TransX

Transaction X

数字货币聚合支付平台

TransX是Transaction X的缩写，定位是数字货币的聚合支付平台，做数字货币领域的Paypal，推动比特币成为下一个时代的国际贸易结算货币。

目录

1.背景

区块链技术处在突破的临界点，币圈氛围浮躁，大量数字货币的行为停留在在交易所炒币这个阶段，无数会议讨论的DeFi大多是空中楼阁，区块链行业急需一款接地气的产品，解决区块链难以走入老百姓生活圈的难题。就像数年前移动支付走入老百姓生活圈一样，到今天，中国的大多数用户出门都可以使用移动支付处理几乎所有支付交易。随着中国最高领导人为区块链技术落地发展打Call后，央行也将DCEP推上了日程，从已有的移动支付组合升级为数字货币支付是未来的趋势。

在移动支付最发达的中国，我们日常使用移动支付都已经非常方便，新的数字货币聚合支付工具具有广阔的使用场景。比如，深圳华强北的矿机销售厂家，其买家都是持有数字货币的客户，完全可以使用数字货币来支付；比如，跨境支付，用户只要持有主流数字货币，依靠数字货币聚合支付的帮助，可以非常便捷完成支付；比如，有些人去娱乐场所消费，并不希望移动支付记录或者信用卡消费被发送到家庭成员的手机上，使用数字货币聚合支付工具可以完美解决这个问题，再比如，在亚洲东南亚市场，很多国家并没有发达的移动支付系统，电商业务发展受到限制，如果有数字货币的支付方式，能将更多只拥有手机的用户带入到快捷方便的移动支付网络中。

1.1 比特币的危机

无论如何，加密数字货币市场都不能忽略房间中这头大象：比特币。其占据接近70%的市场份额，利用数字货币做支付的场景中，如果忽略比特币，那将是舍本求末的操作。

时间节点来到2020年，比特币区块奖励迎来第三次减半，但比特币价格表现却没有迎来预期的上涨，大多数人的减半行情共识破灭。比特币不仅仅不再存在减半行情，可能还存在减半危机。这个减半危机是我总结的减半末尾效应，而且越到减半后期，这种末尾效应也就越来越明显，而且其中的逻辑是非常清晰的。

比特币在一开始设计的时候，中本聪为了使得比特币软件能在低门槛的设备上也能运行，就把比特币区块大小设置在1M大小，使得比特币承载交易的容量非常有限，中本聪在一开始就将比特币定位为点对点的电子现金，在比特币的白皮书标题中也是如此定义比特币的，所以中本聪在设想比特币减半末期的时候，只要有足够多的点对点的电子现金交易，就会有足够多的交易手续费来弥补区块奖励减半后的损失。但是随着比特币的发展，现在整个行业都对比特币的定位出现了偏差，将比特币定位为数字黄金和SoV (Storage of Value)，绝大多数人都将比特币存放在交易所和冷钱包里，就是不再将比特币放热钱包用来支付，使得整个比特币网络的交易手续费一直都增长不上去。随着减半继续进行，那整个比特币矿业所依赖的区块奖励将很快减少，而手续费增长非常缓慢，到了区块奖励末期，整个区块奖励和手续费加起来都不到比特币总市值的1%，这样使用1%的市值来维持比特币网络的安全，在理论上就存在很大问题，比如只需要使用比特币总市值1/1000的资金，加上10倍杠杆，就能尝试发动51%攻击，影响比特币网络的安全，然后通过做空套利。

由于比特币是一个具有2100万总量的通缩货币，也就决定了减半末尾总会到来，如果手续费不能快速增长的话，那我上面描述的减半末尾效应就会如期而至，而且我相信，在2024年再一次减半的时候，这种效应就会非常明显。

1.2 卡尔达肖夫指数与熵增

很多人都质疑比特币挖矿是一种巨大的能源浪费，但这只是从人类普通人的角度看问题，站在一个火星人的视角，地球人把能源用来挖比特币，或者把能源用来开汽车，都是一样的熵增过程，是完全没有区别的。

如果我们能站在一个更高的视角看问题，比如从文明的角度来看能源的开发利用，那就有必要介绍卡尔达肖夫指数，其是根据一个文明能够利用的能源量级，来度量文明层次及技术先进程度的一种假说。根据此定义，我们地球目前的文明还处在相当早期的阶段，还只有0.724型，还达不到I型文明的阶段，I型文明是可以驾驭10^16W数量级的能量，I型文明能够利用星球的所有能量。II型文明能够利用行星的所有能量，可能就需要能构造出“戴森球”装置，当然还有更高级别的能源利用水平，在此不再展开讨论。

经过卡尔·萨根对卡尔达肖夫指数优化后，其表达式为：

$$K = \frac{\log_{10} P - 6}{10}$$

其中K是一个文明的卡尔达肖夫指数，和P是它使用的能源。根据公式推导，一个文明所使用的能源增加10倍，卡尔达肖夫指数才增长0.1。从另外一个角度看，从1973年的石油危机到2012年到40年，工业和互联网科技飞速发展，但能源使用的增长确实少得可怜，在火星人看来，人类的文明指数才增长了0.032。距离I型文明还远得很，根据热力学第二定律，在我们还在太阳系这个孤立系统中，熵增是不可逆的。

要能激励人类开发更高数量级的能源，需要有非常规的手段，而且要能直接变现的财富刺激。比特币挖矿产业能完美承担这样一个角色，只要保证地球人在开发下一个数量级能源使用之前别把地球生态系统弄奔溃。目前比特币挖矿产业对于芯片设计和制造业的推动是有目共睹的，最新的芯片5纳米工艺又要率先使用在比特币矿机芯片的生产上了。接下来，比特币挖矿产业肯定会投资核聚变能源开发。

1.3 点对点电子现金与全球结算货币

有人总质疑比特币的承载能力有限，作为一种点对点的电子现金是很不合适的。于是很多人想出了二层扩展网络、闪电网络等方案，从更快、更低手续费的角度去改良比特币，在此，我的看法是完全不同的，个人觉得所有不将交易跑在比特币主网的（不把手续费留在主网）改良方案都是消费比特币，而不是帮助比特币。根据上面的减半末尾效应，比特币网络的手续费不增长，比特币将酝酿巨大的危机，而且总有一天会爆发。

说比特币的承载能力有限的人，其实只是用一个角度看问题，就是觉得比特币TPS不够高，所以其承载能力有限，但是还有一个角度，那就是比特币网络只要足够安全，单笔转账足够高，其总价值支付承载能力是可以很强的。要想单笔转账金额足够高，那就要清晰定位比特币的价值，国际贸易结算中，单笔转账的金额就足够高，如果比特币能定位成国际贸易结算货币，那将目前中心化金融机构收取的手续费，转移到比特币手续费上，将能够真正实现中本聪最开始的点对点电子现金的设想。

从另外一个角度思考，目前国际贸易结算货币，基本都是美元，都需要经过纽约结算中心，而这个结算中心是中心化的，美国政府可以随意绝罚其他国家出结算体系，比如朝鲜和伊朗，但这些国家跟其他国家贸易的时候，也不见的就使用比特币进行结算，根本原因还是因为比

特币的体量还是太小了，其2000亿美金不到的规模，金额巨大的国际贸易，目前使用比特币做出入金会有巨大的价格波动风险。要想进入国际贸易中结算货币家族，美国M0是一个参考指标，那意味着比特币总市值至少还要增加1个数量级。

目前的比特币定位到其下一个阶段的定位，需要有一个强大的助推动力，使得比特币的手续费能快速增长，从而推动比特币挖矿产业能源进一步消耗，不断构筑更高比特币价格的底部。而这股强大的助推动力不可能来自比特币网络本身，而TransX项目就是扮演这样一种外部的推动力。

2.概述

TransX定位于做数字货币聚合支付平台，会率先支持主流加密数字货币，包括DCEP、USDT、BTC、ETH、EOS、DOT等。TransX重点是将聚合支付这个简单的功能做到极致，让更多第三方钱包兼容支付二维码的格式，就像微信和支付宝在移动支付领域所做的创新一样，小小的一个二维码分布到生活圈的各个角落，形成了庞大的网络效应。TransX是区块链数字货币支付交易服务的平台，本身也是充分利用区块链技术，让各种交易行为都能被验证和量化，最后在TransX主链上记录一次挖矿行为，给进行支付交易的双方一些激励。

TransX将采用Substrate来构建应用链，Substrate作为Polkadot的开发框架，也逐渐发展成区块链的通用开发框架，称之为区块链操作系统都不为过。Polkadot是Web3.0基金会发起的项目，由以太坊前CTO Gavin Wood博士主导的Parity团队进行设计和开发。Polkadot致力于实现链间任意消息通信，将解决区块链的互通性难题，进而实现多链并存，解决区块链的扩展性和互操作难题。Substrate作为Polkadot开发的通用基础框架，实现了混合PoS共识、链上议会治理、WASM虚拟机、智能合约原生执行、高效轻客户端协议等。

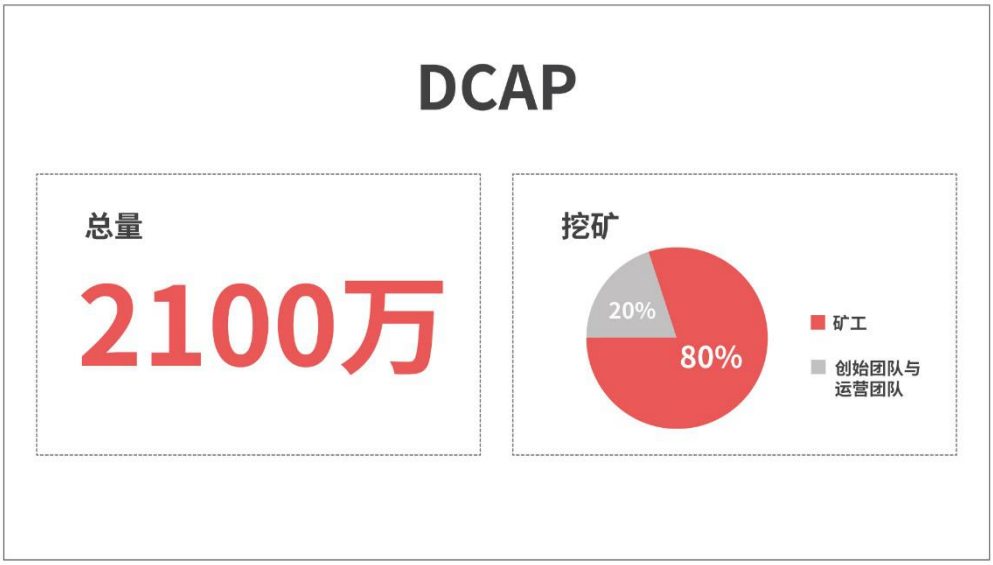
TransX聚合主流数字货币支付的愿景跟Polkadot的跨链能协同合作，数字资产在Polkadot生态中可以跨链和互操作。在现实层面，大家还需要一个聚合支付入口来方便大家使用数字货币，Polkadot是链上实现数字资产互操作，TransX是在链下帮助用户的数字货币通过聚合支付来对接主流区块链。

3.经济模型

3.1 发行模式

TransX发行总量为2100万枚的加密数字通证DCAP(Digital Currency Aggregate Payment,数字货币聚合支付)，每4年减半。发行量的10%归创始团队和运营团队所有，用于持续的开发经费

和项目运营。TransX为遵守绝大多数国家法律法规，不进行任何的公募、私募和ICO行为。



3.2 交易挖矿

欧文·费雪在金融学中提出了“交易方程式”（The Equation of Exchange）：M*V = P*Q。其中M为货币供应总量，V代表货币交易流通速度，P为价格水平（物价指数），Q为全社会的商品和劳务交易总额。费雪认为，Q虽然经常变动，但变动程度很小。后来约翰·梅纳德·凯恩斯对货币流通速度为常量提出质疑，并建立了一种新的货币需求理论，也就是“流动性偏好理论”（Liquidity Preference Theory）。

到了当今，数字货币还不能完全套用经典金融学公式，但基本上从绝大多数数字货币还停留在交易所炒作阶段，就充分说明数字货币在交易场景中存在缺位。其货币交易流通速度V偏小，更多数字货币是一种证券型通证（Security Token），而区块链技术在目前阶段还难以让这种证券型通证落地产生实际价值。

TransX认为，一个数字货币只要不完全是证券型通证属性，就有提高数字货币交易流通速度V的需求，P是价格水平，反过来也是币价的体现，数字货币交易流通速度V越大，币价就越有支撑。

TransX将如何量化交易行为，如何定义算力，更多挖矿细节将在下面章节探讨。数字货币交易行为量化成算力，通过抵押DCAP自由开放注册的方式，保证网络共识安全，不至于出现算力攻击。根据算力占比来获得DCAP奖励。

交易行为量化成算力，有两个基本的指标需要衡量：一个是交易频次，一个是交易金额。TransX主要以这两者来作为衡量指标，辅助其他指标，比如不同数字货币的交易手续费模型，各个账号在单位时间的交易频次和交易金额。

没有成本的挖矿行为，所挖到的Token也不会有一个基础价值支撑，DCAP的价值支撑有两个：

- 转账是需要手续费的，用户消耗了手续费，得到了DCAP的激励。（EOS消耗CPU）

- 有效的转账行为是交易的一部分，交易本身是产生价值的。

DCAP除了有基础价值支撑之外，还能通过所有用户构建的数字货币支付网络，这种支付习惯的养成，最终打造一张巨大的价值网络，而这一切都会把价值沉淀在DCAP上。

4.挖矿模型

为了激励交易支付行为，TransX引入了挖矿模型，让主流链上的资产交易都能被量化，从而计算出具体的算力，挖矿得到DCAP奖励。

交易行为有两个维度，一个是交易频次，一个是交易金额。TransX将两者的权重分别设置为α和β。单位时间内（24小时）单次交易在总交易数量中占比 * α = 频次算力；单位时间内（24小时）单次交易金额在总交易金额中占比*β = 金额算力。

- 单次挖矿总算力 = 频次算力 + 金额算力

这是一个最简单的算力计算逻辑，当然还需要考虑到不同币种在支付交易中的市场份额，不同币种的手续费模型，不同手续费模型其交易成本是不同的，比如EOS交易支付过程中几乎没有成本。如果其算力不做一定的钝化处理，TransX的算力攻击成本将不够高，所以针对不同币种，需要设置一个钝化系数。钝化系数直观理解就是，如果你的算力超过平均的N倍，超出部分的算力就只能统计为1/N。

比如平均算力数值是0.001，而矿机的算力数值是0.002，那么经过钝化处理后，其算力被处理成 (0.002-0.001) / (0.002/0.001) + 0.001 = 0.0015。

5.技术架构

Substrate框架构建TransX的底层，数字货币聚合收款二维码是TransX客户端的核心，TransWallet是TransX整合多链支付的钱包。

Substrate的底层共识采用Babe + Grandpa组合共识，TransX将支持WASM虚拟机和智能合约的开发和部署。等Polkadot主网落地后，TransX接入Polkadot生态，实现跨链，更重要是接入Polkadot的共识引擎为TransX提供共识安全。

5.1 TransX客户端

TransX矿机客户端广义理解是安装了TransX客户端的任何设备，比如手机安装TransX客户端，就能成为一个数字货币聚合收款终端，主流数字货币都能通过这样一个聚合收款二维码来完成收款。TransWallet也能发送交易和收款，如果TransWallet成功注册到TransX主链上了，主流数字货币的交易行为都能进行挖矿。

狭义的TransX矿机客户端是有一个专门的硬件，硬件安装了TransX客户端，并且进行安全加固。同时支持NFC通信，对于定制的数字货币信用卡能够利用近场通信技术完成交易。

5.2 TransX客户端注册

如果所有的数字货币支付行为都能被纳入算力统计范围，那是一个无远弗届的工作，也绝不

是仅仅一个应用链能完成的工作。TransX需要定位非常清晰，数字货币的交易行为需要激励，但也要能够形成经济体系的闭环，矿机客户端需要注册是在为了保证TransX的共识安全。TransX定位是给数字货币做一个聚合支付的通道，任何设备都能安装一个客户端来使用这个聚合支付的功能，只是在早期要想让支付交易数据参与挖矿，就需要进行矿机注册，注册过程需要用户抵押一定的DCAP，主要是为了增加用户做恶的成本，当然用户可以随时提取抵押的Token离场。

TransX的矿机注册是完全开放式的，任何人都能够参与，TransX是一条公链，没有任何一个中心化节点能够授权注册，只要注册成功即可参与挖矿。

5.3 符号和算力

符号	意义	算力相关计算
TW	过去 24小时总算力	$TW = sum(TW_{token})$ token∈{BTC,ETH,EOS,...}
TC	过去 24小时总交易次数	$TC = sum(TC_{token})$ token∈{BTC,ETH,EOS,...}
TA	过去 24小时总金额(以 USDT 计)	$TA = sum(TA_{token})$ token∈{BTC,ETH,EOS,...}
AvW	过去 24小时平均算力	AvW = TW / TMN
TMN	全网总矿机数量	链上已成功注册矿机数
ArC	过去 24小时平均交易次数	ArC = TC / TMN
ArA	过去 24小时平均交易金额	ArA = TA / TMN
PW	矿机 P 过去 24小时累计算力	$PW = sum(PW_{token})$ token∈{BTC,ETH,EOS,...}
PC	矿机 P 过去 24小时累计交易次数	$PC = sum(PC_{token})$ token∈{BTC,ETH,EOS,...}
PA	矿机 P 过去 24小时累计交易金额	$PA = sum(PA_{token})$ token∈{BTC,ETH,EOS,...}
TW_{btc}	过去 24小时 BTC 总算力	$TW_{btc} = TW^1_{btc} + TW^2_{btc} + ... + TW^n_{btc}$
TC_{btc}	过去 24小时 BTC 总交易次数	矿机中 BTC 交易次数超过 LC_{btc} 后不再统计进来
TA_{btc}	过去 24小时 BTC 总交易金额	矿机中 BTC 交易金额超过 LA_{btc} 后不再统计进来
AvW_{btc}	过去 24小时 BTC 平均算力	$AvW_{btc} = TW_{btc}$ / TMN
AvC_{btc}	过去 24小时 BTC 平均交易次数	$AvC_{btc} = TC_{btc}$ / TMN
AvA_{btc}	过去 24小时 BTC 平均交易金额	$AvA_{btc} = TA_{btc}$ / TMN
PW_{btc}	矿机 P 过去 24小时 BTC 累计算力	$PW_{btc} = PW^1_{btc} + PW^2_{btc} + ... + PW^n_{btc}$

PC_{btc}	矿机 P 过去 24小时 BTC 累计次数	矿机中 BTC 交易次数超过 LCbtc 后不再统计进来
PA_{btc}	矿机 P 过去 24小时 BTC 累计金额	$PA_{btc} = PA^{1}_{btc} + PA^{2}_{btc} + ... + PA^{n}_{btc}$
ρ_{btc}	BTC 算力占总算力的最高份额	$0< \rho <1$,这是一个可以治理修正的参数
PPC_{btc}	矿机 P 计算 BTC 频次算力钝化系数	$PPC_{btc} = ((PCbtc + 1) / AvC_{btc}) \% 10$
PCW_{btc}	矿机 P一次 BTC 转账的频次算力	$PCW_{btc} = \alpha * 1 / TC / PPC_{btc} (PC_{btc}<LC_{btc})$
PPA_{btc}	矿机 P 计算 BTC金额算力钝化系数	$PPA_{btc} = ((Price(BTC) * m_{btc} + PA_{btc}) / AvA_{btc}) \% 10$
PAW_{btc}	矿机 P一次 BTC 转账的金额算力	$PAW_{btc} = \beta * m * price(BTC) / TW / PPA_{btc}$ $(PA_{btc}<LA_{btc})$
α	频次算力在总算力中占比系数	$\alpha + \beta = 1$
β	金额算力在总算力中占比系数	$\alpha + \beta = 1$
LC_{btc}	过去 24小时单台矿机允许的 BTC 交易总次数 limit	需要不断治理来修正的系数
LA_{btc}	过去 24小时单台矿机允许的 BTC 交易总金额 limit	需要不断治理来修正的系数
MLA_{btc}	单次转账最大金额	MLA 可治理优化
price(BTC)	USDT 本位的 BTC 价格	来自Offchain Worker 可信节点的价格数据，也可来自可信链上价格数据, 比如 ChainX 的 X-BTC 价格数据
SR	钱包发起交易在这笔交易总算力中占比	SR+RR =1
RR	交易接收方在这笔交易总算	SR+RR =1
SSR	推广上级分润比例	0<SSR<1，可治理优化
OSR	推广上上级分润比例	0<OSR<1，可治理优化
MR	每日最低奖励数量	MR 可治理优化
MSR	矿工分享到手续费比例	MSR 可治理优化

例子： 矿工P进行一次转账挖矿，转账 m 个 BTC，其算力计算如下：

$PCW_{btc} = \alpha * 1 / TC / PPC_{btc}$

$PC_{btc}<LC_{btc}$ or 0

$PAW_{btc}= \beta *m*price(BTC)/TW/PPA_{btc}$

$PA_{btc}<LA_{btc}$ or 0

$PW^{1}_{btc}=(PCW_{btc}+PAW_{btc})*SR$

5.4 挖矿奖励和减半

算力根据各个主流数字货币来分开计算的出发点：各个主流数字货币在交易支付市场中所占份额不同，给予每个数字货币一个最高份额，是考虑到有些数字货币的交易手续费模型比较特殊。比如EOS，是不需要交易手续费的，其转账成本几乎为零，如果其算力没有一个占比限制，那可以在EOS上发起大量的交易，这是一种无成本的攻击。如果直接剔除EOS这一类的数字货币，又跟TransX聚合支付兼容主流数字货币的初衷不符，给予一个可以治理修正的限制是折中的方案。

挖矿奖励是根据一次转账计算出来的算力在过去24小时中占比，然后乘以当日所能铸造的DCAP数量，计算出奖励Token数量后，还需要考虑两种情况：

- 如果矿机有推广上级，则需要分润SSR给上级。
- 如果矿机还有推广上上级，则需要分润OSR给上上级。

TransX每4年减半，早期为了补贴运行出块节点，将TransX上的交易手续费部分给到出块节点，当每天挖矿奖励Token数量小于MR，则可以将手续费MSR的比例给到挖矿奖励，剩下（1-MSR）给到出块节点。当然出块节点除了手续费是其收益之外，还有总发行量的10%作为出块奖励给到所有参与出块的节点，出块节点是整个TransX共识网络最重要的组成部分，同时也提供大量的成本负责出块记账和区块存储，给10%的Token奖励是合理的设置。

5.5 可验证

区块链技术提供了一个去中心化分布式的技术范式，但是众多商业应用场景总需要追求效率，在一个节点众多的去中心化分布式系统中，想要追求完美的共识并能拥有高效率，非常不切实际。但是有一个技术点是区块链技术值得追求的，那就是可验证。只要使用链上公开的数据，然后按照链上或者智能合约的逻辑去运行代码，都能得到相同的结果，这就是可验证的逻辑。

具体到TransX的可验证逻辑，是有两层含义：第一层含义是交易可验证，不管是哪条链上的交易，任何第三方都能够验证，任何一笔交易都需要进入不可逆区块才能够确认为交易完成，才能够参与TransX的交易挖矿；第二层含义是算力计算可验证，整个算力计算逻辑在上面已经公开透明，整个代码也会开源，任何第三方根据任何一笔可验证的交易去计算相应的算力，都能够得到一样的结果。

5.6 抵押和惩罚

出块节点需要自己抵押一定数量的DCAP，以防止出块节点行为不端，特别是在计算算力的时候输入不符合事实的数据，比如转账金额夸大，伪造假的交易数据发起攻击。

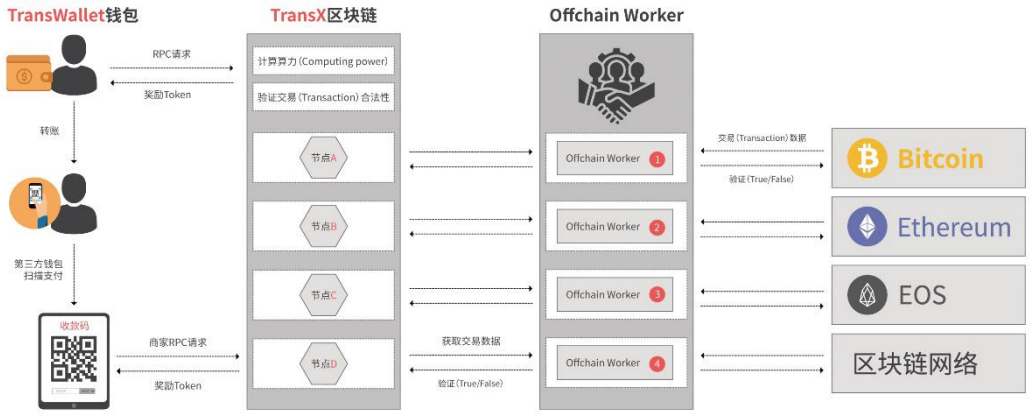
一旦发现这种作弊行为，就能够举报，然后议会就会进行评议，一旦评议通过就会给予惩罚，

TransX设置的惩罚规则是罚掉出块节点的抵押Token，给予部分奖励（初始设置为0.5万DCAP）给发现举报作弊行为的节点，其它直接销毁。

5.7 捕捉作弊和举报

TransX利用Substrate的Offchain Worker来捕捉作弊行为和完成举报工作，但TransX主链也会开放任何第三方举报的通道。Substrate的Offchain Worker可以独立完成一些不确定性和执行时长不确定的工作，对交易进行验证，对交易行为的算力计算进行验证，这些工作都能够通过Offchain Worker来进行。同时，还能够对行为不端的节点和不端行为进行举报。节点在进行举报的时候，或者任何第三方进行举报的时候，是需要抵押一定Token（初始设置500 DCAP），如果TransX议会认定为恶意举报，就会罚扣掉抵押并直接销毁。

5.8 架构图



5.9 各币种系统初始值

(以USDT为价值单位)

币种	占比 ρ	LC	LA	MLA
BTC	70%	100	100,000	100,000
ETH	10%	200	50,000	40,000
EOS	8%	1000	50,000	10,000
USDT	50%	100	100,000	50,000
DCEP	50%	2000	1000,000	5,000
DOT	10%	500	50,000	20,000

DCAP	50%	4000	2000,000	10,000
TUSD	70%	4000	2000,000	50,000

6.TransX稳定币框架

6.1 两种稳定币方案

初略来划分，有两种发行稳定币的方案，一种是中心化的方式，采用抵押法定货币在中心化金融机构，然后中心化机构发行稳定币，典型的是USDT。另外一种是MakerDao这种方式，同样采用有抵押的机制，但不再是中心化的机构来发行稳定币，而且抵押也不再是法币，而是其他有价格波动的数字货币。

以上两种方式各有优缺点，当然如果都没有任何抵押的方式来发行稳定币，或者采用不稳定的资产来做抵押，然后发行稳定的数字货币，我们在此不讨论这种情况。采用法币抵押，中心化机构发行稳定币，是信任来源很难保证，特别是所托管资产的金融机构还不能按时合法披露报表，而采取去中心化来发行稳定币，又存在一定的技术门槛，其推广成本比较高。

6.2 TUSD的发行架构

TransX的稳定币发行架构是结合中心化和去中心化治理的。TransX采用多资产模块，可以发行多个稳定币，也就是说各个国家多法币做抵押的稳定币都能够采用TUSD的框架来发行。TransX为何采用法币来做稳定币抵押品？让我们来思考下，稳定这个共识概念的来源，稳定是每个人对价值对一种感觉，而大部分人对价值对感觉来自物价，关键是人的生命长度有限，对物价短时间感觉造成了法币稳定的错觉，但错误的共识也是共识，TransX的稳定币TUSD也是构建在这种共识基础上。

比如，TransX的美元稳定币TUSD，涉及到的参与主体有中心化的银行机构、铸币者、TransX基金会、TransX议员。稳定币TUSD的发行流程如下：

1. 铸币者购买100万美国30年期长期国债，保存到TransX指定的美国9大银行任意一家。国债持有者是TransX基金会，基金会只持有，不能止兑。

2. 银行开出证明，并且还要定期请可信第三方做审计和信息披露。

3. 铸币者拿着银行的证明，在TransX链上发起铸造100万TUSD的提案。

4. TransX议会验证银行开出的证明，投票表决是否允许铸币。获得绝大多数议员赞成票即可通过。议员和技术委员会拥有一票否决权力。

5. TransX议会通过的提案，就会自动调用铸币方法，发行100万TUSD给到铸币者。

流程中还涉及到TUSD的销毁，后面介绍。

TransX稳定币发行涉及到如此多主体，利益分配合理才是关键，银行帮助铸币者开出证明，借用了中心化银行的信用度，银行将获得国债收益的1/3；铸币者获得国库中一定比例的手

续费，形式是DCAP；TransX基金会代为持有国债，根据跟银行、铸币者的三方协议，TransX基金会将获得国债收益的1/3。

TUSD的销毁流程：持有一定数量TUSD的用户，可以到银行申请国债的止兑，银行审核TUSD转入销毁地址，做好信息披露，然后把美元国债交割，止兑用户拿到相应美元，国债剩下1/3的收益将给到最先铸币的铸币者。

7.钱包入口

7.1 TransWallet

TransX将数字货币聚合支付平台搭建成功之后，需要有一个具体的产品来承接需要支付的用户，一个支持多链的钱包将是必备基础。为了激励用户使用钱包，用户使用TransWallet进行交易时，主流数字货币都能够参与挖矿，前提是用户已经注册激活TransWallet的挖矿功能。

TransWallet作为一款数字货币的钱包，有下面三点创新，使得其不同于已有的数字货币钱包。

- 支持TransX上交易收款即挖矿的功能。
- 定位支持Polkadot等Web3.0生态。
- 支持接入跨链的去中心化交易所，跨链的资产网关，比如ChainX。

深入思考如今区块链行业的中心化交易所所扮演的角色，其有两层作用：

- 价值存储平台，众多用户担心数字资产存放在自己钱包，难以保证资产安全，依赖中心化交易所来保存数字资产。
- 资产交易通道，不管是法币出入通道，还是币币兑换，中心化交易所都能提供这部分功能。

但如果从人性本恶的角度去思考问题，处于中心化垄断地位的交易所在这两方面都有可能作恶。大量用户的数字资产在中心化交易所存储，交易所能动用用户的资产，作恶能轻松盈利的前提下，显然其作恶成本几乎为零。此外，中心化交易所提供了币币兑换和法币出入通道，但也提供了很多赌博性质的东西。这导致很多中心化交易所变成一个庞大赌场，进去参与的用户最后只能认赌服输。

TransX的钱包定位是价值存储，帮助用户将数字资产掌握在用户自己手中，然后在TransWallet中接入多链的去中心化交易所，提供一层币币兑换通道。最后，在TransWallet接入OTC功能，引入法币出入金通道。基于此价值存储的思路，

7.2 冷钱包

TransWallet定位是热钱包，数字资产小额使用热钱包，更加方便完成支付等操作，但大额需要使用冷钱包进行存储，所以，针对TransWallet热钱包方案，还有冷钱包配套方案，冷钱包通过蓝牙跟TransWallet连接，保证私钥不会接触联网设备，从而保证数字资产的安全。

7.3 TC卡

TC卡是TransCredit卡，将小额数字资产存储到信用卡，结合TransX客户端和TransWallet进行交易的发起，通过NFC技术进行刷卡支付，加速数字货币实现支付场景的落地。

8.社区治理

TransX是一个去中心化的应用链，TransX的发展离不开社区治理的推动，对于多方利益博弈的方式，社区治理是帮助TransX完善和落地的必由之路。

TransX议会是治理的核心组织单位，将容纳社区节点和生态节点，比如主流数字货币接入TransX而组织起来的节点。TransX为了议会能高效达成共识，设置13个议会席位，由得票数的前13名且有意加入议会的诚实节点担任，任何有贿选返利的节点将无法参与议会选举。

由于节点总的票数经常变化，但议会需要在一段时间内保持一定的固定群体，所以每届议会的任期为3个月。每届任期满后，将根据新的总的票数和节点诚实度选出下一届议会成员。13位议会成员都可以收集社区意见并向议会提交议案。由议会成员采用一人一票的方式对提案进行初审表决，如果超半数议员同意，则提案通过初审。初审通过即进入公投流程，公投通过所需投票同意率是要根据自适应法定人数偏差算法来定，通过后，将由TransX开发团队负责实施并上线。

由于贿选和返利行为严重影响总得票数的可信性，并增加节点后期作恶的风险，通过不当手段得到的议会席位将严重妨碍社区总体利益。所以议会基金开通贿选钓鱼奖励，贿选标准很明确，不能有任何返利行为，任何社区成员均可匿名提交某节点的贿选和返利行为的截图或转账记录证明，如果超半数议员认为证据有效，则将剔除该节点的下届议员的竞选资格，并从议会基金中酌情给予举报奖励，此外议会将有权惩罚该贿选节点的自抵押。声称不参与议会选举的节点不在举报范围，议会成员是为社区服务的，并不会有更多的出块奖励，所以希望投票成员不要为了短视的返利而引发恶意性竞争。

8.1 链上治理

TransX的链上治理流程借鉴Polkadot，提出议案、投票、提案通过或否决、执行。整个链上治理流程都具有确定性。提案在链上的表现形式是一段代码，实施提案就是函数调用set_code方法，此方法拥有至高无上的权利，可以做任何事情，可以直接改变区块链的状态。链上治理是一种完美的人类群体共识思维跟机器执行逻辑紧密配合的过程。

链上治理的基本原则是：所有协议级别改动必须通过全民公投，链上治理的主体构成有全民公投、议会和财政系统等，执行细则上有自愿锁定增强投票力、延时实施提案和自适应法定人数偏差等。

一个完整的治理流程大致有三个阶段：

- 全民提案阶段，抵押一定数量的Token进行提案。
- 全民公投阶段，每隔一段时间，抵押数量最高的提案将会进入公投阶段。
- 计票实施阶段，提案获得足够支持，按照机制实施提案。

投票阶段，用户可通过自愿锁定更长时间来增强投票力，一个币锁定六天等同于六个币锁定一天的投票力。

自适应法定人数偏差算法：简单理解就是当投票率降低时，通过提案所需要的投票同意率也随之提高。

8.2 议会职能

议会主要有两个任务：

- 发起公投，议会成员多数同意，无一反对，议会可直接发起一个公投。
- 取消公投，议会成员一致同意某些公投会对系统造成危害，或有风险时，可取消公投。

9.发展路线

第一阶段：开发和测试TransX主链，2019-08到2020-03

第二阶段：开发和测试挖矿客户端和矿机硬件，2019-08到2020-04

第三阶段：跟第三方钱包沟通，兼容支持TransX的聚合收款二维码，2019-11到2020-05

第四阶段：多链钱包开发和测试，2019-08到2020-06

第五阶段：TransX上稳定币TUSD的发行，2020-06到2020-12

第六阶段：跨境支付和接入Polkadot生态，2020-08到2021-12

10.布局生态

10.1 跨境支付

今年观察到一个最完美的用来做跨境支付的解决方案，那就是Facebook的Libra，不过Libra不能实现落地成为大概率事件，主要原因是Libra的定位是世界通用货币跟现在主流的主权货币直接碰撞，所遭遇的法律阻力过大。中国央行即将推出的DCEP也是用来做跨境支付的好方案，不过并不是完美方案，因为DCEP背后是人民币，而人民币在全球并不是通用型货币，可能在一带一路能发挥清算结算功能，但在更多其它国家可能会遭遇阻力。TransX的跨境支付功能将是对DCEP的一种补充。

TransX上支持DCEP、USDT等稳定币，同时，TransX链上也将首先发行自己的稳定币TUSD，用户可以自由选择方便的币种进行交易支付。TransX将有一个发行稳定币的框架，也能够发行多个国家的法币对等的稳定币。

跨境支付一个更加广泛的场景发生在线上，数字货币支付的确认时间比较长，对于线上订单的状态更改很难做到及时，但TransX仍然可以延长监控时间，检测到支付到账已被确认时，通过发送异步消息给到商家，商家可以完成跨境的电商交易。当然，商家可以推荐用户使用确认时间较短的数字货币进行支付，比如EOS和TUSD，其确认时间都能达到几秒到一两百

秒。

TransX为了服务这些跨境电商业务，将推出这种免手续费、免佣金的数字货币聚合支付服务，接入SDK也将更加简单和方便。

首先从传统线上支付解决方案说起，其抽象流程如下：

线上未支付订单 -> 用户点击支付 -> 用户完成支付 -> 中心化服务器监测到支付完成 -> 通知客户 / 同时通知商户 -> 商户收到通知，更改订单状态

TransX也是能够支付线上支付场景的，只是其抽象流程稍微有点不一样：

线上未支付订单 -> 用户点击支付 -> TransX JS SDK给出收币二维码 -> 用户扫码支付并点击确认支付 -> 商家中心服务器验证链上支付并完成TransX挖矿 -> 更改订单状态

同样可以简单抽象成以上6步，并且不需要对接中心化的支付机构，存在各种审核和审查。只需要对接TransX的前端JS SDK和服务器端的验证软件即可。将后端的验证软件部署到服务器，服务器接收到前端传过来的已完成支付请求后，丢给验证软件去完成验证，等其完成验证，会异步通信请求设置好的接口，通知服务器更改订单状态，并且该软件还能帮助商家完成TransX链上挖矿。

10.2 可信计算和个人区块链信用分

支付数据、余额数据、借放贷数据、投资数据、股权Token数据等，都是个人隐私数据，基于TransX客户端和TransX Wallet都不会恶意收集用户的隐私数据，等TransX具备对接第三方可信计算方 (比如Phala网络) 的时候，能确保数据安全保存的前提下，TransX客户端和TransX Wallet会本地加密用户的隐私数据，同时存储在去中心化网络中，结合可信计算方，可以在这些数据的基础上计算一个可信的个人信用分。

目前的个人信用体系都是中心化架构的，不仅数据是中心化保存，而且计算过程也是中心化不可信的，最为关键的是，这些数据产生的价值完全被中心化的互联网巨头所把持。

基于TransX实现的是交易去中心化，基于去中心化存储数据是完成数据的去中心化，基于可信计算实现的是计算去中心化，组合这些工具，利用区块链不可篡改的特性，构建个人的信用分是未来更多区块链产品的基础，同时也能够在可信计算的过程中，用户授权更多的个人隐私数据加入计算，使得个人信用分更具有说服力。

10.3 跨链支付快速通道

在TransX上发行稳定币TUSD，使用TransX上的稳定币在TransX生态支付，能够获得更高的算力。数字货币聚合支付领域的稳定币是使用场景更加广泛的，TUSD相比于其他的稳定币，其优点有如下几个：

- 更快速的确认时间。
- 更高的TransX算力奖励。
- 更强的跨链结算能力。

通过以上三个优点来做稳定币，是TransX的主打思路。。

10.4 接入Polkadot生态

接入Polkadot，不仅仅让万链互联，还让资产都能通过聚合支付完成简单支付操作。当TransX接入Polkadot后，将可以接入Polkadot的验证节点，让其为TransX提供共识层面的安全。有了这一层的安全支撑，在TransX上的交易和稳定币发行都能有足够的安全保证。