عملة FTS

نظام المعاملات الخاصةالإلكترونية من نظير إلى نظير

مشروع FTS

whitepaper@ftscoin.xyz
www.ftscoin.xyz

نبذة مختصرة
كانت تعد أنظمة النقد من نظير إلى نظير جزءا متناميًا من النموذج الاقتصادي المتطور خلال السنوات العشر الماضية ، الناشئة مع احتضاننا لعصر جديد من التكنولوجيا ، لا يزال هناك مجال كبير للتحسين مع هذا البرنامج الجديد. تأمل FTS Coin في معالجة بعض هذه المجالات للتحسين ، بما في ذلك على *سبيل المثال لا الحصر :*الخصوصية ، المركزية ، أوقات المعاملات البطيئة ، رسوم المعاملات المرتفعة ، أنظمة المعاملات المربكة ، وفقدان الجمل الأساسية من خلال معالجة هذه المشكلات وتقديم حلول لها،واستخدام عملة FTS Coin للمساعدة في نشر التبني الجماعي من خلال توزيعات صادرة لدينا أملا أن تساعد في دفع العملة المشفرة نحو التبني الجماعي!.

1 المقدمة

على مدار العقد الماضي، عززت عملة التشفير مكانتها في المجتمع العالمي كوسيلة لتخزين القيمة ، وإجراء المعاملات بسهولة عبر الحدود، في حين أن Bitcoin العملة المشفرة الأصلية، مهدت الطريق لتغييرات هذه التكنولوجيا، إلا أنها كانت تعاني من أوجه قصور أصبحت واضحة خلال عقد من الاستخدام في المجتمع.

وتأمل FTS Coin في معالجة هذه المشكلات، مع الاستفادة أيضًا من جزء صغير من العملات الأجنبية ، من إجمالي عرض النقود البالغ 25،000،000 للمساعدة في خلق حافز للناس لتدريس شركات جديدة حول العملة المشفرة.

أما المشكلة الأكثر وضوحًا الموجودة في Bitcoin هي الخصوصية؛ بمجرد إجراء معاملة باستخدام محفظة bitcoin ويعرف أشخاص آخرون عنوان المحفظة، يمكنهم تتبع جميع المعاملات المالية لتلك المحفظة، إذا كانت هذه المحفظة يمكن أن تكون متصلة بشخص ما، فإن جميع المعاملات التي يقوم بها هذا الشخص أصبحت مجرد معلومات عامة، نظرًا لأن عملات الخصوصية قد عالجت هذه المشكلة جيدًا بالفعل

تعد FTS بمثابة جيل لاحق من تقنية Cryptonote، ويستخدم Cryptonote شكلاً من أشكال المدفوعات غير القابلة للإلغاء لضمان الخصوصية؛ يمكن العثور على معلومات حول تقنية Cryptonote في White Cryptonote.

هناك مشكلة أخرى وجدناها مقلقة حول Bitcoin وهي قدرة شخص أو كيان على مركزية قوة تعدين POW للعملة من خلال إنشاء مزارع تعدين كبيرة ASIC، أو شراء قوة التجزئة من خدمة تأجير التجزئة.

تعمل شبكة **CRYPTOCURRENCY** بشكل أفضل إذا كان التوزيع منتشرًا على نطاق واسع قدر الإمكان واستثمر عدد كبير من الأشخاص في مسابقة POW بقيمة صفر مقابل مكافآت الكتلة. إن الإفراط في مركزية قوة تجزئة POW يثبط هذا النمو الطبيعي للشبكة المفيدة ، وقدرتها على جذب أشخاص جدد إلى العملة المشفرة.

تخضع Bitcoin أيضًا إلى أوقات المعاملة البطيئة ، على الرغم من أن معظم "السداد" في Bitcoin يحدث داخل memcoin bitcoin ، إلا أن هناك مشكلة أخرى هي وقت الحظر نفسه. لقد قللنا كثيرًا من الوقت القياسي للكتلة إلى ما يقرب من دقيقتين للكتلةمما تساعد هذه السرعة المتزايدة للكتلة والرسوم المخفضة للمعاملات على التحرك في الوقت المناسب ، مما يسمح باستخدام النظام بسهولة لتبادل البضائع.

أنظمة البرامج المربكة شائعة أيضًا في عالم العملة المشفرة نظرًا لأن معظم الأشخاص الذين انجذبوا في البداية إلى العملة المشفرة ، وهي عملة الإنترنت ، هم من مستخدمي الكمبيوتر المنتظمين ، فهذه هي المجموعة التي صممها هذا البرنامج حتى الآن.
هذا لا يفضي إلى اعتماد عالمي من قِبل أهل العملات. ويعتمد الاعتماد العالمي على أي تقنية جديدة جزئياً على سهولة الاستخدام مقارنة بالأنظمة الأخرى مع تقدم FTS Coin للتطوير المستقبلي ، سيتم الحفاظ على هذا الهدف في المقدمة وفي مركزه في جميع الأوقات ، وسنتعامل مع جميع المساعي على أمل أن يتم استخدامها في يوم ما من قبل الجميع.

جزء من الارتباك المحيط بالعملة المشفرة هو الإدارة وغالبًا ما تخسر الأوقات ، للبذور الأصلية للمحافظ التي يتم تخزين أموال بها. على الرغم من أن هذه المشكلة لن تكون موجودة إذا كان الناس حريصين على بذور محفظتهم ، وعاملوها كأنها نقود ، إلا أننا نعتقد أننا توصلنا إلى حل يسمح للناس بوضع بذور محفظتهم عليهم في جميع الأوقات ، دون إنشاء خطر أمني. من خلال السماح لمجموعة مختارة من بيانات المستخدم الحيوي عوضا عن الكلمات التي تمثل بذرة المحفظة القياسية ، نأمل في سد الفجوة المفقودة بسبب عدم وجود صرف البنك للأموال دائما مجرد أن يتم إنشاؤها من blockchain.
ستقدم FTS Coin كلاً من خيارات POW و POS في المستقبل القريب ، ولكن سيتم إطلاقها باستخدام POW معد للحصول على مكافآت الكتلة ، مع نظام ربح إضافي. يتضمن نظام ربحي للكسب ، وهو تصميم فريد مرتبط بهذه العملة ، منح الناس حافزًا للمساعدة في نشر التبني الشامل للعملات المشفرة. سيتم إدارة نظام POB هذا من خلال موقع FTSMothership.info على الويب وسيتم دفعه من جزء من عملة FTS Coin الأولى.

من أجل النمو والتنمية ، تم إجراء سلسلة صغيرة من FTS Coin أثناء إطلاق العملة. تحتوي FTS Coin على ما مجموعه 25,000,000 قطعة نقدية من العملات المعدنية ، من المقرر أن توزع ببطء على مدى قرن من الزمان ، حيث كانت 2,000,000 قطعة منها ممتازة. هذا يعني أن 8٪ من عرض عملة FTS Coin تم استخراجه مسبقًا ، مع ترك 92٪ أو 23,000,000 ، ليصبح متاحًا على مدار المائة عام القادمة. سيتم تحديد استخدام هذه المقدمة للحصول على الشفافية في وقت لاحق من هذه الورقة البيضاء.

2. خصوصية المعاملات

تم استعارة القسم 2 كلمة لكلمة من ورقة بيضاء Cryptonote!

نقترح حلاً (الخصوصية) يسمح للمستخدم بنشر عنوان واحد وتلقي مدفوعات غير مشروطة غير قابلة للإلغاء. وجهة كل مخرجات CryptoNote (بشكل افتراضي) هي مفتاح عام ، مشتق من عنوان المستلم وبيانات المرسل العشوائية.

الميزة الرئيسية ضد Bitcoin هي أن كل مفتاح وجهة فريد من نوعه افتراضيًا (ما لم يستخدم المرسل نفس البيانات لكل من معاملاته لنفس المستلم). وبالتالي ، لا توجد مشكلة مثل "إعادة استخدام العنوان" حسب التصميم ولا يمكن لأي مراقب تحديد ما إذا كانت قد تم إرسال أي معاملات إلى عنوان محدد أو ربط عنوانين معًا.

يقوم المرسل بإجراء تبادل Diffie-Hellman للحصول على سر مشترك من بياناته ونصف عنوان المستلم. ثم يحسب مفتاح الوجهة لمرة واحدة ، باستخدام السر المشترك والنصف الثاني من العنوان. يلزم وجود مفتاحي EC مختلفين من المستلم لهاتين الخطوتين ، بحيث يكون عنوان CRYPTONOTE القياسي أكبر من ضعف عنوان محفظة Bitcoin. يقوم المتلقي أيضًا بتبادل DIFFIE-HELLMAN لاستعادة المفتاح السري المقابل.

يتبع تسلسل المعاملة القياسي كالتالي:

1. أليس تريد إرسال دفعة إلى بوب ، الذي نشر عنوانه القياسي. SHEUNPACKS العنوان ويحصل على مفتاح بوب العام(A، B).
2. تنشئ Alice عشوائيًا [1، 1 − l] وتحسب keyPal العمومي لمرة واحدة . $P=Hs(rA)G+B$.
3. تستخدم AlicPas مفتاح وجهة للإخراج وأيضًا حزم valueR = rG (كجزء من ذلك).

(تبادل ديفي هيلمان) في مكان ما في الصفقة. لاحظ أنه يمكنها إنشاء نواتج أخرى باستخدام مفاتيح عمومية فريدة: مفاتيح المستلمين المختلفة $(Bi\ 'Ai)$ تعني Pi مختلفة حتى مع نفسها

4. أليس ترسل المعاملة،

5 . يقوم بوب بالتحقق من كل معاملة تمر بمفتاحه الخاص *(B،A)*. ، ويحسب *P = Hs (aR) G + B* إذا كانت صفقة Alice مع Bob هي المستلم فيما بينها ، فعندئذٍ *R=arG=Ra and P=P*

6. يستطيع بوب استرداد المفتاح الخاص المقابل لمرة واحدة

X=Hs(aR)+b مثل *P=xG* يمكنه قضاء هذا الإخراج في أي وقت عن طريق توقيع معاملة مع **x** نتيجةً لذلك يحصل بوب على المدفوعات الواردة المرتبطة بالمفاتيح العامة لمرة واحدة والتي لا يمكن فك ارتباطها لأحد المتفرجين.

***بعض الملاحظات الإضافية** :عندما "يتعرف" بوب على معاملاته (انظر الخطوة 5) فإنه لا يستخدم عملياً سوى نصف معلوماته الخاصة*(B،A)*.

يمكن تمرير هذا الزوج المعروف أيضًا باسم مفتاح التتبع ، إلى جهة خارجية (كارول) يستطيع بوب تفويضها بمعالجة المعاملات الجديدة لا يحتاج بوب إلى الوثوق بكارول صراحة لأنها لا تستطيع استرداد المفتاح السري لمرة واحدة فقط بدون مفتاح بوب الخاص الكامل *(B،A)*. هذا النهج مفيد عندما يفتقر بوب إلى عرض النطاق أو قوة الحساب (الهواتف الذكية ، محافظ الأجهزة وغيرها) • .في حالة رغبة *Alice* في إثبات أنها أرسلت معاملة إلى عنوان Bob ، فيمكنها إما الكشف عن ror باستخدام أي نوع من بروتوكول المعرفة الصفرية لإثبات أنها تعرف) r على سبيل المثال عن طريق توقيع المعاملة مع • .(r إذا أراد بوب الحصول على عنوان متوافق للتدقيق حيث يمكن ربط جميع المعاملات الواردة ، فيمكنه إما نشر مفتاح التتبع الخاص به أو استخدام عنوان مقطوع. لا يمثل ذلك العنوان سوى مفتاح *ec-keyB* عاما واحدا ، ويستمد الجزء المتبقي المطلوب من البروتوكول منه كما يلي *a = Hs (B)* و *A = Hs (B) G* في كلتا الحالتين ، يكون كل شخص قادرًا على "التعرف" على جميع معاملات بوب الواردة ولكن بالطبع ، لا يمكن لأي شخص إنفاق الأموال الموجودة داخلها دون المفتاح السري (*B*).

3. رئيس الوزراء

كانت FTS تمتلك عرضًا أوليًا بنسبة 8٪ تم إصداره من الكتلة الصفرية ، ويتم استخدام هذه العملة الأولية المكونة من 2،000،000 قطعة معدنية لتعزيز العملة ودعم نظام POB. سيتم توزيع هذه القطع النقدية البالغ عددها 2،000،000 قطعة في هذا القسم بأكبر قدر ممكن من التفاصيل.

سيتم استخدام 500،000 من هذا العرض الأساسي للحصول على مكافآت تقنية لمزيد من التطوير. مع تطور العملة ، ونمو المجتمع الذي تستخدمه ، سيكون مكانًا شائعًا لفريق FTS Coin لإصدار مكافآت متاحة للمبرمجين والمطورين الذين يمكنهم إنجاز مهام معينة. ستستند هذه المكافآت على الحاجة إلى العمل المطلوب.

سيتم استخدام 500،000 من هذا العرض الأساسي للتسويق والترويج. سيشمل ذلك مزيجًا العروض الترويجية ، والمكافآت للأنشطة الترويجية لـ IRL ، والمكافآت للترويج لوسائل التواصل الاجتماعي ، وأي إعلانات أو عروض ترويجية أخرى يشعر فريق FTS بأنها ستساعد في دفع العملة إلى الأمام.

سيتم استخدام 500،000 من هذا premine نحو نظام ص. سيوفر نظام POB للأفراد عملة FTS لتدريس الشركات حول العملة المشفرة ، وحملهم على البدء في قبول أي عملة مشفرة حاليًا في السوق. ستتوفر المزيد من التفاصيل على نظام POB لاحقًا في هذا المستند التقني.

سيتم استخدام 50،000 من هذا النموذج الأساسي لتطوير النظام الإيكولوجي ، بأي شكل من الأشكال قد يتخذ ؛ بما في ذلك FTS فقط مخازن التشفير أو الخدمات التي تمولها FTS coin أو أي نشاط آخر من شأنه أن يساعد في دعم قيمة عملة FTS.

تُستخدم العملات المتبقية البالغ عددها 450,000 عملة في اتجاه رسوم التطوير الأولي .

4.خريطة الطريق التقنية

ستطلق FTS Coin أشكالها الأولية كعملة خصوصية متشعبة من Cryptonote ، بإجمالي عرض يصل إلى 25،000،000 قطعة نقدية. يجب أن يكتمل هذا التوزيع البالغ 25،000.000 قطعة نقدية بعد 100 عام مع انخفاض قيمة كل قطعة بشكل مطرد مع مرور الوقت. هذه هي خريطة الطريق لخططنا الحالية مع التكنولوجيا ؛ على الرغم من أنه من المحتمل أن نضيف عناصر إلى جدول الأعمال هذا فمن غير المرجح أن نأخذ أيًا من هذه العناصر في خططنا المستقبلية.

4-1المرحلة الأولى *الأزمة* متوسط الكتل أقل بقليل من دقيقتين مع كل المعاملات التي تتم معالجتها بشكل خاص كما هو موضح أعلاه ، وكتل يجري التعدين باستخدام خوارزمية POW مقاومة .ASIC سيتم إطلاق العملة باستخدام خيارات استخراج وحدة المعالجة المركزية والمحافظ الطرفية ، بالإضافة إلى محافظ واجهة المستخدم الرسومية سهلة الاستخدام لأنظمة Windows و Linux وMac

4-2المرحلةالثانية *حمام التعدين ومحافظ الهاتف*

في هذه المرحلة ، ستقوم FTS Coin بإضافة Pool Mining ومحافظ android و / أو IOS للعملة. ستساعد هذه الخيارات المضافة على توسيع قاعدة عامل المناجم والمستخدم للعملة. ستصبح إضافة محافظ الهاتف جزءًا هامًا من المرحلة 4.5

4-3المرحلة الثالثة *سهلة التعدين والرسائل والتبادل*

تتضمن المرحلة 3 من FTS Coin إضافة زر "منجم الآن" السهل إلى محافظ واجهة المستخدم الرسومية ، بالإضافة إلى إضافة القدرة على إرسال رسائل خاصة من المحفظة ,نأمل في تنفيذ زر "منجم الآن" السهل كجزء من الجهود التي نبذلها لنشر التبني الشامل للعملة المشفرة. نشعر بأن نظام ASIC المقاوم يوفر بسهولة

القدرة على الانخراط في الشبكة ويساعد على المساهمة في أمانه ، ليس فقط ويوفر شبكة أكثر مركزية وصلابة ، بل يوفر أيضًا منصة للأشخاص الجدد ليتم استثمارهم في النظام من *CRYPTOCURRENCY* نفسها من خلال المشاركة في المنافسة على المكافآت كتلة

من خلال توفير وسيلة للأشخاص لإرسال رسائل مشفرة ، يتم دفعها مقابل آلية برمجية واحدة، في هذه المرحلة سنقوم أيضًا بشراء طريق التبادل إذا لم يكن الشخص متاحًا للعملة مجانًا من مجتمع التشفير.

4.4**المرحلةالرابعة** POS / POW *الهجين*

إثبات حصة سوف يأتي في هذه المرحلة. من أجل المساعدة في خلق حافز للناس لتجميع عملة FTS الخاصة بهم ، سنجري شوكة صلبة للنظام لإضافتها على خيارات نقاط البيع. وبالتالي السماح للناس بالحصول على عملة FTS من خلال التمسك بها ، أو توفير POW للمساعدة في أمان الشبكة

أو تقديم أعمال جديدة إلى FTS Coin من خلال نظام POB الخاص بنا على www.ftsmothership.info

5-4المرحلة الخامسة *تكامل البذور البيومترية* تتضمن المرحلة الخامسة والأخيرة من خارطة طريق التكنولوجيا المخطط لها لبرنامج *FTS Coin* إضافة وسيلة ثانوية لإنشاء المحفظة. سيتمكن الأشخاص في هذه المرحلة من إنشاء عنوان قديم قياسي باستخدام كلمة بذرة ، كما هو شائع حاليًا في العملة المشفرة. بدلاً من ذلك ، سيتمكنون من بدء استخدام الماسحات الضوئية وبصمات الأصابع على هواتفهم لاختيار مجموعة من بيانات القياس الحيوي لاستخدامها في اتصال مع خوارزمية تقوم بترجمة هذه المعلومات إلى خوارزمية *SHA 256* الخاصة بك. من خلال هذه الطريقة ، سيتم التأكد من أنه طالما لا يزال لديهم أجزاء رئيسية من الجسم ، فسيكون لديهم بذرة في محفظتهم ، ويجب أن يكونوا قادرين على استخدام أي هاتف لتنزيل برنامج المحفظة واسترداد أموالهم.

5-دليل على الأعمال التجارية

سيتم توجيه 600,000 FTS من premine نحو آلية Proof of Business ، أو الـ POB سيتمكن الأشخاص من تسليم مقطع فيديو مدته 10 ثوانٍ لمالك النشاط التجاري يقولون إنه يقبل الآن العملة المشفرة بفضل المسجل ، وسيحصل الشخص الذي يرسل الفيديو على FTS Coin كتعويض .ستتلقى أول 2000 مشاركة 50 FTS coin لكل منها لإرسال مقاطع الفيديو هذه علىhttp://www.ftsmothership.info بعد التحقق من المعلومات. سوف تتلقى الطلبات الـ 4000 القادمة 25 عملة مقابل تقديمها. سيستمر مبلغ FTS Coinالذي تم استلامه للتقديم إلى النصف مثل كل 100,000 FTS coin حتى يتم ترك 50،000 FTS Coinفي صندوق POB. عند هذه النقطة ، تحتوي محفظة FTS POB Fund فقط على 50000 FTS Coin left، وسيتلقى الأشخاص 1 FTS مقابل كل عمل يقدمونه ال FTS POB التقديمات ؛ ليس من الضروري أن يبدأ العمل في قبول عملة FTS. الشيء الوحيد المهم هو أنهم بدأوا في قبول أي شكل من أشكال عملة التشفير على الإطلاق ، وكانوا على استعداد لالتقاط شريط فيديو يشكرك على تعليمهم حول هذا الموضوع. الهدف من هذا هو دعم اعتماد الكتلة المشفرة ، وليس فقط اعتماد الFTO

الخاتمة

لقد اقترحنا سلسلة من التحسينات على أنظمة العملة المشفرة الحالية والتي ستعمل على تحسين النظام البيئي للعملات المشفرة ككل ، وتوفر عملة مشفرة مصممة ليتم تبنيها واستخدامها بسهولة من قبل الجمهور بشكل عام. مهدت أنظمة العملة المشفرة الحالية ، بما في ذلك Bitcoin ، الطريق لجميع الأنظمة النقدية الحديثة الأقل من نظير إلى نظير ، ولكن عقد الاختبار التجريبي هذا العقد قد أوضح الأخطاء في الأنظمة الحالية. نأمل في

حل هذه المشكلات من خلال توفير مجموعة من التحولات الفنية والأيديولوجية التي ستساعد في استمرار اعتماد هذه التكنولوجيا المذهلة