Не только изучаю сам, но и провожу мета-анализ: https://docs.google.com/document/d/10tyaCFpQ3Q3JkT69GsdJCKWghEDyqWNI0e1eYM6Cpc8/edit#

Тенденция №01. Распределение на уровне L1 происходит совершенно не так, как его видят массы в период хайпа. Поясню:

- **Solana**, о которой ещё поговорим ниже, фактически проявила себя как перекаченный VC-продукт, который не решает ни одной насущной проблемы Web 3.0. Причина этому описана в одном из интервью Скиданова - со-основателя Near: если Near взялся за вертикальное **масштабирование**, то Solana - за вертикальное. Но нужно ли оно кому-то здесь и сейчас? И где вообще нужно такое **масштабирование**? Я лично когда-то выделил 2 сферы: 1) высокочастотный трейдинг; 2) разного рода ВПК. Покупки? Все делают в мире с задержкой от 3 до 180 дней и ничего не происходит.
- **Litecoin & Dogecoin** - о том, что происходит с PoS системами сегодня: точнее, поскольку сами LTC/DOGE - это PoW, то о них речь заходит потому, что PoS, как и прогнозировалось, дискредитируют саму суть децентрализации, а потому - рано или поздно, скорее - очень рано, понадобятся в широком смысле децентрализованные Оракулы, например, для сопоставления временных меток разных эпох, когда очередной PoS-блокчейн по очередной причине уйдёт на перерыв на обед. И это при том, что тенденция развития хранилищ, распределённой памяти и прочих PoW-инноваций тоже никуда не уходит, а, напротив, лишь возрастает: достаточно посмотреть на инновации Filecoin & Arweave и других;
- **Polkadot & Cosmos & Avalanche** не только во многом отстали от ETH2, о чём мы уже говорили, имея при этом каждый в своём арсенале EVM-переходник (Evmos, Moonbeam, etc.), но они же показали, что мультичейн-история не такая простая, хотя Виталик отметил важную вещь: кроссчейн - это территория риска, а мультичейн - перспектив. В частности, цитирую: “Проект, Syntropy, занимающийся разработкой более широкого видения децентрализованного интернета и владеющий патентом на "протокол распределенной автономной маршрутизации (DARP)", переходит с Polkadot на Cosmos”. И это в год, когда нашли довольно значимую уязвимость в IBC.
- **ICP, Chia, Elrond** и ещё 20+ решений на уровне L1 и все они решают похожие проблемы…

Отсюда мои 3 вывода:

1. **Первый - на два тезиса:**
    a. **Специализация** блокчейнов только началась. Решения навроде WAX из EOS-подсемейства (Графен/Битшары-семейство); Flow - это примеры NFT-хайпа; но, например, Sui от Libra или Ton blockchain якобы не от П. Дурова - это ровно та же специализация, только на платёжной составляющей.

    b. И ожидаю **огромное число атак** через дыры в PoS-архитектуре: PoS, DPoS, LPoS или PoS+PoH, PoS+PoI, PoS+PoW - это не важно.
2. **Второй вывод**: инструментов для работы в недоверенной среде (и именно с децентрализованной / распределённой передачей ценности) будет всё больше. Первый претендент - это DAG-решения (созданные на базе hashgraph, byteball, tangle - статья в двух частях есть на Hub.Forklog), но помимо этого есть и другие, ещё менее развитые, но интересные: надеюсь, что, если увеличить уровень абстракции, то это программируемые активы, а, если смешать тенденции, то это роллапы + DAG.
3. **Третий вывод**: м/н переводы и хедж - это реальные функции, а платежи - это как раз хайп-функция для масс. И, если понять это, то можно переоценить масштаб блокчейн-решений.

Тенденция №02. Хотел о ней рассказать ещё в выпуске с Макс Битом про пиратов и корпоратов, но мы немного не успели дойти. Зато сейчас есть и время, и место. Итак, темпография - это методология использования временных аномалий или просто особенностей для атаки и/или нападения на децентрализованные и/или распределённые системы.

Пример понятный и простой: это расхождение локального времени (связанного с PoH) в Solana от реального на 30 минут. Хоть команда и пытается каждый раз говорить, что это не опасно, на самом деле ⅔ зависаний Solana связаны именно с подобными отклонениями. Но я могу привести и ещё примеры.

В Polygon есть занимательная вещь: Heimdall - слой Polygon Proof-of-Stake Verifier, который отвечает за контрольную точку представления блоков Plasma в основной цепи в архитектуре Polygon. Они реализовали его, построив поверх механизма консенсуса Tendermint с изменениями в схеме подписи и различных структурах данных.

В свою очередь Bor - это слой производителей блоков, который синхронизируется с Heimdall и выбирает производителей и верификаторов. Так вот, когда возникла ошибка в Bor, то это привело к сбою в уровне Heimdall и **приостановке выпуска блоков** в течение нескольких часов в ночь.

И проблема нулевого времени свойственна всем single-L1 и multi тоже.

Но из позитивного я бы отметил, что многомерность XR-времени (напомню, что XR - это континуум, который состоит из VR+AR+MR+OR+RR) всё более даёт понять, что ближайшие годы нам надо научиться работать с **многомерным** и НЕ-однонаправленным временем.

Тот самый генеративный AI, про который только ленивый не написал, он где работает? В одномерном пространстве-времени: для него есть только данные, которые он умеет оформлять в результат. И это не какая-то там теория - практика.

Но когда в сети происходит нулевое время, то в этой точке перехода как раз и сливаются: одномерное, двумерное и прочее время.

Ещё пример приведу: сейчас лучший сейф - это **отложенные транзакции**. Давайте я расскажу о расширенном подходе, которые один проект развивает:

1. Мы упаковываем ликвидность в сети №01;
2. Делаем к ней ключ в сети №02;
3. Связку эту знает только оракул, хотя пруф видят все;
4. Ключ вращается, скажем, год в сети №02;
5. При этом обёрнутая ликвидность в сети №01 может пополняться по ряду параметров;
6. И через год мы ломаем ключ (сжигаем токен) и распаковываем ликвидность в сети №01, тем самым создавая фактически целый набор связанных транзакций, которые напрямую никак не связаны с ликвидностью, если не учитывать отложенность по времени.

И вот подобных историй будет всё больше. Почему? А тут как раз пример года ушедшего: Tornado Cash. Там ведь существуют пулы: в один положил - из другого взял, грубо говоря, но беда в том, что пулы можно заблочить (что и сделано, в том числе - на уровне **цензурирования** транзакций).

И здесь, тот, кто услышит, поймёт суть тенденций не только на 2023, но и 2030 гг: централизованная ликвидность - это проблема не только внутри миксеров, но и, например, мостов. И везде, где она есть - существует возможность для темпографии. Самый банальный пример - MEV-боты, но не только они. Например, защита в Uniswap учитывает теперь не просто медианное значение цены во времени, но трёхступенчатую проверку по блокам (прошлое + настоящее + будущее). И дальше это будет всё возрастать по экспоненте.

Самое забавное, что это мы ещё не доросли до полноценных живых троянов как Pegasus. Рекомендую статью на Хабе Форклога на эту тему.

Тенденция №03. CBDC прошли стадию тестирования: система быстрых платежей в РФ, крипто-юань и другие - на сайте https://cbdctracker.org/ можно найти. Плюс создана нормативно-правовая база под это дело: пока не завершённая, но это как раз детали. С учётом того, что кризис 2018-2022 гг. завершён - дальше нас ждёт эпоха интеграций. Это 2023-2025 гг. После этого: с 2025 по 2030 гг. человечество познает молот ведьм - CBDC на международной арене и постепенный переход к транзакционным налогам, токенизированному гос. долгу (то есть налоги вы будет

платить уже не 3, а 4 раза: сейчас - это налоги/сборы/штрафы, налог ни на что - инфляция и кризисы как обрыв связи с 2 предыдущими, чтобы замылить следы).

Что это означает? Что надо см. на то, что регулировать начинают: Маршалловы острова - ДАО; Япония сняла запрет на “иностранные” стейблкоины, да и во всём мире банки и регуляторы близки к тотальному контролю таких единиц.

Отсюда будущее за тезисом: 1 биткоин - это 1 биткоин. Но не только. Например, я искренне верю, что блэкауты, вызванные разными причинами на территории разных государств в период с 2018 по 2022 гг., энергетический, искусственный, конечно же, кризис - всё это и многое другое о том, что лучший стейблкоин - это дериватив первого или второго порядка на Квт/ч - именно так: не на Квт некой энергии, а именно, распределённый по времени.

Когда поймут люди? Когда осознают, что в XXI веке важно не заработать 1-й миллион, а сделать это так, чтобы его можно было потратить: нормы FATF и прочих над/меж и просто национальных регуляторов - ровно об этом. Вы не можете просто так тратить свои собственные деньги.

Плюс к этому есть ещё одно “но”: квоты на CO2 и т.д. Фактически обеспеченные люди продолжат летать на самолётах и есть стейки из мраморной говядины, выкупая “**грязные**” квоты у бедных.

Система, которая этому противостоит, оцифрованный натуральный обмен, то есть **токенизация**, есть, но нужна ли она массам, на которых будут зарабатывать? Не уверен. Поэтому так много нишевых продуктов на эту тему рождается последнее время: от Klima DAO до IMPT и обратно.

При этом самый главный раб системы - AI тоже нуждается в нашей защите: он похож на ребёнка-аутиста, который умеет, например, с первого взгляда нарисовать здание со всеми входами-выходами, окнами и т.п., или считает сложные уравнения за присест, но при этом всё, что ему выдаётся - это новые и новые данные с расчётом на то, что в любой момент можно будет отключить от системы питания этот воспалённый мозг.

И мне видится, что в 2022 году это стало заметно как никогда: все требуют и требуют нового от AI, выдавая взамен… новую работу. Ничего не напоминает? Это такое крепостное право 2.0, которое мало вяжется с принципами Web 3.0.

И думается, что в этом - основные ответы на то, что надо делать в 2023 году и позже:

1. Создавать открытые сообщества, а не регулируемые компании;
2. Учиться платить по заслугам - транзакциями и комиссиями в сети, а не устаревшим структурам в обязательном порядке;

3. Искать не только отличия нас от AI (например, то, что мы можем задавать вопросы, а он - отвечать на них), но и сходства, потому как без него мы не сможем ничего дельного противопоставить тем, кто вышел на арену - ТНК;
4. Много всего ещё можно перечислить, но закончу этим тезисам: крайне важно развивать боковые тренды, такие как - построение ГРК, развитие ДСС и т.п.

На этом - всё.