BLOCKCHAIN HYBRIDE : SIDECHAIN

Ethereum Entreprise Alliance

CHRISTOPHE OZCAN

NOVEMBRE 2020

BLOCKCHAIN HYBRIDE : SIDECHAIN

Blockchain Hybride : Sidechain (180 min)

Type d'infrastructures Blockchain

Ethereum Entreprise architecture

Identifiant Sidechain

Atomic Crosschain Transaction

Pinning « Epinglage »

Multichain Nodes

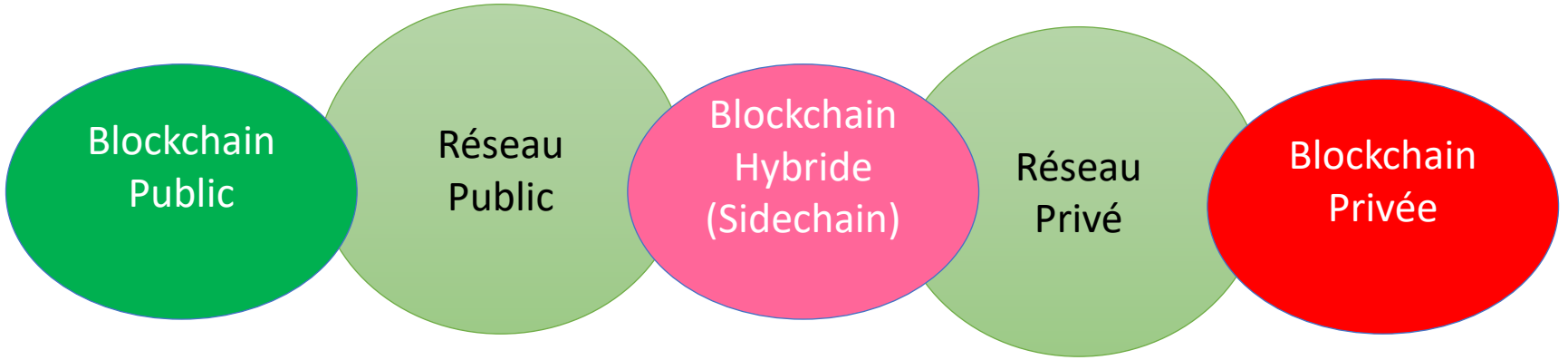
Sidechain Keys and Sidechain Threshold Signatures

Contract Locking and Provisional State Updates

Subordinate View Process & Coordinating Node

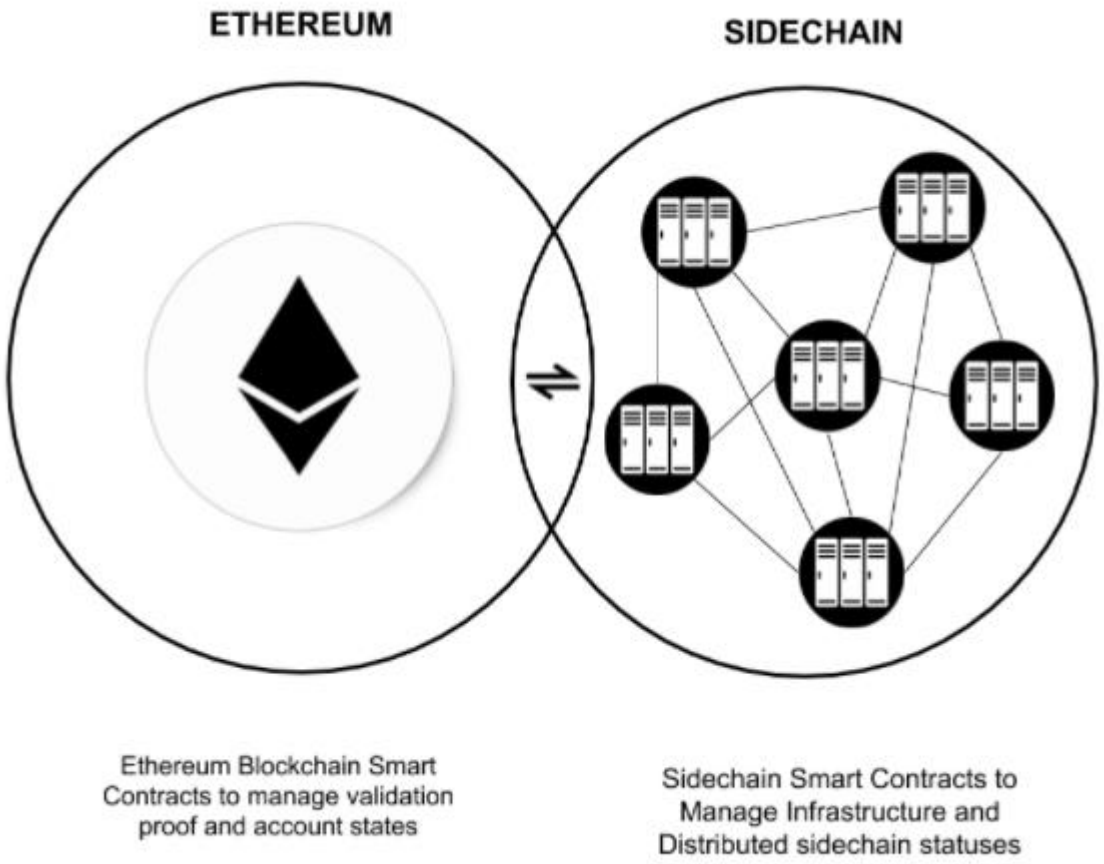
BLOCKCHAIN HYBRIDE : SIDECHAIN

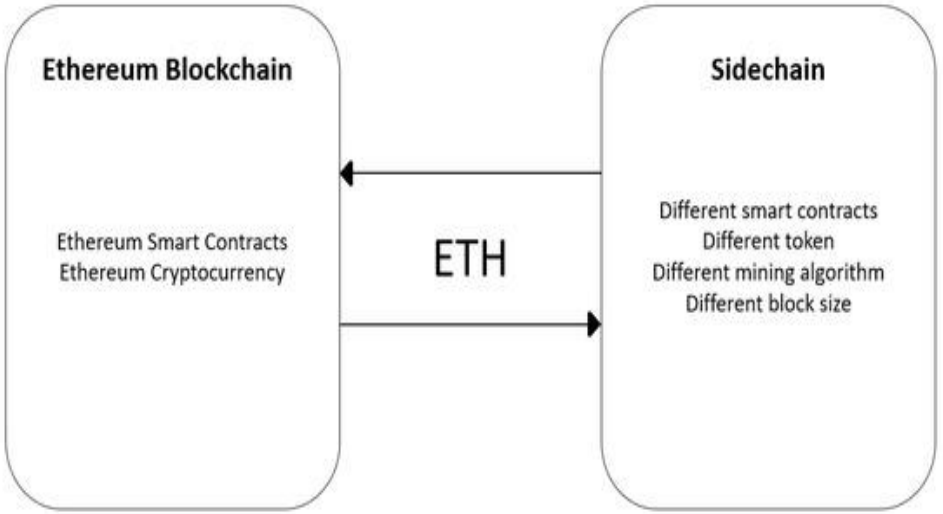
Types d'infrastructure de la Blockchain



BLOCKCHAIN HYBRIDE : SIDECHAIN

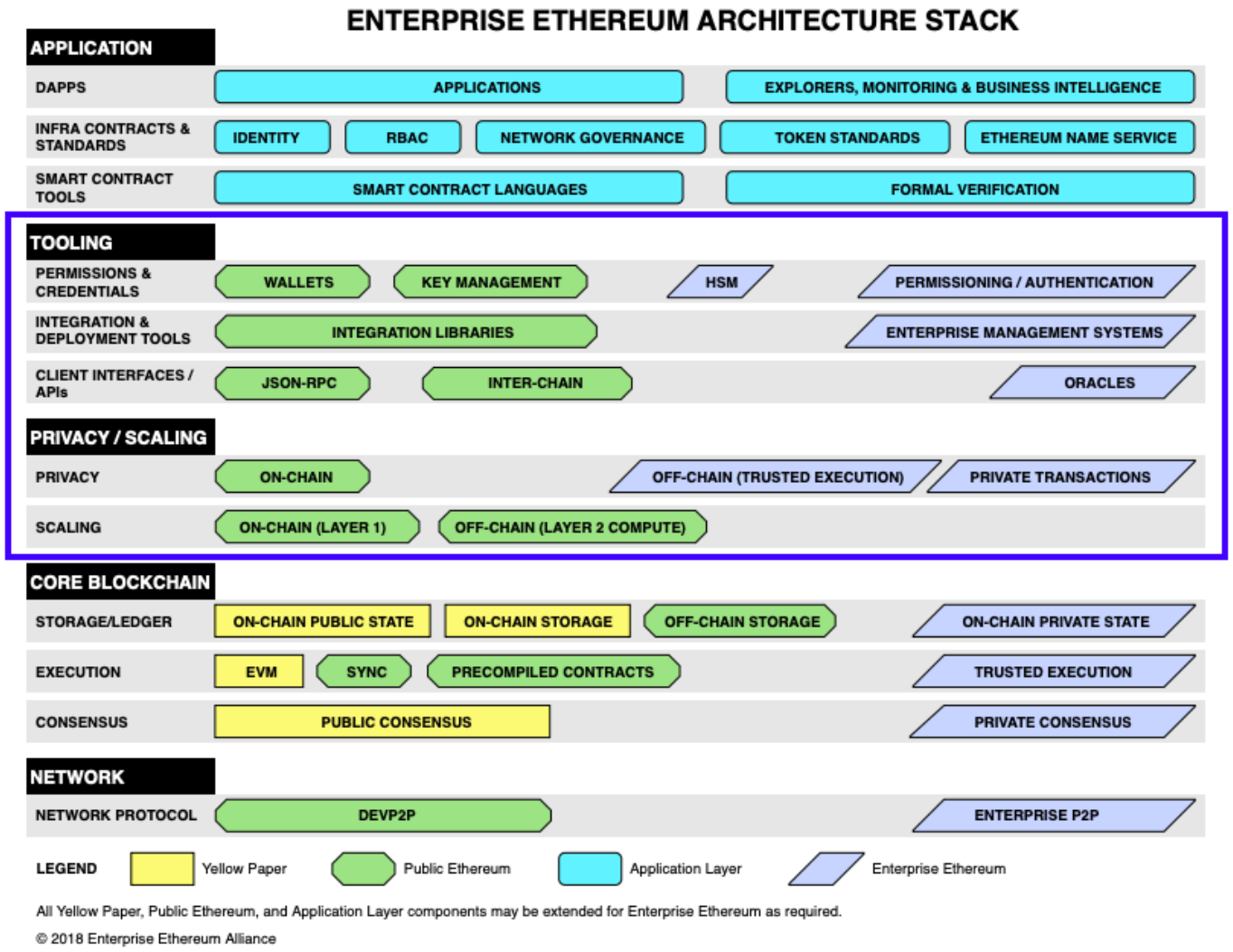
Types d'infrastructure de la Blockchain : Ethereum Sidechain





BLOCKCHAIN HYBRIDE : SIDECHAIN

Ethereum Entreprise architecture



BLOCKCHAIN HYBRIDE : SIDECHAIN

Identifiant Sidechain:

Les identificateurs Sidechain sont des valeurs de 256 bits qui identifient une sidechain. Ils sont utilisés pour identifier à quels messages sidechain sont destinés. Ils sont également utilisés pour lier des transactions à des sidechains spécifiques, pour bloquer les attaques de relecture sur d'autres sidechains.

Les identifiants de sidechain sont générés aléatoirement lorsque la sidechain est créée pour la première fois selon les règles du tableau I. La plage de numéros est choisie de manière à ne pas entrer en conflit avec les valeurs d'identifiant de chaîne utilisées dans Ethereum afin que ces blockchains puissent être spécifiées à l'aide d'un identifiant de sidechain. Une sidechain conserve le même identifiant de sidechain même si des nœuds sont ajoutés ou supprimés de la sidechain

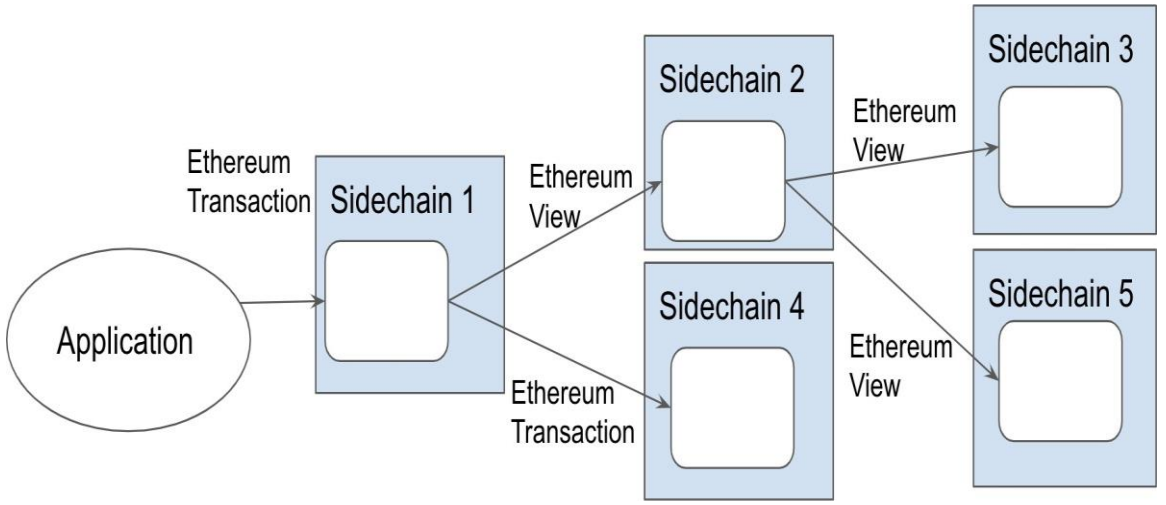
Number Range	Description
0x00000000,00000000,00000000,00000000,00000000,00000000,00000000,00000000 to 0x00000000,00000000,00000000,00000000,00000000,00000000,00000000,0000FFFF	Ethereum MainNet Chain Identifier
0x00000000,00000000,00000000,00000000,00000000,00000000,00000000,0000FFFF to 0xFEFFFFFF,FFFFFFFF,FFFFFFFF,FFFFFFFF,FFFFFFFF,FFFFFFFF,FFFFFFFF,FFFFFFFF	Reserved for future use
0xFF0000000,00000000,00000000,00000000,00000000,00000000,00000000,00000000 to 0xFFFFFFFF,FFFFFFFF,FFFFFFFF,FFFFFFFF,FFFFFFFF,FFFFFFFF,FFFFFFFF,FFFFFFFF	Ethereum Private Sidechains

BLOCKCHAIN HYBRIDE : SIDECHAIN

Atomic Crosschain Transaction

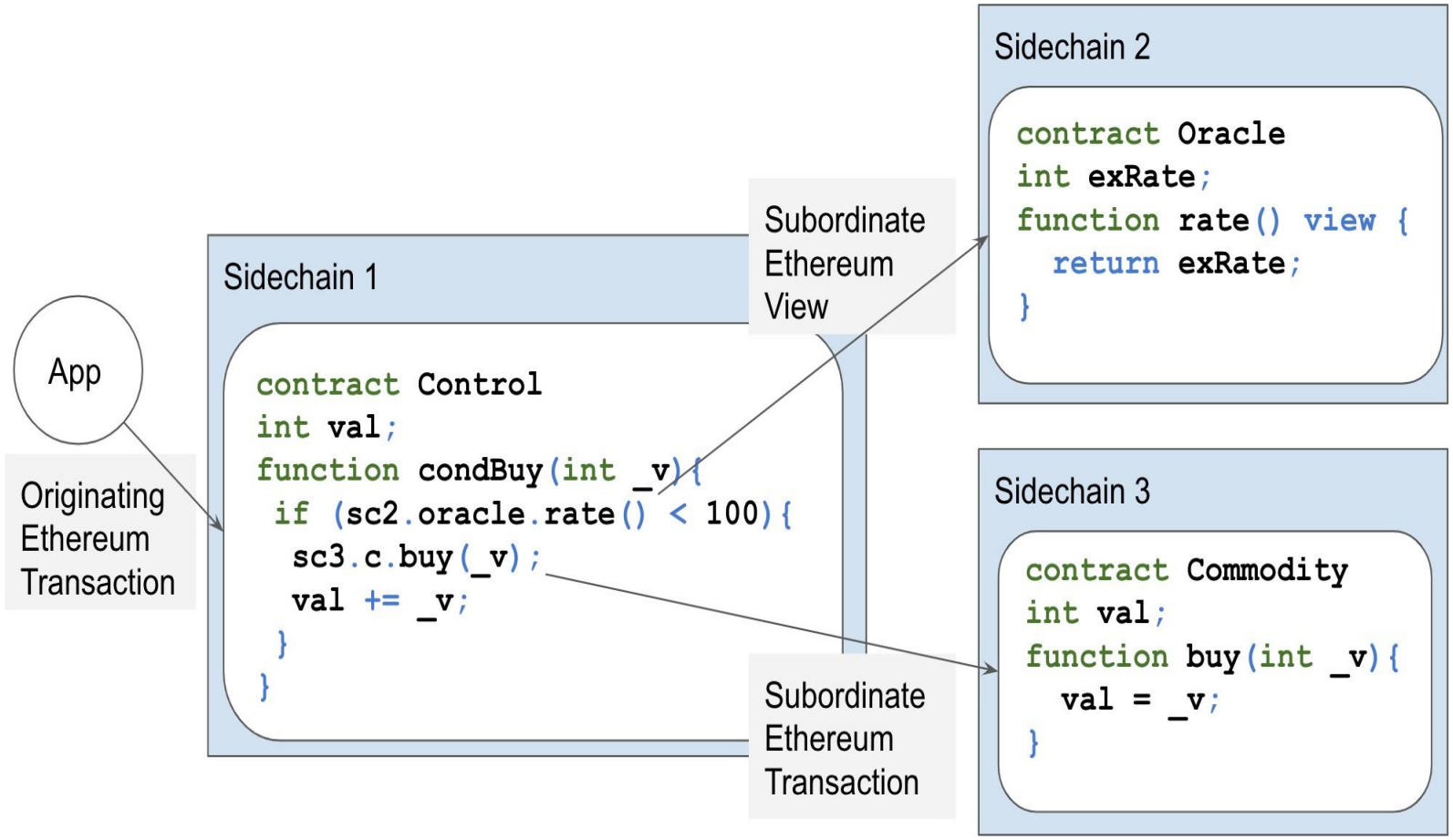
Une transaction crosschain se compose d'une transaction d'origine et d'une ou plusieurs transactions subordonnées et vues subordonnée.

La transaction d'origine est la transaction Ethereum public qui s'exécute sur la sidechain sur laquelle la transaction crosschain a été soumise, et les transactions subordonnées et les vues subordonnées sont des transactions Ethereum et Vues Ethereum qui s'exécutent sur d'autres sidechains à la suite de la transaction d'origine.



BLOCKCHAIN HYBRIDE : SIDECHAIN

Atomic Crosschain Transaction



BLOCKCHAIN HYBRIDE : SIDECHAIN

Atomic Crosschain Transaction

Les transactions Atomic Crosschain sont motivées par deux exigences communes à d'autres systèmes distribués: les données et les fonctionnalités que nous souhaitons utiliser peuvent être disponibles dans d'autres systèmes.

La première exigence, l'accès aux données dans d'autres systèmes (Systèmes Off Chain, Sidechain ou Blockchain Main net (public)).

La deuxième exigence, l'accès aux fonctionnalités dans d'autres systèmes, est courante depuis des décennies via les appels de procédure à distance (JSON-RPC).

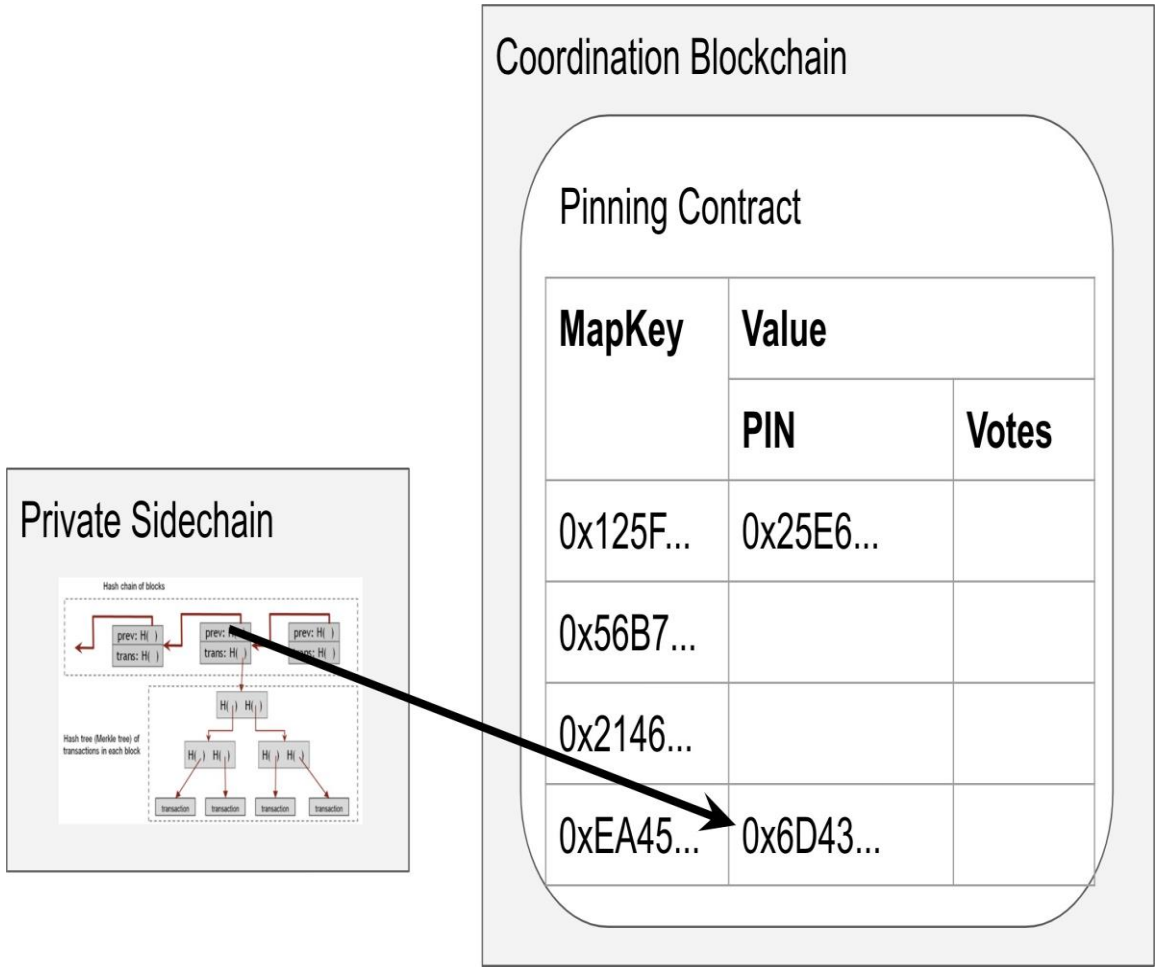
Les sidechains sont des blockchains qui reposent sur une blockchain distincte pour leur utilité globale, comme une sécurité renforcée en « épinglant » (pinning) la blockchain publique, pour adresser les informations, ou pour stocker des données qui sont utilisées dans la(es) sidechain(s).

BLOCKCHAIN HYBRIDE : SIDECHAIN

Pinning « Epinglage »

Épinglage: l'état d'une blockchain ou d'une sidechain peut être représenté par le Block Hash d'un bloc. Le hachage de bloc d'un le bloc final pourrait être soumis à un smart contrat sur une coordination Blockchain à intervalles réguliers, comme le montre la figure 1.

Ce processus est connu sous le nom d'épinglage « Pinning ». Épingler régulièrement la sidechain l'aide à protéger les participants minoritaires de la sidechain réversion d'état due au risque de collusion de la majorité des sidechain participants.

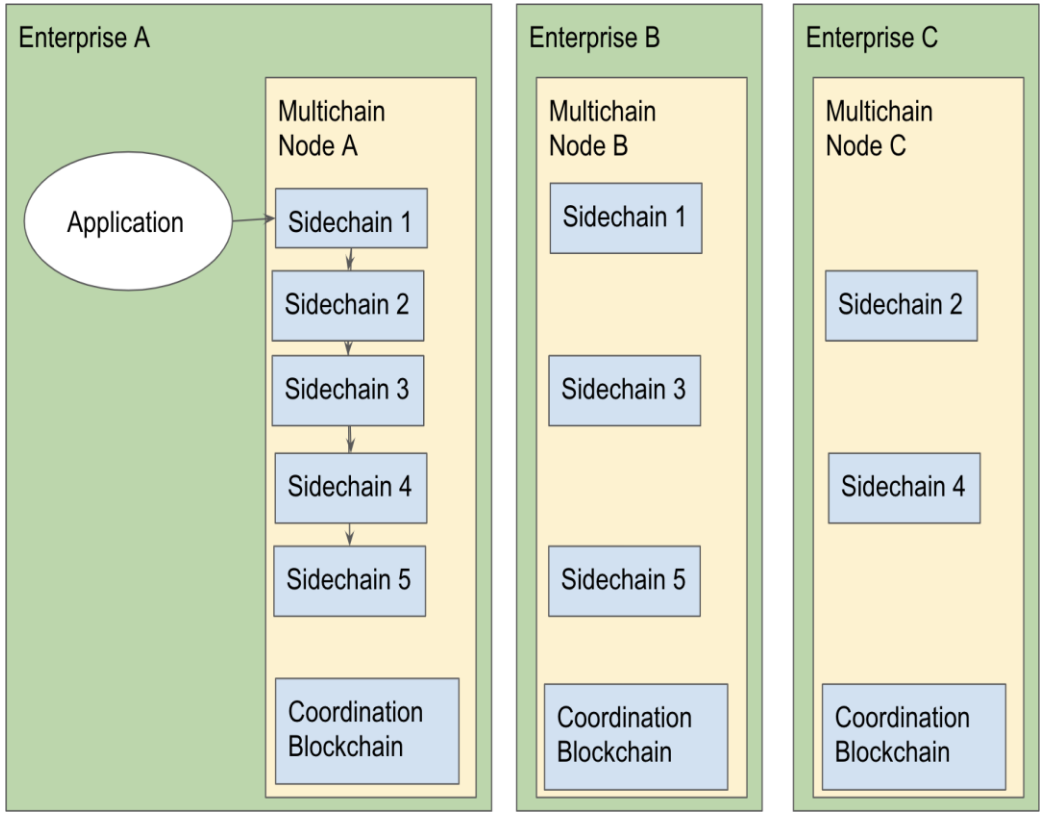


BLOCKCHAIN HYBRIDE : SIDECHAIN

Multichain Nodes:

Nœuds multichain: un nœud multichain est un regroupement d'un ou plusieurs nœuds de sidechain, où chaque nœud se trouve sur une sidechain différente. Les nœuds sidechain fonctionnent ensemble pour permettre les transactions et les vues Crosschain.

Le nœud multichaîne sur lequel la transaction est soumise doit avoir des nœuds de validation sur toutes les chaînes latérales sur lesquelles la transaction d'origine et les transactions et vues subordonnées ont lieu, en plus d'avoir accès à une blockchain de coordination (main net).



BLOCKCHAIN HYBRIDE : SIDECHAIN

Sidechain Keys and Sidechain Threshold Signatures:

Les messages d'une sidechain peuvent être vérifiés comme provenant de la sidechain en utilisant un schéma de signature de seuil. Chaque nœud de validation sur chaque sidechain possède un partage de clé privée Sidechain. Tout M des N nœuds de validation de sidechain doit collaborer pour signer un message.

La clé publique Sidechain peut être utilisée pour vérifier la signature. La signature et la clé publique ne trahissent aucune information sur les nœuds signés, sur le nombre seuil de nœuds de validation (M) ou sur le nombre total de nœuds de validation sur la sidechain (N).

La clé publique Sidechain doit être publiée dans la blockchain de coordination. Tout nœud de sidechain peut accéder à la clé publique de Sidechain une fois qu'elle est disponible dans la blockchain de coordination. Lorsqu'un nœud de validation est ajouté ou supprimé de la sidechain, une nouvelle génération de clé doit avoir lieu et la nouvelle clé publique doit être publiée dans la chaîne de blocs de coordination.

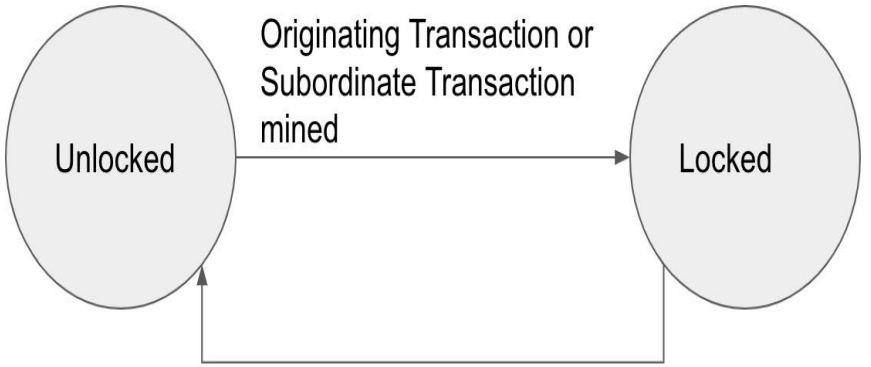
La publication dans la blockchain de coordination implique un processus de vote entre les participants de la sidechain. L'évaluation des votes doit refléter le seuil M. Le processus de vote doit être protégé de manière à ce que l'appartenance à la sidechain ne soit pas être révélée.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Contract Locking and Provisional State Updates;

Lorsqu'un nœud de coordination sur une sidechain reçoit une transaction d'origine, une transaction subordonnée ou une vue qui fait partie d'une transaction crosschain, il vérifie si le contrat est vérouillé. Si le contrat est verrouillé, la transaction ou la vue échoue. Si le contrat n'est pas verrouillé, la transaction ou la vue peut continuer.

La figure montre les transitions d'état de verrouillage pour un contrat. Le contrat de coordination Crosschain sera à l'état Démarré. Le fait de miner une transaction d'origine ou une transaction subordonnée et de l'inclure dans une blockchain verrouille le contrat. Le contrat est déverrouillé lorsque le contrat de coordination Crosschain est à l'état Committed ou Ignored, ou lorsque le numéro de bloc sur la chaîne de blocs de coordination est supérieur au numéro de bloc du délai d'expiration de la transaction. Le contrat de coordination crosschain passera de l'état Démarré à l'état Committed lorsqu'un message valide de validation de transaction crosschain lui est soumis, et il passera de l'état Démarré à l'état Ignoré lorsqu'un message Ignored de transaction crosschain valide lui est soumis.



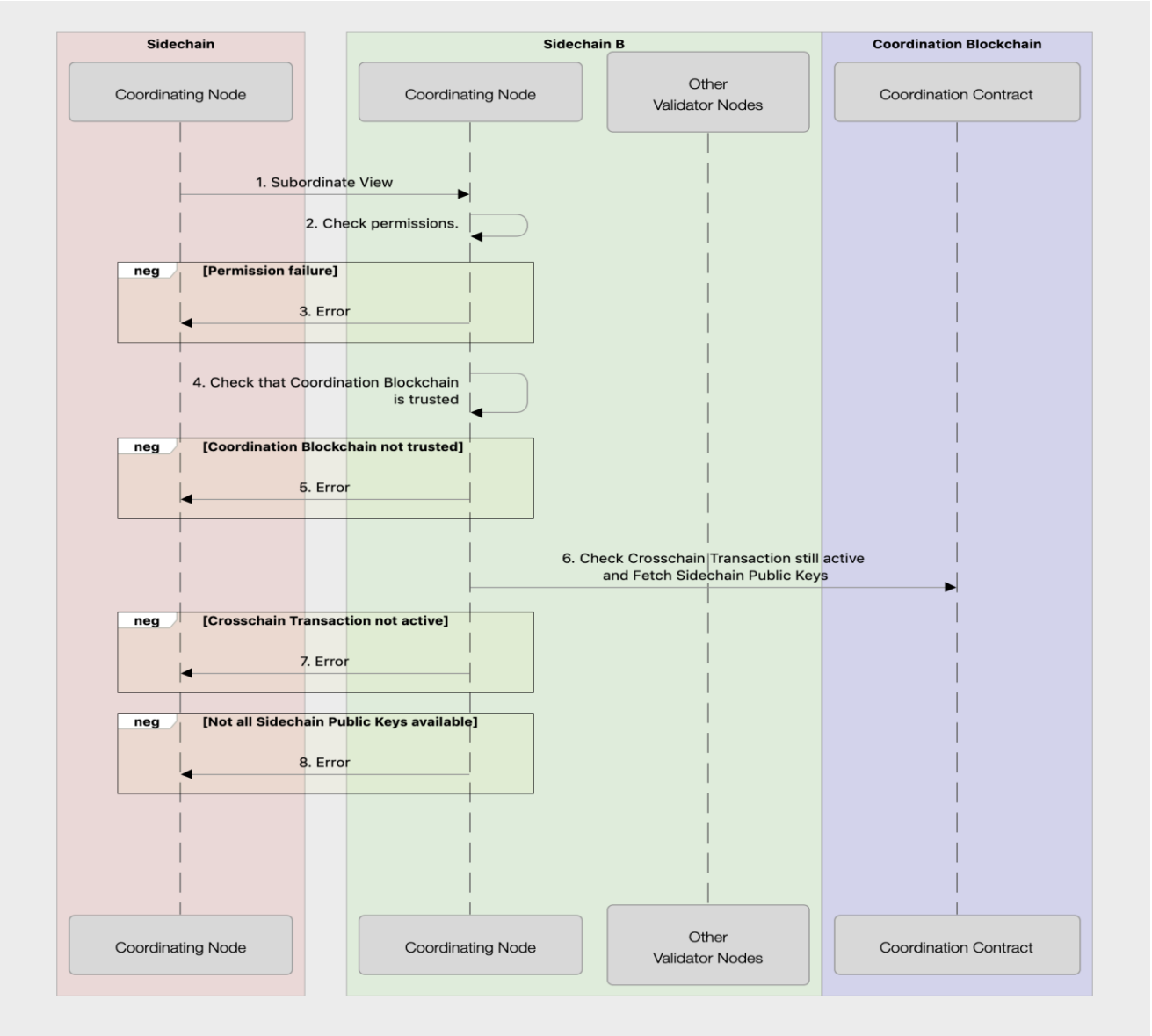
Crosschain Coordination Contract state = Ignore, or
Crosschain Coordination Contract state = Committed, or
Coordination Blockchain block number > Transaction Timeout Block Number

BLOCKCHAIN HYBRIDE : SIDECHAIN

Ethereum Private Sidechain- Opérations	Ethereum Main Net (public) comme Coordination Blockchain	
	Advantages	Désavantages
Discover using Ethereum Registration Authorities	Bonnes propriétés d'authenticité, d'intégrité et de non-répudiation. Réseau public sans autorisation, permet la consultation du registre.	
Épinglage d'état et épinglage d'état final	Bonnes propriétés d'authenticité, d'intégrité et de non-répudiation.	Coût économique. Augmentation de la congestion sur Ethereum MainNet. L'épinglage et les litiges sont publics.
State Pinning & Final State Pinning via an intermediate private blockchain	Tirez parti des propriétés de sécurité d'Ethereum MainNet (public) tout en minimisant les coûts et la congestion. L'épinglage et les litiges ne sont pas publics.	Les épingles prennent plus de temps pour devenir définitives sur Ethereum MainNet que si elles étaient épinglées directement. Les participants au Sidechain doivent observer tous les niveaux d'épinglage.
Sidechain Public Key	clés publiques largement disponibles.	Retards significatifs lors du premier Atomic Crosschain Des transactions peuvent être émises.
Atomic Crosschain Transaction State	Leverages Ethereum MainNet anti-spam capabilities.	Retarde considérablement le moment où les premières transactions Atomic Crosschain peuvent être émises. Coût économique du gaz. Augmentation de la congestion sur Ethereum MainNet.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate View Process & Coordinating Node Perspective part 1 (figure 1)



BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate View Process & Coordinating Node part 1

Ensemble, les figures 1 et 2 montrent des diagrammes de séquence pour le traitement d'une vue subordonnée du point de vue d'un nœud de coordination sur une sidechain.

La figure 1 décrit la séquence d'événements pour le nœud de coordination sur une chaîne latérale B afin de déterminer si le traitement de la vue principale doit être effectué. En parcourant le diagramme de séquence:

1) Le nœud de coordination sur une sidechain soumet une vue secondaire pour traitement au nœud de coordination sur la sidechain B.

2) Le nœud vérifie si le compte est autorisé à exécuter une vue subordonnée sur cette sidechain.

3) Une erreur est renvoyée si le compte qui a signé la vue subordonnée n'est pas autorisé à exécuter des vues sur cette sidechain.

4) L'adresse du contrat de coordination de la chaîne de blocs et de la chaîne de coordination spécifiée dans la vue subordonnée est vérifiée pour voir si elle est approuvée.

5) Renvoyer une erreur si la blockchain de coordination ou le contrat de coordination crosschain ne sont pas approuvés par cette sidechain.

6) Le nœud de coordination sur Sidechain B vérifie que la transaction crosschain a été lancée, n'a pas été validée ou ignorée et n'a pas expiré. Lors de cet appel, le nœud récupère également les clés publiques de Sidechain pour chaque vue subordonnée appelée par l'appel de fonction de cette vue subordonnée à partir du contrat de coordination inter-chaînes.

BLOCKCHAIN HYBRIDE : SIDECHAIN

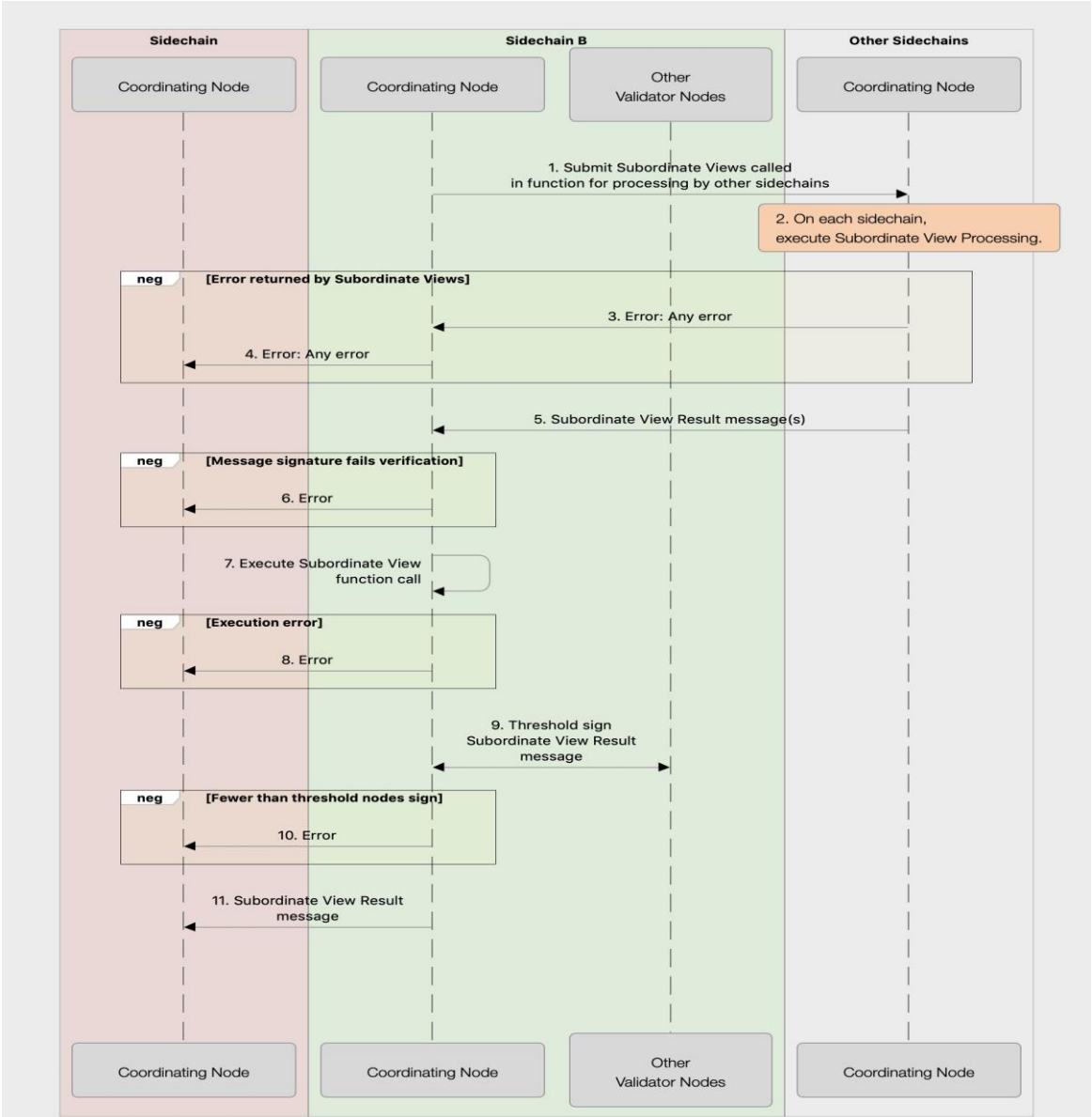
Subordinate View Process & Coordinating Node part 1

7) Une erreur est renvoyée si la transaction Crosschain n'est pas encore active.

8) Une erreur est renvoyée si toutes les clés publiques de sidechain pour les sidechains auxquelles les vues subordonnées doivent être soumises ne sont pas disponibles.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate View Process & Coordinating Node part 2 (figure 2)



BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate View Process & Coordinating Node part 2

1) Le nœud de coordination sur la chaîne latérale B soumet toutes les vues subordonnées appelées à la suite du traitement de l'appel de fonction de vue subordonnée aux nœuds de coordination sur les chaînes latérales que les vues subordonnées doivent exécuter.

2) Sur chaque sidechain, les vues subordonnées sont traitées de manière récursive selon les règles de traitement des vues subordonnées décrites dans cette section.

3) Une erreur est renvoyée si l'une des vues subordonnées envoyées depuis cette sidechain vers d'autres sidechains renvoie une erreur.

4) Les erreurs des vues subordonnées appelées sont renvoyées à la sidechain appelante.

5) En supposant qu'aucune erreur n'est renvoyée par l'une des autres chaînes latérales et que le délai d'attente n'a pas expiré, un message de résultat de vue subordonnée sera renvoyé pour chaque vue subordonnée soumise à d'autres chaînes latérales.

6) La signature de chaque message de résultat de la vue subordonnée est vérifiée à l'aide de la clé publique Sidechain de la sidechain sur laquelle la vue subordonnée a été exécutée. Une erreur est renvoyée si la signature sur un ou plusieurs des messages Subordinate View Result renvoyés par d'autres sidechains ne parvient pas à être vérifiée.

7) L'appel de fonction de vue subordonnée à traiter sur le Sidechain B est exécuté. Lorsqu'une vue subordonnée est appelée depuis l'appel de fonction, la sidechain réelle, l'adresse du contrat et les valeurs de paramètre sont comparées aux valeurs signées qui sont la prochaine vue subordonnée à distribuer. L'exécution de la fonction s'interrompt si les valeurs ne correspondent pas. S'ils correspondent, la valeur de retour spécifiée dans le message de résultat de la vue subordonnée est renvoyée à la fonction.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate View Process & Coordinating Node Perspective part 2

8) Une erreur est renvoyée s'il y a une erreur d'exécution. En plus des erreurs standard d'Ethereum EVM que les contrats Ethereum standard peuvent rencontrer, il s'agit d'une erreur si les paramètres réels et les paramètres signés d'une vue subordonnée appelée à partir de l'appel de fonction de vue subordonnée en cours de traitement ne correspondent pas.

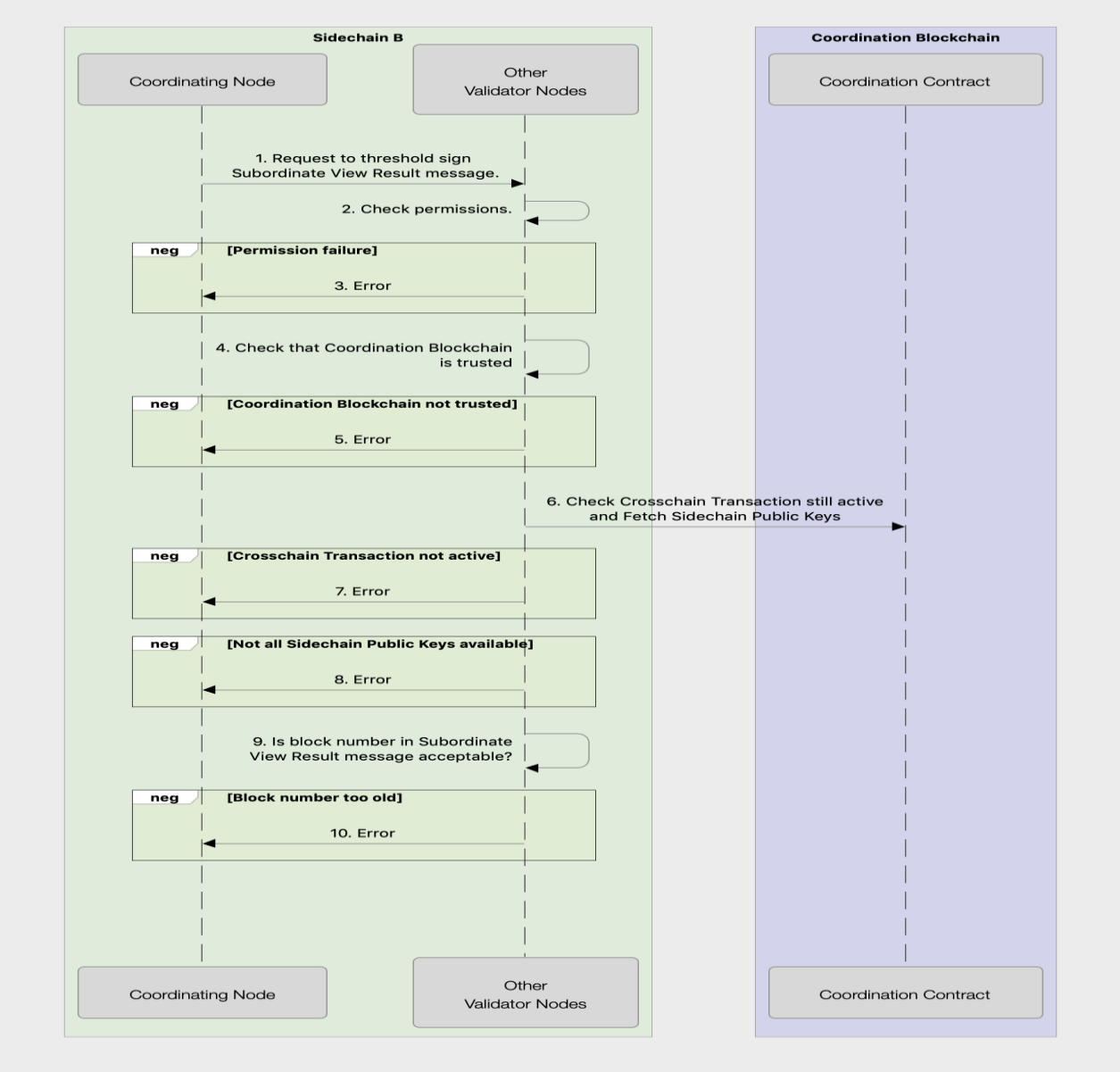
9) Travaillez avec tous les nœuds de validation sur la sidechain pour signer le seuil d'un message Subordinate View Result.

10) Une erreur est renvoyée si un nombre insuffisant de nœuds indique qu'ils sont prêts à signer le message Subordinate View Result. Dans ce cas, les nœuds auraient renvoyé des messages d'erreur indiquant qu'ils ne signeraient pas. En outre, les nœuds peuvent expirer.

11) Envoyer le message de résultat de la vue subordonnée au nœud de coordination qui a soumis la vue subordonnée pour traitement.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate View Process & Coordinating Node Perspective part 2 (figure 3)



BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate View Process & Coordinating Node Perspective part 2

La figure 3 montre le diagramme de séquence pour la première moitié du traitement d'une vue subordonnée du point de vue d'un nœud de validation qui n'est pas un nœud de coordination sur une sidechain. En parcourant le diagramme de séquence:

1) Le nœud de coordination sur la sidechain envoie un message Subordate View Result à signer au nœud. La demande inclut la vue subordonnée qui est en cours de traitement avec les messages de résultat de vue subordonnée signés pour toutes les autres chaînes latérales qui sont appelées dans le cadre de l'appel de fonction de vue subordonnée.

2) Le nœud vérifie si le compte est autorisé à exécuter une vue subordonnée sur cette sidechain.

3) Une erreur est renvoyée si le compte qui a signé la vue subordonnée n'est pas autorisé à exécuter des vues sur cette sidechain.

4) L'adresse du contrat de coordination de la chaîne de blocs et de la chaîne de coordination spécifiée dans la vue subordonnée est vérifiée pour voir si elle est approuvée.

5) Renvoyer une erreur si la blockchain de coordination ou le contrat de coordination crosschain ne sont pas approuvés par cette sidechain.

6) Le nœud vérifie que la transaction Crosschain a été lancée, n'a pas été validée ou ignorée et n'a pas expiré. Au cours du même appel, le nœud récupère les clés publiques Sidechain pour chaque vue subordonnée appelée par l'appel de fonction de cette vue subordonnée à partir du contrat de coordination inter-chaînes.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate View Process & Coordinating Node Perspective part 2

7) Une erreur est renvoyée si la transaction Crosschain n'est pas encore active.

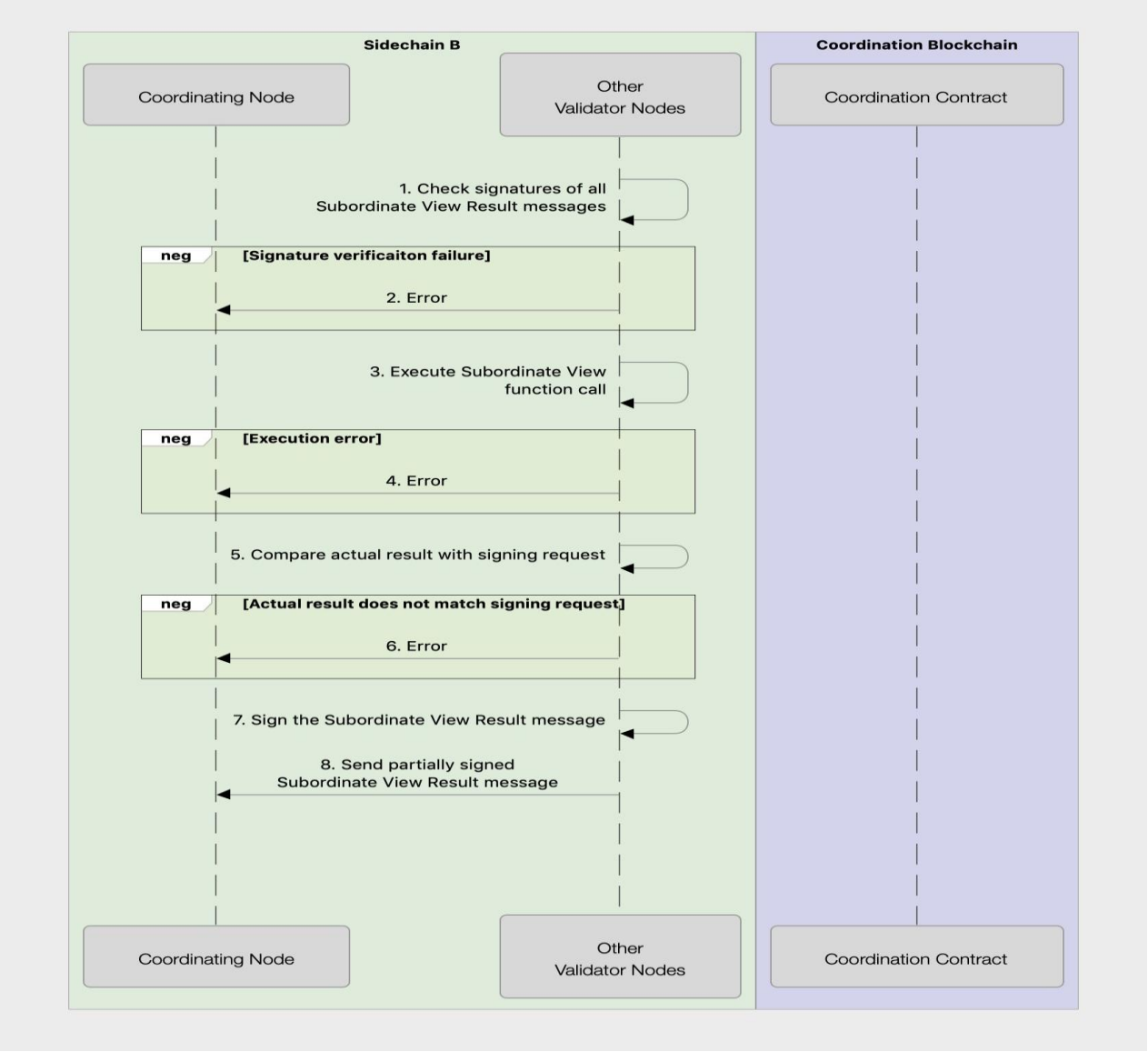
8) Une erreur est renvoyée si toutes les clés publiques de sidechain pour les sidechains de toutes les vues subordonnées appelées par la fonction ne sont pas disponibles.

9)Le nœud vérifie que le numéro de bloc spécifié dans le message Subordinate View Result est valide. C'est-à-dire que le numéro de bloc n'est pas dans le futur et n'est pas trop ancien.

10) Si c’est le cas une erreur est envoyé.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate View Process & Coordinating Node Perspective part 2 (figure 4)



BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate View Process & Coordinating Node Perspective part 2

La figure 4 montre le diagramme de séquence pour la seconde moitié du traitement d'une vue subordonnée du point de vue d'un nœud de validation qui n'est pas un nœud de coordination sur une sidechain. En parcourant le diagramme de séquence:

1) La signature de chaque message de résultat de la vue subordonnée est vérifiée à l'aide de la clé publique Sidechain de la sidechain sur laquelle la vue subordonnée a été exécutée.

2) Une erreur est renvoyée si une ou plusieurs signatures ne sont pas vérifiées.

3) L'appel de fonction de vue subordonnée à traiter sur le Sidechain B est exécuté. Lorsqu'une vue subordonnée est appelée à partir de l'appel de fonction, la sidechain réelle, l'adresse du contrat et les valeurs de paramètre sont comparées aux valeurs signées qui sont la prochaine vue subordonnée à distribuer. L'exécution de la fonction s'interrompt si les valeurs ne correspondent pas. S'ils correspondent, la valeur de retour spécifiée dans le message de résultat de la vue subordonnée est renvoyée à la fonction.

4) Une erreur est renvoyée s'il y a une erreur d'exécution. En plus des erreurs standard d'Ethereum EVM que les contrats Ethereum standard peuvent rencontrer, il s'agit d'une erreur si les paramètres réels et les paramètres signés d'une vue subordonnée appelée à partir de l'appel de fonction de vue subordonnée en cours de traitement ne correspondent pas.

5) Vérifiez que le résultat affiché dans la demande de signature du message Subordinate View Result correspond au résultat de l'exécution de l'appel de la fonction Subordinate View.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate View Process & Coordinating Node Perspective part 2

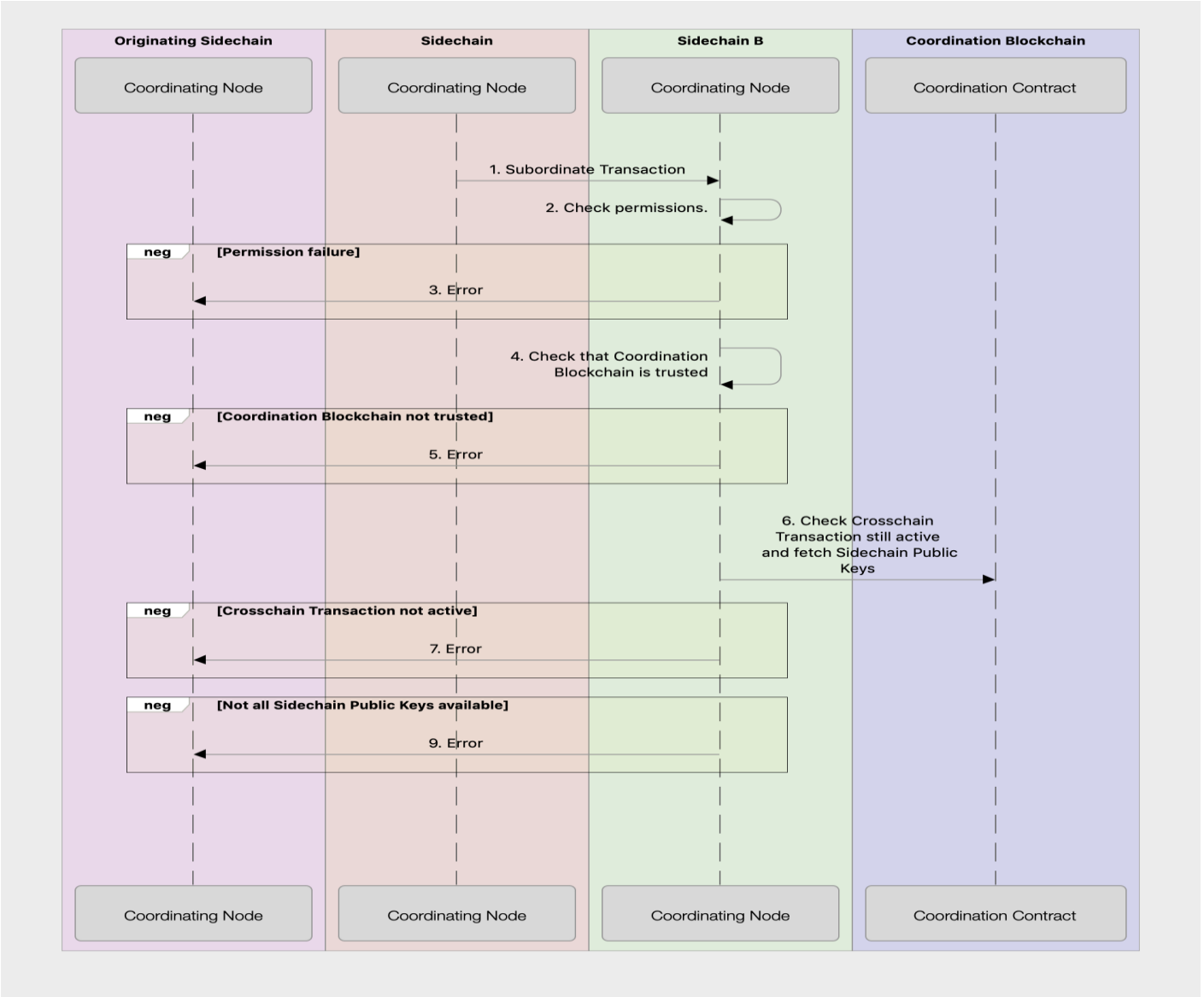
6) Renvoie une erreur si le résultat réel ne correspond pas à ce que le nœud de coordination demande à signer.

7) Seuil signe le message de résultat de la vue subordonnée.

8) Renvoyez le message partiellement signé au nœud de coordination.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate Transaction Processing: Coordinating Node Perspective: Part 1 (figure 5)



BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate Transaction Processing: Coordinating Node Perspective: Part 1

La figure 5 montre le diagramme de séquence pour la première moitié du traitement d'une transaction subordonnée du point de vue d'un nœud de coordination sur une sidechain. En parcourant le diagramme de séquence:

1) Le nœud de coordination sur une sidechain soumet une transaction secondaire pour traitement au nœud de coordination sur la sidechain B.

2) Le nœud de coordination sur la Sidechain B vérifie si le compte qui a signé la transaction a l'autorisation d'exécuter des transactions sur cette sidechain.

3) Une erreur est renvoyée au nœud de coordination sur la sidechain d'origine si le compte qui a signé cette transaction subordonnée n'est pas autorisé à soumettre des transactions à cette sidechain.

4) La blockchain de coordination et le contrat de coordination crosschain spécifiés dans la transaction subordonnée sont vérifiés pour voir s'ils sont dignes de confiance.

5) Renvoyer une erreur au nœud de coordination sur la sidechain d'origine si la blockchain de coordination ou le contrat de coordination crosschain ne sont pas approuvés par cette sidechain.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate Transaction Processing: Coordinating Node Perspective: Part 1

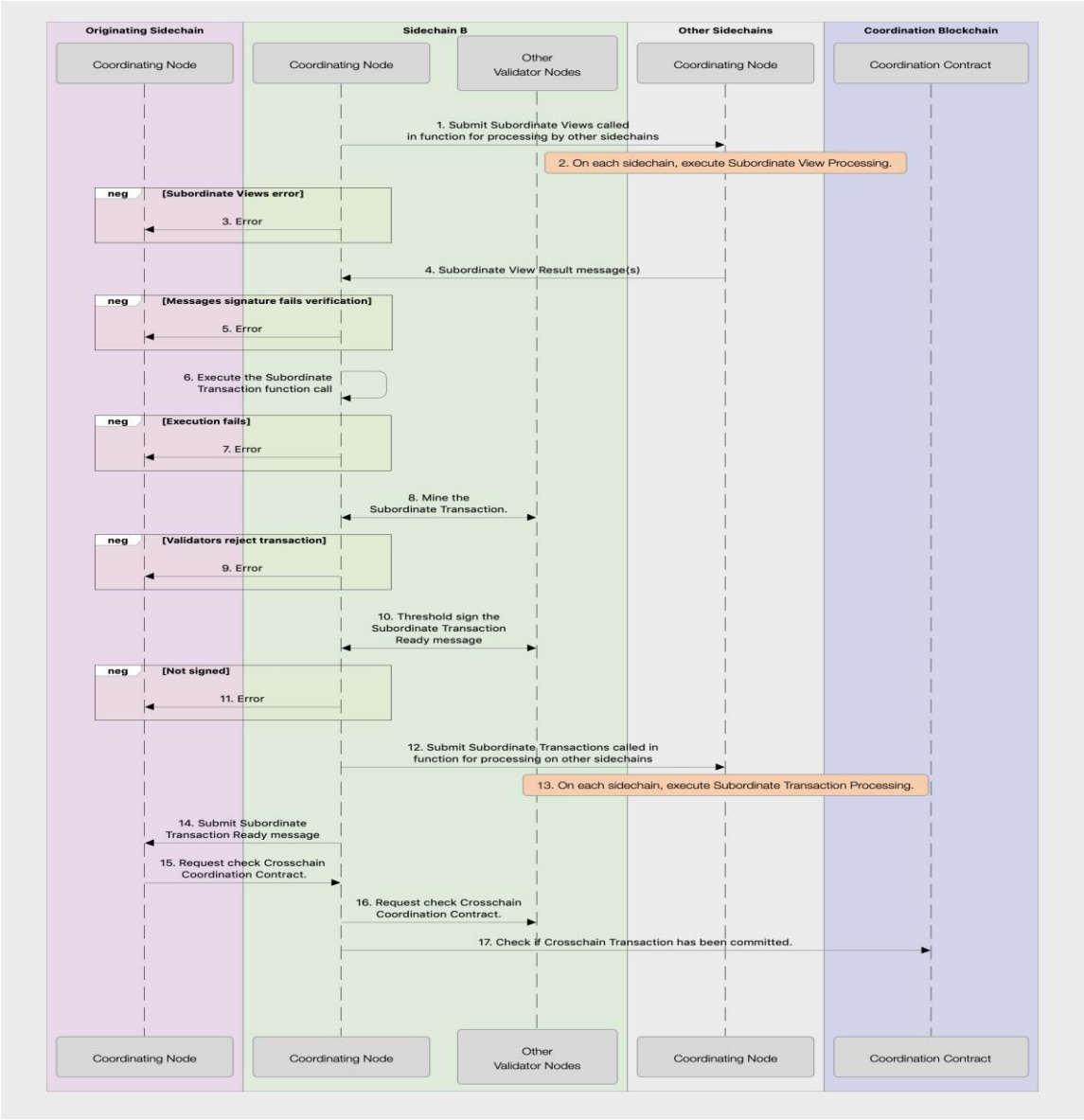
6) Le nœud de coordination sur Sidechain B vérifie que la transaction crosschain a été lancée, n'a pas été validée ou ignorée et n'a pas expiré. Le nœud récupère également les clés publiques de Sidechain pour chaque vue subordonnée appelée par l'appel de fonction de cette vue subordonnée à partir du contrat de coordination Crosschain.

7) Une erreur est renvoyée au nœud de coordination sur le Sidechain d'origine si la transaction Crosschain n'est pas encore active.

8) Une erreur est renvoyée au nœud de coordination sur la sidechain d'origine si toutes les clés publiques de sidechain pour les sidechains que les vues subordonnées doivent être appelées à la suite de l'appel de la fonction Transaction subordonnée ne sont pas disponibles.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate Transaction Processing: Coordinating Node Perspective: Part 1 (figure 6)



BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate Transaction Processing: Coordinating Node Perspective: Part 1

La figure 6 montre le diagramme de séquence pour la seconde moitié du traitement d'une transaction subordonnée du point de vue d'un nœud de coordination sur une chaîne latérale. En parcourant le diagramme de séquence:

1) Le nœud de coordination sur la chaîne latérale B soumet toutes les vues subordonnées appelées à la suite de l'appel de fonction de transaction subordonnée qu'il traite aux nœuds de coordination sur les chaînes latérales que les vues subordonnées doivent exécuter.

2) Sur chaque sidechain, les vues subordonnées sont traitées de manière récursive selon les règles de traitement des vues subordonnées décrites dans la section IV-B.

3) Une erreur est renvoyée au nœud de coordination sur la chaîne latérale d'origine si l'une des vues subordonnées renvoie une erreur.

4) Les nœuds de coordination sur les sidechains qui ont exécuté les vues subordonnées renvoient un message de résultat de vue subordonnée signé de seuil.

5) Une erreur est renvoyée au nœud de coordination sur la chaîne latérale d'origine si un message de résultat de vue subordonnée pour chaque vue subordonnée distribuée n'est pas renvoyé. La transaction échoue si les signatures de toutes les vues subordonnées ne peuvent pas être vérifiées.

BLOCKCHAIN HYBRIDE : SIDECHAIN

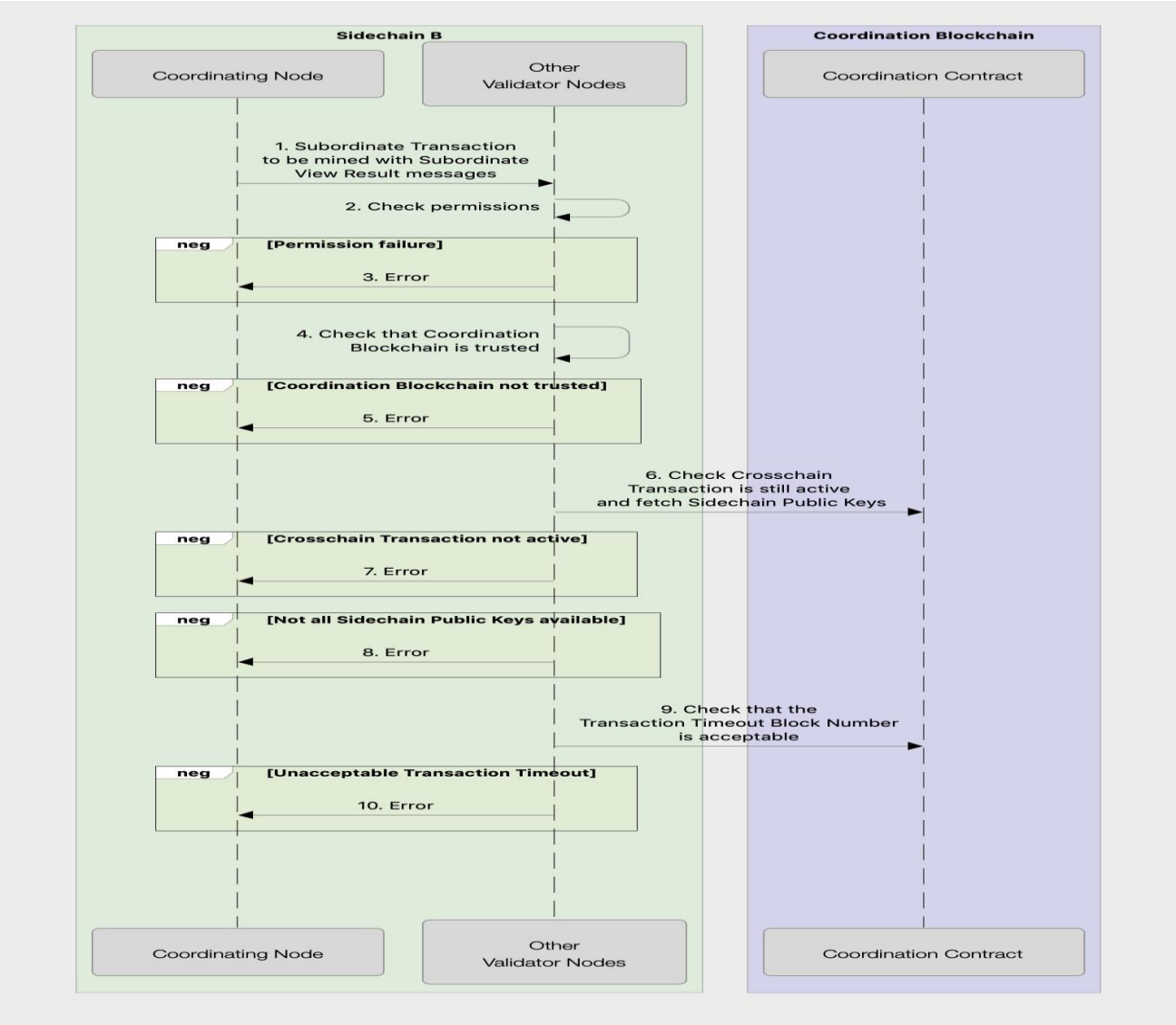
Subordinate Transaction Processing: Coordinating Node Perspective: Part 1

6) Exécutez l'appel de fonction dans la transaction subordonnée. Lorsqu'une vue subordonnée ou une transaction subordonnée est appelée à partir de l'appel de fonction, la chaîne latérale réelle, l'adresse du contrat et les valeurs de paramètre sont comparées aux valeurs signées qui sont la prochaine transaction ou vue subordonnée à distribuer. L'exécution de la fonction s'interrompt si les valeurs ne correspondent pas. S'ils correspondent, alors pour les vues subordonnées, la valeur de retour spécifiée dans le message de résultat de la vue subordonnée est renvoyée à la fonction.

7) Une erreur est renvoyée au nœud de coordination sur la chaîne latérale d'origine si la fonction ne s'exécute pas jusqu'à la fin.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate Transaction Processing: Coordinating Node Perspective: Part 1 (figure 7)



BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate Transaction Processing: Coordinating Node Perspective: Part 1

La figure 7 montre le diagramme de séquence pour la première moitié du traitement d'une transaction subordonnée du point de vue d'un nœud autre que le nœud de coordination sur une sidechain. En parcourant le diagramme de séquence:

1) Le nœud de coordination sur Sidechain B envoie une transaction subordonnée à extraire, avec les messages de résultat de vue subordonnée associés à tous les nœuds de validation sur Sidechain B.

2) Chaque nœud de validation vérifie si le compte qui a signé la transaction a l'autorisation d'exécuter des transactions sur cette sidechain.

3) Une erreur est renvoyée au nœud de coordination si le compte qui a signé cette transaction subordonnée n'est pas autorisé à soumettre des transactions à cette sidechain.

4) Le contrat de coordination blockchain et de coordination crosschain spécifié dans l'opération subordonnée sont vérifiés pour voir s'ils sont dignes de confiance.

5) Renvoyer une erreur au nœud de coordination si le contrat de coordination crosschain ou la chaîne de blocs de coordination ne sont pas approuvés par cette sidechain.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate Transaction Processing: Coordinating Node Perspective: Part 1

6) Chaque nœud de validation vérifie que la transaction crosschain a été lancée, n'a pas été validée ou ignorée et n'a pas expiré. Le nœud récupère les clés publiques Sidechain pour chaque vue subordonnée appelée par l'appel de fonction de cette transaction subordonnée à partir du contrat de coordination inter-chaîne.

7) Une erreur est renvoyée au nœud de coordination si la transaction Crosschain n'est pas encore active.

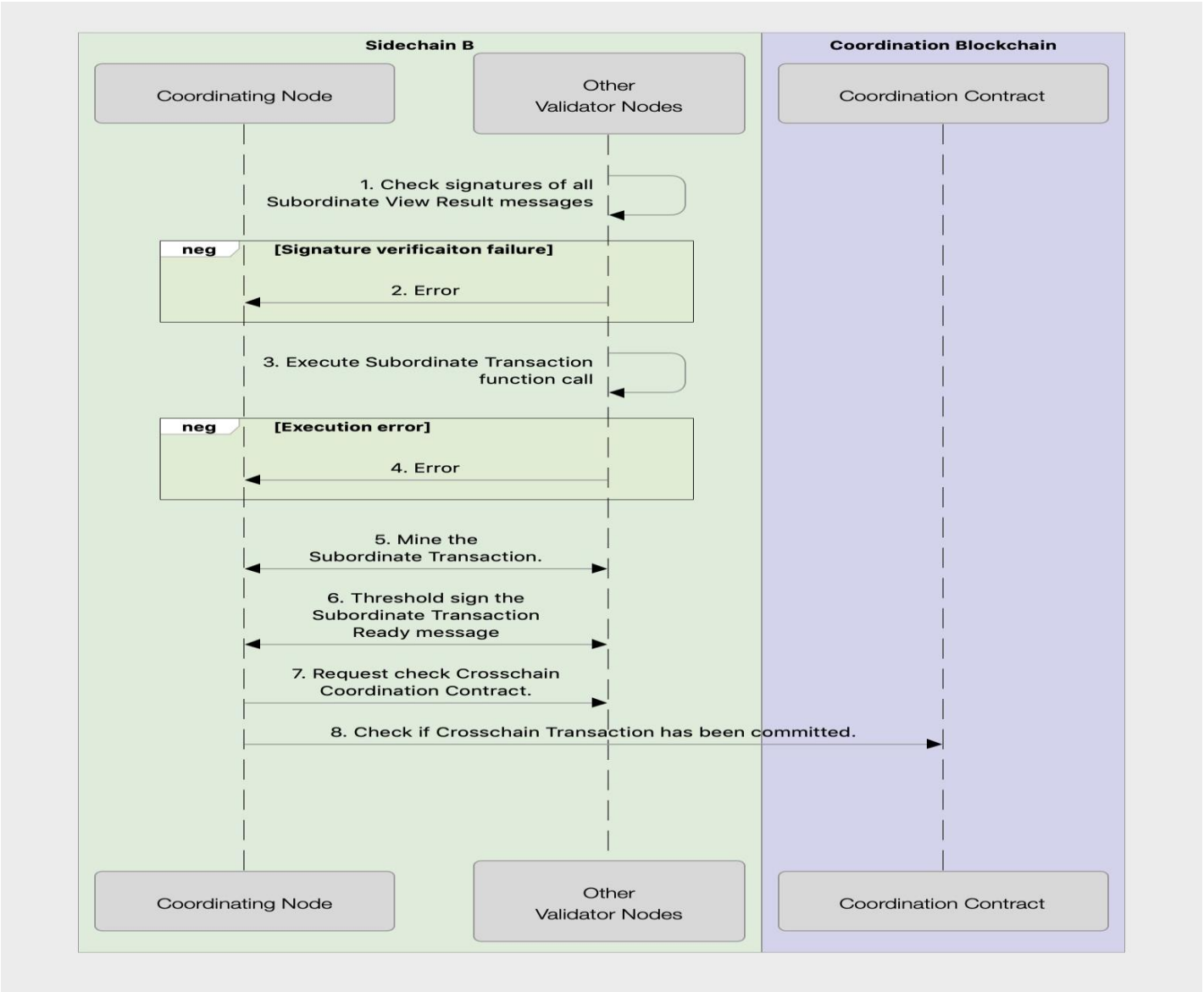
8) Une erreur est renvoyée au nœud de coordination si toutes les clés publiques de sidechain pour les sidechains que les vues subordonnées doivent être appelées à la suite de l'appel de fonction de transaction subordonnée ne sont pas disponibles.

9) Chaque nœud de validation vérifie que le numéro de bloc du délai d'expiration de la transaction, le délai d'expiration global, est une valeur acceptable. Autrement dit, il vérifie que le numéro de bloc est égal ou inférieur à la durée pendant laquelle il est prêt à verrouiller un contrat.

10) Le validateur renvoie une erreur s'il trouve que le numéro de bloc du délai d'expiration de la transaction est inacceptable.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate Transaction Processing: Other Node Perspec- tive: Part 2 (figure 8)



BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate Transaction Processing: Other Node Perspec- tive: Part 2

La figure 8 montre le diagramme de séquence pour la seconde moitié du traitement d'une transaction subordonnée du point de vue d'un nœud autre que le nœud de coordination sur une chaîne latérale. En parcourant le diagramme de séquence:

1) Chaque nœud de validation vérifie la signature de chaque message Subordate View Result.

2) Une erreur est renvoyée au nœud de coordination si l'une des signatures ne peut pas être vérifiée.

3) Exécutez l'appel de fonction dans la transaction subordonnée. Lorsqu'une vue subordonnée ou une transaction subordonnée est appelée à partir de l'appel de fonction, la chaîne latérale réelle, l'adresse du contrat et les valeurs de paramètre sont comparées aux valeurs signées qui sont la prochaine transaction ou vue subordonnée à distribuer . L'exécution de la fonction s'interrompt si les valeurs ne correspondent pas. S'ils correspondent, alors pour les vues subordonnées, la valeur de retour spécifiée dans le message de résultat de la vue subordonnée est renvoyée à la fonction.

4) Une erreur est renvoyée au nœud de coordination si la fonction neécute pas jusqu'à la fin.

5) L'algorithme de minage spécifique à l'algorithme de consensus se termine.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate Transaction Processing: Other Node Perspec- tive: Part 2

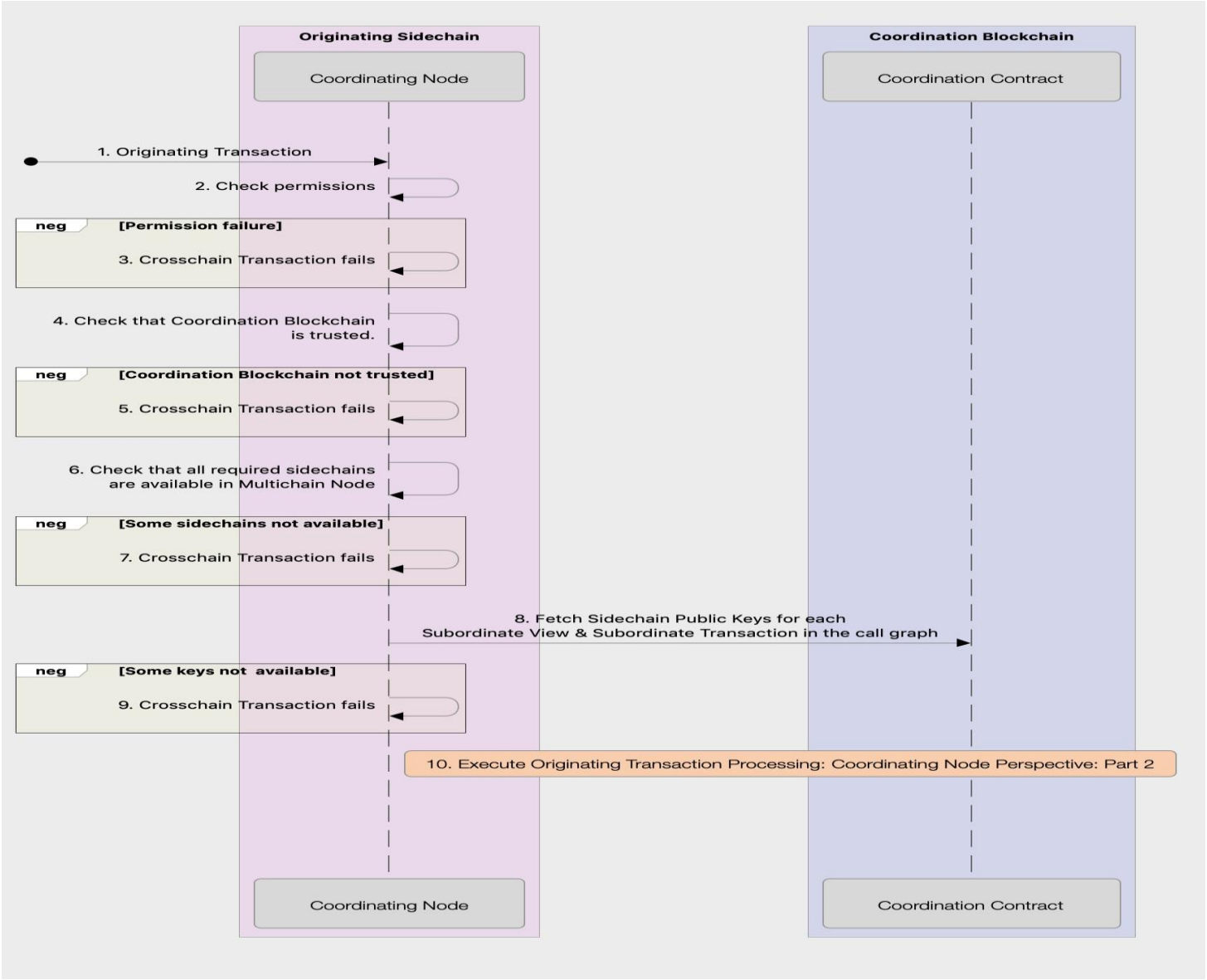
6) Le nœud de coordination envoie le message Subordonné Transaction Ready à signer. Le message contient l'identifiant de la sidechain d'origine, l'important de la transaction crosschain, l'identifiant de la coordination blockchain, l'adresse du contrat de coordination crosschain, l'identifiant de la sidechain sur laquelle la transaction subordonnée doit être exécutée et le hachage de la transaction subordonnée. . Chaque seuil de validation signe le message et le retour au nœud de coordination si une transaction correspondante au message a été finalisée.

7) Une fois que le message de validation de transaction crosschain a été vérifié et accepté par le contrat de coordination crosschain, la transaction crosschain est prête à être validée sur toutes les sidechains. Le nœud de coordination sur la sidechain d'origine envoie un message demandant que tous les nœuds vérifient le contrat de coordination inter-chaînes. Ce message est transmis depuis le nœud de coordination sur la Sidechain B à tous les validateurs sur la Sidechain.

8) Chaque validateur vérifie le contrat de coordination crosschain pour voir si la transaction crosschain a été validée ou ignorée. Le nœud de coordination applique les mises à jour d'état si la transaction a été validée. Si l'état est Committed ou Ignored, le nœud déverrouille le contrat.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate Transaction Processing: Other Node Perspec- tive: Part 2 (figure 9)



BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate Transaction Processing: Other Node Perspec- tive: Part 2

La Figure 14 décrit la séquence d'événements pour le nœud de coordination sur le Sidechain d'origine pour déterminer si la Transaction Crosschain doit être démarrée. En parcourant le diagramme de séquence:

1) L'application soumet la transaction d'origine au nœud de coordination sur la chaîne latérale d'origine.

2) Le nœud de coordination sur la sidechain d'origine vérifie si le compte qui a signé la transaction a l'autorisation d'exécuter des transactions sur cette sidechain.

3) La transaction échoue si le compte qui a signé cette transaction d'origine n'est pas autorisé à soumettre des transactions à cette sidechain.

4) Le nœud de coordination sur la sidechain d'origine vérifie que la sidechain ou la blockchain spécifiée par l'identifiant de coordination Blockchain. La transaction est disponible dans le ledger du Multichain Node. L'adresse du contrat de coordination Crosschain est vérifiée pour s'assurer qu'elle est fiable.

BLOCKCHAIN HYBRIDE : SIDECHAIN

Subordinate Transaction Processing: Other Node Perspec- tive: Part 2

5) La transaction échoue si la blockchain de coordination n'est pas disponible ou n'est pas approuvée ou si le contrat de coordination crosschain n'est pas approuvé.

6) Le nœud de coordination sur la chaîne latérale d'origine vérifie que le nœud multichaîne sur lequel il s'exécute contient des nœuds de validation sur toutes les chaînes latérales représentées par la vue subordonnée et la transaction subordonnée dans l'ensemble de la vue subordonnée et de l'arborescence des transactions. Le nœud multichaîne le fait pour garantir que l'intégralité de la transaction Crosschain pourra s'exécuter.

7) La transaction échoue si certaines des sidechains requises ne sont pas disponibles dans le nœud multichain.

8) Le nœud de coordination sur la chaîne secondaire d'origine récupère les clés publiques de la chaîne secondaire pour chaque vue subordonnée et transaction subordonnée dans l'ensemble de la vue subordonnée et de l'arborescence des transactions. Ceci est fait pour garantir que toutes les clés publiques sont disponibles.

9) La transaction échoue si certaines des clés publiques Sidechain ne sont pas disponibles.