агент агент Belle.

Інше коригування, яке також досягає оптимальност , - це те, що ми називаємо «В дпов дн сть налаштування»:

$$h \sim \left(\frac{\sqrt{}+\sqrt{}}{\sqrt{2}} + \sqrt{}\right)^{2}$$

Причина в матч Осетт нга полягає в тому, що Абду Шоу є частиною деального координуючи групу розм ру 2, ми можемо зменшити вагу їхн х голос в у 2 рази, √щоб компенсувати це координац я. Це призводить до того ж результату, що й кластерний зб г, оск льки в н завжди є оптимальним для а деально скоординован Абду Шоу (=), щоб зробити р вний внесок в цьому випадку

$$h \sim \left(\frac{\sqrt{}+\sqrt{}}{\sqrt{2}} + \sqrt{}\right)^{2}$$

$$= (2\sqrt{+}) \quad \sqrt{}^{2} \quad (2+)$$

Багаторазове членство

Попередн й приклад передбачає, що Абду, Шоу Белль мають єдине членство: робоче м сце. Ще в майже для вс х додатк в це було б значним спрощенням. Люди мають багато сп льнот членство, кооперативн в дносини нав ть неформальн перетини. Абду Белль можуть бути продовжен с м'ї, Шоу Белль могли в дв дувати одну школу, або Шоу Абду могли бути власниками жетон в той самий протокол р вня 1 тощо. Щоб полегшити сп впрацю м ж р зними в дм нностями, ц кореляц ї в членство м ж особами має визнаватися менш б нарним чином. Зараз розглядаємо

розширюючи кожен з наведених вище п дход в для цього. Ми знову зосередимося на найпрост шому приклад поставити суть; нижче ми розглянемо б льш загальн формули.

Ми зосередимося на приклад , коли Абду Шоу под ляють схож сть, Абду Белль под ляють р зне Aliation, а Shou має зв'язок з групою, яка включає нших член в, але н хто з них не бере участ цей в дпов дний раунд. Це повний наб р ал мент в.

Щоб розширити в дпов дн сть кластера на цей випадок, ми включаємо кластер для кожної групи сп льних псевдон м в розпод лити внески кожної особи м ж ус ма групами, в яких вони беруть участь пор вну коеф ц єнти на їхн внески, що становлять одиницю.

$$h \sim \left(\sqrt{\frac{}{2} + \frac{}{2}} + \sqrt{\frac{}{2} + +} \quad \sqrt{\frac{}{2}}\right)^2$$

Щоб продовжити Oset Match, ми повинн розрахувати коеф ц єнти на внесок кожного ндив да компенсувати координац ю, яка приносить користь ц й людин . Зокрема, якщо припустити, що Белль пол нтернал зує ц нн сть Абду, що Абду наполовину засвоює Белль, а чверть нтернал зує ц нн сть Шоу та Шоу чверть нтернал зує Абду, тод нам потр бно знайти коеф ц єнти вир шення

$$\alpha + \frac{\alpha}{2} + \frac{\alpha}{4} = 1$$

$$\alpha + \frac{\alpha}{2} = 1$$

$$\alpha + \frac{\alpha}{4} = 1$$

Розв'язком цього р вняння є $\alpha = \frac{4}{11}$, $\alpha = \frac{9}{11}$, $\alpha = \frac{10}{11}$. Так

$$h \sim \left(\sqrt{\frac{4}{11}} + \sqrt{\frac{9}{11}} + \sqrt{\frac{10}{11}}\right)^2$$

Oset Match, хоча в певному сенс найпрост ший, є майже найб льш непрозорим, приписуючи кожному ндив дуальна вага, що залежить в д її соц альної центральност , яка визначає владу, яку це надає.

Загальн формули

Для кожної особи = 1, ... визначимо к льк сть алиац й, як вона має як ; загалом ми може надавати р зну вагу р зним алиац ям, але нараз ми припускаємо, що вс вони р вн . Нехай Σ є сукупн сть ус х «груп об'єднання», проект в множини власник в даного об'єднання на множину учасник в

|

Σ | 1 .
=1

2

σ |

| —

Σ | √
=1 =1 =1

|

Σ | 1 σ 1 σ
=1

,

,

2

(√)
=1 =1

12

2

+

2

+

[12] Ориг нальний опис дещо в др зняється тим, що в н використовує M зам сть 2M. Техн чно, 2M є правильним, якщо п дсумувати невпорядкованих пар агент в, M є правильним, якщо п дсумовувати впорядкован пари. Тут ми п дсумовуємо невпорядкован пари.

Ключовою метою розробки ц єї формули було обмежити втрати в д неправильного визначення змови групи як незалежн агенти. У Simple Matching втрати безмежн : п дроблен або змовн агенти п д контролем одного того ж реального актора, кожен може зробити внесок у фейковий проект отримати субсид ю * (2) · У Cluster Matching под бне необмежене вилучення можливе, якщо кластеризац я Механ зм помилково визначає нав ть одну змову групу як абсолютно незалежну. У пар Узгодження, навпаки, втрат в д п дроблених або змовних агент в завжди обмежен зверху символом 2) , * (де – параметр системи.

Зауважте, що парна в дпов дн сть не досягає оптимальност : учасники змови все ще мають стимул для цього дещо завищують, наск льки вони оц нюють певн проекти, нав ть можуть отримати певн кошти сприяння фейковому проекту, який вони контролюють. Скор ше, цей п дх д має бути а другий найкращий, оптим зований для випадку, коли доступна обмежена зовн шня нформац я про те, як актори фактично в змов .

Тим не менш, парна в дпов дн сть може бути використана як ф лософський шаблон для того, як врахувати снуюча координац я без надм рного покарання: зам сть кореляц йної оц нки лише включно значення для ц єї конкретної квадратичної системи ф нансування, можна спробувати включити под бн терм ни для вс х випадк в, коли ц дв особи отримували вигоду в д сп впрац . Якщо вигоди в д сп впрац є якщо правильно оц нити, подальша сп впраця н коли не зашкодить жодн й пар агент в; скор ше, чистий прибуток в д подальшої сп впрац просто наблизиться до нуля.