在区块链的世界里，代码即法律，区块即正义？

谭天，加密货币社区Qurea创始人之一，安娜其加密朋克主义者

我来自无涯社区，是一个专注于区块链方向的分布式社区。其实区块链并不仅仅是某种计算机技术，它给整个社会网络提供了更多的解决方案。从社会角度而言，它是一种新的协作模式。很多极客和研究者意图通过区块链技术建立一个乌托邦——实现人类的真正平等和精神自由。

区块链表现出了一种协议乌托邦的概念，即通过不依赖于人的计算机协议来治理社会。作为社会实验的平台，它很开放，人们可以用代码去实现一些关于乌托邦中具体规则和结构的想法，这种实验的代价也相对较小。

其实协作平台在人类社会中存在了很久，在过去，诸如部落、城邦、国家，以及企业、跨国集团……都是协作平台，它们都是建立在某类共同的想象体之下。比如公司、国家，都是人们通过叙事来建立的共同想象。在其中，组织者通过对个体的未来作出许诺，使其加入协作。正是因为基于故事和想象，在这个过程中就会有人掌握故事的解释权、话语权，由此从中汲取权力，获取更多资源。所以权力最初的根源就是来自于血缘和解释权。

协作中有两个重要的部分，一是协作范围，越多的人参与进来肯定是越好的；二是协作程度，比如一场大会，需要高强度的协作。参考这个示意表可以看到，自由市场的协作范围非常广，但是协作程度不高，因为它是竞争的，甚至有时候自由市场会站在协作的反面，因为会存在恶意竞争、广告战等现象，这是没有人受益的。政府的协作程度非常高，但协作范围很小，所以筛选非常严格。企业则处在自由市场和政府这两者之间。而我们想象的一种乌托邦状态，就是实现最大范围，同时协作程度最高，即“世界各地人民团结一心，为了一个共同的命运而奋斗”。

为什么说协作其实很困难？

在现实的协作过程中，存在各种各样的问题，协作范围和协作程度无法同时达到最大。其中，首要问题就是公地悲剧的产生。地球资源不属于任何一个个体，但它们被人为划分开。人类的发展就是要使用资源，本质上来讲，其实就是使用公共资源。在使用公共资源时，就必然会出现公地悲剧的问题——每个人都需要更多的资源去发展自己，但公共资源有限，可能会损害到别人的利益，当资源被不可持续的过度消耗掉，则所有人都会受到损失。

另外还有叙事技术的落后带来的问题。人类学家罗宾·邓巴（Robin Dunbar）提出人类拥有稳定的社交网络的人数约是150人，超过这个数字，协作的困难将加大。为了解决这一问题，公司等组织会设计出管理层，每一百多人中产生一个管理层，或者产生组织分裂。

随着互联网的发展，信息点对点复制，越来越多的知识专利等东西被迫成为一种“公地”，人们越来越难以逃离公地悲剧。现在对于公地悲剧的解决方式有两种，一是私有化，让每个人都自负盈亏，避免过度消耗资源。第二个就是统一调控，像宏观经济调控一样规定各类事项。

私有化是通过市场来协作，在初期，参与者们对资源的占用程度小，大家都和平发展、交易，一旦资源将被耗尽，广告战、价格战等恶性竞争就会出现，私有化最后面临的就是协作与对抗过程的不断循环。如果引入宏观管理，计划、规则本身就是另一个层面的公地，那么谁有权来规定、解释这些规则？因此可能产生新的公地悲剧，利益团体互倾轧，问题不断升维。

比如Facebook、Twitter这种互联网组织，用户提供信息，上传数据、自行创作、与其他用户分享……初期因为用户数量不算太多，每个用户能处理的信息量并没有饱和，所有参与网络的人彼此合作，是一种正和博弈。但一旦到了一定阶段，比如到了人脑处理信息的极限，就会形成信息爆炸。人们会倾向于认为自己的信息更重要、更应该被看到，但其实处理信息的能力有限，假数据、欺诈……各种对抗性的博弈就会出现。

这时，大部分人为了自己的利益会去寻求第三方的解决，由它来制定规则决定谁的信息更有优先级、哪些信息和账户应该被删掉……只有经过调解，网络才能进一步增长。现在很多互联网公司就扮演这一角色，这个过程也让它的权力不断增大，不断集中资源，用户的权力则基本不会变动。所以说，维持增长的方式之一就是不断让第三方集中资源和权力，让它来做宏观调控。

区块链里有一个不一样的地方，它是一个完全公共的领域，每个人都有使用权，并且算法会奖励贡献资源的个人和有益于网络价值的行为。比如，用户更新代码让它更安全、提供算力让它的处理能力更大，就会获得相应的奖励。通过网络效应，区块链网络的价值增长速度会快于用户使用资源的速度。

这过程中也会出现资源的分配，但它是用算法和程序来自动实现的，没有某个人在背后主观操控，没有人能更变它。规则本身又可以自我调节。但这个规则本身也是一种公地，需要通过一种民主的方式来修改、更新，让它更符合我们的发展。目前来说，区块链还没有遇到过去出现的公地问题，是因为它用机器、代码替代了人，因为机器是确定性的，所以它更可信一些。

在叙事技术方面，其实基于语言的协作是不太可信的，因为谁都可以跑出来解释。但在区块链的网络里，是基于代码（而非语言）来协作的，数学不仅能精确地传递信息，还可以传送数据的证明，让信息更可信。基于数学，我们有了验证事实的能力，过去那种操纵解释权并获取权力的现象就变得不太可能了。

从“全景监狱”到“共景剧场”

说到“可验证”，需要延申到“全景监狱”的概念（福柯对人类社会控制的方式的一个比喻：犯人被监禁在不同的牢房中，狱卒处于顶层中心，可以监视所有犯人，并且犯人们彼此之间也缺少有效沟通和传递信息的渠道），通过信息不对称，社会的管理者可以高效地实现社会治理。

在区块链这里，因为网络是开放的，所有人都能加入到这个系统中，都有检验的能力，所以世界更像一个“共景剧场”，所有人检视所有人。好比进入一个剧院，坐在剧院的每个人都能清楚的看到别人的样子，即所谓的“可验证”。如果你想要获得更多资源、对系统做一些改变，就需要走到剧院中心，行动并接受所有人的检视。很多人说区块链是去中心化的，但我认为它是允许任何人走向中心，并且其余所有人都有权参与对他行为正确、规范与否的评断，而不再仅仅通过解释和狡辩就可以获取权力。在人人可验证、人人可证明的情况下，社会就从一个全景监狱变成了一个共景剧场。

区块链技术也可能有负面影响，它可能会被一些掌权者利用，形成的规则反而催生出一种强化中心的超能力。举个例子，过去所有的货币是绝对匿名的，我们不知道这张纸币的来源和用途，只存在货币价值，但现在的支付宝或者微信账单都有了每一笔的交易记录。如果未来某个国家推出了一种基于区块链的数字货币，要求全国都要使用，并且拒收纸币，那么我们和谁交易、用钱做了什么……所有的信息都会被政府获取。

区块链技术本身的数据是加密的，但后来又有一个“超级私钥”的概念。意即可以给一些机构提供“后门”，允许其在整个系统中穿透性地监控所有人的交易数据。权力被集中后，便会出现不断寻租的过程，最后威胁到个人自由和其他的权力。

有的监控系用会专门研究用户在聊天时出现的各种敏感词，做舆情判断。它可以通过检索判断哪里出现了金融风险；哪里会有P2P爆雷；或者哪里出现了维权……有不少P2P（包括借着区块链名义来的一些诈骗）都会被这个系统识破。在区块链上，人人可验证，人人有权搜集所有人的数据，但并不是所有人都有时间和资源处理、维护数据，进而分析不同账户之间的关系。所以一些资本、权力就有能力从中操控，既可以有效地消除腐败，也可能开始过分的货币监督和审查。这时，鼓励个人自治和自由的工具就变成了一种强化中心的武器。

分叉：超越民主的制度？

“分叉”是指一个区块链网络分裂成两个的过程，因为区块链是无准入门槛的网络，所以任何人都可以无代价地加入、退出。又因为区块链的规则和代码都是公开的，因此任何持不同意见的“少数派”都可以对其加以改进，建立自己的规则，并且吸引其他人的加入。分叉是一种超越民主的制度，如果你认为目前设计的制度不好，则可以自己设计或者加入其他制度，而不再是非要在某个户籍制度或国家制度下。以往的民主是少数服从多数，但通过区块链，少数人如果觉得自己权益受损，就可以再建立一套对自己有保障的系统。

通过不断的分叉，会出现很多特质不一的网络，如同物种大爆发。因为每一个人都有选择权，所以好的制度就像一种自然选择的过程，被最终选定。很多区块链是鼓励分叉的，因为它想让大家做更多的尝试，不断试错得到更好的制度。但也有一些人为了自己的私利会恶意地进行分叉。

在一开始，普通民众对区块链的算力占比很大，后来有人设计了“矿机”，有人斥巨资购买大量机器，以获得更大的权力。虽然算法治理的过程没有问题，但是它只考虑到系统内部，对系统外部来说，其实需要诸多变量，比如资金。最终，普通人的权力逐渐降低被压缩，巨头不断的崛起，直至控制了整个网络。

刚刚说的分叉在2017年的时候发生了一次，最原始的区块链网络分裂成了两个，你可以想象成国家分成了两个。它不是任何一个普通民众主导的，而是因为利益集团出现了冲突，这是由控制网络的人操作的一次分叉。现在我们可以看到三个主流的系统同时存在：BTC、BCH和BHV。相当于一个网络分成了三个。根据网络效应的计算公式，分成三个之后，它累加起来的价值远没有只有一个的时候大。

第一次分叉后双方市值合起来出现了增长（可能因为那个时候正好是在上升的周期里），但第二次分叉的时候，原来的BCH、BHV这两个系统市值合起来下跌了33%。在这个过程中，它们出现了非常严重的矛盾，分叉已经不是为了进化，而是为了各自的利益。他们互相通过算力攻击对方，恶意做空对方，导致整个市值损失非常之多，这是非常严重的一次公地悲剧。

关于分叉的讨论很激烈，有人鼓励分叉探索不同方向，有人认为分叉使得系统互相对抗消耗。但这两种思想本身也是一次分叉。这个过程像进化论的方式进行筛选。进化论本身是没有偏好、没有指向的，所以最后得出来的东西能不能称之为进化，这是一个问题。

“代码即法律”的破灭

整个区块链系统的运行是根据一套自动的算法，相当于宪法，每个人都要严格遵循。人们希望在数字世界里不断试验，找出最优的结果——即用最佳的代码去代理人类事务，最大限度地减少腐败和实现社会自由，并且将这些规则不断地运用在现实生活中，实现整个社会都是代码资质。

这里要介绍的这个世界的主人公叫“the DAO”，这是三个英文的翻译，去中心化（Decentralized）、自动的（Automatic；或者说自我治理Self-governance）、组织（Organization）。在这里，系统基于一个共同的契约，在共同的信任（或者一套激励设计）下自动、自洽地执行运作，不需要第三方管理。所有人都是平等的，都有相应的权力。

这就像是一个群策群力的风投机构，有人出钱，有人做调查，有人在市场上找项目……共同的目的就是让“风投基金”赚钱，让它基金净值变高。最开始创立the DAO的是不到20人的团队，他们编写了the DAO的基础代码（也就是区块链的第一版“宪法”）并发布，后来不断有人加入、注资，筹集到可观的资金。

但随后出现了一个臭名昭著的事件。有人发现了第一版代码的漏洞并将其曝光，当时并没有引起人们的关注。后来有黑客利用了已经曝光过的两个漏洞，攻击系统并盗取资金。黑客攻击半个小时之后就被人发现，但由于程序的自动性以及缺乏第三方的监管，没人能阻止资金继续流失（只能用一些其他的办法让黑客盗取的速度慢一点）。当时就此事出现了非常大的争议（也算是一次分叉）。因为涉及到太多资金被盗，很多人觉得应该回滚。但还有一部分人认为这样就违背了之前所有人都认同的“代码即法律”——区块链精神最重要的就是不可篡改，所以不能更改，应该承认错误。

后来，事件中的黑客在社交平台上发了一条消息，称自己做的所有事都是代码允许的。如果“代码即法律”是正确的，那他的行为就是法律允许的，是凭借个人能力获得了最大的激励而非盗窃。他还认为那些指责他的人侵犯了他的声誉，是违反了法律。当时在整个社区内部，都一边倒地支持不能回滚，因为如果回滚，就是承认“代码即法律”是错误的。但后来发起了一次民主投票（当时只有10%的人参与了投票），绝大多数人都投给了回滚，他们放弃了“代码即法律”，来保证自己的利益。最终只有10%的投票率决定了整个系统的走向。

整个社区割裂了。依然坚持“代码即法律”的那部分人，他们运行自己旧的代码，被盗的钱依然在黑客的账户。另一部分选择回滚的人则运行新的代码，使得偷窃事件就像从未发生。最初写代码的20个人，并没有为这个事件而负任何责任，整个社区共同承担了漏洞带来的损失。当时在“代码即法律”的语境下，用户是不用承担责任的，同时加入社区就意味承担风险和后果。

关于the DAO为什么面临失败，有以下一些原因：第一、脱离了人，任何自动化都是有风险的。特别是这个系统是跟利益、资本有关时，脱离了人，就完全为资本服务了，而资本离开人是没有意义的；

第二、代码本身不可信，或者说理性不可信。有人说代码必然存在漏洞，我们需要验证它。但发现验证一个代码需要写另一个代码，再写第三个代码去验证第二个，于是形成了一个无限循环的过程。

第三、代码不能分辨善恶。算法只能判断一致性，判断不了善恶，善恶是由人来决定的。

虽然说the DAO失败了，但是这套系统很好用，于是不断有人尝试把人类社会的一些规则加到系统上做各种各样的实验。比如有人去实践直接民主，发现效率低，又做了一个代理民主，选代表人帮他投票；随后有人发现代理会被巨头控制，就用代码实现了流动民主（可以自己直接投，也可以委托给别人投，委托人也可以再委托一层）。这一切发展仅用了一两年时间。曾经因为代价太大而无法实现的社会学实验和新制度的设想，在区块链代码平台，以代码的形式和软件的速度进行试验和部署，积累了一些社会学的数学基础，正是无数人梦寐以求的。

从预测市场到暗杀市场

还有一个建立在区块链之上的去中心化预测市场Augur，用户可以就任何自己感兴趣的项目进行预测，没有任何限制。如果没有感兴趣的，只需要支付少量加密货币，用户可以自己创建一个，并在预测结果出来后获得部分收益作为回报。经过无数人的预测，会产生一种类似于群体智慧的过程（其理论依据是贝叶斯最优分类，Bayes optimal classifier），从而预测、预防和引导未来。它想获得群体智慧的初衷是好的，但同时它也有另一面。

有一个用户曾在平台上发布“特朗普2018年会被暗杀”的提案，当时虽然没什么人给他押注，但引起了很多讨论。一旦有人押注100万美元提出特朗普在2018年不会被暗杀，就可能会驱使有人为了赢得这100万美元的奖金而真的进行暗杀行为。于是，一个预测市场变成了一个暗杀市场。有人做出进一步的假设，建立一个关于政策、法令的预测市场，通过预测市场来决定哪些议案应该被通过，哪些议案可以获得全民福利的最大化。但其实这个系统显而易见有非常多问题：资本有可能在背后推动某个议案的发生；大部分人其实没有能力判断议案的好坏，而只是跟风投票……所以发起者可能更关心的是提案是不是受大众的喜欢，而不是提案会产生什么价值。