



elastos white paper

Chytrý-web napájený blockchainem

Vytvořila: elastos foundation

Leden 1, 2018

Popis

Tento dokument popisuje Elastos white paper verzi 0.2, který obsahuje dodatečné informace o strategických cílech a technologických plánech Elastos. Elastos bude průběžně aktualizovat tento white paper, aby odrážel nové vývoje. Pro nejnovější informace o Elastos white paper, plánech, týmu, zakladatelskému managementu, investorech a strategických partnerech, prosíme navštivte oficiální Webovou stránku:

<http://www.elastos.org>

Kontakt

Elastos Foundation:

Elastos (Shanghai):

The 11th floor, Huahong International Building

No. 463 the Tanggu Road, Hongkou District

Shanghai, China 200080

Elastos (Beijing):

Plug & Play, Building G

Zhongguancun Yingzao Street

No. 45 Chengfu Road, Haidian District Beijing,

China 100084

Email:

White paper skupina: whitepaper@elastos.org

Globální komunita: global-community@elastos.org

Elastos fund: Elastos-fund@elastos.org

Vztahy s veřejností: pr@elastos.org

Vztahy s investory: ir@elastos.org

Elastos rada: elastos-council@elastos.org

Jiné aféry: contact@elastos.org

Elastos Foundation je registrovaná v Singapuru.

Copyright tohoto dokumentu vlastní Elastos Foundation, všechna práva jsou vyhrazena.

Upozornění na autorská práva

Elastos Foundation si vyhrazuje všechna práva pro tento dokument.

Vyloučení odpovědnosti

Elastos bude neustále vyvíjet svoji technologii a organizační strukturu, ale cílí zachovat současné řídicí principy Elastos komunity a také plánu přidělování Elastos tokenů.

1. Úvod do Elastos

Elastos si klade za cíl vytvořit nový druh Internetu, který bude postaven na blockchainové technologii. Na tomto novém Internetu budou lidé schopni vlastnit digitální aktiva a generovat z nich bohatství. V současné době existuje zdánlivě nekonečná zásoba digitálních knih, filmů, hudby a her. Ale lidé tyto digitální aktiva nezbytně nevlastní. Máte možnost například zakoupit digitální knihu, ale nemůžete ji nikomu jinému prodat. Vlastníte ji tedy doopravdy? Elastos chce vytvořit digitální aktiva, která jsou vzácná, identifikovatelná a obchodovatelná. Vlastnická práva jsou cestou ke generování bohatství a Elastos si klade za cíl vytvořit celosvětovou síť, která tato práva respektuje.

Cílem je vytvořit Internet, který umožňuje uživatelům přístup ke článkům, filmům a hrám přímou cestou, bez využití přehrávače, či jiné platformy vytvořené třetí stranou. Elastos využije blockchainovou technologii k vystavení identifikace pro digitální tvorbu. Toto umožní lidem zjistit, kdo digitální aktivum vlastní. Na Internetu Elastosu budou filmaři vědět, kolikrát byl jejich film shlédnut. Kombinace Elastosu a blockchainové technologie utvoří základ pro důvěryhodný a bezpečný Internet Digitálního Majetkového Bohatství.

Elastos bude platforma pro decentralizované aplikace (Dapps), která poběží na peer-to-peer síti bez centralizované kontroly. Lidé budou mít přístup k těmto Dapps skrze jejich mobilní telefony, bez změny jejich operačního systému. Starý Internet je Web informací. Když kliknete na URL, získáte data. Elastos vytváří Web aplikací. Když kliknete na URL, získáte kód. Elastos Web bude speciální ekonomická zóna, kde budou Elastos tokeny fungovat jako její základní měna.

Elastos je open-source software, jehož vývojový proces byl sponzorovaný giganty průmyslu jako Tsinghua Science Park, TD-SCDMA Industrial Alliance a Foxconn Group za více než 200 milionu čínských juanů. Elastos zveřejnil více než deset milionu řádků zdrojového kódu, zahrnujících čtyři miliony řádků originálního zdrojového kódu.

2. Technologické Pozadí

Bitcoinový blockchain je speciální druh decentralizované a neměnné účetní knihy kryptoměn, která jejím držitelům umožňuje vkládat důvěru v data. Ethereum implementovalo programovatelný blockchain, který podporuje chytré kontrakty, čímž jeho držitelům umožňuje vkládat důvěru v kód. Chytré kontrakty, jednoduše řečeno, umožňují okamžité vypořádání transakcí, jakmile dojde k naplnění všech závazků vyplývajících z kontraktu. Například prodejci dostanou zapláceno až v momentě, kdy je jejich produkt úspěšně přijmut kupující stranou. Společnosti, které dělají crowdfunding mohou přiřadit specifický výrobní úkol až v momentě, kdy získají určitou hranici peněžních prostředků. V opačném případě budou peníze vráceny účastníkům.

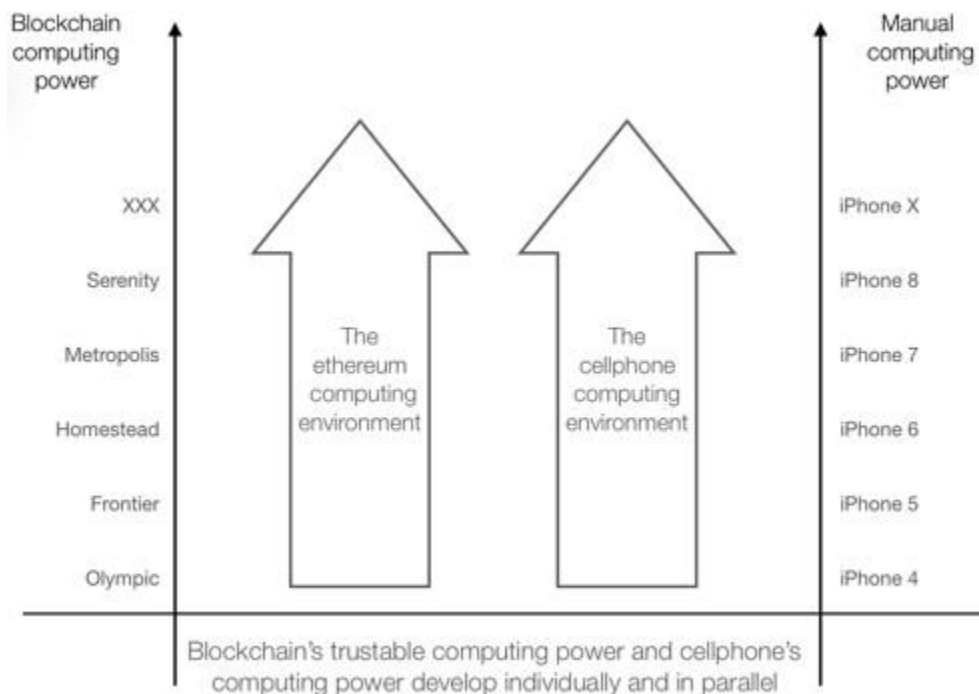
Díky chytrým kontraktům se nemusíme bát o porušení smluv nebo zápočtu kreditů našich obchodních partnerů, jelikož blockchain uskuteční transakci až v momentě, kdy obě strany splnily své sliby. Tento systém eliminuje nedůvěru mezi kupci a prodejci. Otázkou je: Jak můžeme aplikovat tento systém chytrých kontraktů na ještě širší pole podniků? Mohli bychom tento systém využít k řízení elektronických knihkupectví nebo obchodních platformách pro video hry, či filmy?

Chytré kontrakty Ethereum jsou užitečné při aplikaci na finanční, či částečně finanční projekty, a také na online hlasování. Elastos nicméně věří, že Dapps založené na Ethereum mají následující omezení:

- Úložný prostor a rychlost. Kapacita úložného prostoru je limitována na samotný blockchain, který může uložit pouze omezené množství dat a to velmi malou rychlostí. Popularita blockchainové hry CryptoKitties vytvořila zahlcení Ethereum blockchainu, čímž zvýraznila problém fungování chytrých kontraktů pouze na hlavním veřejném blockchainu.
- Chyby. Jakmile jsou chytré kontrakty uvedeny do provozu, jsou nezastavitelné a nevratné. Toto je logické, jelikož jsou obě strany chráněny: Odsouhlasený kontrakt nemůže být zastaven nebo změněn. Ale chyby chytrých kontraktů, jako třeba útok DAO existují. Navíc, neexistuje způsob, který dokáže, že program nemá žádné chyby.

-
- Cena. V současné době, chytré kontrakty, zaznamenávání dat a spouštění kontraktů jsou všechno úkony prováděny na blockchainu. To znamená, že mnoho nodů opakovaně vykonává stejné úkony. Při provedení jakéhokoliv úkonu vyžaduje Ethereum platbu poplatků. To znamená, že vykonávání kontraktů na Ethereum se může prodražit.
 - Odpadní data. Existuje akumulace historických odpadních dat na Ethereum blockchainu. Jakmile je chytrý kontrakt uveřejněn, zůstane uložen na blockchainu navždy. Odpadní a přebytečná data mají negativní vliv na efektivitu blockchainu a toto může vést k zahlcení Ethereum.
 - Nedostatek flexibility. Spojení mezi blockchainem a Ethereum Virtual Machine (EVM), který vykonává chytré kontrakty, je činí neoddělitelnými. Vylepšení blockchainu ovlivňují EVM a vylepšení EVM ovlivňují blockchain.
 - Bezpečnost. Chytré kontrakty běžící na Ethereum nebo systémech založených na Ethereum jsou předmětem hrozby útoku prostředníka, a to kdykoliv jde uživatel mimo blockchain na jiné Webové stránky.

Díky problémům uvedeným výše, Elastos věří, že je obtížné a nevhodné pro uživatele, aby četli digitální knihy, hráli hry nebo používali šifrované chatování pomocí chytrých kontraktů Ethereum. Navíc, lidé jsou zvyklí na provoz aplikací na jejich mobilních telefonech. Elastos chce, aby měli uživatelé přístup k systému založeném na důvěře blockchainu skrze mobilní zařízení, které již používají.



Jak můžeme vidět na obrázku výše, nezáleží na tom, jak výkonný uživatelův mobilní telefon je, neurychlí výpočty Ethereum. Nehledě na to, kolik vylepšení Ethereum má, jeho záruky důvěryhodnosti se netýkají běžného užívání mobilních telefonů. Je to kvůli tomu, že výpočetní síla Ethereum a mobilních telefonů nebyla vyvinuta a provedena souběžně, není tedy integrovaná.

Dnešní chytré kontrakty jsou navrženy tak, aby fungovaly výhradně na blockchainu. Elastos bude naopak spouštět Dapps, které jsou umožněny blockchainovou technologií, ale nemusejí běžet na samotném blockchainu. Elastos umožní uživatelům přístup k Dapps přes jejich současný operační systém. Dapps budou běžet na Elastos Runtime, který funguje na Androidu, iOS a PC.

Pokud si to shrneme, Ethereum je skvělý pro chytré kontrakty. Ale Elastos věří, že existují dva hlavní důvody, proč Ethereum EVM není vhodný pro běh Dapps:

- Blockchainy jsou vytvořeny pro souhlasné vedení záznamů, ale hlavním nedostatkem je výpočetní rychlost a flexibilita.

-
- Současné blockchainya jsou navrženy tak, aby nahrávaly transakce, ne aby uchovávaly data. Na současném blockchainu jednoduše není dostatek místa pro uchovávání většího množství digitálních filmů a knih.

Jako řešení prvního problému, Elastos navrhuje zavést flexibilní hlavní a vedlejší blockchainovou konstrukční strukturu. Hlavní chain bude pouze zodpovědný o základní transakce a převody plateb, zatímco vedlejší chain bude vykonávat chytré kontrakty pro běh různých aplikací a služeb.

Jako řešení druhého problému, Elastos spouští své aplikace na Elastos Runtime, namísto již nyní zahlceného blockchainu. Tato metoda je také více bezpečná. S Elastos, všechna síťová data musí být odeslána skrze důvěryhodné a identifikovatelné kanály. Identifikace a ověření pravosti přichází z blockchainové ID. Tímto způsobem, blockchainová důvěryhodnost může být převedena do Elastos Runtime. Elastos Runtime může mít mnoho podob: nezávislý OS, Virtuální počítač nebo software development kit (SDK), který se integruje do nativních aplikací jiných mainstreamových operačních systémů.

Filozofie designu Elastos je integrace pohodlí mobilních telefonů s důvěryhodností blockchainové technologie, čímž umožní uživatelům přístup k aplikacím bez toho, aniž by museli projít skrze třetího zprostředkovatele. Elastos vytvoří prostředí, ve kterém mohou být digitální aktiva obchodovatelná peer to peer.

3. Elastos: Blockchainem Napájená Celosvětová Síť

Návrhová filozofie Elastosu původem přišla od Rong Chen, bývalého senior software inženýra u Microsoftu. Na základě jeho zkušeností v Microsoftu, Chen chtěl vytvořit platformu, ve které aplikace a služby nemají dovolený přímý přístup k Internetu. Bez přístupu k síti by malware nebyl schopen ukrást uživatelská data nebo zaútočit na jiné služby na Internetu. Chenova vize byla následně vytvořena do open-source, lightweight operačního systému pro virtuální stroje (github.com/Elastos). V roce 2017, blockchainová technologie byla integrovaná do Chenovi vize, čímž umožnila vývoj Elastos Chytrého Webu.

Elastos Chytrý Web je složen ze čtyř pilířů:

-
- Elastos Blockchain. Elastos chce vytvořit decentralizovaný Chytrý Web, kde každé zařízení, jednotlivec, Webová stránka a digitální aktivum má důvěryhodné ID. Blockchainová technologie umožňuje zřízení důvěry na Internetu.
 - Elastos Runtime. Elastos Runtime je lightweight operační systém, který zabraňuje aplikacím a službám přímý přístup k Internetu. Elastos Runtime funguje na mobilních zařízeních nebo PC uživatele.
 - Elastos Carrier. Elastos Carrier je kompletně decentralizovaná peer-to-peer platforma. Tento carrier převezme všechnu síťovou komunikaci mezi virtuálními stroji a předá informace dále jménem aplikací.
 - Elastos Software Development Kit (SDK). Aplikace potřebují Elastos SDK pro přístup k jejich ID a službám Elastos Carrier na Chytrém Webu.

Elastos má následující rysy:

- Elastos veřejný chain je uspořádaný, jednoduchý a skrytý před aplikacemi a službami třetích stran.
- Elastos zabraňuje přetížení hlavního chainu tím, že má několik předdefinovaných vedlejších chainů zabudovaných do Elastos Carrier platformy.
- Elastos podporuje koncept vlastnických práv digitálního obsahu. Elastos je schopný vydávat tokeny pro digitální aktiva nebo aplikace a navázat vlastnictví digitálního obsahu skrze chytré kontrakty.
- Elastos Runtime funguje na OS mobilního zařízení uživatele. Aplikace jsou zdarma a jejich výkon je porovnatelný k již existujícím mobilním aplikacím. Elastos podporuje tradiční programovací jazyky, čímž docílí poměrně snadného způsobu psaní kódu. Elastos také podporuje populární programovací frameworky.
- Oddělení aplikací od sítě zajišťuje, že digitální obsah nemůže uniknout.

-
- I přestože aplikace Elastos fungují na operačních systémech jako iOS, Android a Windows, lokální OS nebude schopný sabotovat vlastnická práva digitálních aktiv. Hodnota digitálních aktiv je zachována.
 - Pro klasické Android nebo iOS aplikace, a ne Elastos aplikace, uživatelé mohou využít přístup k Elastos Chytrému Webu pomocí Elastos SDK. Uživatelé se mohou přihlásit ke klasickým aplikacím pomocí jejich ID Elastos Chytrého Webu. Uživatelé také mohou mít své ne-Elastos aplikace uložené v Elastos cloud storage.
 - Jak Elastos chytré kontrakty, tak i Elastos Dapps fungují na Elastos Chytrém Webu. Toto vytváří uzavřenou platformu, čímž se vyvarujeme nutnosti pohybovat se na a mimo blockchain. Tato uzavřená platforma vytváří speciální ekonomickou zónu, kde se uživatelé mohou cítit bezpečně při obchodování s digitálními aktivy. Tímto způsobem vytvoříme uzavřený okruh produkce, transakcí a spotřeby, která je nezbytná k vytváření digitálního majetkového bohatství.

Zde je krátký souhrn unikátních Výhod Bitcoinu, Ethereum a Elastos:

- Bitcoin = Důvěryhodná Účetní Kniha
- Ethereum = Důvěryhodná Účetní Kniha + Chytré Kontrakty
- Elastos = Důvěryhodná Účetní Kniha + Chytré kontrakty + Zpeněžitelné Dapps a Digitální Aktiva.

Současná blockchainová technologie umožňuje zaznamenávání vlastnických práv. Ale zatímco uživatelé mohou dokázat, že digitální knihy patří jim, nemohou nezbytně zabránit lidem od krádeže nebo četby těchto knih bez povolení. V takovém prostředí je velmi těžké monetizovat digitální aktiva. Elastos cílí vyřešit tento problém tím, že vytvoří prostředí, kde všechny úkony s digitálními aktivy (tj. prohlížení, kupování nebo prodávání digitálních filmů) probíhají na Elastos Chytrém Webu, a tedy podléhají pravidlům chytrých kontraktů. Vývojář digitálního obsahu může použít nástroj, který poskytne Elastos, aby zjistil jaké množství digitálního obsahu má vytvořit. Autoři se například mohou rozhodnout, že chtějí mít pouze 5000 kopií jejich knihy v oběhu na Chytrém Webu. Stanovením konečného čísla digitálního obsahu vytváříme strach z nedostatku a umožňujeme realizaci kapitálu.

Elastos chce také umožnit spotřebitelům stát se investory. Řekněme, že existuje pouze 5000 kopií digitální knihy v oběhu, a že se tyto knihy stanou extrémně populárními. To znamená, že každá z těchto knih vzroste na hodnotě, čímž se vytvoří potencionální bohatství pro osoby, které je zakoupili. Poté, co si spotřebitel knihu užije, ji může dále prodat někomu jinému za vyšší cenu. Uživatelé také mohou nakoupit limitované edice herních aplikací. Jakmile si zahrají tyto hry v Elastos Runtime v jejich mobilních telefonech, mohou je prodat jiným lidem. Jelikož jsou tyto hry jsou limitovanými edicemi, jejich hodnota bude na trhu fluktuovat.

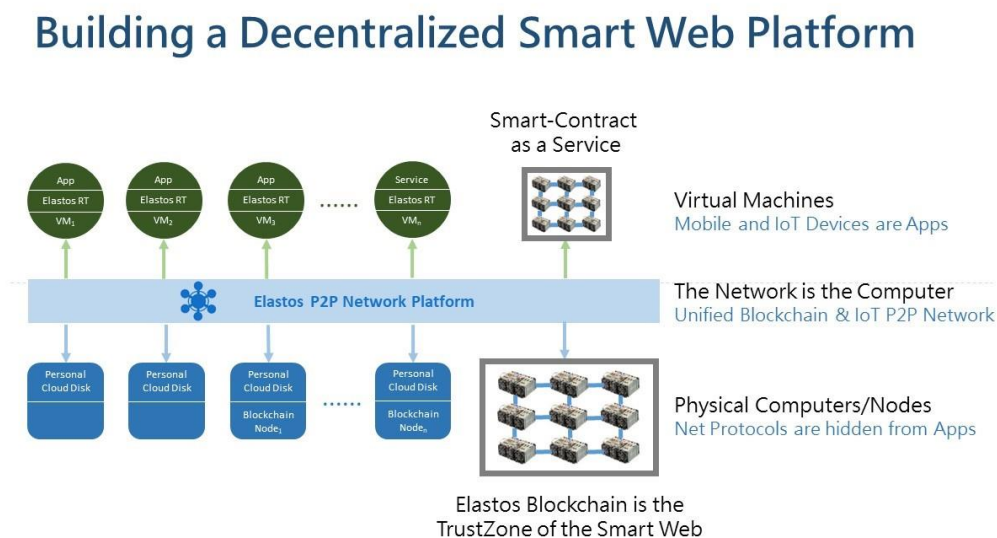
V dalším případě využití, mohou filmaři sbírat peníze pro jejich filmy pomocí crowdfundingu, skrze vydání jejich tokenů. Filmaři mohou napsat chytrý kontrakt, který říká, že pokaždé, když někdo shlédne film, dostanou držitelé tokenů malý podíl z poplatku. Filmaři také mohou napsat další chytrý kontrakt, který umožní filmovým divákům prodat film peer-to-peer nebo skrze sociální média a získat komise.

Tento systém vytváří finanční příležitosti jak pro tvůrce, tak i pro spotřebitele, čímž motivuje více lidí k využití Elastos. Akumulace většího množství uživatelů bude motivovat více tvůrců

k vytváření digitálního obsahu na Elastos platformě. Tento růst obsahu může přitahovat ještě více uživatelů a tito další uživatelé budou vytvářet ještě více obsahu. Jedná se o pozitivní cyklus, který bude mít za následek zvýšení počtu cenného digitálního obsahu, který může být využit ke generaci digitálního majetkového bohatství.

4. Platforma Decentralizovaného Chytrého Webu

Schéma zobrazené níže ilustruje vztahy mezi klíčovými komponenty Elastos platformy:



4.1 Ověřování Práv Digitálních Aktiv, Obchodování a Oběhu

Strach z nedostatku v zemědělském věku byl nahrazen velkými daty v informativním věku. V dnešní době, digitální zdroje mohou být bez nákladů duplikovány. I přesto, že digitální aktiva jsou široce produkována a konzumována, negenerují nezbytně bohatství. Pokud nejsou digitální zdroje ověřeny, často to vede k vedlejším efektům jako pirátství a nedostatku motivace pro originální inovaci.

Blockchainová technologie řeší tento problém tím, že tvoří ověřitelná a vzácná digitální aktiva. Elastos poskytuje potřebnou infrastrukturu pro autentifikaci, obchodování a oběh

digitálních aktiv. Kdykoliv je jakýkoliv digitální obsah zveřejněn online skrze blockchain, získá správné oprávnění, a poté může být tento obsah použit k obchodování a oběhu.

Elastos peněženka musí být použita k publikaci digitálních aktiv, zůstatek peněženky by měl být dostačující pro pokrytí těžařských poplatků. Vydavatel digitálních aktiv poté může vytvořit žádost o autentifikaci, která bude zahrnovat informace jako například adresa uživateli peněženky, Uniform Resource Identifier (URI), hodnota a množství aktiva. Poté bude hash číslo vypočítáno a transakce bude nahrána jako unspent transaction output (UTXO) na chainu. Poté co je záznam autentifikace aktiva zveřejněn na blockchain se z něj stane obchodovatelné digitální aktivo. Jakmile je aktivo zakoupeno, vlastnictví zakoupeného digitálního aktiva je převedeno zákazníkovi, což znamená, že může být opět prodáno.

4.2 Decentralizované Aplikace (Dapps)

Na základě již existujících kryptoměn a blockchainové technologie, zatím neexistuje jediná Dapp, která by mohla konkurovat mainstreamovým aplikacím. Důvodem je, že výpočetní síla a input/output operations per second (IOPS) decentralizovaných aplikací je poměrně slabá. Současná infrastruktura blockchainu může být jednoduše zahlcena. Elastos představí novou výpočetní paradigmu a umožní decentralizovaným aplikacím fungovat s IOPS, které bude srovnatelné s mainstreamovými aplikacemi.

Elastos blockchain je navržen pro využití hlavního a vedlejších chainů. Abychom předešli zahlcení, hlavní chain se zbytečnými daty, všemi chytrými kontrakty a aplikacemi bude fungovat na vedlejším chainu. Uživatelé mohou jednoduše vyvíjet bezpečné Dapps, které dále mohou spouštět z hardwarových zařízeních založených na Operačním Systému Elastos. V opačném případě mohou využít Elastos Runtime prostředí na tradičních operačních systémech (Android, iOS, Windows, atd.) pro vývoj decentralizovaných aplikací. K Elastos Runtime můžeme získat přístup skrze VM a SDK.

5. Elastos Blockchain

Podobně jako je tomu na operačních systémech na mobilních zařízeních, uživatelé potřebují důvěryhodnou lokaci pro ukládání důležitých dat. Elastos blockchain funguje jako tato zóna důvěry pro celou síť operačního systému.

Elastos blockchain používá řešení hlavního a vedlejšího chainu pro usnadnění chytré ekonomie a zdravého decentralizovaného prostředí pro aplikace. Toto znamená, že každá aplikace si může vytvořit svůj vlastní vedlejší chain. Elastos blockchain poskytuje již zabudovanou, kompletní a snadno použitelnou podporu. Zároveň budou přizpůsobitelné a umožní klientům vybrat si svojí vlastní consensus metodu podle toho, jak jim to bude vyhovovat.

Tokeny mohou být vydány na vedlejších chainech. Tyto tokeny se mohou účastnit v oboustranné výměně aktiv skrze hlavní a vedlejší chain. Zároveň bude díky sloučenému těžení spotřeba energie minimalizována, čímž se vyhneme rozsáhlým nákladům za elektřinu a uhelné emise.

5.1 Design Obchodu a Blocku

Struktura blockchainu Elastos je založena na již existujícím designovém systému kryptoměn, kterou prvně zavedl Bitcoin. Tento systém zahrnuje požadavky pro ověření pravosti blocku, jako například předchozí block hash, Merkle tree root hash, nonce pro konsensus algoritmus, časová razítka, cíle obtížnosti a další.

Elastos vylepšuje současný zážitek digitálních měn a adoptuje designovou filozofii vedlejších chainů. Elastos může do budoucna adoptovat funkce, které vylepšují vedlejší chainy, jako například odstranění validačních skriptů ze struktury transakcí. Vedlejší chain tvoří základ pro fungování Dapps na Elastos, zatímco struktura hlavního chainu Elastos poskytuje infrastrukturu a podporu pro vedlejší chainy, zároveň umožňuje převody aktiv.

5.2 Spojené Těžení

Elastos blockchain využívá spojené těžení s Bitcoinem. Jedná se o proces, při kterém je konsensus dosažen na obou chainech zároveň. V tomto případě, blockchain Bitcoinu funguje jako rodič blockchainu Elastos s Elastos chainem, jako jeho podpůrným blockchainem. Těžební pooly nasadí sloučený kód pro těžení a těžaři předloží proof of work pro oba blockchainya zároveň. Spotřeba energie se nezvýší se společným těžením a bude stejná, jako spotřeba energie pro těžbu u jednoho blockchainu. Skrze tento mechanismus má Elastos blockchain extrémně silnou garanci výpočetní síly a bude schopen poskytnout blockchainovou inovaci na globálním měřítku. Tímto způsobem Elastos plně využívá Bitcoinové výpočetní zdroje a také zůstává přátelský k životnímu prostředí. Dodatečné výhody spojeného těžení zahrnují:

1. Převod důvěry skrze několika chainy. Elastos hlavní chain je těžebně spjatý s Bitcoinovým hlavním chaine. Tato charakteristika spojeného těžení může být použita i na Elastos vedlejší chainy, a to v případě, že vedlejší chainy použijí stejný proof of work konsensus. Tím pádem, vrstvy chainů mohou být společně těženy rekurzivně, což zřizuje hierarchii důvěry mezi chainy.
2. Izolované Nodes. Pomocný blockchain nebo vedlejší chain, závislí na spojeném těžení nepotřebuje konsensus od několika nodů. V extrémních případech, jeden chain potřebuje pouze jeden node, čímž zároveň nezeslabuje spolehlivost informací účetní knihy na hlavním chainu nebo jiných chainech. Žádný jiný blockchain konsensus algoritmus nemá takovou výhodu.

5.3 Plán Distribuce Tokenů

Elastos Token (ELA) je platformový token na Elastos blockchainu. Může být použit pro obchodování, investování v digitálních aktivech, placení za blockchainové poplatky a podobně.

ELA je základní jednotka. Dodatečně, abychom uznali úctu zakladateli kryptoměn Satoshi Nakamoto, Elastos by chtěl použít Satoshi ELA (Sela) jako minimální jednotku měny pro ELA. 1 ELA se rovná 10^8 Sela.

Elastos vydá konečné množství tokenů. Celková výše Bitcoinů bude nakonec 21 milionu, Elastos by chtěl vytvořit celkem 33 milionu ELA. Plán distribuce a implementace ELA je následující:

ELA (jednotky: 10000)	Účel	Poznámky
1650 (50%)	Vývoj Ekosystému	Na základě času, kdy je Elastos genesis block vytvořen, Elastos potvrzuje držitele Bitcoinu a může jim odeslat ELA zdarma. Detailní pravidla jsou následující: <ul style="list-style-type: none"> • Cíl: Zpětná vazba kryptoměnové komunity a vytvoření efektivní cirkulace • Množství: Držitele Bitcoinu mohou dosáhnout ekvivalentního množství v ELA • Kanál: Vydávání ELA pouze skrze autorizované kryptoměnové směnárny • Metoda: Elastos Foundation povolí směnárnám vydat tokeny, nikdo nemůže automaticky obdržet ELA • Všechn ELA, který není nárokován, bude investován do Elastos. Tyto tokeny nebudou použity pro denní operace Elastos Foundation.
500 (15%)	Andělští Investoři	Andělští investoři Elastos se skládají z Elastos zakladatelů a klíčových partnerů. Výnosy z Bitcoinu poputují do Elastos Foundation.
800 (24%)	Soukromý & Veřejný Crowdfunding	Investorská komunita je páteří Elastos, bude podporovat a umožňovat vývoj Elastos. Všechny získané kryptoměny budou patřit Elastos Foundation a budou použity k vývoji Elastos platformy. Bitcoinové výdělků poputují do Elastos Foundation.
350 (11%)	Elastos Foundation	Tyto prostředky jsou předem přiděleny pro podporu operací Elastos Foundation a investic do Elastos ekosystému.

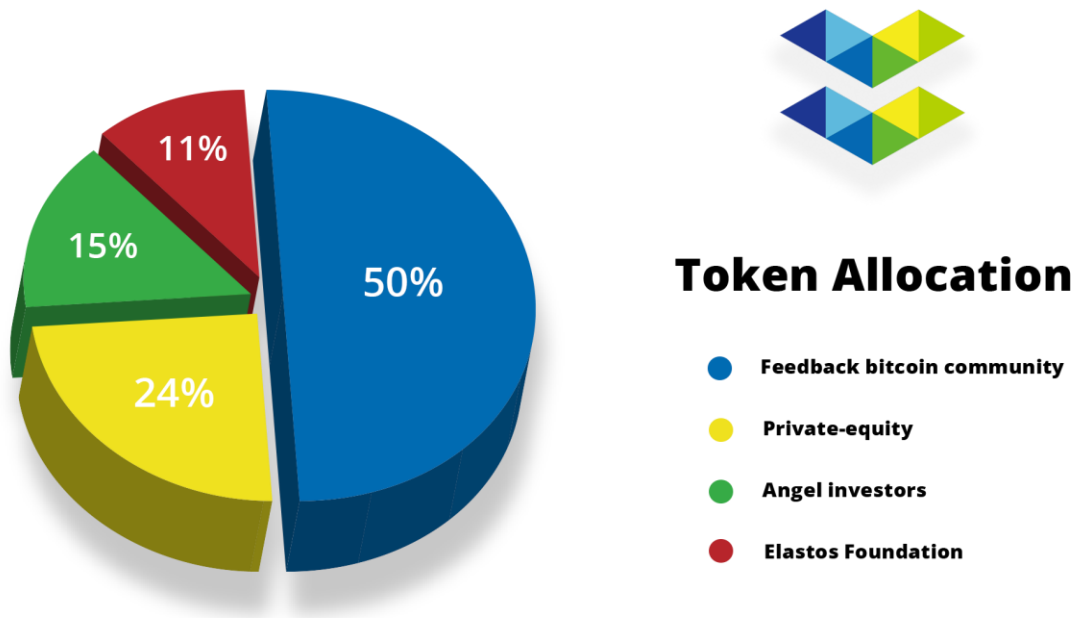


fig2. conversion relationships

Pro kompenzaci přirozeně ztracených tokenů, například když uživatel ztratí své peněženky, a k boji proti inflaci, množství ELA v cirkulaci budou ročně zvýšeno fixním množstvím 4%.

ELA bude vytvořen každé dvě minuty během spojeného Bitcoin těžení. Tyto nově vytvořené tokeny budou přiděleny Elastos Foundation a těžařům. Elastos Foundation získá 30%, zbývajících 70% bude patřit těžařům.

5.4 Vedlejší chainy

Jakýkoliv systém postavený na blockchainové technologii má méně výpočetní síly než tradiční počítač, tudíž nebude schopen splnit různé požadavky Internetových aplikací (například video hry nebo streamování filmu s vysokým rozlišením). Jedná se o základní důvod, proč blockchainy nemohou být stále aplikovány na Internet v širším měřítku. Elastos

tým rozpoznává tuto skutečnost, a věří, že blockchainový vývoj by neměl spoléhat pouze na hlavních chainech pro výpočty. Elastos si dává za cíl rozšířit blockchainový systém tím, že poskytne podporu pro vedlejší chainy, což pomůže splnit požadavky pro aplikace s vysokým IOPS.

Elastos hlavní chain bude zodpovědný za malé, ale velmi důležité role obchodování a převádění ELA, čímž poskytne stabilitu blockchainovému systému. Elastos se chce vyhnout zahlcováním hlavního chainu zbytečnými chytrými kontrakty. Místo toho, pouze hlavní vylepšení infrastruktury se budou odehrávat na hlavním chainu. Všechny ostatní chytré kontrakty mohou být implementovány na vedlejších chainech, což umožní škálovatelnost.

Tento druh hierarchie a filozofie strukturovaného designu bude tvořit cestu pro budoucí blockchainovou paradigmatu, jako třeba výše zmíněný vývoj ze samostatného výpočítávání do distribuovaného. Jedná se o klíčovou inovaci v blockchainové technologii a je důležitější než částečná technologie singulárního konsensuového algoritmu a chainů.

Náš tým implementuje základní služby jako vedlejší chainy pro globální a veřejné použití. Tyto služby zahrnují generaci ID, distribuce tokenů, obchodování digitálních aktiv a rychlé platební systémy. Tyto základní služby jako všechny důležité infrastrukturní komponenty, které jsou součástí Elastos Chytrého Webu. Dodatečně náš tým poskytne podporu pro vývoje vedlejších chainů třetích stran.

Transakce jsou nejdůležitější částí rozhraní mezi hlavními a vedlejšími chainy. Transakční postup pro odesílání tokenů z hlavního chainu na chain vedlejší je stejný, jako odesílání z uživatelského účtu na hlavním chainu na multisignature adresu odpovídající vedlejšímu chainu. Tento proces automaticky zkontroluje schopnost vedlejšího chainu identifikovat transakci a vložit rovnocennou hodnotu tokenů vedlejšího chainu na účet vedlejšího chainu.

Proces Transakcí z Hlavního do Vedlejšího Chainu:

- Uživatel vytvoří náhodný secret a jeho odpovídající hash.
- Uživatel vytvoří multisignature adresu na hlavním chainu. Pro odemčení musí být poskytnut secret a privátní klíč uživatele k multisignature adrese.

-
- Uživatel odešle transakci a jeho secret hash do nodu vedlejšího chainu, který zpracovává transakce.
 - Node zpracovávající transakce na vedlejším chainu vygeneruje transakci odesílání tokenů po ověření hash a privátního klíče multisignature peněženky.
 - Uživatel poskytne secret k odemčení transakce a obdrží tokeny z vedlejšího chainu.
 - Tokeny jsou uloženy na multisignature adrese.

Transakční postup pro odesílání ELA z vedlejšího chainu na chain hlavní je ekvivalentní k odesílání ELA z multisignature adresy na hlavním chanu do uživatelského účtu na hlavním chainu.

Proces Transakcí z Vedlejšího do Hlavního Chainu:

- Uživatel vytvoří náhodný secret a jeho odpovídající hash.
- Uživatel vytvoří transakci na vedlejším chainu. Pro odemčení musíme poskytnout secret.
- Uživatel odešle transakci a jeho secret hash do nodu hlavního chainu, který zpracovává transakce.
- Node zpracovávající transakce na hlavním chainu vygeneruje transakci odesílání tokenů po ověření hash a privátního klíče multisignature peněženky.
- Uživatel poskytne secret k odemčení transakce a obdrží tokeny z hlavního chainu.
- Multisignature adresa, která odpovídá vedlejšímu chainu odemkne výběr a utratí příslušné tokeny.

Pro kontrolu zabezpečení ELA tokenů na multisignature adrese může adresa pouze vygenerovat transakci výběru tokenů, jak je uvedeno výše.

5.5 Chytré Kontrakty

Pokud jsou na hlavní chain nasazeny výpočetně náročné chytré kontrakty, každý node v síti je musí neustále aktualizovat, a to i v případě, kdy nejsou zrovna vyvolány. Jedná se o zátěž pro verifikační nodes, jelikož těžařské nodes stále mohou získávat poplatky za zpracování transakcí. Abychom se tomuto vyhnuli, Elastos hlavní chain limituje použití chytrých

kontraktů a přiděluje je vedlejším chainům. Každý vedlejší chain může designovat funkci chytrých kontraktů nezávisle, podobně jako NeoContract podporuje NEO blockchain.

6. Elastos Carrier: Decentralizovaná P2P Síť

Elastos Carrier je decentralizovaná internetová služba poskytnuta ekosystémem Elastos. Jeho nodes mohou být aktivovány skrze jakékoliv prostředí připojené k internetu, včetně místní sítě v rámci domova, či pracoviště. Díky použití transparentní techniky UDP založené na NAT (User Datagram Protocol, Network Address Translator) budou mít všechny páry nodů dostatek energie k navázání připojení navzájem, dokonce i k přímému spojení. To umožní bohaté využití každé individuální kapacity nodu, což způsobí efektivní zvýšení síly sítě jako celek.

Soubor základních služeb bude zahrnovat decentralizované domény, decentralizovanou komputace a decentralizovaný úložný prostor. Zásadní podpora bude poskytnuta pro vývoj Dapps. V takovémto prostředí má uživatel možnost vlastnit jeho data a komputaci pod hojnou úrovní ochrany soukromí. Zároveň bude mít uživatel možnost pronajmout jeho počítačovou výpočetní sílu nebo jeho vlastní vybavení pomocí Elastos Blockchainu. Za tento pronájem získá odměnu, která se bude rovnat výši komputace a úložného prostoru, který byl spotřebován. Toto vytvoří motivaci pro funkci Elastos trhu.

7. Elastos OS: Bezpečný, Všeobecný Operační Systém

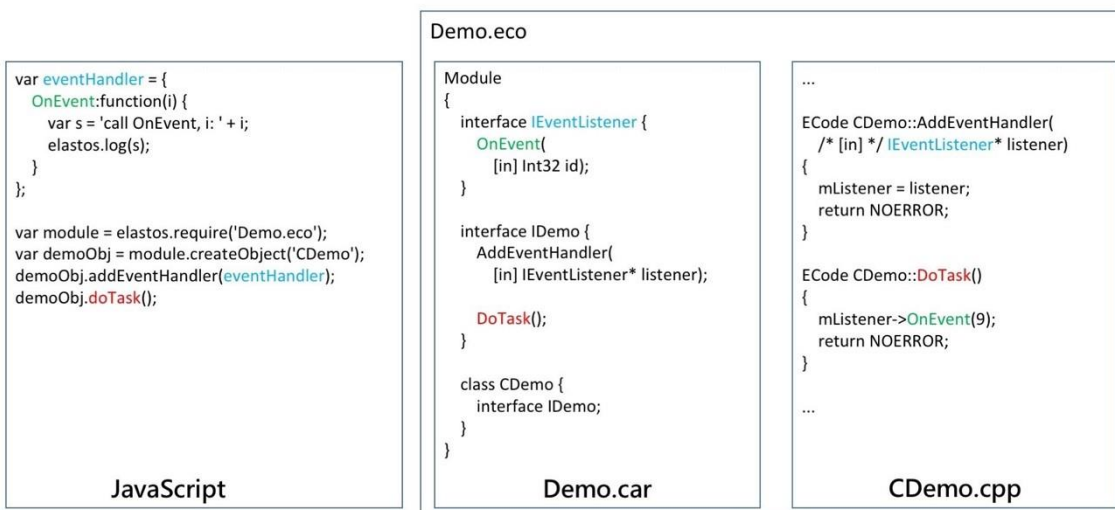
Elastos OS je všeobecný operační systém založený na respektu ochrany bezpečnosti. Jedná se o operační systém, který adresuje potřeby Internetu Věcí (Internet of Things), sady vynálezů jako Raspberry Pi a mobilních zařízeních. Nejnovější verze, tedy třetí, podstupuje procesem komoditizace a to od května roku 2013. OS úspěšně dosáhl beta kvality, byl spuštěn a překontrolován na Moto X (XT1085) telefonu a Lamobo-R1S chytrém routeru. Celkový počet kódu, který byl použit, přesáhl 10 milionu řádků.

S ohledem na bezpečnost, Elastos OS zakazuje přímé vytváření procesů a nedovoluje přímou interakci s TCP/IP, v závislosti na tom, zda systém automaticky vytvoří a určí polohu lokálních, nejbližších a vzdálených (nebo cloud) mikroslužeb. Systém automaticky vygeneruje remote procedure calls (RPC) a poskytne odezvu založenou na údalostech,

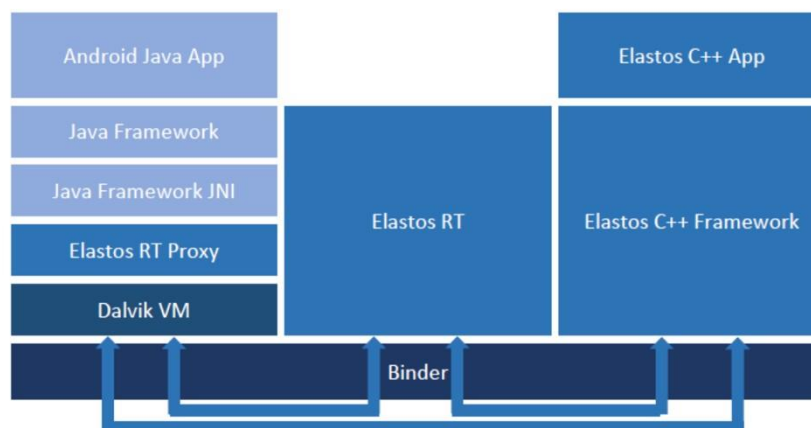
čímž se vyhne možným škodlivým akcím na straně aplikace nebo vzdálené služby. Tímto způsobem zamezí dalšímu přenášení virů.

Elastos OS poskytuje skutečný a vylepšený decentralizovaný systém podpory pro aplikace, které jsou vytvářeny. Usnadňuje propojení s Elastos Carrier, což umožňuje obdržení základních služeb, dále propojení s Elastos Chain pro obdržení služeb souvisejících s kreditem a směnou. Dapps, které z vývoje vzniknou, mohou bezstarostně a současně spravovat Elastos transakce a jiné typy digitálních aktiv, včetně: zdrojového kódu, dat, elektronických knih, videa a herních předmětů. Dále mohou spravovat autorská práva, transakce a cirkulaci mimo jiné věci.

Systém využije C/C++, Java a HTML5/JS jako hlavní způsoby vývoje. C++ API bude do značné míry kopírovat Android Java API, což umožní sjednocení tří v jednom: řízení přístupu do cloud, monitorování a propojení. Komponenty napsané v Java, HTML5/JS a C/C++ budou schopny volat sami sebe modulárním způsobem bez nutnosti manuálního řešení pomocí JNI. Systém skutečně odpovídá maximu “napsaný jednou, funguje všude”. Systém bude podporovat Component Assembly Runtime (CAR) architekturu, jak demonstrujeme na příkladu níže, využíváme CAR komponent pro navázání komunikace mezi programy napsanými v C/C++ a HTML5/JS.



C++ framework Elastosu OS využívá rozhraní aplikací Androidu, což vede k příhodnosti pro vývojáře, a také k portabilitě. Elastos OS jde dokonce až tak daleko, že přímo spouští Android programy, čímž vytváří situaci, která je popsána níže.



Nad Elastos Runtime můžete přemýšlet jako o C++ verzi Java Virtual Machine, stejně jako framework Java. Můžeme na něj dokonce odkazovat jako na C Virtual Machine (CVM). Elastos OS služby a aplikace budou fungovat skrze CVM, což umožní těmto službám existovat v harmonii s rozsáhlým spektrem nodů a hardwarových platform.

8. Elastos Runtime Prostředí pro Dapps

Ačkoliv Elastos OS můžeme získat kdykoliv si chceme užít kompletní a primární podporu pro vývoj Dapps, existují i jiné případy, kde by uživatel preferoval využití operačního systému, který již používá. V takových případech stačí využít Elastos Runtime, runtime prostředí, které taktéž nabízí kompletní podporu pro dané aplikace. Vývojáři budou mít možnost vybrat si z Elastos Runtime pro Android, Elastos Runtime pro iOS a Elastos Runtime pro Ubuntu Linux, záleží na potřebách vývojáře.

8.1 P2P Síťové Rozhraní

Dapps mezi sebou musí komunikovat prostřednictvím komponentních rozhraní, jelikož nemají žádný přímý přístup k internetu. Tento postup je jednodušší, bezpečnější a přirozenější:

```
4
5
6 TrustID myfriend = "0xE94b04a0FeD112f3664e45adb2B8915693dD5FF3";
7 IChat * pChat = CChat::New(myfriend);
8 pChat->Chat("hello");
9
```

Kód zobrazený výše nemusí brát ohled na serializaci/deserializaci nebo šifrování/dešifrování. Programátor ani nemusí psát nové protokoly. Všechny tyto věci jsou řešeny v Elastos Runtime CAR prostředí. Jediné, co člověk musí udělat, je upravit CAR dokument zobrazený níže, a poté navrhnout korespondující funkce.

V porovnání s customary socket-based API je Elastos Runtime mnohem jednodušší na použití. Navíc je možné provádět přenos digitálních aktiv, jak můžeme vidět níže:

```
13
14 interface IChat {
15     Chat(String message);
16 }
17
18 class CChat {
19     interface IChat;
20 }
21
```

Následující kód demonstruje jak na transakce:

```
24
25 ECode CChat::Chat(String message) {
26     // your code ....
27
28     return NOERROR;
29 }
30
31
```

Aplikace napsané s použitím Elastos Runtime jsou jednodušší než P2P síťové aplikace napsané s použitím customary socket API.

8.2 Provoz Digitálních Aktiv

Jak jste si mohli všimnout v předcházejících příkladech, již nepoužíváme IP adresy, ani jména domén pro síťovou komunikaci, jelikož současný Internet není důvěryhodný. Nicméně

Elastos Runtime bude provádět runtime verifikaci, potvrzení během vývoje Elastos Runtime prostřednictvím zóny důvěry, tedy Elastos Blockchainu.

```
33
34 ECode _CChat::Chat(String message) {
35
36     ... ..
37
38     // Check whether ID is exist
39     if (Exist(trustID) == FALSE) {
40         return ERROR;
41     }
42     // Check whether the current APP ID is on the blacklist
43     if (InBlackList(_Current_App_TrustID) == TRUE) {
44         return ERROR;
45     }
46     // Check whether the current user ID is on the blacklist
47     if (InBlackList(_Current_User_TrustID) == TRUE) {
48         return ERROR;
49     }
50     // Check whether the called count has exceeded the upper limit
51     if (Called_Count > MAX_CALL_COUNT) {
52         return ERROR;
53     }
54
55     // More checks
56     ... ..
57
58     ec = CChat::Chat(message);
59
60     ... ..
61
62     return ec;
63 }
64
```

V současné chvíli můžeme provádět transakce digitálních aktiv. Následující příklad ověří vlastnictví digitálního aktiva:

```
66
67 TrustID aMovie = "0x32B77CBB265175D1A927c9A3F816de577BDDdE05";
68 TrustID owner = "0xd4fa1460F537bb9085d22C7bcCB5DD450Ef28e3a";
69
70
71 if (Elastos.RT.Trust.CheckOwner(owner, aMovie) == TRUE) {
72     // yes, He is its owner.
73 }
74 else {
75     // error
76 }
77
```

Ve finále je transakce vytvořena a odeslána:

```
82
83 Elastos.RT.Trust.SendTransaction(buyerID, sellerID, 1000, aMovieID);
84
```

9. Elastos Foundation

Elastos projekt má za sebou dlouhou historii. Jeho předchůdce se objevil již v roce 2000, kdy se zakladatel Rong Chen vrátil do Číny, aby začal s jeho podnikáním. Od té doby se Rong Chen věnuje vývoji bezpečného a všeobecného operačního systému pro dobu Internetu. V roce 2017 se Elastos projekt stál globálním, zdarma open-source software projektem, který je veden Elastos komunitou. Vyvíjený softwarový zdrojový kód a dokumenty jsou vydávány zdarma s open-source softwarovou licencí. Elastos projekt funguje skrze Elastos Foundation. Elastos podporuje zdarma open-source, digitální měnovou komunitu, vzájemné učení a rozvoj lidské civilizace.

9.1 Elastos Komunita

Mezinárodní komunita Elastos zahrnuje fanoušky, vývojáře, organizátory komunity a držitele Elastos tokenů, kteří jsou rozprostřeni po celé zemi. Elastos je zavázán k nadálému budování této komunity. Elastos má také komunity skupin lokálních uživatelů po celé planetě, kteří pro Elastos pracují jako dobrovolníci. Tyto skupiny lidí organizují, udržují a vyvíjejí lokální komunitu Elastos. Jejich úkoly zahrnují například propagaci digitálních měn a blockchainové filozofie, studování Elastos technologie, účast ve vývoji Elastos projektů, psaní a překládání dokumentů, organizování měsíčních lokálních shromáždění komunity a asistenci v organizaci oficiálních Elastos mezinárodních aktivit.

9.2 Elastos Talent

Stále se nacházíme v ranném vývoji digitálních měn a blockchainu. Průmysl se rapidně vyvíjí, ale existuje nedostatek talentu. Zakladatele Elastos vytvořili program “We are All Satoshi Nakamoto”, který se nachází v Tsinghua iCenter a je zprostředkovaný skrze Distributed Autonomous Coalition Asia (DACA), který si dává za cíl kultivovat talent blockchainové technologie na vysoké úrovni. Od jeho uskutečnění, program kultivoval velké množství talentu v průmyslu, někteří z nich se dokonce postupně stali pilířem Elastos týmu. Elastos Foundation bude nadále podporovat výcvikový program DACA a spolupráci s Tsinghua iCenter za cílem kultivace technologického vývoje pro Čínskou blockchainovou komunitu.

9.3 Elastos Vize

Elastos pracuje na cíli stát se technologií, která zprostředkuje fungování chytré ekonomie. Elastos Fund bude investovat do nadálého vývoje decentralizovaných aplikací. Elastos chce vytvořit nový, bezpečnější a chytřejší World Wide Web, který může být jednoho dne známý jako Internet Digitálního Majetkového Bohatství.