(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 140 462**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **22 09987**

(51) Int Cl[8] : ***G 06 F 9/44*** *(2023.01), G 06 F 21/64, H 03 K 17/62, H 04 L 9/14, 9/30, G 06 F 12/00*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 30.09.22.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 05.04.24 Bulletin 24/14.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *LEDGER Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** HAMEAU Patrice, Emmanuel, Denis, THIERRY Philippe et GUILLEMET Charles.

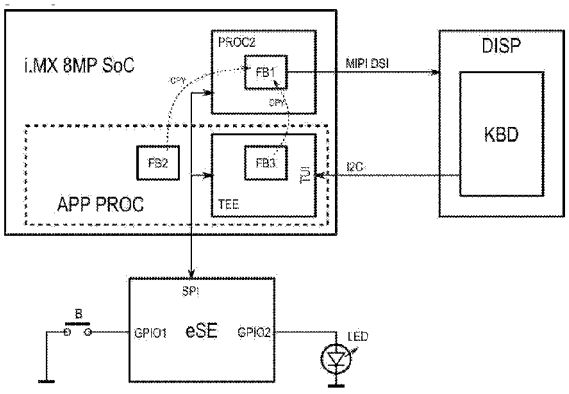
(73) **Titulaire(s) :** LEDGER Société par actions simplifiée.

(74) **Mandataire(s) :** OMNIPAT.

(54) Smartphone intégrant un portefeuille matériel de stockage de clés cryptographiques mettant en œuvre un multiplexage logiciel de l'afficheur du smartphone.

(57) L'invention est relative à un terminal connecté comprenant une interface homme-machine incluant un afficheur (DISP) gérable par un bus de commande (MIPI DSI); un processeur d'application (APP PROC) intégrant un premier gestionnaire d'affichage (FB2, FB3) configuré pour gérer l'afficheur (DISP); un processeur secondaire cloisonné (PROC2) intégrant un deuxième gestionnaire d'affichage (FB1) configuré pour prendre la main sur le premier gestionnaire d'affichage pour gérer l'afficheur (DISP); un élément sécurisé embarqué (eSE) connecté au processeur d'application et au processeur secondaire (PROC2) par un bus câblé (SPI), configuré pour effectuer des calculs cryptographiques avec un secret stocké dans l'élément sécurisé, sur une transaction reçue d'une application exécutée sur le processeur d'application; et un dispositif de validation de transaction (B) actionnable par un utilisateur et accessible exclusivement par l'élément sécurisé (eSE). L'élément sécurisé (eSE) et le processeur secondaire (PROC2) sont configurés pour que l'élément sécurisé transmette au processeur secondaire des données d'affichage liées à la transaction reçue et que le processeur secondaire réagisse en prenant la main sur la gestion de l'afficheur (DISP) pour afficher les données d'affichage transmises par l'élément sécurisé.

Figure pour l'abrégé : Fig. 4



FR 3 140 462 - A1

Description

Titre de l'invention : Smartphone intégrant un portefeuille matériel de stockage de clés cryptographiques mettant en œuvre un multiplexage logiciel de l'afficheur du smartphone

Domaine technique

[0001] L'invention est relative à des dispositifs portatifs sécurisés pour le stockage et la mise en œuvre de clés cryptographiques privées de façon cloisonnée par rapport à un réseau (stockage "à froid"), notamment des clés permettant d'effectuer des transactions sur une blockchain.

Arrière-plan

[0002] Ces dernières années, le développement des cryptomonnaies ou autres types de cryptoactifs gérés par la blockchain, tels que les jetons non fongibles (« NFT ») et les contrats intelligents ("Smart Contracts"), a donné naissance à divers moyens de stockage et de conservation des clés privées attachées à ces différents types de cryptoactifs. C'est ainsi que sont apparues les notions de "portefeuille", de "stockage à froid" et de stockage "à chaud" de clés privées. Un "portefeuille", appelé aussi "porte-monnaie", est un appareil ou un programme dont la fonction est de gérer des cryptoactifs, et donc de stocker les clés privées qui y sont attachées. Les portefeuilles dits "chauds" ("hot wallets") sont connectés à Internet et susceptibles d'attaques de pirates ou d'exposition à des virus et malwares. Il peut s'agir de portefeuilles gérés par des plateformes d'échange centralisé, qui n'offrent pas le plus haut niveau de sécurité. Ainsi, de nombreuses plateformes centralisées ont été pillées de centaines de millions de dollars par des pirates au fil des ans. Les portefeuilles "chauds" peuvent aussi prendre la forme de programmes installés sur des téléphones mobiles, tablettes ou ordinateurs personnels ("software wallets"). De tels portefeuilles sont en permanence connectés à Internet et intègrent de nombreuses applications non sécurisées, donc eux-mêmes susceptibles d'attaques.

[0003] Les portefeuilles froids ("cold wallets") constituent la solution la plus sûre pour le stockage à froid ("cold storage") de clés privées, c'est-à-dire hors de tout accès direct à Internet, ce qui réduit la surface d'attaque et donc le risque de vol par piratage informatique. Les transactions mettant en jeu des clés privées sont signées dans un environnement hors ligne. Toute transaction initiée en ligne est temporairement transférée vers le portefeuille matériel hors ligne, où elle est ensuite signée numériquement avant d'être transmise au réseau en ligne. Comme la clé privée n'est pas communiquée au serveur en ligne pendant le processus de signature, un pirate informatique ne peut pas y accéder.

[0004] La forme la plus simple de stockage à froid est le stockage passif. Un portefeuille passif peut être un document papier ou un fichier image sur lequel sont inscrites des clés publiques et privées de l'utilisateur. Le stockage passif comporte généralement un code QR intégré qui peut ensuite être scanné pour signer une transaction. L'inconvénient de ce support est que si le stockage passif est perdu, illisible ou détruit, l'utilisateur ne peut plus accéder à ses fonds.

[0005] Les portefeuilles ou portes-monnaies matériels appelés "hardware wallets" constituent une alternative pratique aux portefeuilles passifs pour stocker des clés privées. De plus, ils sont généralement configurés pour générer des phrases de récupération ("recovery phrases") permettant de restaurer les clés privées s'ils sont perdus. Rappelons que les cryptoactifs ne sont jamais stockés dans un porte-monnaie matériel, mais se trouvent enregistrés sur la blockchain. Le porte-monnaie matériel ne fait que stocker les clés privées permettant de gérer les transactions sur la blockchain. Les clés publiques correspondant aux clés privées pointent vers une adresse sur la blockchain où se trouvent réellement les actifs.

[0006] Comme montré sur la [Fig.1], un portefeuille matériel HW n'est jamais directement connecté à Internet. Pour être utilisable, le portefeuille matériel HW doit être relié à un dispositif hôte HDV au moyen d'une liaison de données LNK, par exemple USB ou Bluetooth. Le dispositif hôte HDV peut être un ordinateur, un téléphone mobile ou une tablette, et exécute un logiciel dit "compagnon" permettant de conduire des transactions sur la blockchain BCN, tel que le logiciel "Ledger Live" développé par la demanderesse. Alternativement, le portefeuille matériel HW peut être utilisé, par l'intermédiaire du dispositif hôte HDV avec des plateformes d'échange décentralisées ou "DEX", sur lesquelles l'utilisateur peut réaliser des transactions tout en conservant ses clés dans le portefeuille matériel.

[0007] Les portefeuilles matériels HW commercialisés par la demanderesse ont connu un important succès commercial en raison du haut degré de sécurité qu'ils offrent, grâce à l'utilisation d'un élément sécurisé ou "secure element" pour conserver les clés privées et signer les transactions. Un élément sécurisé est une plate-forme matérielle capable de stocker et de manipuler des données en conformité avec les règles et les exigences de sécurité fixées par une autorité de confiance. Il se présente sous la forme d'une puce de semi-conducteur mettant en œuvre diverses contre-mesures visant à contrer des attaques de fraudeurs.

[0008] La [Fig.2] montre l'architecture d'un portefeuille matériel HW1 du type commercialisé par la demanderesse sous l'appellation "Nano S", décrit plus en détail dans le document https://developers.ledger.com/docs/nano-app/bolos-hardware-architecture/. Le portefeuille matériel HW1 comporte un élément sécurisé SE1 associé à un micro-

contrôleur MCU1. Le processeur MCU1 comporte une interface USB U1 et agit comme un dispositif mandataire (proxy) à l'égard de l'élément sécurisé SE1, pour la communication avec un dispositif hôte externe HDV exécutant un logiciel compagnon (Cf. [Fig.1]). L'élément sécurisé SE1 possède son propre système d'exploitation OS sécurisé (micrologiciel) lui permettant d'exécuter des programmes, et intègre un co-processeur cryptographique CRY. Le portefeuille matériel HW1 comporte également un afficheur DISP1 et deux boutons B1, B2 gérés par le microcontrôleur MCU1. Ces deux boutons jouent un rôle important dans la sécurisation de certaines opérations : l'utilisateur doit appuyer en même temps sur les deux boutons afin de manifester son accord ou consentement pour la réalisation ou la finalisation de ces opérations.

[0009] Les portefeuilles matériels tels qu'exposés ci-dessus sont généralement des dispositifs portables détachés que l'on vient relier temporairement à un dispositif hôte "connecté", comme un terminal mobile ou smartphone, au moment d'effectuer une transaction. Le caractère détaché de ces portefeuilles matériels offre un degré supérieur de sécurité du fait qu'ils sont la plupart du temps inaccessibles via les réseaux publics, et donc peu exposés aux attaques. Cependant, cette caractéristique rend ces portefeuilles matériels peu ergonomiques et susceptibles d'égarement ou d'oubli.

[0010] On connaît des smartphones blockchain, qui sont conçus pour stocker de façon sécurisée certains actifs virtuels comme des cryptomonnaies et disposant d'un espace de stockage interne inaccessible par l'Internet pour constituer un portefeuille froid : le modèle Galaxy S10 de Samsung®, le modèle Exodus 1 de HTC®, ou le modèle Finney de Sirin Labs®. Ces smartphones sont équipés d'un élément sécurisé embarqué (désigné par eSE pour "Embedded Secure Element") qui est une puce spécialement conçue pour stocker des données sensibles et les partager uniquement avec des applications et des personnes autorisées.

[0011] En matière de cryptomonnaie, il est requis un degré de sécurité très élevé. Les smartphones blockchain exposés ci-dessus offrent un certain degré de sécurité par l'utilisation d'une enclave sécurisée ou environnement d'exécution de confiance TEE ("Trusted Execution Environment"), mais la fonction de portefeuille matériel numérique, qui n'est pas la première fonction d'un tel téléphone, exige davantage. En effet, la mise en œuvre d'un portefeuille matériel à l'intérieur d'un smartphone supprime en partie les avantages en termes de sécurité d'un portefeuille matériel détaché que l'on connecte seulement en cas de besoin. Cela augmente inévitablement l'exposition du portefeuille aux attaques par Internet.

Résumé

[0012] On prévoit de façon générale un terminal connecté comprenant une interface homme-machine incluant un afficheur gérable par un bus de commande ; un processeur d'application intégrant un premier gestionnaire d'affichage configuré pour gérer

l'afficheur ; un processeur secondaire cloisonné intégrant un deuxième gestionnaire d'affichage configuré pour prendre la main sur le premier gestionnaire d'affichage pour gérer l'afficheur ; un élément sécurisé embarqué connecté au processeur d'application et au processeur secondaire par un bus câblé, configuré pour effectuer des calculs cryptographiques avec un secret stocké dans l'élément sécurisé, sur une transaction reçue d'une application exécutée sur le processeur d'application ; et un dispositif de validation de transaction actionnable par un utilisateur et accessible exclusivement par l'élément sécurisé. L'élément sécurisé et le processeur secondaire sont configurés pour que l'élément sécurisé transmette au processeur secondaire des données d'affichage liées à la transaction reçue et que le processeur secondaire réagisse en prenant la main sur la gestion de l'afficheur pour afficher les données d'affichage transmises par l'élément sécurisé.

[0013] L'interface homme-machine peut inclure en outre un dispositif de saisie commandé par un bus correspondant, le terminal comprenant en outre un démultiplexeur commandé par l'élément sécurisé pour : dans un mode inactif, connecter le bus du dispositif de saisie pour qu'il soit géré par le processeur d'application, et dans un mode actif, connecter le bus du dispositif de saisie pour qu'il soit exclusivement géré par l'élément sécurisé.

[0014] Le dispositif de saisie peut être une dalle tactile et le dispositif de validation de transaction un bouton virtuel sur la dalle tactile dans le mode actif.

[0015] Le dispositif de validation de transaction peut être un bouton physique.

[0016] Le terminal peut comprendre en outre un commutateur physique bistable actionnable par l'utilisateur et accessible exclusivement par l'élément sécurisé, configuré pour, dans une première position, passer l'élément sécurisé en mode actif et, dans une deuxième position, passer l'élément sécurisé en mode inactif ; et des moyens pour solliciter l'utilisateur à actionner le commutateur.

[0017] L'élément sécurisé peut être configuré pour, en mode actif, inhiber des circuits capables de mesurer des paramètres du terminal pour déduire des informations sensibles.

[0018] Le terminal peut comprendre en outre un indicateur dédié perceptible par l'utilisateur, commandé exclusivement par l'élément sécurisé pour être activé pendant le mode actif et désactivé pendant le mode inactif.

[0019] On prévoit également un procédé de validation et signature d'une transaction sur la blockchain utilisant un terminal du type susmentionné, comprenant les étapes suivantes : le commutateur étant dans la position du mode inactif, solliciter à travers l'application et à l'aide d'un message sur l'afficheur que l'utilisateur bascule le commutateur dans la position du mode actif ; au basculement du commutateur, envoyer par l'élément sécurisé un acquittement à l'application ; à la réception de l'acquittement,

transmettre par l'application des informations de la transaction à l'élément sécurisé ; dans l'élément sécurisé, gérer l'affichage, la validation et la signature de la transaction, et envoyer le résultat à l'application ; et solliciter par l'élément sécurisé à l'aide d'un message sur l'afficheur que l'utilisateur bascule le commutateur dans la position du mode inactif.

[0020] Le processeur d'application et le processeur secondaire peuvent être intégrés dans un même système-sur-puce.

Description sommaire des dessins

[0021] Des modes de réalisation seront exposés dans la description suivante, faite à titre non limitatif en relation avec les figures jointes parmi lesquelles :

[0022] La [Fig.1] illustre des exemples classiques d'utilisation d'un portefeuille matériel par l'intermédiaire d'un dispositif hôte ;

[0023] La [Fig.2] illustre une architecture classique de portefeuille matériel ;

[0024] La [Fig.3] représente un schéma bloc partiel d'un premier mode de réalisation de terminal mobile ou autre dispositif connecté embarquant un portefeuille matériel ;

[0025] La [Fig.4] représente un schéma bloc d'un premier mode de réalisation de terminal connecté mettant en échec un premier type de fraude pouvant cibler un terminal du type de la [Fig.3] ;

[0026] La [Fig.5] représente un schéma bloc d'un deuxième mode de réalisation de terminal connecté mettant en échec le premier type de fraude pouvant cibler un terminal du type de la [Fig.3] ;

[0027] La [Fig.6] représente un schéma bloc d'un mode de réalisation de terminal connecté mettant en échec un deuxième type de fraude ciblant un terminal du type de la [Fig.5] ;

[0028] La [Fig.7] représente un schéma bloc d'un mode de réalisation de terminal connecté dans lequel l'utilisation d'un élément sécurisé embarqué est sous le contrôle de l'utilisateur ; et

[0029] La [Fig.8] illustre un agencement de composants d'un terminal mobile connecté selon l'une des figures 4 à 6.

Description détaillée

[0030] Dans la présente demande, on vise à embarquer un portefeuille matériel dans un terminal connecté (smartphone ou autre dispositif connecté) tout en évitant des attaques rendues possibles compte tenu de cette configuration. Pour ne pas créer un écosystème entièrement nouveau et ne pas nuire à l'expérience utilisateur, on cherche en outre une compatibilité avec du matériel et des systèmes d'exploitation existants (Android, iOS), et à utiliser les voies traditionnelles de distribution des applications. De tels terminaux mobiles peuvent donc installer et exécuter des applications pouvant provenir de sources inconnues, voire douteuses, ce qui augmente le défi de la sécu-

risation des transactions avec le portefeuille matériel embarqué.

[0031] On part donc du principe que les applications installables peuvent gagner un accès à des ressources matérielles intervenant lors d'une communication avec un élément sécurisé mettant en œuvre le portefeuille matériel.

[0032] En général, les applications officielles des services concernés, notamment des services financiers (banques, cryptomonnaies), sont certifiées et signées et sont plus compliquées à modifier par du code malveillant. Lorsqu'elles sont chargées pour exécution, la vérification de signature échoue si elles ont été modifiées. Par contre, un logiciel malveillant peut déduire certaines interactions de l'application officielle avec le matériel et modifier les entrées et sorties de l'application officielle.

[0033] Par exemple, il est possible que le logiciel malveillant enregistre des touches appuyées pour voler un code secret, simule des touches appuyées pour fausser une transaction, modifie l'affichage pour tromper l'utilisateur sur la transaction qu'il est en train d'effectuer...

[0034] Plus spécifiquement, la validation d'une transaction sur un téléphone par un clavier virtuel peut être interceptée par un logiciel espion de bas niveau ayant accès à l'interface de l'écran tactile en relevant les coordonnées des appuis sur la dalle tactile. Sans savoir ce qui est affiché, le logiciel espion peut se baser sur l'hypothèse que le clavier virtuel affiché est l'un des nombreux claviers traditionnels disponibles sur la plateforme, de sorte que les coordonnées des appuis révèlent les touches du clavier. Le logiciel espion peut également avoir accès aux accéléromètres ou autres capteurs habituellement présents dans un terminal mobile - les appuis sur différentes positions de la dalle se traduisent par des valeurs d'accélération différentes en rotation sur deux axes, de sorte que les positions des appuis peuvent être déduites.

[0035] Pour y remédier partiellement, les applications affichent, pour la saisie des codes d'identification personnels, un clavier virtuel numérique avec des touches aléatoirement positionnées. Cependant, bien que cette mesure soit utile pour entraver la déduction d'un code d'identification, cela n'empêche pas un logiciel malveillant de déduire qu'une transaction est en cours et, avant que l'utilisateur n'ait terminé, modifier le montant ou le destinataire et simuler la validation (modifications des entrées de l'application sans modifier l'application elle-même).

[0036] La [Fig.3] représente un schéma bloc partiel d'un premier mode de réalisation de terminal mobile ou autre dispositif connecté embarquant un portefeuille matériel.

[0037] Un terminal mobile intègre traditionnellement un processeur d'application APP PROC relié à divers dispositif périphériques, notamment un écran tactile incluant un afficheur DISP et une dalle tactile KBD. Le processeur gère l'afficheur par une interface dédiée, souvent MIPI DSI. Le processeur gère la dalle tactile par une autre interface, généralement I2C. Pour des raisons de clarté, tous les éléments d'un terminal

mobile ne sont pas représentés.

[0038] Lorsque le terminal mobile est conçu pour effectuer des transactions sécurisées, comme la plupart des terminaux mobiles aujourd'hui, le processeur d'application intègre généralement une enclave sécurisée ou un environnement d'exécution de confiance TEE ("Trusted Execution Environment"). Une telle enclave comprend généralement un processeur, une mémoire et un gestionnaire d'écran tactile dédiés et est conçue pour mettre en œuvre une interface utilisateur de confiance TUI ("Trusted User Interface"), par exemple comme le préconise le document "Trusted User Interface API" de GlobalPlatform® (https://globalplatform.org/wp-content/uploads/2013/06/GlobalPlatform_Trusted_User_Interface_API_v1.0.pdf). Ainsi, cette enclave peut, selon les instructions exécutées par l'application, gérer l'affichage DISP et la saisie sur la dalle tactile KBD, comme cela est représenté.

[0039] Une telle enclave est distincte d'un élément sécurisé habituellement utilisé dans les portefeuilles matériels, et ne procure pas à elle seule un degré de sécurité suffisant pour les transactions de cryptoactifs gérés par la blockchain. En effet, les portefeuilles matériels pouvant donner accès à des valeurs très élevées en cryptoactifs, les moyens mis en œuvre par les pirates sont à la hauteur des sommes qu'ils peuvent extorquer.

[0040] Selon les modes de réalisation décrits ici, le terminal mobile inclut en outre un élément sécurisé embarqué eSE mettant en œuvre un portefeuille matériel. L'élément eSE peut être semblable à celui intégré dans les portefeuilles matériels détachés exposés précédemment. Il peut s'agir du microcontrôleur ST33 de STMicroelectronics® qui possède, entre autres, une interface SPI sécurisée ("Serial Peripheral Interface"), deux interfaces I2C et diverses broches d'entrée/sortie programmables GPIO. Le lien désigné par LNK à la [Fig.1] entre le terminal mobile HDV et le portefeuille matériel détaché HW, généralement une interface USB ou Bluetooth, est ici réalisé par une liaison câblée permanente entre l'élément sécurisé eSE et le processeur d'application via l'interface SPI. Pour assurer une meilleure sécurité de la communication, la liaison peut être gérée par l'enclave TEE, comme cela est représenté.

[0041] La réalisation de la fonction de portefeuille matériel dans l'élément eSE et les échanges entre l'élément eSE et le processeur d'application peuvent être en tout point similaires à ce qui est connu des figures 1 et 2 et ne seront pas décrites plus en détail.

[0042] Par ailleurs, une des broches d'entrée/sortie GPIO1 est reliée à un bouton physique B prévu pour valider des transactions par une opération mécanique. La broche GPIO1 est exclusivement gérée par l'élément sécurisé et son changement d'état est impossible à simuler par du logiciel exécuté sur le processeur d'application. Une autre broche d'entrée/sortie GPIO2 commande un indicateur LED pour signaler qu'une opération sécurisée est en cours avec le portefeuille matériel dans l'élément eSE. Le bouton B est

un bouton physique dédié agencé, par exemple, sur une paroi latérale du terminal mobile, qui se distingue visuellement des autres boutons habituellement prévus sur le terminal mobile. L'indicateur LED est également dédié et ostensible par rapport aux autres indicateurs lumineux habituellement prévus sur le terminal mobile.

[0043] Avec cette configuration, une transaction est préparée de façon usuelle par une application officielle, comme "Ledger Live", exécutée sur le processeur d'application. A partir du moment où l'utilisateur doit valider la transaction, l'application passe par l'enclave TEE pour afficher la transaction sur l'afficheur DISP et, le cas échéant, gérer une phase de saisie sur la dalle tactile KBD, comme la saisie d'un code d'identification pour déverrouiller l'élément sécurisé. La validation et la signature de la transaction sont déléguées à l'élément sécurisé eSE (le portefeuille matériel) par des commandes émises sur le bus SPI par l'intermédiaire de l'enclave TEE. Le cas échéant, la saisie du code de déverrouillage est transmise à l'élément sécurisé par le bus SPI. L'élément sécurisé eSE réagit à ces commandes par l'activation de l'indicateur LED et l'attente d'un appui sur le bouton B.

[0044] Lorsque le bouton B est appuyé, l'élément sécurisé eSE calcule la signature de la transaction avec les clés privées stockées dans le portefeuille et transmet la signature à l'application par le bus SPI. L'élément sécurisé, ayant réalisé sa tâche, désactive l'indicateur LED et attend de nouvelles commandes. L'application met à jour la blockchain à travers un service réseau, affiche les informations utiles, et attend une nouvelle interaction avec l'utilisateur.

[0045] Si aucune action n'est détectée sur le bouton après l'écoulement d'un délai, la transaction est annulée. L'élément sécurisé le signale à l'application par le bus SPI, désactive l'indicateur LED, et attend de nouvelles commandes.

[0046] Le bouton B a une fonction similaire à celle des boutons B1, B2 d'un portefeuille matériel détaché du type de la [Fig.2]. Un logiciel malveillant, s'il parvient à modifier le montant ou l'adresse de la transaction, ne pourra pas simuler une validation, qui nécessite l'actionnement d'un bouton physique détectable seulement par l'élément sécurisé eSE. Ainsi, l'utilisateur, avant de valider, pourra confirmer que la transaction telle qu'affichée est bien celle qu'il a initiée. Si la transaction a été modifiée, l'utilisateur peut en principe le constater sur l'affichage et annuler la transaction. L'annulation pourra être effectuée classiquement par un appui sur un bouton virtuel sur l'écran tactile. La fonction du bouton d'annulation ne peut pas être détournée en une fonction de validation, puisqu'une validation n'est possible qu'à l'aide du bouton physique B géré exclusivement par l'élément sécurisé eSE.

[0047] L'indicateur LED rassure l'utilisateur sur le fait que l'élément sécurisé est en train de prendre en charge les opérations et que, en principe, les demandes qui lui sont faites sont de source sûre.

[0048] Selon une variante un peu plus coûteuse en termes de fabrication du boîtier du terminal mobile, on pourra prévoir deux boutons physiques sur lesquels il faut appuyer simultanément pour valider une transaction, comme on le fait avec les portefeuilles matériels détachés.

[0049] Maintenant, un logiciel malveillant plus sophistiqué, comme on l'a précédemment indiqué, peut modifier les données d'entrée et/ou de sortie de l'application pour les détourner. Par exemple, le logiciel peut intercepter des données de transaction saisies dans l'application pour les remplacer (comme le montant et l'adresse). Même si cela est difficile lorsque la saisie est faite en mode sécurisé à l'aide de l'enclave TEE, ce n'est pas impossible compte tenu du degré de sécurité offert par une enclave TEE classique. L'application génère alors une transaction avec ces données modifiées pour l'élément sécurisé eSE et un affichage correspondant. L'affichage, qui trahit alors la modification, peut aussi être intercepté et modifié, même si cela est difficile, pour qu'il corresponde à la transaction initialement souhaitée par l'utilisateur. Ainsi, l'utilisateur verra des données de transaction apparemment correctes sur l'afficheur et validera la transaction, mais cette validation opère alors sur la transaction frauduleuse modifiée qui a été déléguée sournoisement à l'élément sécurisé eSE.

[0050] Dans un portefeuille matériel détaché classique, ce type de fraude est déjoué par le fait que le portefeuille reproduit la transaction sur son propre afficheur : l'utilisateur se fie à la transaction affichée par le portefeuille détaché, et peut la comparer à celle affichée par l'application sur le terminal. Une telle fonctionnalité n'est pas envisageable lorsque le portefeuille matériel est embarqué dans un smartphone, compte tenu de la difficulté de prévoir un deuxième écran et du surcoût.

[0051] La [Fig.4] est un schéma bloc d'un premier mode de réalisation de terminal mobile intégrant un portefeuille matériel et mettant en échec ce type de manipulation de l'affichage.

[0052] Par rapport à la [Fig.3], le processeur d'application APP PROC est intégré dans un système-sur-puce SoC intégrant aussi un processeur secondaire PROC2. Le SoC peut être le circuit i.MX 8M Plus de NXP®. Le processeur PROC2 dispose de son propre gestionnaire d'affichage et peut être considéré comme ayant un degré de sécurité élevé du fait qu'il est cloisonné par rapport aux autres circuits du SoC, de façon semblable à un élément sécurisé. Comme un élément sécurisé, le processeur PROC2 peut recevoir un jeu de commandes de l'enclave TEE par un bus SPI. Le gestionnaire d'affichage du processeur PROC2 est seul maître du bus MIPI DSI de l'afficheur et comporte une mémoire de trame FB1 que le processeur PROC2 peut remplir à partir d'une mémoire de trame FB2 du processeur d'application, d'une mémoire de trame FB3 de l'enclave TEE (flèches CPY), ou à partir de données d'affichage générées en interne, selon les besoins. Dans un autre mode, le processeur PROC2 peut afficher directement des

données de la mémoire FB2 ou FB3 à partir d'un pointeur qui lui a été fourni. Les mécanismes d'affichage sont documentés et ne seront pas décrits plus en détail. Ainsi, selon les besoins d'une application en cours d'exécution, l'afficheur DISP reçoit ses données du processeur d'application, de l'enclave TEE, ou du processeur secondaire PROC2 lui-même.

[0053] Un objectif de ce type de SoC est de pallier des failles potentielles reconnues d'un affichage géré par l'enclave TEE.

[0054] Dans ce mode de réalisation, l'élément sécurisé eSE est en outre relié par le bus SPI au processeur PROC2, dans l'objectif de gérer l'affichage selon les modalités exposées ci-après. La dalle tactile KBD peut toujours être gérée par l'enclave TEE pour effectuer une saisie sécurisée.

[0055] Avec cette configuration, une transaction est préparée de façon usuelle par une application officielle, comme "Ledger Live", exécutée sur le processeur d'application. A partir du moment où l'utilisateur doit valider la transaction, l'application utilise de préférence l'enclave TEE si une saisie de code de déverrouillage est requise et délègue le traitement de la transaction à l'élément sécurisé par le bus SPI.

[0056] En ce qui concerne l'affichage de la transaction avant validation, les données d'affichage produites par l'application peuvent, comme à la [Fig.3], être transmises au gestionnaire d'affichage de l'enclave TEE, qui remplit la mémoire de trame FB3 de l'enclave avec les données graphiques correspondantes, mais elles pourraient aussi être transmises au gestionnaire d'affichage du processeur d'application et la mémoire de trame FB2. Peu importe, ces données ne seront pas affichées.

[0057] Parallèlement, l'élément sécurisé eSE, ayant reçu les données de la transaction, transmet par le bus SPI des données d'affichage au processeur PROC2 pour qu'il les affiche via son gestionnaire d'affichage FB1 à la place des données qui seraient présentes dans les mémoires de trame FB2 et FB3.

[0058] Si d'aventure les données d'affichage de la transaction produites par l'application sont compromises, ces données se retrouvent dans la mémoire de trame FB2 ou FB3, mais elles sont ignorées, car ce sont les données produites par l'élément sécurisé dans la mémoire de trame FB1 qui sont effectivement affichées.

[0059] L'architecture de la [Fig.4] impose l'utilisation d'un système-sur-puce intégrant un jeu de cœurs de processeurs particulier, qui peut ne pas convenir à certains fabricants de smartphones.

[0060] La [Fig.5] est un schéma bloc d'un deuxième mode de réalisation de terminal mobile intégrant un portefeuille matériel, mettant en échec une manipulation de l'affichage, et offrant une solution compatible avec une multitude de chipsets disponibles pour les smartphones. Par rapport à la [Fig.3], le bus MIPI DSI de l'afficheur DISP est relié à la sortie d'un aiguillage sous la forme d'un multiplexeur MUX. Ce multiplexeur reçoit sur

une première entrée les données d'affichage produites par le processeur d'application APP PROC. Ces données d'affichage n'ont plus besoin d'être gérées par l'enclave TEE, comme cela est représenté. Une deuxième entrée du multiplexeur reçoit des données d'affichage générées par un gestionnaire d'affichage DISP CTRL géré exclusivement par l'élément sécurisé eSE. Une borne d'entrée/sortie GPIO3 de l'élément sécurisé eSE est programmée pour opérer la sélection SEL du multiplexeur. Le signal SEL pourrait aussi être prélevé sur la borne GPIO2 qui commande l'indicateur LED.

[0061] Le gestionnaire d'affichage reçoit des commandes d'affichage de l'élément sécurisé eSE, par exemple par le bus I2C. Le bus I2C offre un débit de données relativement bas, mais ce bus est utilisé pour véhiculer seulement des commandes d'affichage textuelles et vectorielles, utilisant une faible bande passante. L'élément sécurisé eSE est ainsi programmé pour générer des commandes d'affichage basiques pour les transactions qu'il traite et les transmettre au gestionnaire d'affichage.

[0062] Le gestionnaire d'affichage DISP CTRL est ici un circuit séparé, car les puces des éléments sécurisés couramment disponibles n'en sont pas dotés ou n'ont pas suffisamment de bande passante pour générer les images matricielles attendues sur le bus d'un afficheur tel que celui d'un smartphone moderne.

[0063] Dans l'attente d'une transaction, l'élément sécurisé eSE commande le multiplexeur MUX pour envoyer à l'afficheur les données d'affichage provenant du processeur.

[0064] Lorsqu'une application délègue une transaction à l'élément sécurisé eSE, celui-ci envoie les commandes d'affichage correspondant à la transaction au gestionnaire d'affichage DISP CTRL et commute le multiplexeur MUX pour que les données produites par ce gestionnaire d'affichage parviennent à l'afficheur DISP. L'indicateur LED est activé et l'élément sécurisé eSE attend la validation par le bouton B.

[0065] Avec cette configuration, l'afficheur DISP présente les données de transaction effectivement reçues par l'élément sécurisé eSE. Si elles ont été modifiées par rapport au souhait initial, l'utilisateur le verra et pourra annuler la transaction.

[0066] Il est bien entendu préférable que d'éventuelles saisies de codes de déverrouillage ou autres informations sensibles servant à la gestion de l'élément sécurisé eSE présentent un degré de sécurité au moins de même niveau que l'affichage.

[0067] La [Fig.6] est un schéma bloc d'un mode de réalisation de terminal mobile utilisant l'élément sécurisé eSE à la place d'une enclave TEE pour gérer la dalle tactile KBD, et réhaussant le degré de sécurité au niveau de celui d'un élément sécurisé. Par rapport à la [Fig.5], le bus I2C de sortie de la dalle tactile KBD est relié à un aiguillage sous la forme d'un démultiplexeur DMUX dont une première sortie est reliée au processeur d'application APP PROC et une deuxième sortie est reliée à l'interface I2C de l'élément sécurisé eSE. La sélection du démultiplexeur DMUX peut être opérée par le même signal SEL que le multiplexeur MUX. Dans cette structure, le bouton de validation

physique B est optionnel, comme on le comprendra ci-après. De plus, l'enclave TEE n'est plus requise et elle n'est plus représentée.

[0068] Dans l'attente du traitement d'une transaction, l'élément sécurisé eSE positionne le multiplexeur MUX et le démultiplexeur DMUX pour relier l'afficheur DISP et la dalle tactile KBD au processeur d'application, dans une configuration traditionnelle.

[0069] Puisque le clavier tactile échappe au contrôle de l'application lors de la délégation à l'élément sécurisé, l'application ne peut plus mettre en œuvre la phase de saisie. Ainsi, la phase de saisie est aussi déléguée à l'élément sécurisé, qui est pour l'occasion programmé pour gérer un clavier virtuel quant à la saisie et l'affichage.

[0070] Quand une transaction est déléguée par l'application à l'élément sécurisé par le bus SPI, sans passer cette fois par l'enclave TEE, l'élément sécurisé eSE bascule le multiplexeur et le démultiplexeur pour relier l'afficheur DISP et la dalle tactile KBD respectivement au gestionnaire d'affichage DISP CTRL et à l'élément sécurisé eSE. L'élément sécurisé eSE met en œuvre la phase de saisie, si une saisie est requise (fourniture d'un code de déverrouillage). La saisie sur la dalle tactile ne peut plus être interceptée ou modifiée par un logiciel s'exécutant sur le processeur d'application, tandis que toute tentative de modification de l'affichage par un logiciel s'exécutant sur le processeur d'application est ignorée.

[0071] Compte tenu de cette configuration, un logiciel s'exécutant sur le processeur d'application ne peut pas simuler des fausses validations sur le clavier tactile, de sorte que le bouton physique B est optionnel ; la validation peut être faite en toute sécurité à l'aide de la dalle tactile.

[0072] La sécurisation de la dalle tactile KBD a été décrite en partant de la structure de la [Fig.5], mais elle est applicable à la structure de la [Fig.4] où en mode sécurisé, la gestion de la dalle tactile est commutée sur l'élément sécurisé à la place de l'enclave TEE.

[0073] Selon un mode de réalisation, le signal SEL, ou tout autre indicateur du mode sécurisé (comme le signal de commande de l'indicateur LED), est utilisé pour inhiber des circuits en principe inutilisés pendant le mode sécurisé. Le signal SEL est relié, par exemple, à une borne INHIB servant à arrêter le processeur d'application. Un arrêt peut être réalisé en activant une entrée de réinitialisation du processeur, en coupant son signal d'horloge, ou en coupant son alimentation. Dans ce cas, tout logiciel malveillant s'exécutant sur le processeur d'application effectuant des analyses pour déduire des clés cryptographiques ou autres informations sensibles est rendu inopérant pendant la transaction sécurisée.

[0074] L'inactivation totale du processeur d'application est possible dans la configuration de la [Fig.6], où toutes les fonctions devant rester actives pendant la transaction sont déportées sur l'élément sécurisé eSE. Dans des cas où le processeur d'application ne

peut être désactivé, on peut utiliser le signal SEL pour désactiver des circuits annexes pouvant servir à la déduction d'informations sensibles, comme les accéléromètres permettant de déduire les positions des appuis sur la dalle tactile. Les accéléromètres sont généralement intégrés dans un circuit dédié de centrale inertielle ou IMU ("Inertial Measurement Unit"). Une telle centrale inertielle peut être désactivée et arrêtant son horloge, en coupant son alimentation ou en coupant son lien de communication avec le processeur d'application, généralement un bus I2C.

[0075] Un logiciel malveillant peut être conçu pour initier des transactions alors que l'élément sécurisé est dans une configuration où il ne demande pas de code de déverrouillage, par exemple pendant une durée limitée après avoir effectué une transaction précédente. Le logiciel malveillant tente de modifier l'affichage, mais cette tentative échoue du fait que c'est l'élément sécurisé eSE qui est maître de l'affichage dans les figures 5 et 6. Ainsi, l'affichage reflète la transaction effectivement initiée par le logiciel malveillant, tandis que l'élément sécurisé eSE attend la validation de l'utilisateur sur la dalle tactile (dans la configuration de la [Fig.6]), ou sur le bouton physique B (dans la configuration de la [Fig.4] ou 5). Dans le cas de la [Fig.3], la modification frauduleuse de l'affichage est possible, de sorte que l'utilisateur peut être trompé quant à la nature de la transaction.

[0076] Si la transaction frauduleuse est initiée à un moment où l'utilisateur a son terminal mobile en vue, il voit, sans l'avoir sollicité, passer le terminal mobile en mode sécurisé (indicateur LED), afficher la transaction et demander sa validation. L'utilisateur pourra vérifier l'affichage et annuler la transaction, mais cela demande à l'utilisateur d'être attentif et ne pas valider la transaction par mégarde.

[0077] Si l'utilisateur n'a pas le terminal mobile en vue, la transaction est en principe annulée automatiquement à l'expiration d'un délai d'attente. Toutefois, si le terminal mobile est soumis à des secousses dans une poche ou un sac, une validation intempestive pourrait survenir avant l'expiration du délai d'attente, soit par un appui sur le bouton physique B (figures 3 à 5), soit par un appui sur la dalle tactile ([Fig.6]) qui pourrait être configuré pour être opérant sur l'écran de veille du terminal mobile au moment de demander une validation.

[0078] La [Fig.7] est un schéma bloc d'un mode de réalisation de terminal mobile mettant en échec ce type de fraude. On vise ici à simuler en quelque sorte le fonctionnement d'attachement et détachement d'un portefeuille détaché classique. En plus des éléments de la [Fig.6], un commutateur bistable S physique est connecté pour relier une broche d'entrée/sortie GPIO4 de l'élément sécurisé eSE à un niveau logique bas dans une première position, et à un niveau logique haut dans une deuxième position. Le commutateur S est agencé, par exemple, sur l'une des parois latérales du terminal mobile.

[0079] L'élément sécurisé eSE est programmé pour être muet aux commandes reçues par le

bus SPI (mode inactif) dans l'une des positions du commutateur S, par exemple dans la première position, et accepter des transactions par le bus SPI (mode actif ou sécurisé) dans l'autre position. Le terminal est conçu pour que le commutateur S soit le seul moyen disponible pour commuter le mode de l'élément sécurisé, c'est-à-dire qu'une application ne peut plus à elle seule déléguer le traitement d'une transaction.

[0080] Ainsi, le mode de l'élément sécurisé est exclusivement sous le contrôle de l'utilisateur qui choisit le mode à l'aide du commutateur S selon les besoins.

[0081] Le commutateur S étant initialement dans la position du mode inactif, une application susceptible d'initier des transactions est alors conçue pour solliciter l'utilisateur à changer de mode lorsqu'elle s'apprête à déléguer le traitement de la transaction à l'élément sécurisé eSE. Elle peut envoyer à l'afficheur DISP un message du type "Veuillez placer le téléphone en mode sécurisé à l'aide du commutateur", de préférence avec les informations relatives à la transaction en cours. Ce message est analogue à un message invitant l'utilisateur à connecter son portefeuille détaché classique au terminal mobile.

[0082] L'utilisateur bascule alors le commutateur pour passer en mode actif. L'élément sécurisé eSE réagit en prenant diverses mesures protectrices, comme basculer le signal SEL pour relier l'afficheur DISP et la dalle tactile KBD respectivement au gestionnaire d'affichage dédié DISP CTRL et à l'élément sécurisé eSE. L'indicateur LED est aussi activé pour signaler à l'utilisateur que le terminal mobile est en mode sécurisé. L'élément sécurisé eSE envoie un acquittement à l'application qui reprend l'exécution en transmettant les informations de la transaction à l'élément sécurisé. L'élément sécurisé eSE opère la phase de saisie sur la dalle tactile KBD, le cas échéant, et demande la validation à l'utilisateur en affichant de nouveau les informations relatives à la transaction.

[0083] Lorsque la transaction est validée et signée, l'élément sécurisé eSE communique la transaction signée à l'application qui l'inscrit sur la blockchain. L'élément sécurisé sollicite l'utilisateur à changer de mode, en envoyant à l'afficheur DISP un message du type "Veuillez quitter le mode sécurisé en basculant le commutateur". Ce message est analogue à celui indiquant que l'utilisateur peut retirer son portefeuille détaché classique. Lorsque le commutateur est basculé, les connexions initiales de l'afficheur et de la dalle tactile sont rétablies, et l'indicateur LED est désactivé.

[0084] Le commutateur S peut aussi être mis en œuvre dans les structures des figures 4 et 5, où la dalle tactile KBD n'est pas reliée à l'élément sécurisé. Dans ce cas, c'est l'application qui opère la phase de saisie avant de solliciter le basculement du commutateur S.

[0085] Bien entendu, le commutateur S, à la merci de l'utilisateur, pourrait être basculé à des moments où ce n'est pas requis, ou ne pas être basculé quand c'est requis. Différentes

combinaisons ne sont ainsi pas "normales", et cela peut être signalé à l'utilisateur par des messages affichés ou des alarmes, incitant l'utilisateur à basculer le commutateur pour que les opérations puissent reprendre normalement.

[0086] Un logiciel malveillant pourrait également se comporter comme une application officielle en demandant le basculement de mode. Toutefois, comme l'utilisateur n'a pas initié la transaction et qu'on lui demande une action relativement contraignante, il est susceptible d'être plus vigilant. Le logiciel malveillant ne peut plus afficher un message trompeur hors propos dans ce contexte, puisque l'utilisateur s'attend à voir des informations de transaction. De telles informations de transaction seront difficiles à rendre crédibles, d'autant plus si elles sont vraies - typiquement un transfert d'un montant élevé à une adresse inconnue. Si le logiciel malveillant tente de cacher la nature de la transaction, celle-ci sera révélée et différente au moment où elle est affichée pour validation par l'élément sécurisé eSE, si l'utilisateur a quand même été incité à basculer en mode sécurisé.

[0087] En tout cas, une transaction en attente, qu'elle soit frauduleuse ou non, ne peut plus être validée par un appui intempestif sur un bouton physique ou virtuel, car l'utilisateur doit intentionnellement basculer le terminal mobile en mode sécurisé pour valider la transaction.

[0088] La [Fig.8] illustre un agencement de composants d'un terminal mobile (smartphone) selon l'une des figures 4 à 7. Le processeur d'application APP PROC et son enclave TEE peuvent faire partie d'un système-sur-puce SoC ("System-on-Chip"). Le SoC comporte des broches soudées à des pistes respectives d'un circuit imprimé ou autre support d'interconnexion recevant un certain nombre d'autres composants. Des groupes respectifs de broches sont associés aux différents liens de communication entre les composants, notamment les bus MIPI DSI, SPI et I2C précédemment mentionnés.

[0089] L'afficheur DISP et la dalle tactile KBD sont généralement déportés et parallèles au circuit imprimé. Leurs bus de commande sont alors reliés au circuit imprimé par des connecteurs soudés sur des pistes du circuit imprimé.

[0090] Les différents éléments exposés ci-dessus pour mettre en œuvre un portefeuille matériel embarqué, choisis parmi les éléments eSE, DISP CTRL, MUX, DMUX, et des connecteurs pour les éléments B, S et LED, selon les modes de réalisation, peuvent être intégrés dans un système-en-boîtier SiP ("System-in-Package") conçu pour être monté sur un circuit imprimé, ou dans un autre SoC.

[0091] Pour adapter un terminal mobile classique à l'intégration d'un portefeuille matériel embarqué, on aménage une place sur le circuit imprimé pour souder le SiP, on redessine les pistes des différents bus utilisés en les interrompant pour qu'elles passent par le SiP, et on amène des pistes pour établir la liaison sécurisée SIP entre le

processeur APP PROC et l'élément sécurisé eSE.

[0092] Les différents éléments physiques discrets gérés par les circuits du SiP (le bouton B, le commutateur S, l'indicateur LED) peuvent être fixés sur le boîtier du terminal et reliés à des connecteurs du SiP, ou à des connecteurs déportés sur le circuit imprimé, eux-mêmes reliés par des pistes à des broches dédiées du SiP.

[0093] Avec cette configuration, un terminal mobile classique peut être transformé en un terminal mobile avec portefeuille matériel embarqué par le simple ajout d'un SiP sur un circuit imprimé portant les composants du terminal classique. Bien que la conception du circuit imprimé adapté représente un certain coût de développement et de production, ce coût reste négligeable du fait qu'il n'y a pas d'adaptation à faire au niveau de la plateforme matérielle du terminal classique.

[0094] La description qui précède a été effectuée essentiellement dans le contexte des smartphones embarquant un portefeuille matériel pour signer des transactions sur la blockchain (“smartphones blockchain”). Les principes décrits s’appliquent toutefois à tout type de terminal connecté (à Internet ou à un réseau local) stockant des secrets servant à diverses utilisations impliquant des calculs cryptographiques, comme la signature de transactions en général et l’authentification, y compris l’authentification “zero knowledge”. Dans d’autres types de terminaux connectés, l’interface homme-machine peut être un afficheur associé à un clavier physique, ou à un joystick.

Revendications

[Revendication 1] Terminal connecté comprenant :
une interface homme-machine incluant un afficheur (DISP) gérable par un bus de commande (MIPI DSI) ;
un processeur d'application (APP PROC) intégrant un premier gestionnaire d'affichage (FB2, FB3) configuré pour gérer l'afficheur (DISP) ; et
un processeur secondaire cloisonné (PROC2) intégrant un deuxième gestionnaire d'affichage (FB1) configuré pour prendre la main sur le premier gestionnaire d'affichage pour gérer l'afficheur (DISP) ;
caractérisé en ce qu'il comprend :
un élément sécurisé embarqué (eSE) connecté au processeur d'application et au processeur secondaire (PROC2) par un bus câblé (SPI), configuré pour effectuer des calculs cryptographiques avec un secret stocké dans l'élément sécurisé, sur une transaction reçue d'une application exécutée sur le processeur d'application ;
un dispositif de validation de transaction (B) actionnable par un utilisateur et accessible exclusivement par l'élément sécurisé (eSE) ; et
l'élément sécurisé (eSE) et le processeur secondaire (PROC2) étant configurés pour que l'élément sécurisé transmette au processeur secondaire des données d'affichage liées à la transaction reçue et que le processeur secondaire réagisse en prenant la main sur la gestion de l'afficheur (DISP) pour afficher les données d'affichage transmises par l'élément sécurisé.

[Revendication 2] Terminal selon la revendication 1, dans lequel l'interface homme-machine inclut en outre un dispositif de saisie (KBD) commandé par un bus correspondant (I2C), le terminal comprenant en outre :
un démultiplexeur (DMUX) commandé par l'élément sécurisé (eSE) pour :
dans un mode inactif, connecter le bus du dispositif de saisie pour qu'il soit géré par le processeur d'application, et
dans un mode actif, connecter le bus du dispositif de saisie pour qu'il soit exclusivement géré par l'élément sécurisé.

[Revendication 3] Terminal selon la revendication 2, dans lequel le dispositif de saisie (KBD) est une dalle tactile et le dispositif de validation de transaction est un bouton virtuel sur la dalle tactile dans le mode actif.

[Revendication 4] Terminal selon la revendication 1, dans lequel le dispositif de validation

de transaction est un bouton physique (B).

[Revendication 5] Terminal selon la revendication 1, comprenant en outre :
un commutateur physique bistable (S) actionnable par l'utilisateur et accessible exclusivement par l'élément sécurisé (eSE), configuré pour, dans une première position, passer l'élément sécurisé en mode actif et, dans une deuxième position, passer l'élément sécurisé en mode inactif ; et
des moyens (DISP) pour solliciter l'utilisateur à actionner le commutateur.

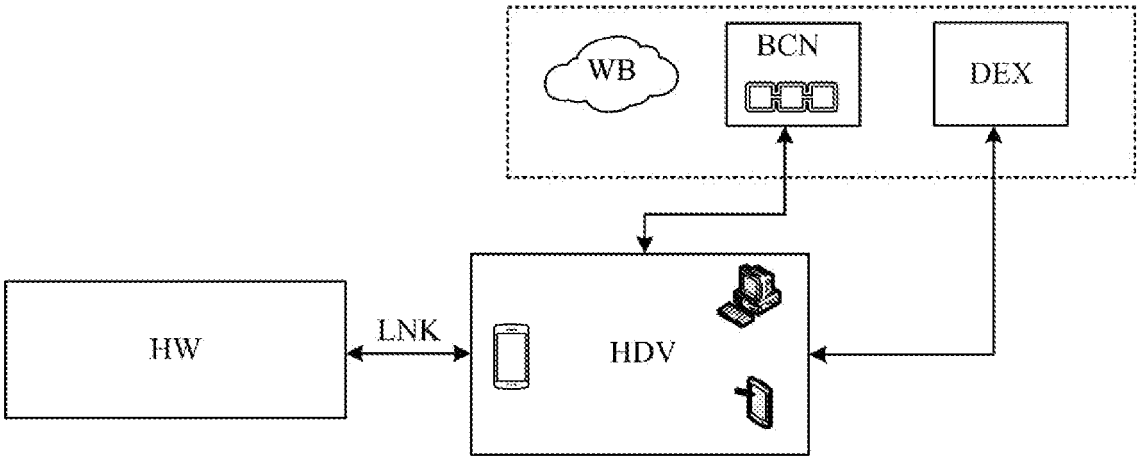
[Revendication 6] Terminal selon la revendication 1, dans lequel l'élément sécurisé est configuré pour, en mode actif, inhiber (INHIB) des circuits capables de mesurer des paramètres du terminal pour déduire des informations sensibles.

[Revendication 7] Terminal selon la revendication 1, comprenant en outre un indicateur dédié (LED) perceptible par l'utilisateur, commandé exclusivement par l'élément sécurisé pour être activé pendant le mode actif et désactivé pendant le mode inactif.

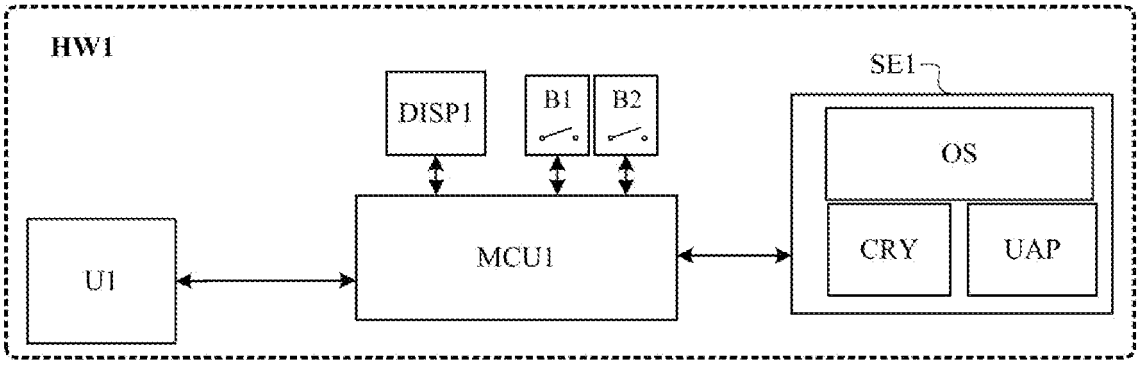
[Revendication 8] Procédé de validation et signature d'une transaction sur la blockchain utilisant un terminal selon la revendication 5, comprenant les étapes suivantes :
le commutateur (S) étant dans la position du mode inactif, solliciter à travers l'application et à l'aide d'un message sur l'afficheur (DISP) que l'utilisateur bascule le commutateur dans la position du mode actif ;
au basculement du commutateur, envoyer par l'élément sécurisé un acquittement à l'application ;
à la réception de l'acquittement, transmettre par l'application des informations de la transaction à l'élément sécurisé ;
dans l'élément sécurisé, gérer l'affichage, la validation et la signature de la transaction, et envoyer le résultat à l'application ; et
solliciter par l'élément sécurisé à l'aide d'un message sur l'afficheur (DISP) que l'utilisateur bascule le commutateur dans la position du mode inactif.

[Revendication 9] Terminal selon la revendication 2, dans lequel le processeur d'application (APP PROC) et le processeur secondaire (PROC2) sont intégrés dans un même système-sur-puce.

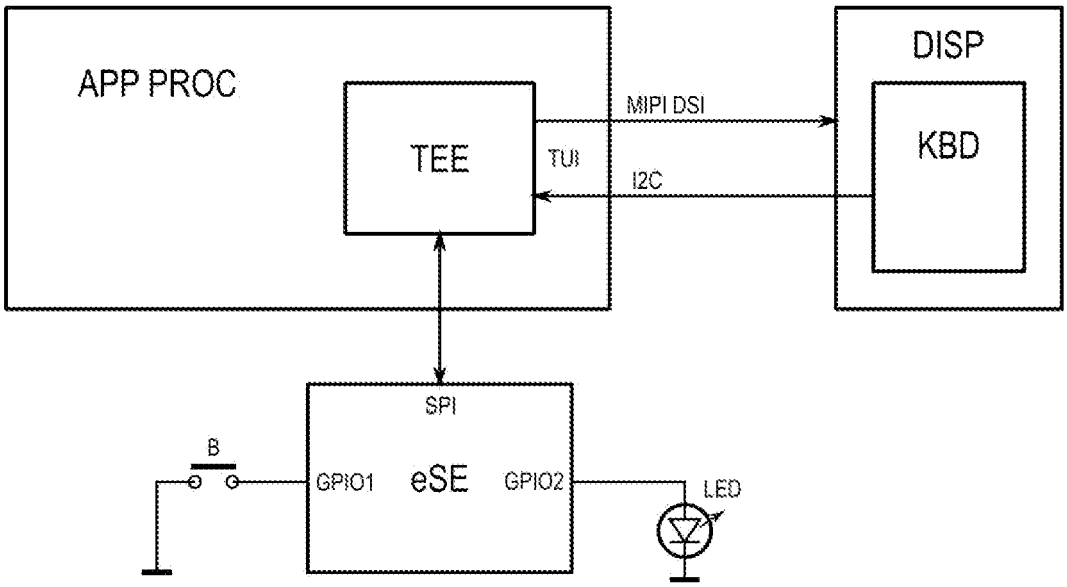
[Fig. 1]



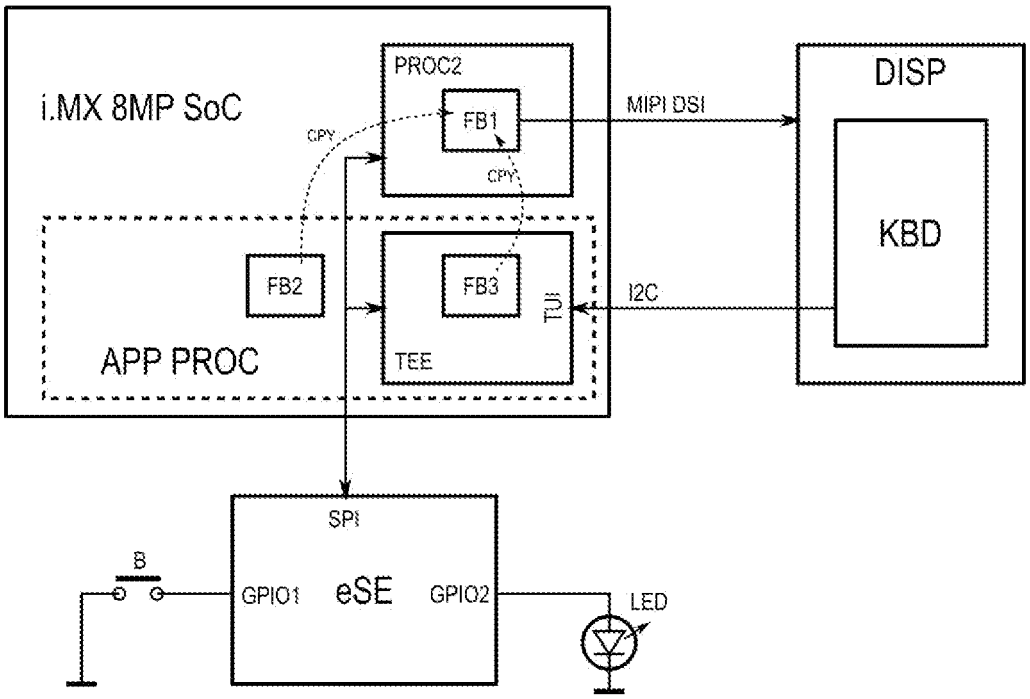
[Fig. 2]



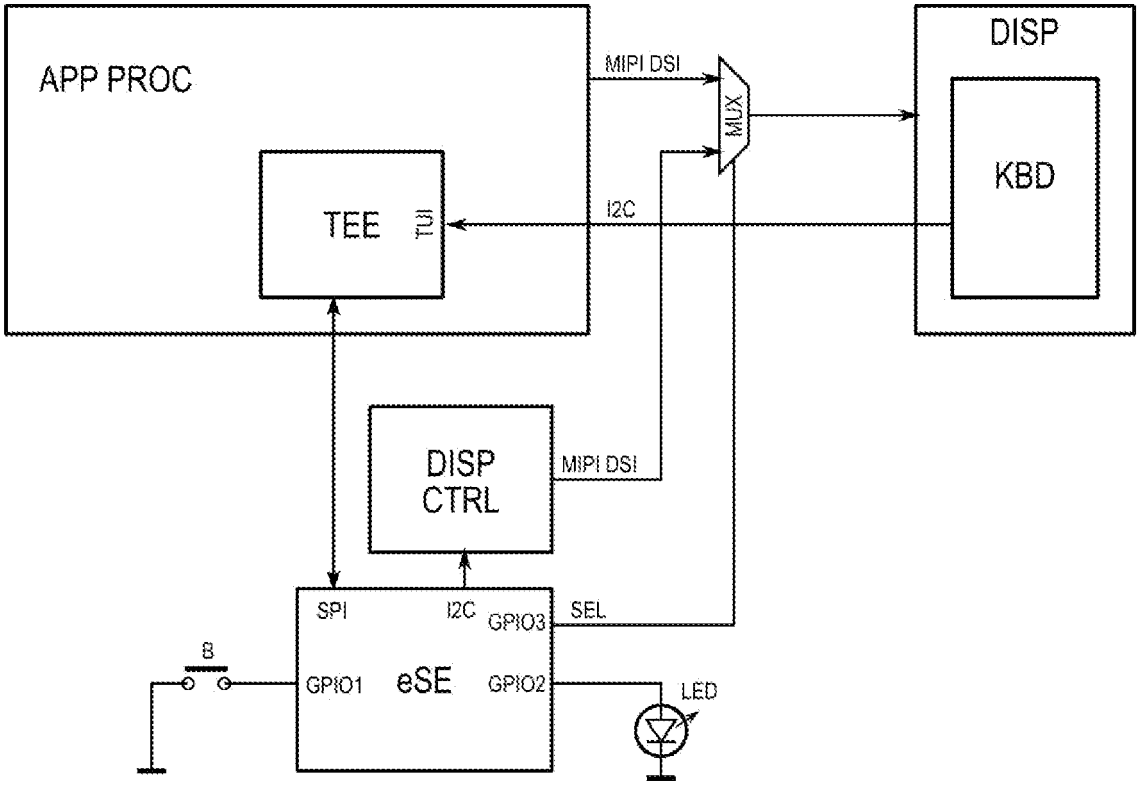
[Fig. 3]



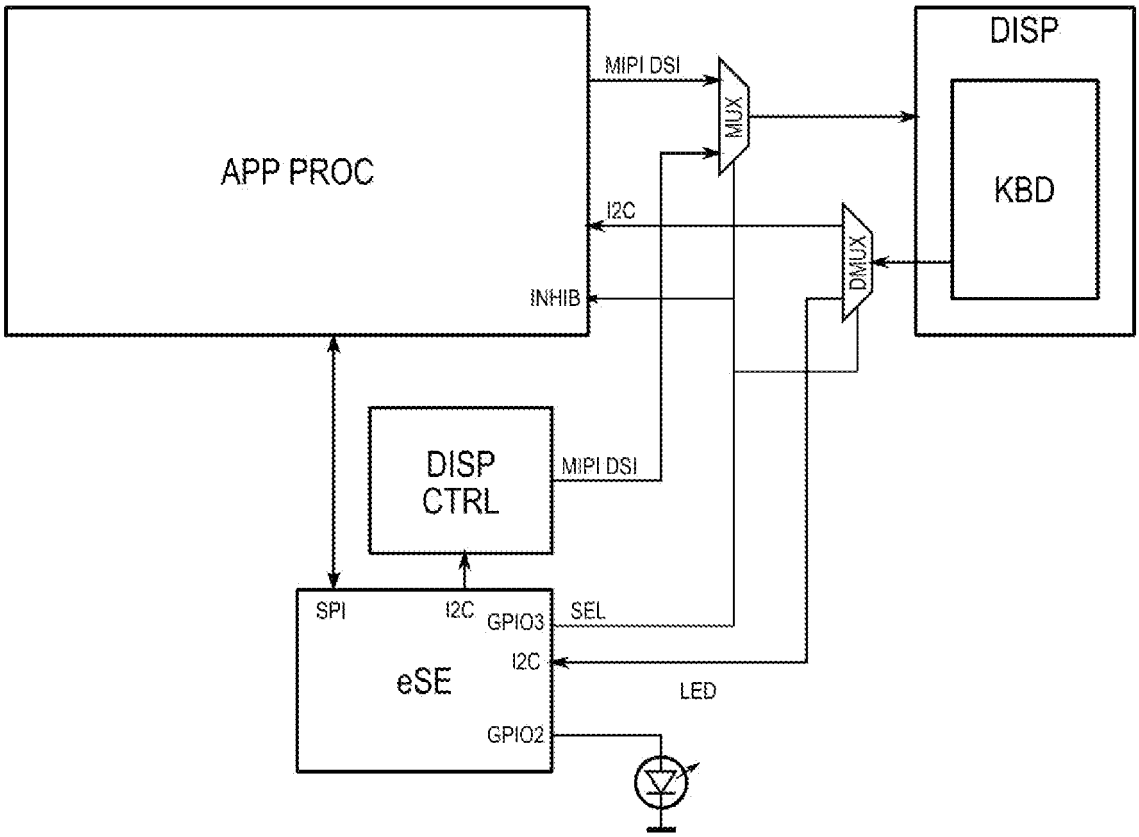
[Fig. 4]


i.MX 8MP SoC
PROC2
FB1
CPY
CPY
MIPI DSI
DISP
KBD
FB2
FB3
TUI
I2C
APP PROC
TEE
SPI
B
GPIO1
eSE
GPIO2
LED

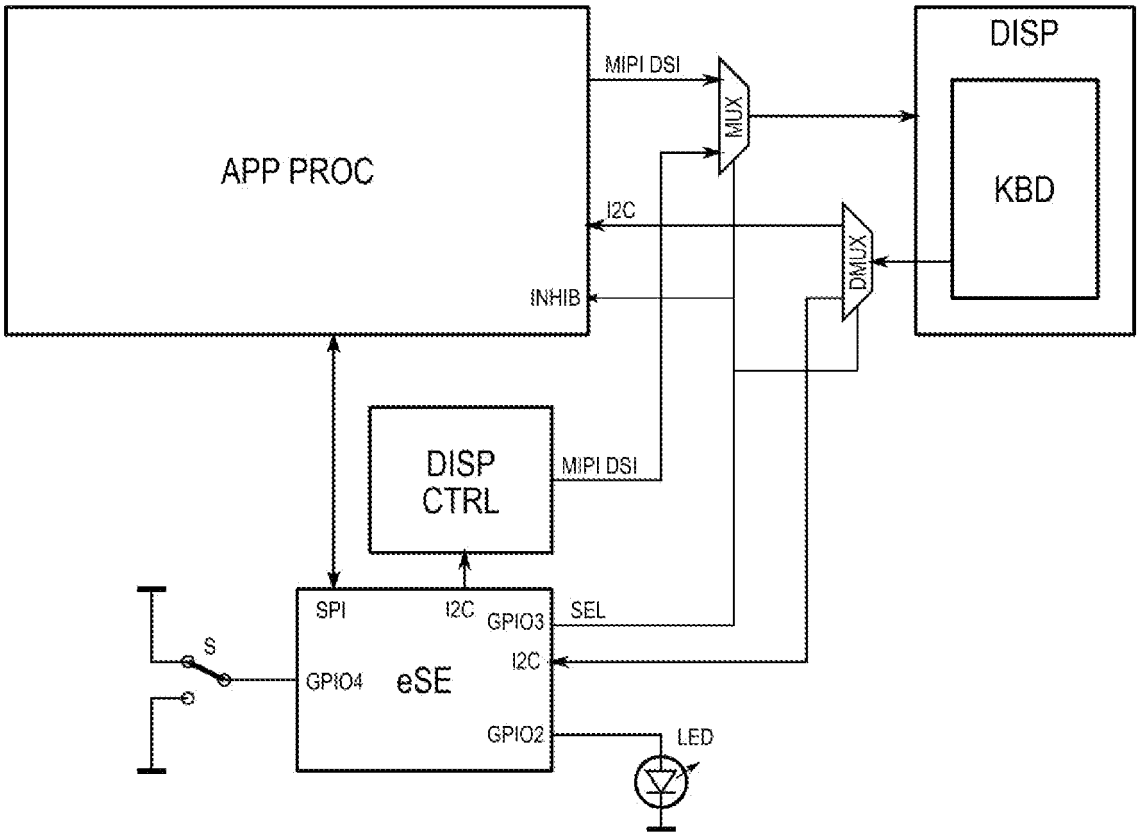
[Fig. 5]


APP PROC
MIPI DSI
MUX
DISP
KBD
TEE
TUI
I2C
DISP
CTRL
MIPI DSI
SPI
I2C
GPIO3
SEL
B
GPIO1
eSE
GPIO2
LED

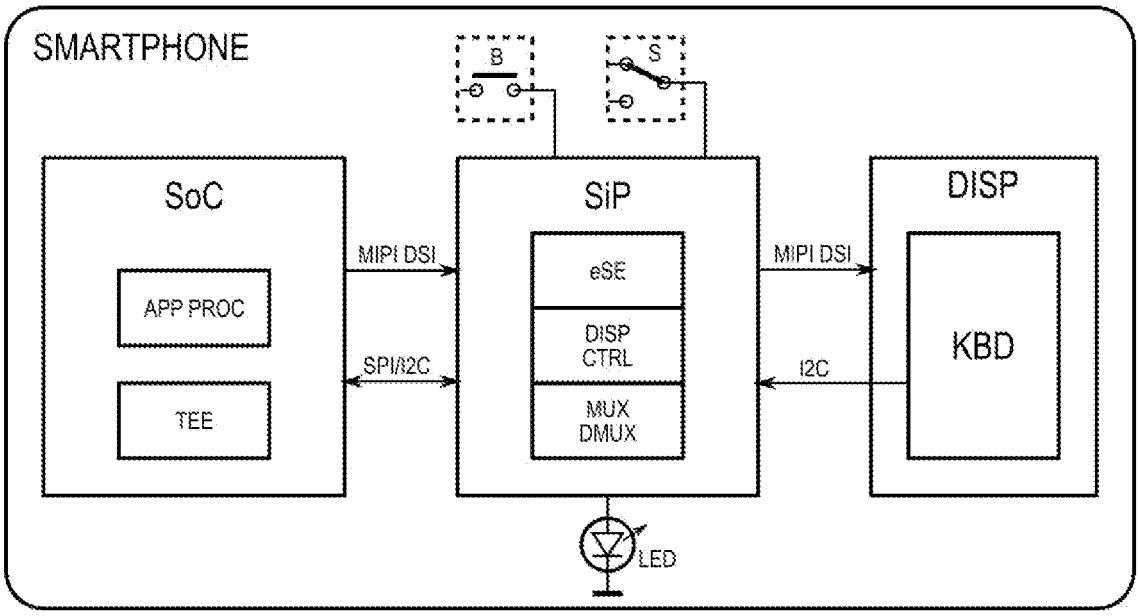
[Fig. 6]


APP PROC
MIPI DSI
MUX
DISP
KBD
I2C
DMUX
INHIB
DISP CTRL
MIPI DSI
SPI
I2C
GPIO3
SEL
I2C
eSE
LED
GPIO2

[Fig. 7]


APP PROC
MIPI DSI
MUX
DISP
KBD
I2C
DMUX
INHIB
DISP CTRL
MIPI DSI
SPI
I2C
GPIO3
SEL
S
GPIO4
eSE
I2C
GPIO2
LED

[Fig. 8]


SMARTPHONE
B
S
SoC
APP PROC
TEE
MIPI DSI
SPI/I2C
SiP
eSE
DISP CTRL
MUX DMUX
MIPI DSI
I2C
DISP
KBD
LED

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 911806
FR 2209987

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	REZAEIGHALEH HOSSEIN ET AL: "Efficient Off-Chain Transaction to Avoid Inaccessible Coins in Cryptocurrencies", 2020 IEEE 19TH INTERNATIONAL CONFERENCE ON TRUST, SECURITY AND PRIVACY IN COMPUTING AND COMMUNICATIONS (TRUSTCOM), IEEE, 29 décembre 2020 (2020-12-29), pages 1903-1909, XP033900943, DOI: 10.1109/TRUSTCOM50675.2020.00260 [extrait le 2021-01-29] * Page 6, colonne de gauche, paragraphes 4-5; figure 1 * * Page 3, colonne de droite, troisième paragraphe *	1-9	G06F9/44 G06F21/64 H03K17/62 H04L9/14 H04L9/30 G06F12/00

A	Ledger: "Ledger Nano S Security Target", , 18 octobre 2018 (2018-10-18), XP093033870, Extrait de l'Internet: URL:https://www.ssi.gouv.fr/uploads/2019/02/anssi-cible-cspn-2019_03en.pdf [extrait le 2023-03-22] * abrégé; figure 3 *	1-9	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06F G07G G06Q

A	Release: "Ledger Documentation Hub", , 1 août 2017 (2017-08-01), XP055607219, Extrait de l'Internet: URL:https://buildmedia.readthedocs.org/media/pdf/ledger/stable/ledger.pdf [extrait le 2029-01-01] * figure 10.1 *	1-9	

Date d'achèvement de la recherche	Examinateur
23 mars 2023	Hoareau, Samuel

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)